Bundesministerium des Innern

POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

1. Untersuchungsausschuss 18. WP
Herrn MinR Harald Georgii
Leiter Sekretariat
Deutscher Bundestag
Platz der Republik 1
11011 Berlin

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
POSTANSCHRIFT 11014 Berlin

TEL +49(0)30 18 681-2310
FAX +49(0)30 18 681-52230
BEARBEITET VON Jürgen Blidschun

E-MAIL Jürgen.Blidschun@bmi.bund.de
INTERNET www.bmi.bund.de
DIENSTSITZ Berlin
DATUM 11.09.2014
AZ PG UA-20001/7#4

BETREFF **1. Untersuchungsausschuss der 18. Legislaturperiode**
HIER Beweisbeschluss BMI-7 vom 03. Juli 2014
ANLAGEN 16 Aktenordner VS - NfD, 1 Aktenordner offen, 1 Aktenordner GEHEIM

Sehr geehrter Herr Georgii,

in Erfüllung Beweisbeschluss BMI-7 übersende ich Ihnen die oben aufgeführten Unterlagen als zweite Teillieferung.

In den übersandten Aktenordnern wurden Schwärzungen oder Entnahmen mit folgenden Begründungen durchgeführt:

- Schutz Mitarbeiterinnen und Mitarbeiter deutscher Nachrichtendienste,
- Schutz Grundrechter Dritter,
- Fehlender Sachzusammenhang zum Untersuchungsauftrag und
- Kernbereich exekutiver Eigenverantwortung.

Die einzelnen Begründungen bitte ich den in den Aktenordnern befindlichen Inhaltsverzeichnissen und Begründungsblättern zu entnehmen.

Soweit der übersandte Aktenbestand vereinzelt Informationen enthält, die nicht den Untersuchungsgegenstand betreffen, erfolgt die Übersendung ohne Anerkennung einer Rechtspflicht.

Soweit die Dokumente im Rahmen des Beweisbeschlusses BMI-1 vorgelegt werden, erfolgt keine Übersendung im Rahmen des Beweisbeschlusses BMI-7.

Bundesministerium
des Innern

Ich sehe vor diesem Hintergrund den Beweisbeschluss BMI-7 als vollständig erfüllt an.

Mit freundlichen Grüßen
Im Auftrag

Akmann

Titelblatt

Ressort	Berlin, den
BMI	25. August 2014

Ordner

34

Aktenvorlage

an den

1. Untersuchungsausschuss

des Deutschen Bundestages in der 18. WP

gemäß Beweisbeschluss:	vom:
BMI-7	03.07.2014

Aktenzeichen bei aktenführender Stelle: IT II 1

IT3-606 000-9/31#1
IT3-606 000-2/28#1
IT3-606 000-9/9#14
IT3-606 000-2/26#7
IT3-606 000-2/112#18
IT3-M-601 000-9/3#5
IT3-606 000-2/122#25
IT3-606 000-21 CHN/1#24
IT3-606 000-9/7#6
IT3-606 000-2/77
IT3-606 000-2/72#16
IT3-606 000-2/136#3
IT3-606 000-3/0#33
IT3-606 000-2/28#1

VS-Einstufung:

VS - NUR FÜR DEN DIENSTGEBRAUCH

Inhalt:

IT-Schutz kritischer Infrastrukturen; Ministergespräche mit Wirtschaftsvertretern

Cyber-Sicherheitsrates
Rede „Bürgernahe Sicherheitskommunikation für Städte und Gemeinden - Schutz kritischer Infrastrukturen“
Fachkonferenz des BSI am 30.05.2012
Sitzung der AG 4 des IT-Gipfels
Überarbeitung von Außenwirtschaftsgesetz (AWG) und Außenwirtschaftsverordnung (AWV); Kompromissvorschlag zur Investitionsprüfung
1.Fachgespräch zu Cyberfragen zwischen D und CHN
Aktive Netzverteidigung
Termin Messwesen mit der ... Gruppe
Einladung als Keynote Speaker auf dem Cyber Security Summit
Dankschreiben des Zentralverbands für Elektrotechnik- und Elektroindustrie e.V.
Aktuelle Erkenntnisse zur Schadsoftware „Flame“
Cyber Security Award
Information US-Cert an BSI bzgl. SCADA-Aktivitäten von Islamisten
Sicherheitsvorfall EC-Karten-Terminal
Besuch des Präsidenten und CEO ..., S...

Bemerkungen:

geschwärzt

Inhaltsverzeichnis

Ressort	Berlin, den
BMI	25. August 2014

Ordner

34

Inhaltsübersicht
zu den vom 1. Untersuchungsausschuss der
18. Wahlperiode beigezogenen Akten

des/der:	Referat/Organisationseinheit:
BMI	IT II 1

Aktenzeichen bei aktenführender Stelle:

IT3-606 000-9/31#1
IT3-606 000-2/28#1
IT3-606 000-9/9#14
IT3-606 000-2/26#7
IT3-606 000-2/112#18
IT3-M-601 000-9/3#5
IT3-606 000-2/122#25
IT3-606 000-21 CHN/1#24
IT3-606 000-9/7#6
IT3-606 000-2/77
IT3-606 000-2/72#16
IT3-606 000-2/136#3
IT3-606 000-3/0#33
IT3-606 000-2/28#1

VS-Einstufung:

VS - NUR FÜR DEN DIENSTGEBRAUCH

Blatt	Zeitraum	Inhalt/Gegenstand *[stichwortartig]*	Bemerkungen
1 - 48	14.05.2012	IT-Schutz kritischer Infrastrukturen; Vorbereitung Ministergespräch mit Vertretern des IKT-Sektors	Entnahme (BEZ): S. 40, 41 Schwärzungen DRI-U: S. 3, 6, 30, 31, 34,

			35, 36, 43 bis 46 DRI-N: S. 3, 6, 43
49 - 57	16.05.2012	IT-Schutz kritischer Infrastrukturen; Ministergespräch mit Wirtschaftsvertretern	Schwärzungen: DRI-U, DRI-N: S. 54, 55
58 - 136	22.05.2012	3. Sitzung des Cyber-Sicherheitsrates	VS-NfD: S. 81 bis 89, 114 bis 117, 119 bis 122 Schwärzungen: DRI-U: S. 63, 68, 73, 85, 87, 88, 108, 110, 129 DRI-N: S. 68, 73, 118, 129
137 - 165	23.05.2012	Rede „Bürgernahe Sicherheitskommunikation für Städte und Gemeinden - Schutz kritischer Infrastrukturen“	Entnahme (BEZ): S. 137 bis 165
166 - 186	23.05.2012	Fachkonferenz des BSI am 30.05.2012	Entnahme (BEZ): S. 166 bis 186
187 - 223	29.05.2012	Fachkonferenz des BSI am 30.05.2012	Entnahme (BEZ): S. 187 bis 223
224 - 238	29.05.2012	Cyber-Sicherheitsrat am 31.05.2012	Schwärzungen: DRI-U, DRI-N: S. 225
239 - 279	04.06.2012	Sitzung der AG 4 des IT-Gipfels am 11.06.2012	Entnahmen (BEZ): S. 241 bis 247, 260 bis 272 Schwärzungen: DRI-U: S. 248, 249, 251 bis 254, 273, 274, 275, 277, 278, 279 DRI-N: S. 248, 249, 251 bis 253, 259, 273 bis 278
280 - 285	05.06.2012	Überarbeitung von Außenwirtschaftsgesetz (AWG) und Außenwirtschaftsverordnung (AWV); Kompromissvorschlag zur Investitionsprüfung	Schwärzungen: DRI-U: S. 283, 284
286 - 294	05.06.2012	Schreiben des Herrn Ministers an Herrn ...; Wechsel zu M...	Entnahme (BEZ): S. 286 bis 294
295 - 300	07.06.2012	1. Fachgespräch zu Cyberfragen zwischen D und CHN	Entnahme (BEZ): S. 295 bis 300
301 - 341	07.06.2012	IT-Schutz kritischer Infrastrukturen; Vorbereitung Ministergespräch mit Vertretern des Energiesektors	VS-NfD: S. 319, 320 Schwärzungen: DRI-U: S. 305, 306, 325, 327 bis 333, 336, 337, 338,

			339 bis 341 DRI-N: S. 305, 306, 327 bis 329, 337
342 - 390	11.06.2012	Aktive Netzverteidigung	VS-NfD: S. 387 bis 390
391 - 418	11.06.2012	Termin Messwesen mit der ... Gruppe	Entnahme (BEZ): S. 391 bis 418
419 - 429	12.06.2012	Einladung als Keynote Speaker auf dem Cyber Security Summit	Entnahme (BEZ): S. 419 bis 429
430	14.06.2012	Dankschreiben des Zentralverbands für Elektrotechnik- und Elektroindustrie e. V.	Entnahme (BEZ): S. 430
431 - 436	14.06.2012	Aktuelle Erkenntnisse zur Schadsoftware „Flame“	Schwärzung: DRI-U: S. 431
437 - 441	07.06.2012	Cyber Security Award	Entnahme (BEZ): S. 437 bis 441
442 - 457	21.06.2012	Information US-Cert an BSI bzgl. SCADA-Aktivitäten von Islamisten	VS-NfD: S. 452 bis 454
455 - 457	02.07.2012	Sicherheitsvorfall EC-Karten-Terminal	Entnahme (BEZ): S. 455 bis 457
458 - 467	25.06.2012	Besuch des Präsidenten und CEO ..., S...	Entnahme (BEZ): S. 458 bis 467
468 - 474	25.06.2012	IT-Schutz kritischer Infrastrukturen; Ministergespräch mit Wirtschaftsvertretern	Schwärzung: DRI-U, DRI-N: S. 474
475 - 502	27.06.2012	Finales Protokoll der 3. Sitzung des Cyber-SR am 31.05.2012	VS-NfD: S. 480 bis 488; 493 bis 502 Schwärzungen: DRI-U: S. 484, 485, 485, 488, 497 DRI-N: S. 484, 485, 486, 488
503 - 535	28.06.2012	IT-Schutz kritischer Infrastrukturen; Vorbereitung Ministergespräch mit Vertretern des Sektors Transport und Verkehr	Schwärzungen: DRI-U: S. 506, 507, 528, 532 bis 535 DRI-N: S. 507

Anlage zum Inhaltsverzeichnis

Ressort	Berlin, den
BMI	21. August 2014

Ordner

34

VS-Einstufung:

VS-NUR FÜR DEN DIENSTGEBRAUCH

Kategorie	Begründung
BEZ	**Fehlender Bezug zum Untersuchungsauftrag** Das Dokument weist keinen Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss auf und ist daher nicht vorzulegen.
DRI-U	**Namen von Unternehmen** Die Namen von Unternehmen wurden unkenntlich gemacht. Im Rahmen einer Einzelfallprüfung wurden das Informationsinteresse des Ausschusses einerseits und das Recht des Unternehmens unter dem Schutz des eingerichteten und ausgeübten Gewerbebetriebs andererseits gegeneinander abgewogen. Hierbei wurde zum einen berücksichtigt, inwieweit der Name des Unternehmens ggf. als relevant für die Aufklärungsinteressen des Untersuchungsausschusses erscheint. Zum anderen wurde berücksichtigt, dass die Namensnennung gegenüber einer nicht kontrollierbaren Öffentlichkeit den Bestandsschutz des Unternehmens, deren Wettbewerbs- und wirtschaftliche Überlebensfähigkeit gefährden könnte. Soweit diese Abwägung zugunsten des Unternehmens ausfiel, wurden im Geschäftsbereich des Bundesministeriums des Innern dennoch der erste Buchstabe des Unternehmens sowie die Rechtsform ungeschwärzt belassen, um jedenfalls eine allgemeine Zuordnung und ggf. spätere Nachfragen zu ermöglichen. Eine Ausnahme hiervon erfolgte lediglich in den Fällen, in denen aufgrund der Besonderheiten des Einzelfalls eine Zuordnung bereits mit diesen verbleibenden Angaben mit an Sicherheit grenzender Wahrscheinlichkeit möglich gewesen wäre. Sollte sich im weiteren Verlauf herausstellen, dass aufgrund eines konkreten zum gegenwärtigen Zeitpunkt für das Bundesministerium des Innern noch nicht absehbaren

	Informationsinteresses des Ausschusses an dem Namen eines Unternehmens dessen Offenlegung gewünscht wird, so wird das Bundesministerium des Innern in jedem Einzelfall prüfen, ob eine weitergehende Offenlegung möglich erscheint.
DRI-N	**Namen von externen Dritten** Namen von externen Dritten wurden unter dem Gesichtspunkt des Persönlichkeitsschutzes unkenntlich gemacht. Im Rahmen einer Einzelfallprüfung wurde das Informationsinteresse des Ausschusses mit den Persönlichkeitsrechten des Betroffenen abgewogen. Das Bundesministerium des Innern ist dabei zur Einschätzung gelangt, dass die Kenntnis des Namens für eine Aufklärung nicht erforderlich erscheint und den Persönlichkeitsrechten des Betroffenen im vorliegenden Fall daher der Vorzug einzuräumen ist. Sollte sich im weiteren Verlauf herausstellen, dass nach Auffassung des Ausschusses die Kenntnis des Namens einer Person doch erforderlich erscheint, so wird das Bundesministerium des Innern in jedem Einzelfall prüfen, ob eine weitergehende Offenlegung möglich erscheint.

354/12

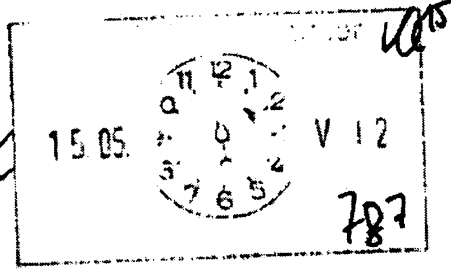
BMI

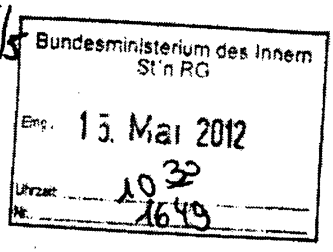
IT3-606 000-9/31#1

Refl: Dr. Dürig
Ref: Dr. Pilgermann/RRn Otte

Berlin, den 14. Mai 2012

Hausruf: 1374/1527/2808





Herrn Minister

über

Frau Stn Rogall-Grothe
Herrn IT-D
Herrn SV IT-D

Abdrucke:

Herrn PSt Dr. Bergner;
Herrn St Fritsche;
Herren LLS, AL ÖS und AL KM;
Referate Presse und Z 9

RR'n Otte z.d.V.

1.) Hr. Pilgermann, Fr. Nimmo m.d.B.u.K.

2.) Wv.

Betr.: IT-Schutz kritischer Infrastrukturen; Vorbereitung Ministerspräch mit Vertretern des IKT-Sektors

Bezug: Ministervorlage vom 17. April 2012; Az. IT3-606 000-9/31#1

Anlage: Vorbereitungsmappe

Zur Vorbereitung Ihres Gesprächs mit Vertretern des IKT-Sektors am 23. Mai 2012 erhalten Sie anliegende **Vorbereitungsmappe**.

Nach dem Auftakt am 9. Mai mit Vertretern des Finanz- und Versicherungswesens findet am 23. Mai 2012 der zweite Termin der Gesprächsreihe mit Vertretern des IKT-Sektors statt. Ziel ist es, gemeinsam mit Vorständen und Verbänden der betroffenen Branchen den IT-Schutz Kritischer Infrastrukturen zu stärken und umfassende und flächendeckende IT-Sicherheitsstandards und Meldewege zu etablieren.

Teilnehmer: Bisher haben10 Teilnehmer aus der Wirtschaft zugesagt. Teilnehmen wird zudem Herr Abteilungsleiter Dr. Schuseil, BMWi (s. Teilnehmerliste, **Fach 1**).

Hinweis Ministerbüro: Eine aktualisierte Teilnehmerliste wird rechtzeitig zum Termin vorgelegt.

Dr. Dürig

Dr. Pilgermann / Otte

Stand: 22. Mai 2012

Ministergespräche IT-Schutz kritischer Infrastru

Teilnehmerliste Informationstechnik & Kommuni

Fach 1 (Austausch)

Teilnehmer Wirtschaft

1. [redacted], Leiter des Zentralbereichs Politik und Regulierung, T[redacted]
2. [redacted] Head of Office IT, V[redacted] GmbH
3. [redacted] Vorsitzender der Geschäftsführung, E[redacted] GmbH & Co. KG
4. [redacted], Vice President Internal Audit & Corporate Security, T[redacted] GmbH & Co. OHG
5. [redacted] Vorstand [redacted] AG, U[redacted] AG
6. [redacted] Leiter Corporate & Regulatory Affairs, U[redacted] AG
7. [redacted], Mitglied der Geschäftsleitung, K[redacted] AG
8. [redacted] Vorstand, D[redacted] eG
9. [redacted], Hauptgeschäftsführer, B[redacted].
10. [redacted] Vorstandsvorsitzender, e[redacted]. V.
11. [redacted] Geschäftsführer, V[redacted] GmbH
12. [redacted] Vertriebsdirektor, V[redacted] GmbH

Stand: 22. Mai 2012

Staatliche Teilnehmer

13. **Herr Dr. Andreas SCHUSEIL,** Abteilungsleiter, Bundesministerium für Wirtschaft und Technologie

14. **Frau Gertrud HUSCH,** Referatsleiterin, Bundesministerium für Wirtschaft und Technologie

BMI

15. **Frau Cornelia ROGALL-GROTHE,** Staatssekretärin

16. **Herr Martin SCHALLBRUCH,** IT-Direktor

17. **Herr Arne SCHLATMANN,** Leiter Leitungsstab

18. **Frau Barbara KLUGE,** Leiterin Ministerbüro

19. **Frau Dr. Barbara SLOWIK,** Leiterin ÖS II 1

20. **Herr Rene DUBOIS,** Referatsleiter KM 1

21. **Herr Dr. Markus DÜRIG,** Leiter IT 3

22. **Frau Kathrin OTTE,** Referat IT 3

Geschäftsbereich

23. **Herr Michael HANGE,** Präsident, BSI

24. **Herr Ralph TIESLER,** Vizepräsident, BBK

25. **Herr Prof. Dr. Jürgen STOCK,** Vizepräsident, BKA

26. **Herr Dr. Burkhard EVEN,** Abteilungsleiter 4, BfV

Stand: 14. Mai 2012

Staatliche Teilnehmer

11. **Herr Dr. Andreas SCHUSEIL,** Abteilungsleiter, Bundesministerium für Wirtschaft und Technologie

12. **Frau Gertrud HUSCH,** Referatsleiterin, Bundesministerium für Wirtschaft und Technologie

BMI

13. **Frau Cornelia ROGALL-GROTHE,** Staatssekretärin

14. **Herr Martin SCHALLBRUCH,** IT-Direktor

15. **Herr Norbert SEITZ,** Abteilungsleiter KM

16. **Herr Arne SCHLATMANN,** Leiter Leitungsstab

17. **Frau Barbara KLUGE,** Leiterin Ministerbüro

18. **Herr Dr. Markus DÜRIG,** Leiter IT 3

19. **Herr Dr. Michael PILGERMANN,** Referat IT 3

Geschäftsbereich

20. **Herr Michael HANGE,** Präsident, BSI

21. **Herr Christoph UNGER,** Präsident, BBK

22. **Herr Jürgen MAURER,** Vizepräsident, BKA

23. **Herr Dr. Burkhard EVEN,** Abteilungsleiter 4, BfV

Stand: 14. Mai 2012

Ministergespräche IT-Schutz kritischer Infrastrukturen

Teilnehmerliste Informationstechnik & Kommunikation

Teilnehmer Wirtschaft

1. [redacted], Leiter des Zentralbereichs Politik und Regulierung, T[redacted]AG
2. [redacted], Head of Office IT, V[redacted]GmbH
3. [redacted] Vorsitzender der Geschäftsführung, E[redacted]
4. [redacted], Vice President Internal Audit & Corporate Security, T[redacted]
5. [redacted], Vorstand [redacted] U[redacted]AG
6. [redacted], Leiter Corporate & Regulatory Affairs, U[redacted]
7. [redacted], Mitglied der Geschäftsleitung, K[redacted]AG
8. [redacted], Vorstand, D[redacted]
9. [redacted], Hauptgeschäftsführer, B[redacted]
10. [redacted] Vorstandsvorsitzender, e[redacted]V.

Provich

Referat IT 3
Verfasser RRn Otte

14. Mai 2012
Hausruf 2808

Ministergespräche IT-Schutz kritischer Infrastrukturen
Gesprächsführungsvorschlag Begrüßung

Begrüßung teilnehmende Wirtschaftsvertreter,
Herr **Dr. Schuseil** (Abteilungsleiter, Bundesministerium für Wirtschaft und Technologie)

Die Gewährleistung von IT-Sicherheit ist eine der zentralen Fragen unserer Zeit.

- In unserer **global vernetzten Welt** sind Staat, Wirtschaft und Bevölkerung **auf das verlässliche Funktionieren** von **Informations- und Kommunikationstechnologie** und des **Internets** angewiesen.
  Wir profitieren als **Industrienation**: Die **rasante Fortentwicklung** der IT und die zunehmende Vernetzung eröffnen **Chancen** und schaffen Innovationen. Sie sind ein wichtiger Baustein für Produktivität, **wirtschaftliches Wachstum und Wohlstand**.

- Gleichzeitig steigen mit der Abhängigkeit die **Risiken**: **IT-Ausfälle** stellen eine **reale Gefahr** dar.
  Stuxnet 2010 war ein Weckruf und hat gezeigt, dass selbst vom Internet abgekoppelte Prozesse und Systeme angreifbar sind und aufgrund des weitverbreiteten Einsatzes gleicher Systeme (hier SCADA) weitreichende Folgen haben können.
  Auch die **Informations- und Kommunikationstechnologie** steht **im Fokus**: Die Vorfälle beim ehemaligen Telekom-Ausrüster **Nortel**, der **KPN-Hack** Ende Januar oder die jetzt entdeckten Hintertüren in den **WLAN-Routern von Arcadyan** verdeutlichen die Bandbreite der Gefahren und Angriffe.

Herr **Hange**, der **Präsident** des Bundesamtes für die Sicherheit in der Informationstechnik, wird im Anschluss einen **Überblick über die Gefährdungslage** geben.

- Die **Gefährdungslage ist real** und **Anlass** für mich, **Sie heute einzuladen.** Lassen Sie uns **gemeinsam** überlegen, wie wir uns **besser aufstellen** können. Ihnen kommt als **Vertreter der großen Unternehmen und Verbände** der **Informations- und Kommunikationstechnologie** in Deutschland eine **unverzichtbare wirtschaftliche und gesellschaftliche Rolle** zu.

Schutz kritischer Infrastrukturen: Daseinsvorsorge des 21. Jahrhunderts

- Als Bundesminister der Innern ist mir der Schutz der für unsere Gesellschaft elementaren **Infrastrukturen ein besonderes Anliegen. Widerstandsfähige Infrastrukturen** und ein sicheres, verfügbares und vertrauliches Internet über nationale Grenzen und Rechtssysteme hinweg sind das **Rückgrat unserer globalisierten Welt**. Es ist Aufgabe des Staates, die **Grundversorgung sicherzustellen** und kritische Infrastrukturen zu schützen (Daseinsvorsorge und Gefahrenabwehr).

- Dabei geht es um das **robuste Funktionieren** und die **permanente Verfügbarkeit der für die Bevölkerung elementaren Dienstleistungen**. Die **Folgen** einer längeren Unterbrechung können für Bevölkerung, Staat und Wirtschaft **katastrophal** sein. Das wissen Sie so gut wie ich.

- Kritische **Informationsinfrastrukturen** sind ein **zentraler Bestandteil** nahezu aller kritischen Infrastrukturen. Dies haben mir die **Vertreter der Finanz- und Versicherungswirtschaft**, mit

denen ich Anfang Mai gesprochen habe, bestätig. **Sichere IKT** ist die **Grundlage ihres Handelns**.

Rolle und Aufgabe BMI

- Die Bundesregierung hat den Schutz der kritischen Infrastrukturen mit der **Cyber-Sicherheitsstrategie** (Februar 2011) in den Mittelpunkt ihrer Maßnahmen zur Cyber-Sicherheit gestellt.

- Hiermit habe ich auch den Auftrag erhalten, **gesetzgeberische Maßnahmen zu prüfen**. Dies entspricht der **internationalen Diskussion**. Ich war gerade in den **USA**, wo entsprechende Gesetzesvorschläge zur Cyber-Sicherheit im Kongress intensiv beraten werden.

- Ich bin der Auffassung, dass wir auch in **Deutschland bundesweit einheitliche Mindestanforderungen und Meldewege** brauchen und dass der Weg der USA auch für uns eine Möglichkeit ist. Dabei sollten wir auf Vorhandenes aufbauen. Mit dem gerade **novellierten Telekommunikationsgesetz (TKG)** besteht eine **solide Grundlage** für den Telekommunikationsbereich. Solche Regelungen brauchen wir auch für andere kritische Infrastrukturen.

- **TK-Provider** müssen meiner Meinung nach noch einen Schritt weiter gehen (Warnungen der Nutzer, Bereitstellen von Sicherheitswerkzeugen etc.). Wenn wir von den Innovationen moderner Informationstechnologie weiter profitieren und den Weg von **eBanking** und **eGovernent** bis hin zu **Smart Metern** weiter gehen wollen, müssen wir die **Sicherheit der Nutzer** noch stärker im Blick behalten. **Sichere Endkundenrechner** sind von zentraler Bedeutung.

- Für den IT-Schutz kritischer Infrastrukturen spielt der Ausbau der Zusammenarbeit im **Umsetzungsplan KRITIS** eine wesentliche Rolle. Hier haben wir seit 2007 ein Gremium der **Zusammenarbeit** etabliert. Dieses Erfolgsmodell wollen wir weiter voranbringen und stärken. Der Anfang des Jahres von BITKOM und BSI mit der **Cyber-Allianz** initiierte **gesamtwirtschaftliche Informationsaustausch** bildet eine notwendige und **sinnvolle Ergänzung.** Die enge Kooperation **kritischer Infrastrukturen und die Mitwirkung der IKT-Branche im Umsetzungsplan KRITIS** sind darüber hinaus jedoch unabdingbar.

- Zudem haben wir mit dem **Cyber-Abwehrzentrum** die Basis für die operative Zusammenarbeit der zuständigen Bundesbehörden geschaffen und bringen **Know-how und Sachverstand** zusammen. Hiervon kann und soll auch die Wirtschaft profitieren.

Sicherheit kann nur gemeinsam gelingen

- Der **Staat** kann jedoch nur den **Rahmen** und die **Grundlagen** schaffen. Für die **Gewährleistung der Cyber-Sicherheit** sind wir auf Ihre Mitwirkung angewiesen. Sie sind als Betreiber in der Pflicht. **Nur gemeinsam** und in enger Kooperation können wir die Versorgungssicherheit und die Wettbewerbsfähigkeit in Deutschland sicherstellen.

- Ein sehr gutes Beispiel sind die Zusammenarbeit von **BSI, BKA** und **Telekom** sowie die Initiative von **eco** beim **DNS-Changer**, für die ich mich an dieser Stelle bei der **Telekom** und bei **eco** ausdrücklich **bedanken** möchte. Auch das **Anti-Bootnet-Beratungszentrum,** das Nutzern Hilfe bei der Bereinigung infizierter Rechner bietet, ist das Ergebnis einer gelungenen **Public Private Partnership** (durchgeführt von eco mit technischer Unterstützung durch BSI und finanziert durch BMI).

- Die IKT-Branche ist in weiten Bereichen vorbildlich. Neben einem soliden Regelungswerk für den Telekommunikationsbereich haben wir trotz aller Anfangsbedenken heute eine **sehr gute und erfolgreiche Zusammenarbeit im Umsetzungsplan KRITIS**.

Ziel der Gespräche: IT-Schutz flächendeckend stärken

- Unser heutiges Gespräch ist der **zweite Termin** in einer Reihe. Zu den kritischen Infrastrukturen zählen auch Wasser, Energie, Verkehr, Gesundheitswesen, die Ernährungswirtschaft sowie Medien und Kultur. Mit der Finanzwirtschaft habe ich bereits gesprochen. (Die kritischen Infrastrukturen in Staat und Verwaltung können wir mit Strukturen wie dem IT-Rat in anderer Form schützen.)

- Ich möchte mit Ihnen **gemeinsam überlegen**, wo wir weiter tätig werden müssen und **wie wir die IT-Sicherheit kritischer Infrastrukturen bundesweit flächendeckend gewährleisten** können. Was aus meiner Sicht grundlegend für den IT-Schutz kritischer Infrastrukturen ist, habe ich Ihnen mit der Einladung übermittelt (**Diskussionspapier** liegt aus). Bevor wir nachher in die Diskussion einsteigen, wird **Herr Schallbruch**, der IT-Direktor in meinem Haus, Ihnen **unsere Überlegungen vorstellen**.

- Ich möchte dieses Dokument **gemeinsam mit Ihnen weiterentwickeln** und wäre Ihnen dankbar, wenn Sie mir im Nachgang Ihre **Anmerkungen** zum Dokument und zur Diskussion **schriftlich zukommen lassen könnten**.

Überleitung zu weiteren Vorträgen und zur Diskussion ⇒ Fach 3

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 14.05.2012
Hausruf: 1527

2. Cybersicherheit im IKT-Sektor aus fachspezifischer Sicht

Herr Dr. Schuseil (BMWi) wurde mit Einladungsschreiben von Stn. Rogall-Grothe um Vorbereitung eines kurzen Beitrags gebeten.

I. Sprechempfehlung

- Darstellung der gemeinsamen Vorgehensweise zw. Innenminister als KRITIS-Koordinierer und Fachressorts mit sektorspezifischer Kompetenz
- Hinweis auf die bereits verankerte IT-Sicherheit in der Aufsichtspflicht über den IKT-Sektor; zudem Mitwirkung von BMWi und BNetzA im UPK
- Verweis auf Herrn Dr. Schuseil für einen Beitrag „Cybersicherheit im IKT-Sektor aus fachspezifischer Sicht"

II. Aktueller Sachstand

- BMWi ist seit Beginn der Arbeiten im UPK (ab 2005) Teil der Kooperation mit der Wirtschaft. Die Aufsichtsbehörde BNetzA nimmt ebenfalls an den Sitzungen der Arbeitsgruppen teil.

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 14.05.2012
Hausruf: 1527

3. Cybersicherheitslage in Deutschland

Herr P BSI Hange hat (in Abstimmung mit BKA / BfV) einen kurzen Vortrag zur Cyber-Bedrohungslage vorbereitet – Übergabe an diesen

I. Sprechempfehlung

- Einführung zu Stuxnet als Schadprogramm, welches Ende 2010 mit seinen potentiellen Auswirkungen auf Atomkraftwerke das Thema Cybersicherheit endgültig auf die Tagesordnung aller Entscheider gesetzt hat
- Erinnerung an letzte LÜKEX-Übung von Nov. 2011, bei welcher im Bereich Kritischer Infrastrukturen breitflächige Ausfälle ein Bestandteil waren -> im Ergebnis der Übung Schlussfolgerung einer aktiven Zusammenarbeit zw. Staat und IKT-Sektor.
- Verweis an P BSI Herr Hange m.d.B. um einen Einblick in die Bedrohungslage im Cyberspace

II. Aktueller Sachstand

- Angespannte IT-Sicherheitslage, weil Abhängigkeit der Gesellschaft von Informations- und Kommunikationsinfrastrukturen (IKT) erheblich gestiegen ist und die Angreifer sich professionalisiert haben
- Kritische Infrastrukturen aus allen Sektoren sind von IKT abhängig – dem IKT-Sektor kommt beim IT-Schutz Kritischer Infrastrukturen also eine besondere Rolle zu

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 14.05.2012
Hausruf: 1527

4. Anforderungen an den IT-Schutz KRITIS aus Sicht BMI

Herr ITD Schallbruch hat einen Vortrag zur Vorstellung des Diskussionspapiers vorbereitet

I. Sprechempfehlung

- mit verschärfter Bedrohungslage Notwendigkeit zum sektorübergreifenden, koordinierten Vorgehen
- alle Betreiber in allen Sektoren müssen ein gewisses Mindestmaß an KRITIS-Schutz gewährleisten
- BMI hat dies in 7 Kernforderungen in einem Diskussionspapier zusammengefasst und mit der Einladung übersandt
- Verweis an ITD zur Vorstellung der konkreten Forderungen aus Sicht BMI

II. Aktueller Sachstand

- BMI hat Diskussionspapier „IT-Schutz Kritischer Infrastrukturen in Deutschland" mit 7 grundlegenden Forderungen zum IT-Schutz KRITIS erarbeitet
- An Wirtschaftsvertreter übersandt im Rahmen der Einladungsschreiben von Herr Minister

Bundesamt
für Sicherheit in der
Informationstechnik

Robuste IKT: Rückgrat für Cyber-Sicherheit

Michael Hange
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

23. Mai 2012

Bundesamt
für Sicherheit in der
Informationstechnik

Gefährdungen

Gefährdungen für das Internet

- Angriffe auf die Infrastruktur
- Fehlkonfiguration...

Beispiele

- DigiNotar
- Fehlkonfiguration in China bringt Routing weltweit durcheinander

Gefährdungen über das Internet

- Botnetze/DDos mittels Botnetzen
- Drive-by-Downloads
- Identitätsdiebstahl durch Malware
- Advanced Persistent Threats...

Beispiele

- Miner-Botnetz
- RSA
- KPN-Hack
- Hintertür in WLAN-Routern

Bundesamt
für Sicherheit in der
Informationstechnik

Herausforderungen

Technische Entwicklung

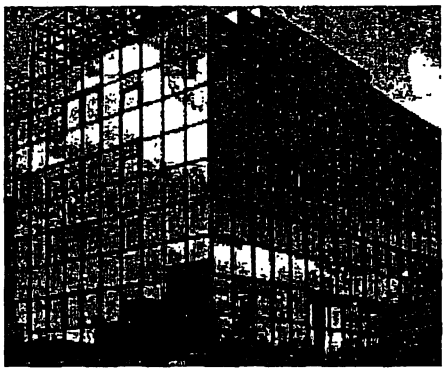
- Zusammenwachsen von TK und Internet (z.B. Smartphones)

Bedarf

- Infrastruktur Internet stabil gestalten.
- Für die Anwender Robustheit und Schutz in die Angebote bzw. Dienst integrieren.
- Gemeinsames Lagebild erstellen, um präventive Maßnahmen ergreifen zu können.

Bundesamt
für Sicherheit in der
Informationstechnik

Kontakt



Bundesamt für Sicherheit in der Informationstechnik (BSI)

Michael Hange
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-5200
Fax: +49 (0)22899-10-9582-5200

Michael.Hange@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 14.05.2012
Hausruf: 1527

5. Diskussion der Anforderungen an den IT-Schutz

Diskussionspapier aus 4) war Wirtschaftsvertretern in Vorbereitung zur Verfügung gestellt worden

Moderation: Minister (entlang Diskussionspapier)

(Vorgeschlagener Fragesteller (Min/StnRG/ITD) jeweils in Klammern; **prioritäre Fragen fett**)

I. Sprechempfehlung

(TK-Unternehmen unterliegen gesetzl. Auflagen bzgl. IT-Sicherheit.)

(Min) **Allgemeine Fragen:**

- Einschätzung zum Sachstand des IT-Schutzes der Kritischen Infrastrukturen im Sektor insgesamt
- **Kompatibilität von Auflagen und Rahmenbedingungen in Deutschland mit denen in anderen Ländern?**
- Erfahrungen aus der Zusammenarbeit im UPK seit 2007?
- **Im relativ stark regulierten und umkämpften TK-Markt: wie sind (zusätzliche) Investitionen in Sicherheit ohne Regulierung bei Verantwortung ggü. Aktionären möglich?**

Fragen zu den Punkten aus dem Diskussionspapier:

1) *Mehr Transparenz schaffen*

(Die kritischen Geschäftsprozesse müssen identifiziert; die Abhängigkeit dieser Prozesse von IKT bekannt sein.)

- *StnRG:* **Besteht bei den IKT-Unternehmen übergreifend Transparenz bzgl. der Abhängigkeiten, die anderen Unternehmen (kritische Infrastrukturen) elementar an diese stellen?** (Bezug auf Aussage der Banken vom 09.05. mit enormer Abhängigkeit von IKT und Energie).
- *ITD:* Wie werden Risiken für die Gesellschaft im Risikomanagement prominent abgebildet?

2) *Robuste Grundlagen*

(Mindeststandards müssen definiert sein. Regelmäßige Überprüfungen (Audits) verifizieren deren Umsetzung.)

Mindeststandards

- *StnRG:* **TKG setzt Standards nur für Ausschnitt des IKT-Sektors: wie wird Erreichung mindestens dieses Niveaus in den nicht- /weniger regulierten Bereichen sichergestellt?**

Audits

- *ITD:* Wie groß ist inzwischen der Anteil von IT-Anforderungen in den regelmäßigen Audits (intern oder auch durch Externe)?
- *ITD:* Wir könnte in diesem Bereich eine Zusammenarbeit mit dem BSI aussehen?

3) *Kritische Prozesse autonom gestalten*

(Kritische Prozesse dürfen weder mit dem Internet verbunden sein noch von dessen Funktionstüchtigkeit abhängen.)

- *StnRG:* **Können zentrale IT-Systeme (zur Aufrechterhaltung der eigenen, zentralen Prozesse) unabhängig vom öffentlichen Internet fortbetrieben werden?**

4) *Produkt- und Dienstleistungssicherheit*

(Für besonders sensible Bereiche kommen zertifizierte Produkte zum Einsatz; IT-Sicherheit fließt von Anfang an mit in Planung von IKT-Diensten ein.)

- *Min:* **In BReg besondere Zulassungsverfahren für IT in sensiblen Bereichen. Gibt es vergleichbare Vorkehrungen zum Einsatz ausschließlich zertifizierter Systeme in den kritischen Bereichen?**

5) *Lagefortschreibung und Frühwarnung*

(Alle Unternehmen sind über die Warn- und Alarmierungsmechanismen des UPK an das BSI angeschlossen.)

- *StnRG:* Vergleichsweise **geringes Meldeaufkommen über UPK-Strukturen** im Vergleich zur Lage in der Bundesverwaltung. Wie ist großer Unterschied zu erklären?

6) *Regelmäßige Übungen*

(Mit regelmäßigen Übungen werden aufgebaute Strukturen überprüft.)

- *ITD:* LÜKEX als erste nationale IT-Übung (Bund, Länder, KRITIS) Ende 2011 ein Erfolg – welche Formate des gemeinsamen Übens werden gebraucht?
- *ITD:* Wie ergänzen die Branchen die übergreifenden regelmäßigen Übungen aus dem UPK sektorspezifisch?

7) *Institutionalisierte Kooperation*

(Alle Branchen müssen im UPK vertreten sein. Darüber hinaus muss das Thema Cybersicherheit auch in allen Branchen intern in einer institutionalisierten Zusammenarbeit aufgearbeitet werden.)

- *Min:* Hinweis auf hohen Organisationsgrad des IKT-Sektors im UPK – im Hinblick auf branchenspezifische Kreise; Frage zur Bereitschaft, diese mit dem UPK zu verzahnen?

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 14.05.2012
Hausruf: 1527

6. Zusammenfassung und Ausblick

I. Sprechempfehlung

- Dank für die Diskussion; Anmerkungen zum Diskussionspapier willkommen, Prozess soll gemeinsam weitergestaltet werden; Vorschlag:
  - Betreiber / Verbände erarbeiten und übersenden branchenspezifische Beantwortung der Fragen,
  - Diskussion, Weiterentwicklung und sektorspezifische Umsetzung sollte im UPK fortgeführt werden
- 4 weitere Gespräche bis Ende August: Kommunikation als entscheidendes Merkmal beim KRITIS-Schutz – sowohl branchenintern als auch branchenübergreifend
- Ziel, bundesweit und flächendeckend Standards zu etablieren
  - gesetzgeberische Maßnahmen nicht ausgeschlossen; großer Teil des IKT-Sektors ja aber bereits IT-Sicherheitsspezifischer Regulierung unterworfen
  - Hoffnung, dass sich alle Branchen des Themas verstärkt annehmen und die notwendigen Maßnahmen auf den Weg bringen.
- Appell:
  - an die Verbände, branchen- und sektorspezifisch das Thema IT-Schutz Kritischer Infrastrukturen und Cybersicherheit aktiv voranzutreiben,
  - an den gesamten Sektor, Zusammenarbeit zum IT-Schutz KRITIS branchenübergreifend im UPK intensiv fortzuführen und mitzugestalten und branchenspezifisch zu institutionalisieren,
  - an die Betreiber, für ein nationales Lagebild zur IT-Lage im BSI mit diesem im engen Kontakt zu bleiben und relevante Vorfälle zu melden,

II. Aktueller Sachstand

- IKT-Sektor zu weiten Teilen reguliert (grdsl. aktive Mitarbeit im UPK; auch wenn Geschäftsinteressen hier teilweise den Sicherungsinteressen vorgehen)
  ➔ mögliche gesetzliche KRITIS-Regelungen sollten begrenzt Auswirkungen in diesem Bereich haben
- Nachhaltigkeit: Auftrag aller Sitzungs-Beteiligten an den UPK, das Diskussionspapier weiterzuentwickeln, und auf dieser Basis zeitnah Transparenz und Vergleichbarkeit zum IT-Schutz KRITIS in allen Branchen herzustellen

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 14.05.2012
Hausruf: 1527

Potentielle Fragen/Themen der Wirtschaft (und Antworten)

I. Sprechempfehlung Allgemeine Fragen

Was sind kritische Infrastrukturen – anhand welcher Kriterien werden diese ausgewählt?

- Definition von BMI ist systemisch; die kritischen Sektoren und Branchen sind identifiziert. Niemand stellt in Fragen, dass im heutigen Deutschland sich die Gesellschaft hochgradig von IKT-Dienstleistungen und sogar dem Internet abhängig gemacht hat.
- Schwerpunkt zur Bestimmung der Kritikalität ist die Bereitstellung von Dienstleistungen an die Bevölkerung/Gesellschaft, bei Ausfall/Beeinträchtigung dieser der Wohlstand/Lebensstandard in DE beeinträchtigt würde.

Schwerpunktstaatsanwaltschaften für Computerkriminalität?

- Grundsätzlich wird die Einrichtung von Schwerpunktstaatsanwaltschaften zur Bekämpfung der Computerkriminalität für sinnvoll gehalten. Die Frage fällt in die Zuständigkeit der Länder (§ 143 GVG). In einer Reihe von Ländern wurde von dieser Möglichkeit auch bereits Gebrauch gemacht.

Was machen Bundesregierung/BMI/BSI/BBK selbst um den Schutz Kritischer Infrastrukturen zu verbessern?

- Schwerpunkt der Aktivitäten ist und bleibt Umsetzungsplan KRITIS als institutionalisierte Zusammenarbeit zw. Wirtschaft und Verwaltung seit 2007. Aktuell Fortschreibung des UPK, um Inhalte und Struktur an geänderte Lage anzupassen.
- Mit überarbeitetem BSIG von 2009 wurde der Blickwinkel der Behörde explizit verbreitert – Dienstleistungen und Produkte werden auch explizit Partnern aus der Wirtschaft zur Verfügung gestellt. Offensichtlich erster Partner: KRITIS-Betreiber!
- Für einheitliches Mindestniveau über alle Kritischen Infrastrukturen wird ebenfalls gesetzlicher Handlungsbedarf evaluiert.

Wie verhält sich der KRITIS-Schutz zur iPPP-Initiative? Ist eine Verlinkung mit den UPK Single Points of Contact (SPOC) angestrebt?

- Anders als die Initiativen zum KRITIS-Schutz hat die Einrichtung einer zentralen Stelle auf Bundesebene zur institutionalisierten Zusammenarbeit der deutschen Polizeien mit privaten Institutionen (institutionalisierte Public Private Partnership = iPPP) das Ziel den **Informationsaustausch** zwischen den Polizeien und der Industrie zu verbessern und so die **Bekämpfung der Computerkriminalität** zu verbessern. Vertreter verschiedener, von IuK-Kriminalität betroffener Industriezweige (**Banken**, Hard- und Softwareunternehmen, Kreditkartenfirmen usw.) sollen dort zusammenarbeiten und sich zu aktuellen Phänomenbereichen der IuK-Kriminalität austauschen. Eine Zusammenführung der SPOCs ist wegen der unterschiedlichen Zielrichtung nicht geplant.

Wie stellt der Staat einen risikobasierten Ansatz sicher?

- Staat unterhält Strukturen, um Bedrohungen bewerten zu können.
- Unternehmen treffen Vorsorge, ihre Kritischen Prozesse zu identifizieren und abzusichern.
- An der Schnittstelle (z.B. im UPK – entsprechende IKT-Studie im Abschluss) werden die Kompetenzen zusammengeführt, um Risiken für die Gesellschaft zu bewerten und auf nationaler Ebene angemessen zu priorisieren.

II. Sprechempfehlung spezifisch für IKT-Sektor

Wie positioniert sich die BReg bzgl. der potentiellen Ausweitung der EKI-Richtlinie (Europ. Kritische Infrastrukturen) auf den IKT-Sektor?

- EKI-Richtlinie befindet sich aktuell in Evaluierung – die KOM erarbeitet zu diesem Zeitpunkt die Handlungsoptionen.
- BMI unterstützt das übergreifende EPSKI-Programm (Europ. Programm zum Schutz von KI); sieht Aufwand und Nutzen der darin enthaltenen Richtlinie jedoch nicht im Verhältnis.
- DE hält die bestehende Richtlinie für verfehlt und lehnt eine Ausweitung ab.

Ein hohes Sicherheitsniveau erfordert deutlich höhere Investitionen.

Öffentliche Ausschreibung meist preisoptimierend: Wie kann erhöhtes Sicherheitsniveau in öffentlichen Ausschreibungen abgebildet werden?

- Etablierte Strukturen mit Zertifizierungen und Zulassungen, um notwendige Sicherheit in der Verwaltung sicherstellen zu können.
- Verantwortung auch der Unternehmen, Geschäftsmodelle zu entwickeln und auch außerhalb der Verwaltung Produkte zu platzieren (Bsp.: Simko)

Referat IT 3 14.05.2012
Verfasser RRn Otte Hausruf 2808

Hintergrundinformation IT-Schutz kritischer Infrastrukturen

Ausgangslage: **Kritische Infrastrukturen** (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. KRITIS-Schutz wird von BMI als sicherheitspolitisches Aufgabenfeld in Koordinierungsfunktion wahrgenommen. Grundlage: Nationale Strategie zum Schutz Kritischer Infrastrukturen (Juni 2009, s. **Anlage**).

Informations- und Kommunikationstechnik (IKT) heute für KRITIS von erheblicher Bedeutung, stetige Zunahme der **Abhängigkeit von IKT und Internet**; Kerngeschäftsprozesse in vielen Branchen IT-basiert (Zahlungsverkehr der Banken, Disposition bei Häfen/Logistikunternehmen etc.); häufig Standard-IT-Systeme für einen Infrastrukturbereich, zum Teil keine strikte Entkopplung vom Internet. Hinzu kommt Zunahme der **Abhängigkeiten der Infrastrukturen untereinander** (Finanzwesen von Telekommunikation, Telekommunikation von Energie etc.) ⇒ **stark erhöhte Verletzbarkeit durch Cyberbedrohungen.**

Initiative der Bundesregierung: **2005** erste IT-Sicherheitsstrategie der Bundesregierung (Nationaler Plan zum Schutz der Informationsinfrastrukturen) und auf dieser Basis Erarbeitung des **Umsetzungsplan KRITIS** (UPK, September 2007, s. **Anlage**) von BMI und Branchenvertretern: Nationale Initiative zwischen KRITIS-Betreibern und Staat zum Schutz kritischer Informationsinfrastrukturen mit **Ziel insbes. der Prävention durch erhöhte IT-Sicherheitsniveaus, schneller Reaktionsfähigkeit** durch Erkennungsmaßnahmen, Ausbau der **Kommunikation zur Alarmierung und Krisenbewältigung** und der **branchenübergreifenden Zusammenarbeit** (40 Unternehmen, 4 Arbeitsgruppen).
Schutz kritischer Informationsinfrastrukturen Priorität der Nationalen **Cyber-Sicherheitsstrategie der Bundesregierung** (Februar 2011). Aufträge: Ausbau der Zusammenarbeit durch UPK, Einbeziehung weiterer Branchen und Prüfung

möglicher rechtlicher Verpflichtungen der KRITIS-Betreiber sowie Prüfung der Notwendigkeit, Schutzmaßnahmen vorzugeben, der Schaffung zusätzlicher Befugnisse für den Fall konkreter Bedrohungen sowie der Harmonisierung der Regelungen zur Aufrechterhaltung der KRITIS in IT-Krisen.
Abstimmung des Vorgehens durch Cyber-Sicherheitsrat (Oktober 2011).

Cebit 2012: Zur Stärkung der Kooperation zwischen Staat, Wirtschaft und Forschung haben BSI und BITKOM eine **Cyber-Allianz** verkündet; Allianz befindet sich derzeit in der Konzeption und soll den UPK ergänzen.

International: **USA** arbeiten derzeit an **IT-Sicherheitsgesetz**, in dessen Kern die IT-Sicherheit von KRITIS sowie der Schutz kritischer Informationsinfrastrukturen steht.

Auf **EU-Ebene** regelmäßiger Austausch im Programm zum Schutz der kritischen Informationsinfrastrukturen (**CIIP**, Generaldirektion Informations-Gesellschaft) i.R.d. Aktionsplans der Kommission zum Schutz kritischer Informationsinfrastrukturen (2009) einschließlich gemeinsamer Cyberübungen und Aufbau von Kooperationsmechanismen in IT-Lagen.

Schutz kritischer Informationsinfrastrukturen zudem Schwerpunkt der diesen November von Deutschland ausgerichteten **Meridian-Konferenz** (von Großbritannien 2005 im Rahmen von G8 initiierter Prozess; Regierungsvertreter).

Definition „Kritische Infrastrukturen"

- Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.[1]

Sektoren- und Brancheneintellung Kritischer Infrastrukturen

Sektoren	Branchen
Energie	• Elektrizität • Gas • Mineralöl
Informationstechnik und Telekommunikation	• Telekommunikation • Informationstechnik
Transport und Verkehr	• Luftfahrt • Seeschifffahrt • Binnenschifffahrt • Schienenverkehr • Straßenverkehr • Logistik
Gesundheit	• Medizinische Versorgung • Arzneimittel und Impfstoffe • Labore
Wasser	• Öffentliche Wasserversorgung • Öffentliche Abwasserbeseitigung
Ernährung	• Ernährungswirtschaft • Lebensmittelhandel
Finanz- und Versicherungswesen	• Banken • Börsen • Versicherungen • Finanzdienstleister
Staat und Verwaltung	• Regierung und Verwaltung • Parlament • Justizeinrichtungen • Notfall-/ Rettungswesen einschließlich Katastrophenschutz
Medien und Kultur	• Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse • Kulturgut • symbolträchtige Bauwerke

[1] Bundesministerium des Innern, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/SicherheitAllgemein/kritis.html (17.06.2009)

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 14.05.2012
Hausruf: 1527

IT-Schutz KRITIS im Finanzsektor

I. Hintergrundinformationen

Der KRITIS-Sektor „Informations- und Kommunikationstechnik" (IKT) ist in folgende zwei Branchen aufgeteilt:

- Telekommunikation (TK)
- Informationstechnik (IT)

Marktsituation und Branchenorganisation

Auf Grund der Konvergenz von TK und IT lässt sich eine strikte Zuordnung von Organisationen zu einer Branche nicht vollziehen. Es lassen sich grob unterscheiden:

- Zugangsanbieter (Telefon, Internet) für Endkunden (Festnetz und Mobilfunk) sind [redacted] und [redacted]
- Zur Aufrechterhaltung von Diensten im Internet wirken verschiedene Organisationen auf unterschiedlichen Ebenen zusammen:
    - Internet-Knotenpunkte wie DE-CIX stellen eine Verbindung zw. den dezentral organisierten öffentlichen Netzen in DE und darüber hinaus her.
    - Diensteanbieter wie Denic oder Verizon stellen elementare, für die Funktion des Internets unverzichtbare Infrastrukturdienstleistungen zur Verfügung, mit denen das Internet erst sicher und komfortabel genutzt werden kann.
    - Auf diesen operieren Anbieter für Endkunden (Privatnutzer und auch Enterprises) und stellen ihre Dienste (z.B. Email) zur Verfügung.

Auf Grund der Lukrativität des Inhaltegeschäftes verschwimmen die Grenzen; die Zugangs- /Infrastrukturanbieter drängen aktiv auch in dieses Geschäft.

Zwei Verbände sind im Sektor herausragend relevant: B[redacted]versteht sich als Interessenvertreter für den gesamten Sektor und umfasst neben Betreibern auch Hersteller von Geräten und Anwendungen. [redacted]fokussiert sich als Interessenvertreter auf die Internetindustrie.

Aufsichtssituation

Das Telekommunikationsgesetz (TKG) enthält Regelungen für öffentliche Telekommunikationsnetze und öffentlich zugängliche Telekommunikationsdienste.

Es regelt u.a. Notwendigkeit für Sicherheitskonzept, Audits und Meldepflichten. Die Anforderungen werden ausgestaltet in Form des Sicherheitskatalogs, welcher aktuell im Benehmen mit BSI überarbeitet wird.

Aufsichtsfunktion nimmt Bundesnetzagentur (BNetzA) wahr; diese ist eine Bundesoberbehörde – weitere Fachbehörden werden zu Spezialthemen einbezogen.

Die Aufsichtsregelung nach TKG beschränkt sich auf einen Teil der Dienstleistungen aus dem IKT-Sektor. Zusätzlich existierende Regelungen aus dem Telemediengesetz decken IT-Sicherheit nicht ab. Lt. BMWi ist Ausklammerung weiter Teile des IT-Bereichs (primär Internet) intendiert.

Zudem existieren Verpflichtungen durch PTSG[3], ein Spezialgesetz für Krisenfälle mit bestimmten Sicherstellungs- und Mitwirkungspflichten.

IKT-Abhängigkeit

Selbstredend ist im IKT-Sektor von einer hohen IKT-Abhängigkeit auszugehen.

Vor dem Hintergrund der Sicherheit ist daher primär auf eine angemessene Entkopplung von Netzbereichen zu drängen. Dies wird in Anbetracht der Konvergenz der Technologien immer schwieriger. Es ist jedoch davon auszugehen, dass die Betreiber gemäß Stand der Technik Netzkopplungen restriktiv auslegen, um ungewünschte Einwirkungen aus anderen Netzen (z.B. dem Internet) zu minimieren.

---

1 B[redacted]n

2 [redacted].

3 Post- und Telekommunikations-Sicherstellungsgesetz

Besondere Relevanz kommt den Betreibern aus dem IKT-Sektor zu, weil neben der Bereitstellung von IKT-Dienstleistungen an die Gesellschaft auch andere KRITIS-Sektoren hochgradig von Services aus diesem Sektor abhängig sind (so auch dargestellt von Vertretern aus Finanzsektor im Minister-Gespräch am 09. Mai).

Diese Abhängigkeit führt auch im Umsetzungsplan KRITIS regelmäßig zu Diskussionen: während fast alle Branchen als Konsumenten von IKT-Dienstleistungen agieren sind die Vertreter des IKT-Sektors primär die Bereitsteller der eingeforderten Leistungen. So gehen auch die Vorstellungen zur Robustheit eben dieser Prozesse auseinander:

- Alle anderen Sektoren (als Konsumenten) plädieren für eine (ggf. auch gesetzliche) Verpflichtung von Anforderungen bzgl. der Verfügbarkeit/Sicherheit von IKT-Dienstleistungen
- IKT-Dienstleister plädieren dagegen für bilaterale Verträge / Service Level Agreements, bei welchen hohe Verfügbarkeitsanforderungen zu zusätzlichem Geschäft führen.

Schutzniveau und Lücken

Für den IKT-Sektor ist die Bereitstellung von IKT-Dienstleistungen Kerngeschäft – die Betreiber beschäftigen sich seit Jahren aktiv mit der Absicherung ihrer Prozesse und Infrastrukturen.
Anforderungen an die Sicherheit sind gesetzlich vorgeschrieben und werden von der Aufsicht überprüft.

Sehr weite Teile des Sektors haben Frühwarnmechanismen etabliert und sind auch an die BSI-Strukturen zur Lagefortschreibung angeschlossen. Ungünstig wirkt sich die operative Anbindung von Teilen des Sektors an das BSI über die BNetzA aus, da eine aktive Zusammenarbeit hier nicht etabliert ist.

Lücken: Die gesetzlich festgeschriebenen Anforderungen greifen nur für einen Teil des IKT-Sektors (weite Bereiche des Internet sind ausgeklammert).

BMWi übt sich seit Jahren in Zurückhaltung bei der Zusammenarbeit mit BMI zum Schutz Kritischer Infrastrukturen – dies wird im Kompetenzkonflikt begründet sein; BMWi sieht BMI hier grdsl. in seinem Zuständigkeitsbereich agieren.

Organisationsgrad

Der Finanzsektor ist grdsl. gut im UPK repräsentiert. Bis auf Kabel Deutschland sind alle anwesenden Organisationen im UPK vertreten.

Wegen allgemeiner Teilnehmerbeschränkungen im UPK sollte für eine Intensivierung der Zusammenarbeit im Grunde auf branchenspezifische Strukturen ausgewichen werden.

Auch branchenspezifisch wird das Thema aktiv aufgegriffen. Bislang partizipiert BSI jedoch nicht an diesen Strukturen; über eine Verstärkung dieser Zusammenarbeit hinaus sollte für die Zukunft auf eine Verzahnung mit dem branchenübergreifenden UPK hingearbeitet werden.

Aktuelle Entwicklungen

- EU KOM (DG HOME) evaluiert in Zusammenarbeit mit den MS aktuell die EKI-Richtlinie (Europ. Kritische Infrastrukturen) von 2008, die Teil des Europ. Programms zum Schutz Kritischer Infrastrukturen (EPSKI) ist. In der Richtlinie wurden nur Regelungen für Energie und Transport/Verkehr getroffen. Die Evaluierung, die bis Ende 2012 angelegt ist, ist ergebnisoffen. Eine denkbare Zukunftsoption ist die Ausweitung auf andere Sektoren; im Vordergrund steht dabei die IKT. DE hält die bestehende Richtlinie für verfehlt und lehnt eine Ausweitung ab.
- Zum 10.05.2012 trat die Novellierung des Telekommunikationsgesetzes (TKG) in Kraft. Grsdl. bringt diese nur geringe inhaltliche Änderungen mit sich; die Änderungen berühren aber insb. Aspekte der IT-Sicherheit.

Stand: 27.04.2012

KRITIS-Sektor „IKT"

Teilnehmende Unternehmen

Name	Aktien-Index	Umsatz in Mrd. (2011)	Mitarbeiter (2011)	Hauptsitz	Mitglied UPK (Bezug Nr. 5)	Übungs-beteiligung (Bezug Nr.6)	Kurzbeschreibung
[redacted]	[redacted]	59	235.132	[redacted]	Ja	Ja	[redacted] Telekommunikationsunternehmen. Das Unternehmen betreibt technische Netze für den Betrieb von Informations- und Kommunikationsdiensten (IuK), etwa Telefonen (Festnetz und Mobilfunk) oder Onlinediensten, es bietet selber auch Onlinedienste an.
[redacted]	-	9	12.000	[redacted]	Ja	Ja	[redacted]. Sie vertreibt in Deutschland Mobilfunk-, DSL- und Festnetz-Angebote
[redacted]	-	3	2.765	[redacted]	Ja	Ja	Gehört zum [redacted] und ist der [redacted] Mobilfunknetzbetreiber in Deutschland.
[redacted]	-	5	5288	[redacted]	Ja	Ja	Ist eine Tochtergesellschaft der [redacted] und der [redacted] Mobilfunknetzbetreiber in Deutschland.
[redacted]	[redacted]	2	5.018	[redacted]	Ja	Ja	Ist mit insgesamt zehn Marken in zwei Geschäftsfeldern aktiv. In seinem Produktgeschäft richtet es sich mit Internet-Mehrwertdiensten an Privatanwender, Klein- und Heimbüros sowie kleine

Stand: 27.04.2012

Name	Aktien-Index	Umsatz in Mrd. (2011)	Mitarbeiter (2011)	Hauptsitz	Mitglied UPK (Bezug Nr. 5)	Übungs-beteiligung (Bezug Nr.6)	Kurzbeschreibung
							und mittlere Unternehmen (KMUs).
[redacted]	[redacted]	1,5	2.700	[redacted]	*Nein*	*Nein*	Bezeichnet sich selbst als [redacted] in Deutschland und betreibt Kabelnetze und Kabelanschlüsse in allen Regionen Deutschlands, außer in den Bundesländern HE, NRW und BW.
[redacted]	-	-	-	[redacted]	Ja	Ja	Verwaltet den [redacted] Dieser ist nach angeschlossenen Internet Service Providern der [redacted]
[redacted]	-	-	-	[redacted]	Ja	Ja	[redacted] der Top-Level-Domain .de. Eine solche Domain darf nur erhalten, wer entweder seinen Wohnsitz in Deutschland hat oder einen rechtlichen Vertreter mit Wohnsitz in Deutschland benennt.
[redacted]	-	-	-	[redacted]	Ja	*Nein*	[redacted] unternehmen. Unter dem Namen [redacted] ausschließlich Dienstleistungen für Geschäftskunden und Behörden an

Stand: 27.04.2012

Teilnehmende Verbände

Name	Angeschlossene Institutionen	Beschäftigte der angeschlossenen Institutionen	Hauptsitz	Mitglied UPK (Bezug Nr. 5)	Übungs-beteiligung (Bezug Nr. 6)	Kurzbeschreibung
[redacted]	1700	700000	[redacted]	Ja	*Nein*	Ist der Branchenverband der deutschen Informations- und Telekommunikationsbranche. Unter den Mitgliedern sind Geräte-Hersteller, Anbieter von Software, IT-Services sowie von Dienstleistungen im Bereich Telekommunikation, Consumer Electronics und Content Provider.
[redacted]	>550	-	[redacted]	Ja	Ja	Der Verband versteht sich als Interessenvertretung der deutschen Internetindustrie und hat sich zum Ziel gesetzt, die kommerzielle Nutzung des Internet voranzutreiben.

BSI 11.05.2012

Einschätzung BSI

Änderung des Telekommunikationsgesetzes

- Inkrafttreten der Änderung des Telekommunikationsgesetzes (TKG) am 10. Mai 2012.
- Kaum BSI-relevante Änderungen in Bezug auf das Zusammenwirken mit BNetzA aus der Novellierung des § 109 TKG.
- Der von der BNetzA im Benehmen mit dem BSI und dem BfDI zu erstellende Katalog von Sicherheitsanforderungen gilt nicht nur auf für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen, sondern nunmehr auch für die Verarbeitung personenbezogenen Daten. (Anmerkung: bereits mit dem „Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes" aus 2009, in dem auch das BSIG novelliert wurde, wurde § 109 TKG dahingehend geändert, dass die BNetzA einen Katalog von Sicherheitsanforderungen im Benehmen mit dem BSI und dem BfDI zu erstellen hat.)
- Unter bestimmten Voraussetzungen müssen TK- und Diensteanbieter Sicherheitsverletzungen der BNetzA melden (§ 109 Abs. 5 TKG – Umsetzung Art. 13a der RL 2009/140/EG (Telekom-Paket). „Erforderlichenfalls" unterrichtet die BNetzA unter anderem das BSI und ENISA über die Sicherheitsverletzungen.
- Die BNetzA muss ein Mal jährlich u.a. dem BSI und ENISA einen zusammenfassenden Bericht über die eingegangenen Mitteilungen zu Sicherheitsverletzungen sowie die ergriffenen Abhilfemaßnahmen vorlegen (§ 109 Abs. 5 TKG - Umsetzung Art. 13a der RL 2009/140/EG).
- Status des Katalogs für Sicherheitsanforderungen
- Bezüglich der Erstellung des Katalogs für Sicherheitsanforderungen fand der letzte Kontakt mit der BNetzA Ende Dezember 2011 statt.
- Bisherige Zusammenarbeit des BSI mit BNetzA und BfDI sehr konstruktiv.
- Nach bisherigen Aussagen der BNetzA ruhte die Bearbeitung des Katalogs bis zum Inkrafttreten der TKG-Novelle. BSI geht davon aus, dass BNetzA zeitnah die Arbeit am Sicherheitskatalog wieder aufnehmen wird.

Bundesministerium des Innern

Diskussionspapier
IT-Schutz Kritischer Infrastrukturen in Deutschland

25. Januar 2012

Der Cyberraum ist von ständig wachsender Bedeutung. Damit Deutschland auf Dauer wettbewerbsfähig bleibt, ist es auf solide und sichere Informationsinfrastrukturen angewiesen. Sie sind ein Standortfaktor mit Zukunft.

An oberster Stelle steht die Sicherung von solchen Organisationen und Einrichtungen, die eine wichtige Bedeutung für das Gemeinwesen haben und deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere weitreichende Folgen für unsere Gesellschaft hätte. Deswegen hat die Bundesregierung mit der Cyber-Sicherheitsstrategie dem Schutz Kritischer Infrastrukturen höchste Priorität gegeben. Betreibern dieser Kritischen Infrastrukturen kommt eine Schlüsselfunktion zu. Nur gemeinsam und in enger Kooperation können wir die Versorgungssicherheit und Wettbewerbsfähigkeit in Deutschland sicherstellen. Hierfür ist die Einhaltung von grundlegenden IT-Schutz-Anforderungen essentiell:

1. **Mehr Transparenz schaffen**
   Viele Kernprozesse sind unmittelbar von Informations- und Kommunikationstechnik (IKT) abhängig.
   Um diese zu schützen, müssen sowohl deren Kritikalität als auch die Abhängigkeiten bekannt sein. Auswirkungen von Störungen oder Ausfällen dieser Kernprozesse auf die Gesellschaft wird ein hoher Stellenwert im organisatorischen Risikomanagement eingeräumt.

2. **Robuste Grundlagen durch ein standardisiertes und überprüfbares Sicherheitsniveau**
   Kritische Infrastrukturen können nur dann ohne nennenswerte Unterbrechungen funktionieren, wenn ihre Kernprozesse und die zugrunde liegenden IT-Prozesse robust ausgestaltet sind.
   Eine umfassende und konsequent wirkungsvolle Umsetzung von Schutzmaßnahmen, die dem jeweiligen Schutzbedarf entsprechen, ist grundlegend. Dazu gehören auch die Festlegung und allgemeine Anwendung von branchenspezifischen und übergreifenden Mindestanforderungen an den IT-Schutz oder entsprechende Standards.
   Für eine nachvollziehbare Überprüfung bedarf es regelmäßiger Sicherheitsaudits.

3. **Kritische Prozesse autonom gestalten**
   Besonders kritische Prozesse bedürfen besonderer Sicherheitsmaßnahmen durch Abschottung.
   Diese Prozesse sind weder mit dem Internet oder öffentlichen Netzen verbunden, noch von über das Internet angebotenen Diensten abhängig.

4. **Produkt- und Dienstleistungssicherheit gewährleisten**
Umfassende IT-Sicherheit lässt sich nur durch Security-by-Design erreichen.
Daher fließen IT-Sicherheitsaspekte von Beginn an in die Planung von IKT-Netzen und –anwendungen sowie bei der Beschaffung von IKT-Produkten mit ein. Wo verfügbar, kommen für besonders sensible Bereiche zertifizierte Produkte bzw. Dienstleistungen zur Anwendung.

5. **Durch Lagefortschreibung und Frühwarnung Gefahren vorbeugen**
Eine umfassende Information aller Akteure über die aktuelle Cyber-Gefährdungslage ist Voraussetzung für die eigene Handlungsfähigkeit und Grundlage für eine abgestimmte, nationale Reaktion.
Mechanismen zur Früherkennung von Gefährdungen und eine Anbindung an die Warn- und Alarmierungsmechanismen (i.d.R. über sogenannte Single Points of Contact, SPOCs) des Umsetzungsplan KRITIS gewährleisten die nationale Handlungsfähigkeit – hierfür sind gegenüber dem BSI „Warn- und Alarmierungskontakte" benannt. Nur so kann sichergestellt werden, dass bei schwerwiegenden Beeinträchtigungen oder Cyber-Angriffen andere betroffene kritische Infrastrukturen und das Lagezentrum des BSI unverzüglich informiert werden.

6. **Mit Übungen auf den Ernstfall vorbereiten**
Regelmäßige Cyber-Sicherheitsübungen und die Teilnahme an größeren, branchenübergreifenden Übungen schaffen Vertrauen in die Strukturen und die gegenseitige Zusammenarbeit in IT-Krisensituationen.

7. **Durch Kooperation an Know-How und Stärke gewinnen**
Der Umsetzungsplan KRITIS hat sich als wirksames Instrument der Zusammenarbeit erwiesen.
Alle Branchen der Kritischen Infrastrukturen schließen sich an den Umsetzungsplan KRITIS an. In Ergänzung dazu etablieren und institutionalisieren Betreiber einen regelmäßigen, brancheninternen Informationsaustausch im Rahmen von Branchenarbeitskreisen zum Thema Cybersicherheit.

Die Maßnahmen werden mess- und nachvollziehbar umgesetzt, sodass der Vorsprung an IT-Schutz im Sektor- und auch internationalen Vergleich sichtbar gemacht werden kann.

Dieses Blatt ersetzt die Seiten 40 - 41

Die Entnahme erfolgte mangels Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss

Ministergespräch IT-Schutz kritischer Infrastrukturen

IKT-Sektor

BMI, Raum 1.071, 23. Mai 2012, 13-15 Uhr

➢ Agenda und Teilnehmerliste	**Fach 1**
➢ Gesprächsführungsvorschlag Begrüßung	**Fach 2**
➢ Gesprächsleitfaden Cybersicherheit aus fachspezifischer Sicht	**Fach 3**
➢ Gesprächsleiterfaden und Unterlagen Cybersicherheitslage	**Fach 4**
➢ Gesprächsleitfaden und Diskussionspapier Anforderungen an IT-Schutz aus Sicht BMI	**Fach 5**
➢ Gesprächsleitfaden Diskussion der Anforderungen	**Fach 6**
➢ Gesprächsleitfaden Zusammenfassung / Ausblick	**Fach 7**
➢ Potentielle Fragen der Wirtschaft (und Antworten)	**Fach 8**
➢ Hintergrundinformationen KRITIS Allgemein	**Fach 9**
➢ Hintergrundinformationen KRITIS im IKT-Sektor	**Fach 10**
➢ Cybersicherheitsstrategie	**Fach 11**

[redacted]

Positionspapier

zum Diskussionspapier "IT-Schutz Kritischer Infrastrukturen in Deutschland" anlässlich des Treffens mit BM Friedrich am 23. Mai 2012

22.05.2012
Seite 1

– Vt-Dublich –

Der B[redacted]edi-[redacted] vertritt mehr als 1.700 Unternehmen, davon über 1.100 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software & IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der B[redacted] setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

[redacted]

[redacted]

Ansprechpartner

[redacted]

Präsident

[redacted]

Hauptgeschäftsführer

[redacted]

Vorbemerkung

B[redacted] begrüßt die von der Bundesregierung im Jahr 2011 veröffentlichte Cybersicherheitsstrategie sowie eine Umsetzung in konkrete Maßnahmen. Wir unterstützten daher nachdrücklich die Aktivitäten zum Schutz der ITK-Infrastrukturen in Deutschland, denn wir verstehen die Sicherheit unserer Prozesse und Systeme als eines der wesentlichen Erfolgskriterien für unser Geschäft. Die B[redacted]-Branche führt daher bereits heute permanent umfangreiche technische und organisatorische Maßnahmen zur Absicherung der Verfügbarkeit und Servicequalität der ITK-Infrastruktur als physikalische und logische Grundlage für den "Cyberraum" durch.

Die deutschen Netzbetreiber haben durch einen proaktiven Umgang mit dem Thema Sicherheit und permanent weiter entwickelte Sicherheitsstandard im internationalen Vergleich eine Spitzenposition erreicht. Aktuell bestehende regulatorischen Anforderungen wie z.B. das Sicherheitskonzept auf Basis TKG, § 109, haben sich bewährt. Darüber hinaus verfolgen die Netzbetreiber schon aus Eigeninteresse einen umfassenden Informations- und Erfahrungsaustausch, um das Know-how über die Funktionsweise der "kritischen Infrastrukturen" und angemessener Schutzmaßnahmen zu teilen und gemeinsam weiterzuentwickeln. Hier hat sich die Arbeit in den Projektgruppen des UP KRITIS unter Federführung des Bundesamtes für Sicherheit in der Informationstechnik ebenfalls bewährt. Durch diesen umfassenden Ansatz wird gewährleistet, dass bei den beteiligten Unternehmen ein branchenweites, angemessenes Sicherheitsniveau besteht, das stetig den neuen Herausforderungen angepasst wird.

Weitere regulatorische Verpflichtungen der Branche bringen nicht notwendigerweise einen Gewinn an Sicherheit, sondern tragen im schlechtesten Fall dazu bei, dass für Unternehmen wesentliche Wettbewerbsnachteile entstehen. Grundlage von regulatorischen Anforderungen der Aufsichtsbehörden sollte daher immer ein Abgleich mit internationalen Standards und Vorgehensweisen sein. Ein von internationalen Entwicklungen entkoppelter, rein deutscher Standard, wirkt daher nicht im Sinne einer Stärkung des Cyberraums. Vor diesem Hinter-

[redacted]

Positionspapier
zum Diskussionspapier "IT-Schutz Kritischer Infrastrukturen in Deutschland"
Seite 2

grund schlägt der B[redacted] vor, die aktuell laufenden, diversen Aktivitäten von Bund, Ländern und Verbänden stärker abzustimmen, um hier eine einheitliche und für alle Beteiligten effiziente Vorgehensweise zu schaffen. Vermieden werden sollte auf jeden Fall eine Zersplitterung der bisherigen Aktivitäten in parallelen und redundanten Maßnahmen verschiedener Akteure.

Die in dem Diskussionspapier aufgeführten Maßnahmen sind nach unserer Sicht prinzipiell geeignet, das Sicherheitsniveau der kritischen Infrastrukturen in Deutschland zu erhöhen In weit überwiegenden Teilen sind diese Forderungen in den Unternehmen der TK-Branche bereits umgesetzt und werden aktiv gelebt. Dies schließt Verbesserungsmöglichkeiten in Einzelpunkten natürlich nicht aus.

Im Einzelnen sehen wir die im Diskussionspapier genannten Maßnahmen im Status der Netzbetreiber wie folgt:

Telefon: IT-Sich / 109 TKG

1. **Mehr Transparenz schaffen**

STATUS: Etabliert, Verbesserungen möglich

- Ein organisatorisches Risiko-Management ist implementiert. Die großen TK- Mitgliedsunternehmen betreiben ein Management-System zur Informationssicherheit (ISMS) sowie ein BCM (Business Continuity Management).
- Die Meldewege gegenüber den Aufsichtsbehörden sind etabliert. Damit entsprechend wir bereits heute den künftigen gesetzlichen Forderungen (§ 109 TKG in der novellierten Fassung).
- Ggf. verbesserungswürdig ist die Transparenz über den Stand von Störungen oder Ausfällen branchenweit - hier sind wir dabei entsprechende Organisationsstrukturen international zu verzahnen. Hierfür sollten die bestehenden Strukturen wie der UP KRITIS genutzt bzw. im Rahmen der „Allianz für Cybersicherheit" als gemeinschaftlichen Ansatz von BSI und B[redacted] erweitert werden.

2. **Robuste Grundlagen durch ein standardisiertes und überprüfbares Sicherheitsniveau**

STATUS: Etabliert

- Die Umsetzung etablierter Normen und Vorgaben (wie z.B. BSI IT-Grundschutz und ISO-IEC 27001) sind aus unserer Sicht aktuell ausreichend.
- Zur Dokumentation des Sicherheitskonzeptes existieren regulatorische Grundlagen.(§109 TKG), nach dessen Maßgabe die verpflichteten Unternehmen regelmäßig aktuelle Sicherheitskonzepte der BNetzA zuleiten. Diese werden dort geprüft und zum Teil bei den Unternehmen vor Ort auditiert.
- Gemäß des in der Norm ISO-IEC 27001 festgeschriebenen "Plan-Do-Check-Act"(PDCA)-Zyklus werden regelmäßig Prüfungen auf die Wirksamkeit und ggf. notwendige Korrekturen der eingeführten Sicherheitsmaßnahmen ausgeführt. Einige der Mitgliedsunternehmen sind nach diesem Standard zertifiziert und werden von externen unabhängigen

hinreichend? alle?

[redacted]

Positionspapier
zum Diskussionspapier "IT-Schutz Kritischer Infrastrukturen in Deutschland"
Seite 3

- Die Unternehmen führen regelmäßig systematische Schutzbedarfsanalysen für wesentliche Systeme / Prozesse durch, aus denen bei Bedarf zusätzliche Sicherheitsmaßnahmen abgeleitet werden.

3. Kritische Prozesse autonom gestalten

STATUS: Etabliert

- Soweit als kritisch eingestufte Prozesse betrieben werden, sind diese bereits heute physisch vom öffentlichen Netz getrennt, so dass unerlaubte Zugriffe von dort nicht möglich sind. Dies gilt insbesondere für Betriebs- und Wartungszugänge kritischer Systeme.
- In wie weit Prozesse kritisch sind, sollte dabei weiterhin von Seiten der Unternehmen definiert und eingeschätzt werden, da nur dort die spezifische Sachkenntnis über Funktion und Ausfallsrisiko vorhanden sind. Eine enge Verzahnung mit den internen Risikomanagementsystemen ist dafür die Grundlage.
- Gemäß des vorbeugenden personellen Sabotageschutzes sind Mitarbeiter in sicherheitsempfindlichen Stellen schon heute besonders sicherheitsüberprüft und zusätzliche organisatorische und technische Schutzmaßnahmen umgesetzt.

4. Produkt- und Dienstleistungssicherheit gewährleisten

STATUS: Etabliert, Verbesserungen möglich

- Generell ist bei den Produkten und Dienstleistungen der Grundsatz „Security-by-design" Basis der Entwicklung, etwa durch entsprechende prozessuale Vorgaben. Gleichwohl ist dieses Vorgehensmodell noch nicht in allen Unternehmen Standard. Verbesserungen sind durch einheitliche Standards für eine sichere Produktentwicklung möglich. Hierbei sollte die öffentliche Hand als Vorbild agieren und auch Sicherheitsaspekte auch auf prozeduraler Ebene einbeziehen.
- Lieferanten werden bezüglich der Sicherheitsvorgaben bewertet und auditiert. Ein wesentliches Bewertungskriterium ist zum Beispiel die internationale Norm ISO-IEC 27001.
- Viele Unternehmen bieten darüber hinaus seit geraumer Zeit Sicherheitspakete für ihre Endkunden an. Auch im Bereich der Geschäftskunden stehen entsprechende Dienstleistungsangebote zur Verfügung. Hier kann der Kunde durch Auswahl entsprechender Optionen in der Regel selbst das Niveau an Verfügbarkeit gemäß seiner individuellen Anforderungen bestimmen.

5. Durch Lagefortschreibung und Frühwarnung Gefahren vorbeugen

STATUS: Etabliert, Verbesserungen notwendig

- Cyber Emergency Response Teams (CERT) sind etabliert und extern vernetzt. Die Zusammenarbeit erfolgt z.B. im Rahmen des deutschen CERT-Verbund (BSI) und des Forums of Incident Response Teams

[redacted]

Positionspapier
zum Diskussionspapier "IT-Schutz Kritischer Infrastrukturen in Deutschland"
Seite 4

(FIRST). Zum Teil wird ein zusätzlicher regelmäßiger bilateraler Austausch mit dem BSI praktiziert

- Über Frühwarnsysteme (Honeypot) werden laufend Erkenntnisse über neue Bedrohungen der IT-Sicherheit gewonnen und auch extern zur Verfügung gestellt.
- SPoCs sind benannt und Meldeprozesse gegenüber den. Aufsichtsbehörden etabliert
- Das von B[redacted] und BSI angestrebte zentrale Lagebild im Rahmen der „Allianz für Cybersicherheit" halten wir für besonders erfolgversprechend, da hier durch eine zentrale Kopplung der Wirtschaft mit dem bestehenden Cyberabwehr-Zentrum (NCAZ) gewährleistet werden könnte.

6. Mit Übungen auf den Ernstfall vorbereiten

STATUS: Etabliert

- B[redacted] Unternehmen nehmen regelmäßig an Übungen teil (z B. LÜKEX 2011 – Schwerpunkt IT-Krise, mehrmals jährlich, übergreifende Kommunikationsübungen mit Hilfe des TK-SPoC) und sind darüber hinaus zur Diskussionen konkreter Szenarien offen.
- Die Branche hat sehr gute Erfahrungen mit gemeinsamen Übungen gemacht. Dies unterstreicht die Relevanz und Notwendigkeit für eine Zusammenarbeit zwischen Wirtschaft und Sicherheitsbehörden.

7. Durch Kooperationen an Know-how und Stärke gewinnen

STATUS: Etabliert, organisatorische Verbesserungen möglich

- Es gibt nach unserer Einschätzung für den Sektor Telekommunikation eine ausreichende Anzahl von Arbeitskreisen und weiteren Organisationen, die eine Kooperation sicherstellen. Eine weitere Verbesserung wäre aber durch eine thematische Synchronisierung der verschiedenen Aktivitäten im Umfeld von Bund, Ländern und Verbänden erreichbar
- Für einen branchenübergreifender Informations- und Erfahrungsaustausch unterstützen die B[redacted] Mitglieder die „Allianz für Cybersicherheit" als gemeinsame Initiative von BSI und B[redacted]. Weiterhin könnte ergänzend eine jährliche KRITIS-Konferenz sinnvoll sein.
- Das Thema Schutz kritischer Infrastrukturen steht auf der politischen Agenda vieler Staaten. Diese Ansätze miteinander auf politischer Ebene zu verzahnen, ist besonders wichtig.

– tgl. 2500 [illegible]
– 5-10 [illegible]

Bundesministerium
des Innern

– Staat / Wirtschaft / User

Hage: – [illegible] -> 80% [illegible]

– StB / Wi / Kultur / [illegible]

1) §109 TKG: Transparenz / Meldepflicht — Dürig[illegible] — Dr.

2) Standards (?) -> wer leistet ?

3) ~~[illegible]~~ UP Kritis: seit 2007

Pileck:

SPD

Kopf (Telekom): Standards! — Prüfung f. [illegible] -> Empfehlung /

Dirks: Dynamik der [illegible] ->

Kelber (SPD): Verbände / Standards — 95% aller Standards [illegible]?

einheitliche Konzepte?

- Definition of cyber attack
- Single-point-of-attack

360/12
49

BMI

IT3-606 000-9/31#1

Refl: MinR Dr. Dürig
Ref: RRn Otte

Berlin, den 16. Mai 2012
Hausruf: 1374/2808

Frau Stn Rogall-Grothe 21/5

über

Herrn IT-D
Herrn SV IT-D } SB 16/5.

Abdruck:
Referat Z 9

Betr.: IT-Schutz kritischer Infrastrukturen; Ministergespräche mit Wirtschaftsvertretern

Bezug: Vorlage vom 13. April 2012; Az. IT3-606 000-9/31#1

Anlage: - 3 -

1. Votum

Billigung der Einladung des BMELV, des BMG und des BMU zu dem Ministergespräch mit den Sektoren Ernährung und Wasser und Zeichnung des anliegenden Einladungsschreibens.

2. Sachverhalt/Stellungnahme

Wie von Herrn Minister gebilligt (Ministervorlage vom 30. Januar 2011; Az. IT3-606 000-9/31#1) sind sechs Gespräche mit jeweils 10 bis 15 Wirtschaftsvertretern zum Thema IT-Schutz kritischer Infrastrukturen für Mai bis August geplant. Die zuständigen Staatssekretäre der Ressorts hatten

Anlage 1

Briefkopf Stn Rogall-Grothe

Berlin, den 21. Mai 2012

Herrn Staatssekretär
Dr. Robert Kloos
Bundesministerium für Ernährung,
Landwirtschaft und Verbraucherschutz
Postfach 14 02 70
53107 Bonn

Herrn Staatssekretär
Thomas Ilka
Bundesministerium für Gesundheit
Rochusstraße 1
53107 Bonn

Herrn Staatssekretär
Jürgen Becker
Bundesministerium für Umwelt,
Naturschutz und Reaktorsicherheit
11055 Berlin

Sehr geehrte Herren Kollegen,

mit Schreiben vom 27. März 2012 hatte ich Sie darüber informiert, dass Herr Bundesminister Dr. Hans-Peter Friedrich in Gesprächen mit der Wirtschaft die IT-Sicherheit kritischer Infrastrukturen adressieren und voranbringen möchte.

Das Gespräch mit den Vorständen aus den Sektoren Ernährung und Wasser wird am 26. Juli 2012 von 15:00 bis 17:00 Uhr im Bundesministerium des Innern statt-

finden. In der Anlage übermittle ich Ihnen das Einladungsschreiben von Herrn Minister und den Verteiler.

Dr. Friedrich

Zu diesem Gespräch möchte ich Sie herzlich einladen. Wir würden uns freuen, wenn Sie den Prozess aktiv unterstützen und im Anschluss an die Begrüßung durch Herrn Bundesminister Dr. Friedrich einleitende Worte aus Ihrer Sicht an die Teilnehmer richten würden.

Mit freundlichen Grüßen

z.U.
N.d.Fr. Stn RG

Anlage 2

Versand
gemäß anliegendem Verteiler

DATUM Berlin, den 21. Mai 2012

Sehr geehrte Damen und Herren,

die Bundesregierung hat im Februar 2011 die nationale Cybersicherheitsstrategie verabschiedet. Damit wurde der erste Schritt zur Adressierung der jüngsten Entwicklungen bezüglich der Abhängigkeiten vom und der Bedrohungslage im Cyberspace getan.

Als Betreiber Kritischer Infrastrukturen bzw. diese vertretende Verbände kommt Ihnen eine besonders verantwortungsvolle Aufgabe bei der Mitwirkung in der Cybersicherheit zu. Die von Ihrer Organisation bereitgestellten Dienste sind für das gesellschaftliche, wirtschaftliche und auch staatliche Handeln unverzichtbar. Die Durchdringung von Informations- und auch Kommunikationstechnologien ist in den letzten Jahren kontinuierlich vorangeschritten und hat alle Branchen der Kritischen Infrastrukturen erreicht.

Seit 2007 arbeitet die Bundesregierung im Umsetzungsplan KRITIS mit Betreibern Kritischer Infrastrukturen zusammen, um die notwendige Vorsorge zu erfüllen – den beteiligten Organisationen danke ich für Ihr Engagement.

Auch mit der Ende November 2011 durchgeführten LÜKEX als erste nationale IT-Übung konnte gezeigt werden, dass die gemeinsamen Anstrengungen zur Verbesserung des IT-Schutzes Kritischer Infrastrukturen weiter optimiert werden sollten.

Als Bundesminister des Innern habe ich eine Pflicht zur Sicherheitsvorsorge in Deutschland. Die Aufrechterhaltung der von Ihnen betriebenen Kritischen Infrastrukturen ist dabei ein integraler Bestandteil. Die Entwicklungen machen es unverzichtbar, dass sich alle Branchen explizit und umfassend mit dem IT-Schutz bei Kritischen Infrastrukturen auseinandersetzen, um ein umfassendes Mindestniveau in Deutschland zu erreichen.

Als Anlage übersende ich Ihnen ein Arbeitspapier mit Anforderungen an den IT-Schutz Kritischer Infrastrukturen, welche zu diesem Zweck von jeder Branche erfüllt sein sollten. Ich wäre Ihnen dankbar, wenn Sie einen Umsetzungsstand innerhalb der Branche eruieren und bei Bedarf Nachbesserungen initiieren würden.

Für den 26. Juli 2012 möchte ich Sie in das Bundesministerium des Innern einladen, um die Ausrichtung des Papiers und die Resultate aus den branchenspezifischen Aufarbeitungen in der Zeit von 15:00 bis 17:00 Uhr zu diskutieren. Für eine kurze Bestätigung Ihrer Teilnahme, spätestens bis Mittwoch, den 11. Juli 2012, danke ich Ihnen. Für Rückfragen steht Ihnen in der Zwischenzeit auch das zuständige Referat im Bundesministerium des Innern (it3@bmi.bund.de, Tel.: 030 / 18 681 - 1642) zur Verfügung.

Mit freundlichen Grüßen

Anlage 3

[redacted]
Technischer Geschäftsführer
Z[redacted]

[redacted]
Vorsitzender des Vorstandes
G[redacted]AG

[redacted]
Vorsitzender des Vorstandes
B[redacted]

[redacted]
Sprecher der Geschäftsführung
H[redacted]

[redacted]
Vorsitzender des Vorstandes
E[redacted]

[redacted]er
Vorsitzende der Hauptgeschäftsführung
B[redacted]

[redacted]
Vorsitzender des Vorstandes
E[redacted]

[redacted]s
Vorsitzender des Vorstandes
R[redacted]

[redacted]
Komplementär der
S[redacted]KG
S[redacted]GmbH

[redacted]
Vorsitzender des Vorstandes
M[redacted]AG

[redacted]
U[redacted]

[redacted]
Vorsitzender des Vorstandes
N[redacted]

[redacted]
Hauptgeschäftsführer
H[redacted]e. V.

[redacted]n
Hauptgeschäftsführer
Bu[redacted]e. V.

[redacted]

Hauptgeschäftsführer
B[redacted]

[redacted]

Bundesministerium
des Innern

Cornelia Rogall-Grothe
Staatssekretärin
Beauftragte der Bundesregierung
für Informationstechnik

Bundesministerium des Innern, 11014 Berlin

Herrn Staatssekretär
Dr. Robert Kloos
Bundesministerium für Ernährung,
Landwirtschaft und Verbraucherschutz
Postfach 14 02 70
53107 Bonn

Herrn Staatssekretär
Thomas Ilka
Bundesministerium für Gesundheit
Rochusstraße 1
53107 Bonn

Herrn Staatssekretär
Jürgen Becker
Bundesministerium für Umwelt,
Naturschutz und Reaktorsicherheit
11055 Berlin

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin

TEL +49 (0)30 18 681-1109
FAX +49 (0)30 18 681-1135
E-MAIL StRG@bmi.bund.de

DATUM 23. Mai 2012
AKTENZEICHEN IT 3 – 606 000-9/31#1

ab am 25.5.

1.) [illegible] Name ZNV
2.) [illegible]
[illegible] 24.5.

IT 3

Sehr geehrte Herren Kollegen,

mit Schreiben vom 27. März 2012 hatte ich Sie darüber informiert, dass Herr Bundesminister Dr. Hans-Peter Friedrich in Gesprächen mit der Wirtschaft die IT-Sicherheit kritischer Infrastrukturen adressieren und voranbringen möchte.

Das Gespräch mit den Vorständen aus den Sektoren Ernährung und Wasser wird am 26. Juli 2012 von 15:00 bis 17:00 Uhr im Bundesministerium des Innern stattfinden. In der Anlage übermittle ich Ihnen das Einladungsschreiben von Herrn Minister Dr. Friedrich und den Verteiler.

Zu diesem Gespräch möchte ich Sie herzlich einladen. Wir würden uns freuen, wenn Sie den Prozess aktiv unterstützen und im Anschluss an die Begrüßung durch Herrn Bundesminister Dr. Friedrich einleitende Worte aus Ihrer Sicht an die Teilnehmer richten würden.

Mit freundlichen Grüßen

Rogall-Grothe

Sie bereits über die Gespräche informiert (Schreiben vom 27. März) und zu den ersten vier Terminen eingeladen (zuletzt Schreiben vom 25. April).

Das Ministerbüro plant für den 21. Mai 2012 die Versendung des Schreibens für den gemeinsamen Termin mit den Sektoren Ernährung und Wasser am 26. Juli 2012.
Zu diesem Termin sollte das BMELV aufgrund der Zuständigkeit für den Sektor Ernährung eingeladen werden.

Für den Sektor Wasser liegt die Zuständigkeit primär bei den Ländern und Kommunen. Auf Bundesebene ist das BMU für die Grundwasserqualität zuständig. Für die Trinkwasserqualität liegt die Zuständigkeit beim BMG zusammen mit dem Umweltbundesamt, über das das BMG diesbezüglich die Fachaufsicht hat. Beide Ressorts haben in den bisherigen Besprechungen jeweils auf die Zuständigkeit des anderen Ressorts verwiesen und sollten daher gemeinsam eingeladen werden.

Dr. Dürig

Otte

376/58
58

Referat IT 3
IT 3 - 606 000-2/28#1
Refl: MR Dr. Dürig
Sb: AR Spatschke

Berlin, den 22. Mai 2012
Hausruf: 1374/2045

Frau Stn Rogall-Grothe

Über

Herrn IT-Direktor
Herrn SV IT-Direktor

Betr.: 3. Sitzung des Cyber-SR am 31.05.2012
Anlage: - 1 -
- 1 Mappe -

1. Votum

Kenntnisnahme und Billigung der sitzungsvorbereitenden Unterlagen für die 3. Sitzung des Cyber-SR am 31. Mai 2012.

2. Sachverhalt

Die ursprünglich für den 14. Februar anberaumte und aus terminlichen Gründen abgesagte 3. Sitzung des Nationalen Cyber-Sicherheitsrates (Cyber-SR) findet am 31. Mai von 11:00 bis 13.30 Uhr statt (Der zwischenzeitlich kommunizierte Termin am 3. Mai wurde wegen terminlicher Schwierigkeiten des BMWi abgesagt).

Der **TOP 3** der Tagesordnung (**Vortrag P-BSI**) sollte direkt im Anschluss an **TOP 1** (**Begrüßung**) erfolgen (TOP ist aufgrund der urspr. intendierten Zweiteilung der Sitzung noch nach Cyber-Außenpolitik aufgeführt).
BSI hat gem. Ziffer 4 der Nationalen Cyber-Sicherheitsstrategie einen **Statusbericht des Cyber-AZ** zur Unterrichtung des Cyber-SR vorgelegt (siehe Mappe). Der Bericht beschränkt sich auf die Schilderung besonderer Angriffe, grundsätzliche Schlussfolgerungen im Sinne einer strategischen Befassung des politischen Gremiums Cyber-SR fehlen jedoch. P-BSI bittet gleichwohl um eine restriktive Weitergabe des Berichts nur innerhalb der Behörden. Der die Schlussfolgerungen des Berichts aufgreifende Vortrag des P-BSI hingegen soll den Mitgliedern des Cyber-SR zur Verfügung gestellt werden können.

Entsprechend der Entscheidung von Herrn Minister in der als Anlage 1 beigefügter Vorlage („*IT-Sicherheitsgesetzgebung als eine Option im Rahmen des Cyber-SR ansprechen*") wurde ein entsprechender Sz für **TOP 6** (**Sonstiges**) vorbereitet.
Ferner böte sich unter diesem TOP eine kurze Information der Mitglieder des Cyber-SR über den Aufbau der CERT-Strukturen in den einzelnen Bundesländern an. Die „Kooperationsgruppe Informationssicherheit" des IT-Planungsrates ist mit dieser Thematik befasst. U.U. wird dieser Punkt seitens der Ländervertreter BW oder HE ohnehin aufgegriffen bzw. in die IMK-Arbeitsgruppe „Cybersicherheit" getragen.

3. Stellungnahme

Es wird vorgeschlagen, den Statusbericht des Cyber-AZ für den Cyber-SR allen Mitgliedern des Cyber-SR im Nachgang der Sitzung zusammen mit dem Protokoll zur Verfügung zu stellen. Einerseits ist dies ohnehin in Ziffer 4 der Cyber-Sicherheitsstrategie so vorgesehen, andererseits könnte man somit auch den vermehrt auftretenden Forderungen aus dem parlamentarischen Raum entgegentreten (Übersendung des Berichts im Nachgang der Sitzung des Cyber-SR an Innenausschuss des BT)

Der Statusbericht des Cyber-AZ stellt im Übrigen fest, dass die Hauptbetroffenen der durch das Cyber-AZ von April 2011 bis März 2012 registrierten ca. 500 IT-Sicherheitsvorfälle Privatanwender waren.
Vor diesem Hintergrund wird angeregt, den Mitgliedern des Cyber-SR unter **TOP 6 (Sonstiges)** vorzuschlagen, als nächsten Aspekt des Arbeitsschwerpunktepapiers des Cyber-SR den Punkt 2 „*Koordinierung von Maßnahmen zur Verbesserung der Sicherheit von IT-Systemen in Deutschland*" im Rahmen der nächsten Sitzung vertieft zu erörtern.
Herr Minister wird im Nachgang zur Sitzung unaufgefordert unterrichtet werden.

Dr. Dürig

Spatschke

Fächerübersicht

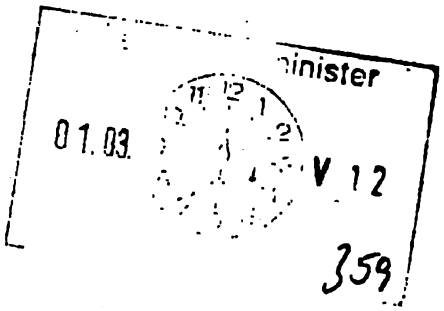
Anlage 14/12

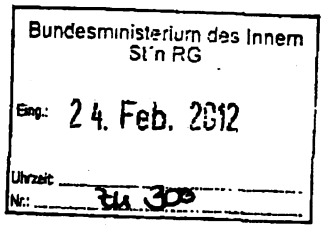
Referat IT 3
IT 3 - 606 000-2/28#1

Berlin, den 23. Februar 2012
Hausruf: 1374/2045

Refl: MR Dr. Dürig
Sb: AR Spatschke

Herrn Minister





über

Frau Staatssekretärin Rogall-Grothe
Herrn IT-Direktor
Herrn SV IT-Direktor

Betr.: Nationaler Cyber-Sicherheitsrat (Cyber-SR)

Anlage: - 4 -

1. Votum

Kenntnisnahme der Ergebnisse der ersten beiden Sitzungen und Billigung der strategischen Zielsetzung für die nächste Sitzung im Mai 2012.

2. Sachverhalt

Die vor einem Jahr am 23. Februar 2011 mittels Kabinettbeschluss verabschiedete Cyber-Sicherheitsstrategie der Bundesregierung beinhaltet als Kernelemente den Aufbau eines Nationalen Cyber-Abwehrzentrums (Cyber-AZ), den verstärkten IT-Schutz Kritischer Infrastrukturen und die Implementierung eines Nationalen Cyber-Sicherheitsrates (Cyber-SR).
Mitglieder des Cyber-SR sind das BK und die Staatssekretäre von BMI, BMF, BMJ, BMWi, BMBF, AA, BMVg sowie zwei Ländervertreter (HE und

bislang BE). Insgesamt vier Wirtschaftsvertreter fungieren als sogenannte assoziierte Mitglieder (B[redacted] D[redacted], B[redacted], Übertragungsnetzbetreiber A[redacted]).

In seiner konstituierenden Sitzung am 3. Mai 2011 hat sich der Cyber-SR insbesondere über ein Arbeitsprogramm bis zum Ende der Legislaturperiode verständigt (siehe Anlage 1 und Protokoll in Anlage 2).
In der zweiten Sitzung des Cyber-SR am 18. Oktober 2011 – an der erstmals auch die assoziierten Wirtschaftsvertreter teilgenommen haben – wurden zwei Schwerpunkte des Arbeitsprogramms vertieft erörtert: zum einen der IT-Schutz Kritischer Infrastrukturen und zum anderen das Thema Cyber-Außenpolitik (vgl. Protokoll in Anlage 3).
Im Ergebnis der Erörterungen zu KRITIS wurde beschlossen, dass unter Koordinierung von BMI/BSI die zuständigen Bundesministerien und -behörden jede einzelne KRITIS-Branche auf deren Umsetzungsstand bezüglich der IT-Sicherheit überprüfen und branchenbezogene Handlungsnotwendigkeiten erarbeiten. Das BSI unterstützt branchenübergreifend und liefert die notwendigen Kriterien zur Bewertung.
Bei der Thematik Cyber-Außenpolitik ist AA – noch als Auftrag der 1. Sitzung - in der Verantwortung, ein mit den betroffenen Ressorts abgestimmtes Grundsatzpapier zu Zielen und Strategien der internationalen Zusammenarbeit im Bereich der Cyber-Sicherheit vorzulegen.

3. Stellungnahme

In der nächsten Sitzung des Cyber-SR (Vorschlag Büro StRG: **3. Mai 2012** von **11:00-13:30h** im Besucherzentrum) sollen wiederum die Themen IT-Schutz KRITIS sowie Cyber-Außenpolitik aufgerufen werden.
Neben der **Sachstandserörterung der Arbeitsaufträge** aus der 2. Sitzung des Cyber-SR sollen die Ressorts und die assoziierten Wirtschaftsvertreter über die sog. **„Ministergespräche" mit Branchenvertretern** informiert werden. Ob hingegen eine Unterrichtung der Ressorts über die geplante Normierung der IT-Sicherheitsanforderungen für Kritische Infrastrukturen (**„IT-Sicherheitsgesetz"**) bereits in dieser Sitzung erfolgen soll, ist zeitnah zum Termin zu entscheiden.

scheint mir möglich; allerdings würde ich
Thema als eine Option in die Sitzung vorgesehen, aber
nicht weiter!

Darüber hinaus ist vorgesehen, die Mitglieder des Cyber-SR über den Themenkomplex **Trusted Computing** sowie die damit einhergehenden Fragestellungen zu informieren und eine abgestimmte Position herbeizuführen.
Weitere Einzelheiten zur strategischen Themenplanung für die 3. Sitzung des Cyber-SR können dem in Anlage 4 beigefügten Rücklauf der StRG-Unterrichtungsvorlage entnommen werden.

Referat IT 3 wird Sie über die Ergebnisse der 3. Sitzung des Cyber-SR unterrichten.

Dr. Dürig

Spatschke

Bundesministerium
des Innern

Cornelia Rogall-Grothe
Staatssekretärin
Beauftragte der Bundesregierung
für Informationstechnik

Bundesministerium des Innern, 11014 Berlin

An die
Mitglieder des
Nationalen Cyber-Sicherheitsrates

gemäß Verteiler

Per E-Mail

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
TEL +49 (0)30 18 681-1109
FAX +49 (0)30 18 681-1135
E-MAIL StRG@bmi.bund.de

DATUM 23. März 2012
AKTENZEICHEN IT 3 – 606 000-2/28#1

Sehr geehrte Damen und Herren,

nachdem die letzte Sitzung des Nationalen Cyber-Sicherheitsrates (Cyber-SR) am 18. Oktober 2011 stattgefunden hatte, möchte ich Sie für den 31. Mai 2012 zur 3. Sitzung des Cyber-SR einladen.
Die Sitzung findet statt im

Bundesministerium des Innern
Alt-Moabit 101D, 10559 Berlin
von 11.00 – 13.30 Uhr im Raum 1.071.

Für die Tagesordnung habe ich folgende Punkte vorgesehen:

TOP 1: Begrüßung
TOP 2: Cyber-Außenpolitik
TOP 3: Vortrag P – BSI
TOP 4: IT-Schutz Kritischer Infrastrukturen
TOP 5: Trusted Computing
TOP 6: Sonstiges

Bitte bestätigen Sie Ihre Teilnahme bis zum 20. April 2012 gegenüber Herrn Spatschke (Norman.Spatschke@bmi.bund.de).

Mit freundlichen Grüßen

Rogall-Grothe

außenwirtsch. Exp. – Austral. Bericht
VN Gruppe Reg Exp. Sommer Bericht
G8 gescheitert

Weltfunkkonferenz (Int. Telekomm.
BMWi
Bilaterale Kontakte
Europa / Malmström / Kroes / Ashton
Sept. AA 2. Konf. zu Menschen R in Internet

europ. Router

russ. Vorschlag subversiv

Referat IT3
AR Spatschke

24.5.2012

[redacted]

- Begrüßung der Mitglieder und der assoziierten Wirtschaftsvertreter
- Ggf. kurzen bedauernden Hinweis auf zweimal verschobene Sitzung geben (14. Februar aus terminlichen Gründen abgesagt, 3. Mai wegen Task-Force IT-Sicherheit des BMWi)
- Bedeutung des Nationalen Cybersicherheitsrats als politisch-strategisches Gremium in Anbetracht der stetig zunehmenden Bedeutung des Themas „Cyber" herausstellen; Cyber-SR ein Kernelement der Nytionalen Cyber-Sicherheitsstrategie der BuReg.
- (Urspr. TOP 3 (Vortrag P-BSI) wird vorgezogen)
- Sonstige Hinweise/Wünsche zur Tagesordnung erfragen.
- Nächster Cyber-SR möglichst in der KW 42 oder 43 (IT-Gipfel bereits am 13.11.)
  (ab 15.10.)

3 T. / Jahr

Loose, Katrin

Von: Spatschke, Norman
Gesendet: Freitag, 25. Mai 2012 17:56
An: StRogall-Grothe_
Cc: ITD_; SVITD_; Dürig, Markus, Dr.; Engel, Simone
Betreff: Informationspunkte IT 3 nach heutiger R. bei Frau StnRG

Lieber Hanebeck,
nach heutiger R. bei Frau Rogall sollte IT 3 folgenden Punkten nachgehen:

* In Bezug auf KRITIS-TOP Übersendung Vermerk Gesetzgebung USA → bereits erledigt

liegt in Fach 6

* Formelle Benennung des BW-Vertreters Dr. Zinell als Ländervertreter im Cyber-SR → Anruf in BW ergab, dass dieser Punkt für TO der CdS am 14.6. angemeldet worden ist. Dr. Zinell ist also zum Zeitpunkt der Sitzung „nur" vorläufiger Ländervertreter.
* TN B[redacted] → Für E[redacted] wird „aller Voraussicht" nach Herr VP [redacted] teilnehmen (übrigens auch Mitglied in AG 4)
* TN HE → Herr Viktor Jurk ist amtierender Leiter der Abteilung VII (E-Government und Verwaltungsinformatik) des Hessischen Innenministeriums. Er vertritt Herrn St Koch, der aufgrund der Anwesenheitspflicht bei der Plenarsitzung im Hessischen Landtag und der Teilnahme von Herrn Minister Rhein an der zeitgleich stattfindenden Innenministerkonferenz verhindert ist.
* Cyber-SR im BT-Innenausschuss → Cyber-SR stand auf TO des IA am 25.5.2011. Wie vorhin ausgeführt, wurde im Rahmen der IA-Sitzung jährliche Berichterstattung an IA angeregt (siehe Kurzbericht über Sitzung und Bericht über Arbeit des Cyber- SR in Anlage).

↳ Dem wollte IT-D nach dem J.F. heute auf ITS zugehen.

In Bezug auf Ihr avisiertes Telefonat mit Frau Feyerbacher zum Vortrag des P-BSI: Sie rief vorhin bei mir an und fragte zur beabsichtigten Übersendung des Berichts des Cyber-AZ an Mitglieder des Cyber-SR. Ich habe sie darüber informiert, dass Fr. Rogall entschieden hat, den Bericht dem Protokoll beizufügen. Er wird nicht ausliegen und auch nicht vorher übersandt. BSI wird Bericht bei Patras glätten und nach der Sitzung neue Fassung übersenden.
Ich habe zudem erwähnt, dass Sie sich bei ihr bzgl. des Vortrags von P-BSI melden wollen und dieser „strategischer" werden soll.

↳ Mit Frau Feyerbacher habe ich telefoniert und die Anlagen / Fotten aus der Leitungsrunde mit IT 3 weitergegeben. Sie wird am kommenden Dienstag entsprechend mit dem Berg sprechen

a.d. HH 25/5

WG: Bericht 17(4)262
:r 41. Sitzung - Bericht - Art

Beste Grüße+Schöne Pfingsten,
N.Spatschke

Loose, Katrin

Von: Dürig, Markus, Dr.
Gesendet: Donnerstag, 26. Mai 2011 15:52
An: Knaack, Tillmann; KabParl_; Müller, Margarete
Cc: ITD_; Spatschke, Norman; Kutzschbach, Gregor, Dr.
Betreff: WG: Bericht über 41. Sitzung des Innenausschusses am 25.5.

KabParl

über
Hrn. IT-Direktor gez. iV Dü 26/05
Hrn. SV-IT –Direktor gez. iV Dü 26/05
Hrn. RL IT 3 gez. Dü 25/5

Bericht über Verlauf und Ergebnisse der Erörterungen zu TOP 17 der 41. Sitzung des Innenausschusses am 25. Mai 2011

MdB Korte und MdB Jelpke (Die LINKE) stellten - entgegen der TO - auch Fragen zum Nationalen Cyber-Abwehrzentrum (Cyber-AZ), beispielsweise zur Einbeziehung der beteiligten Behörden (Stand Kooperationsvereinbarungen) und bezüglich militärischer Aufgaben des Cyber-AZ, insbesondere unter Bezugnahme auf die Erwähnung der NATO in der Cyber-Sicherheitsstrategie der BuReg. Darüber hinaus war von Interesse, wieviele Lagebilder das Cyber-AZ bereits für den Cyber-SR erstellt habe.
MdB von Notz (Grüne) warf die Frage des rechtsstaatlichen Trennungsgebots hinsichtlich der im Cyber-AZ tätigen Behörden auf. Zudem fragte er nach dem Kriterien der Einbeziehung assoziierter Wirtschaftsvertreter in den Cyber-SR. Sollte geplant sein, private Unternehmen einzubeziehen, würde sich die Frage nach Wettbewerbsvorteilen stellen, sollten vertrauliche Informationen ausgetauscht werden.
MdB Lühmann (SPD) fragte nach der parlamentarischen Kontrolle des Cyber-SR und bat in diesem Zusammenhang um Beschlussfassung, wonach das BMI dem Innenausschuss einmal jährlich über die Tätigkeit des Gremiums berichten solle. Dem wurde entsprochen.

PStS antwortete auf der Grundlage der durch IT 3 erstellten Vorbereitungsunterlagen und des im Vorfeld übersandten schriftlichen Berichts zur Tätigkeit des Cyber-SR. MinR Dr. Dürig ergänzte zum Cyber-SR und Cyber-AZ wie folgt: Das Cyber-AZ habe seit dem 1. 4. mit den Kernbehörden BSI, BfV und BBK seine Tätigkeit aufgenommen. Aktuell würden Kooperationsvereinbarungen mit den weiteren zu beteiligenden Behörden BND, BKA, BPOL, ZKA und Bundeswehr geschlossen. Im Übrigen unterliege das Cyber-AZ selbstverständlich dem rechtsstaatlichen Trennungsgebot und nehme keine militärischen Aufgaben wahr. Aufgabe des Cyber-AZ sei vielmehr der Informationsaustausch aller Beteiligten zu technischen Angriffsszenarien und möglichen Ausnutzungsvarianten.
Die Einbindung der Wirtschaft im Cyber-SR sei in der Sitzung am 3.5. besprochen aber noch nicht abschließend beschlossen worden. Es könne davon ausgegangen werden, dass nicht Vertreter einzelner Unternehmen sondern eher Verbandsvertreter als assoziierte Mitglieder eingebunden werden würden.
Bezüglich des Cyber-AZ sei die Einbindung der KRITIS-Unternehmen über das BSI und den UP-KRITIS sichergestellt. Darüber hinaus werde aktuell die Einbindung weiterer Unternehmen erörtert.

Freundliche Grüße
Im Auftrag
Norman Spatschke

Bundesministerium des Innern
IT 3 - IT-Sicherheit
Telefon: (030)18 681 2045
PC-Fax: (030)18 681 59352
mailto:Norman.Spatschke@bmi.bund.de

Bundesministerium
des Innern

POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

An den
Sekretär des 4. Ausschusses
des Deutschen Bundestages (Innenausschuss)
Herrn Ministerialrat Dr. Heynckes
Platz der Republik 1
11011 Berlin

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)262

Kabinett- und Parlamentsreferat
HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
POSTANSCHRIFT 11014 Berlin

TEL +49 (0)30 18 681 - 1069
FAX +49 (0)30 18 681 - 1019
E-MAIL KabParl@bmi.bund.de
INTERNET www.bmi.bund.de

DATUM Berlin, 23. Mai 2011

BETREFF **TOP 17 der TO der 41. Sitzung des Innenausschusses des Deutschen Bundestages am 25. Mai 2011**
Antrag vom 3. Mai 2011 der Fraktion DIE LINKE. für einen schriftlichen Bericht der Bundesregierung zur Arbeit des Nationalen Cyber-Sicherheitsrates

ANLAGEN - 1 -

Sehr geehrter Herr Dr. Heynckes,

anbei übersende ich Ihnen einen Bericht zur Arbeit des Nationalen Cyber-Sicherheitsrates mit der Bitte um Weiterleitung an die Mitglieder des Innenausschusses.

Mit freundlichen Grüßen
Im Auftrag

Dr. Klos

Bundesministerium
des Innern

Bericht für den Innenausschuss des Deutschen Bundestages

TOP 17 der TO der 41. Sitzung des Innenausschusses des Deutschen Bundestages am 25. Mai 2011

Gegenstand

Mit Antrag vom 3. Mai 2011 bittet die Fraktion DIE LINKE. darum, einen schriftlichen Bericht der Bundesregierung zur Arbeit des Nationalen Cyber-Sicherheitsrates (Cyber-SR) vorzulegen. Insbesondere soll darin im Hinblick auf die konstituierende Sitzung des Cyber-SR am 3. Mai 2011 auf die Teilnehmer, die Arbeitsschwerpunkte und konkrete Arbeitsplanung des Gremiums eingegangen werden. Zudem sei Liste der Kooperationspartner, einschließlich der Kooperationsvereinbarungen, die Darstellung der Entscheidungsabläufe im Cyber-SR sowie Fragen der politischen Kontrolle von Interesse. Zur Frage der Sicherheitsaspekte, die die Einbeziehung der Bundeswehr zur Folge gehabt hätten, sollen ebenso berücksichtigt werden wie die Kriterien und Maßstäbe, die zur Übertragung der Federführung im Cyber-SR an das BSI geführt hätten.

Sachstand

Am 23. Februar 2011 wurde die Cyber-Sicherheitsstrategie für Deutschland mittels Kabinettbeschluss implementiert. Die sichtbaren Elemente dieser Strategie sind die Etablierung eines Nationalen Cyber-Abwehrzentrums (Cyber-AZ) und die Einberufung eines Nationalen Cyber-Sicherheitsrates.

Der Cyber-SR wird auf Staatssekretärsebene unter dem Vorsitz der Beauftragten für Informationstechnologie, Frau Staatssekretärin Rogall-Grothe, dreimal jährlich und darüber hinaus anlassbezogen tagen. Der Cyber-SR trägt auf einer politisch-strategischen Ebene zur besseren Vernetzung und Koordination von Strukturen und bereits bestehenden Ansätzen im Bereich der Cyber-Sicherheit bei. Dabei werden bedeutsame Themenfelder politisch zusammengeführt und zukunftsorientiert beraten. Die Ergebnisse der Diskussionen des Cyber-SR haben empfehlenden Charakter.

Bundesministerium
des Innern

Am Dienstag, dem 3. Mai 2011 hat die konstituierende Sitzung des Cyber-SR stattgefunden. Entsprechend der Nummer 5 der Cyber-Sicherheitsstrategie haben Vertreter des BMI, Bundeskanzleramts sowie der Ressorts Auswärtiges Amt, Bundesministerium der Verteidigung, Bundesministerium für Wirtschaft und Technologie, Bundesministerium der Justiz, Bundesministerium der Finanzen und Bundesministerium für Bildung und Forschung teilgenommen. Darüber hinaus haben die Ländervertreter aus Berlin und Hessen teilgenommen. Ihre Benennung erfolgte mittels Umlaufbeschluss der Chefinnen und Chefs der Staats- und Senatskanzleien (CdS). Der Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI) hat als Gast ebenfalls teilgenommen.

Im Rahmen der konstituierenden Sitzung des Cyber-SR wurde u.a. auch über die Einbeziehung assoziierter Wirtschaftsvertreter beraten. Eine abschließende Festlegung ist noch nicht erfolgt.

Die kommende Sitzung des Cyber-SR soll Ende des Jahres 2011 stattfinden. Es wurde festgelegt, dass in diesem Rahmen die Themen „Schutz kritischer Infrastrukturen gegen IT-Vorfälle" und „Internationale Zusammenarbeit zur Cyber-Sicherheit" schwerpunktmäßig zu beraten sind.

Die im Antrag zur Aufsetzung dieses Tagesordnungspunktes erwähnte Liste der Kooperationspartner und Kooperationsvereinbarungen, die Fragestellungen hinsichtlich der Einbeziehung der Bundeswehr und der Federführung des BSI im Cyber-SR spielen im Kontext des Nationalen Cyber-Sicherheitsrat keine Rolle. Insoweit sind diesbezügliche Ausführungen weder möglich noch geboten. Weder die Bundeswehr noch das BSI sind Mitglieder im Cyber-Sicherheitsrat, der Cyber-Sicherheitsrat hat weder Kooperationspartner noch Kooperationsvereinbarungen geschlossen.

Im Übrigen unterliegt die Tätigkeit des Cyber-SR den üblichen Regelungen zur parlamentarischen Kontrollfunktion des Deutschen Bundestags.

Referat IT 3
AR Spatschke

22. Mai 2012
2045

[redacted]

BMI:	Stn Rogall-Grothe, Hr. Dr. Dürig, Hr. Spatschke
BK:	Hr. Dr. Wettengel, NN, NN
AA:	Stn Dr. Haber, Hr. Fleischer
BMVg:	St Beemelmans, Hr. Dr. Theis
BMWi:	Hr. Dr. Schuseil, Fr. Husch
BMJ:	Stn Dr. Grundmann, Fr. Schmierer
BMF:	Fr. Dr. Stahl-Hoepner, NN
BMBF:	St Dr. Schütte, Hr. Lange
HE:	Hr. Jurk
BW:	Hr. Dr. Zinell, Hr. Dr. Hermann
BSI:	Hr. Hange

Assoziierte Wirtschaftsvertreter:

D[redacted]
A[redacted]
B[redacted] NN (Absage [redacted]; VP-Ebene erbeten) Tusnik / Rohleder
B[redacted]

Hinweis: Mit Schreiben vom 8.5. hatten Sie als derzeit amtierende Vorsitzende des IT-Planungsrats ggü. Herrn Sts Murawski (Chef der Staatskanzlei BW) angeregt, einen entsprechenden Beschluss der CdS-Konferenz für die Vertretung der A-Länder im Cyber-Sicherheitsrat durch MD Dr. Zinell herbeizuführen.

3. Cyber-Sicherheitsrat am 31. Mai 2012
Kernbotschaften P BSI

Wo stehen wir heute?

Kernbotschaft 1 (Gesamtlage): Die IT-Durchdringung und IT-Vernetzung steigern die Attraktivität für Cyber-Angriffe verschärfen die Gefährdungslage.

- Die IT ist aus unserem Alltag nicht mehr wegzudenken: Sie durchdringt alle Lebensbereiche und ist Bestandteil wesentlicher (Geschäfts-)Prozesse.
- Die Durchdringung ist so weit fortgeschritten, dass die administrative Handlungsfähigkeit und die wirtschaftliche Leistungsfähigkeit von einer gut funktionierenden und sicheren IT abhängen.
- Quer durch alle Branchen ist die Hälfte der deutschen Unternehmen schon heute vom Internet abhängig.
- Eine fast durchgängige Vernetzung verbindet fast alle IT mit dem Internet, sodass sich IT-Sicherheit zur Cyber-Sicherheit entwickelt.

Kernbotschaft 2 (aktuelle Gefährdungslage): Die Angriffsmethodiken sind ausgeklügelt und individuell auf bestimmte Ziele zugeschnitten (Stichwort zweistufige Angriffe/APT).

- Im letzten Jahr haben wir beobachtet, dass die Quantität und Qualität der Angriffe weiter zunimmt. Aktuelle Fälle wie etwa DigiNotar bzw. RSA zeigen, dass sogar Unternehmen im (IT-)Sicherheitsbereich, also Unternehmen, die sich aufgrund ihrer unternehmerischen Ausrichtung mit dem Thema (IT-)Sicherheit intensiv befassen, getroffen werden können.
- Qualitativ sind insbesondere die zweistufigen Angriffe (Einstieg und „Nachladen") hervorzuheben.
- So z.B. im Fall DigiNotar: Der Angriff auf eine niederländische Zertifizierungsstelle war nur die erste Stufe des Angriffs. Mit den dort entwendeten Zertifikaten konnten sich die Angreifer in den Internetverkehr einklinken und so Daten abgreifen.
- Das Beispiel DigiNotar ist nicht nur wegen der Angriffsmethodik von besonderer Bedeutung. Es zeigt auch: Das Internet wird nicht nur als Transportinfrastruktur für Angriffe genutzt (z.B. DDoS-Angriffe), es ist auch als Infrastruktur selbst gefährdet.

3. Cyber-Sicherheitsrat am 31. Mai 2012
Kernbotschaften P BSI

- Wir, die Bundesverwaltung verzeichnen täglich 2.500 Infektionsversuche (ungezielte Angriffe). Trotz hoch entwickelter Virenscanner und Firewalls finden wir weiterhin eine Infektion pro Woche auf einem PC in der Bundesverwaltung.
- Darüber hinaus verzeichnen wir täglich 5 gezielte Angriffe auf Bundesverwaltung mit manipulierten Mails.
- Auf der Seite der Angreifer beobachten wir zugleich, dass mit den so genannten „Hacktivisten" ein neuer Typus von Angreifer agiert. Seine Motivationslage ist unterschiedlich und auch die Angriffsfähigkeiten bewegen sich auf unterschiedlichstem Niveau.
- Aus unserer Zusammenarbeit mit der Wirtschaft wissen wir, dass diese Gefährdungslage die Wirtschaft gleichermaßen trifft bzw. sie ebenfalls dieser ausgesetzt ist.

IT: Wohin führt der technische Trend?

Kernbotschaft 3 (Trendaussagen): Neue Technologien bzw. technische Entwicklungen (z.B. Smartphones, Cloud Computing, VoIP) forcieren die IT-Durchdringung und IT-Vernetzung weiter. Die Gefährdungslage wird sich – auch in der Breite - weiter verschärfen.

- Neue Technologien bzw. technische Entwicklungen forcieren die IT-Durchdringung und IT-Vernetzung weiter. Hierzu gehören insbesondere die Trends im Mobilsektor als auch das Cloud Computing.
- Allein die Zahlen belegen, der Trend ist schon da. Die Prognose für Deutschland 2012 im Mobilsektor ist: Verkauf von 28,9 Millionen Handys, davon 15,9 Millionen Smartphones. Beim Cloud Computing 2012 in D erwarteter Umsatz: 5,3 Mrd. €.
- Zugleich sind Smartphones mit Sicherheitsmechanismen schwach ausgestattet (bestimmte für den Kunden attraktive Services sind dadurch auch erst möglich). Unter dem Motto „Bring your own Device" erfolgt eine Durchmischung dienstlicher und privater Nutzung von IT. Informationen und Daten werden in Clouds ohne vereinbarte Sicherheitsstandards ausgelagert.

3. Cyber-Sicherheitsrat am 31. Mai 2012
Kernbotschaften P BSI

Was können wir tun?

Kernbotschaft 4 (Handlungsschwerpunkte aus BSI-Sicht): Eine Reihe von Aktivitäten bringt die Cyber-Sicherheit in der Breite voran.

- Eigeninitiatives melden und systematisches Erfassen von Sicherheitsvorfällen (auch in anonymisierter Form) für Aktualisierung der Gefährdungslage und Verbesserung der Prävention (Stichwort für TOP 6 für CERT-Strukturen).
- Konzept der Mindestanforderungen ist fachlich in die Breite und durch Good Practise fortzuentwickeln.
- Aktives Zugehen auf Kritis-Sektoren (Stichwort für nachfolgenden TOP 3).
- Übergreifende nationale Kooperation ist auszubauen → Allianz: Anwender/Nutzer, Hersteller, Diensteanbieter.
- Die Analysefähigkeit von Sicherheitsvorfällen ist bei allen Handelnden auszubauen.

Kernbotschaft 5 (Fazit): Erstes Jahr war insbesondere vom Aufbau der Zusammenarbeit geprägt. Zur weiteren inhaltlichen Vertiefung der Zusammenarbeit sollen Projektgruppen gegründet werden.

- Das erste Jahr des Cyber-Abwehrzentrums war insbesondere vom Aufbau der Zusammenarbeit geprägt (Zusammenarbeit des Nukleus ab März 2011; ab Juni 2011 Einbindung der assoziierten Behörden; Kommunikationswege etabliert etc.).
- Ein weiterer Schwerpunkt im ersten Jahr war zudem das Zusammenspiel bei der Vorfallsbewertung zwischen den Behörden.
- Um die weitere inhaltliche Zusammenarbeit weiter zu vertiefen, planen wir die Einrichtung von Projektgruppen, die sich mit unterschiedlichen Themen wie etwa dem Hacktivismus beschäftigen sollen. Hierzu befinden wir uns jedoch derzeit noch in der Abstimmung mit den beteiligten Behörden.

Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
Cyber-Abwehrzentrum

Cyber-Abwehrzentrum

Michael Hange
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

3. Sitzung des Cyber-Sicherheitsrates
31. Mai 2012

Evaluierung

Botnetze:
Miner-Botnetz

Datendiebstahl:
Sony

Bloßstellung:
PATRAS

Sicherheitsinfrastrukturen:
DigiNotar, Duqu

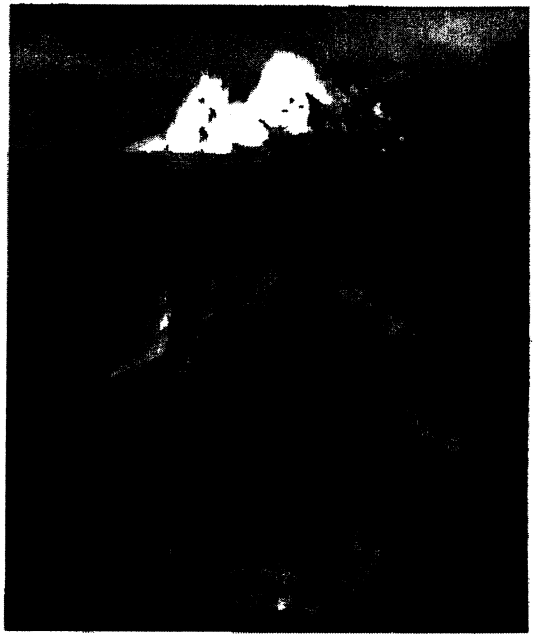
Im Cyber-AZ bearbeitete Fälle: 483

Ausführlich analysiert: 9

Höher VS-NfD: 2

Folgerungen für mehr Cyber-Sicherheit

- Diskrepanz zwischen bekannten Cyber-Angriffen und festgestelltem Angriffspotential.
- Sicherheitsmaßnahmen:
  - Standard für 80 Prozent der Cyber-Angriffe.
  - Individuelle für 20 Prozent der Cyber-Angriffe.
- Bisher konnte aus den Cyber-Angriffen nur ein unklares Täterbild (Aussagen zu Fähigkeiten, Ressourcen, Zielen) abgeleitet werden.



→ Maßnahmen gegen Standardangriffe: CERT-System, Lage- und Krisenreaktionszentren

→ Maßnahmen gegen (individuelle) Angriffe: Austausch zu Vorfällen

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Michael Hange
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)228 99-9582-5200
Fax: +49 (0)228 99-109582-500

Michael.Hange@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de

Nationales
Cyber-Abwehrzentrum

Statusbericht Nationales Cyber-Abwehrzentrum

zur Unterrichtung des Cyber-Sicherheitsrates

Nationales Cyber-Abwehrzentrum
Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6000
E-Mail: cyber-az@bsi.bund.de

Inhaltsverzeichnis

1 Überblick

Am 1. April 2011 hat das Nationale Cyber-Abwehrzentrum mit 10 Mitarbeitern aus den Behörden BBK, BfV und BSI seine Arbeit aufgenommen. Ab 16. Juni 2011 wurde es um Mitarbeiter der assoziierten Behörden BKA, BND, Bundespolizei, Bundeswehr, MAD und ZKA erweitert. Aufgabe des Nationalen Cyber-Abwehrzentrums ist, im Sinne einer Informationsdrehscheibe Cyberangriffe behördenübergreifend zu analysieren und zu bewerten sowie Handlungsempfehlungen zur Verbesserung der Cybersicherheit vorzuschlagen.

Das Nationale Cyber-Abwehrzentrum hat im Zeitraum April 2011 bis März 2012 rund 500 nationale und internationale IT-Sicherheitsvorfälle registriert. Im Ergebnis kann festgehalten werden, dass der Großteil der Vorfälle kriminell motiviert war und eine Gewinnerzielungsabsicht zum Hintergrund hatte. Hauptopfer waren dabei Privatanwender.

An zweiter Stelle findet sich mit dem „Hacktivismus" ein recht junges Phänomen wieder. Mit nicht klar einzuordnenden, oft divergierenden Zielsetzungen wurden Unternehmen und staatliche Stellen durch Angriffe auf ihre Datenbestände und anschließende Veröffentlichung der Daten bloßgestellt. Oftmals wurden dabei unbeteiligte Dritte zum Opfer, deren Daten im Nachgang von Kriminellen missbraucht wurden.

Angriffe auf die Kommunikationsnetze und Internetauftritte deutscher Bundes- und Landesbehörden gehören mittlerweile zum Alltag in der Angriffsbeobachtung des BSI, blieben im Betrachtungszeitraum jedoch ohne nennenswerte Erfolge. Auf internationaler Ebene konnten im Jahr 2011 jedoch einige Angriffe beobachtet werden, die erfolgreich waren, aufgrund ihrer Beschaffenheit weltweit einsetzbar sind und daher Anlass zur Besorgnis geben. Dies gilt insbesondere deshalb, da sie nach Einschätzung der am Cyber-Abwehrzentrum beteiligten Dienste staatlich gelenkt waren.

Insgesamt hat sich die Gefährdungslage verschärft, was angesichts einer immer stärker werdenden Vernetzung und der zunehmenden Nutzung des Internets durch mittlerweile alle Bevölkerungsgruppen zu erwarten war. Zu beobachten war zum einen eine weitere Professionalisierung der Angreifer, die sich einer arbeitsteilig organisierten Underground Economy bedienen können. Auffällig waren zudem eine kleine Anzahl äußerst versiert ausgeführter mehrstufiger Angriffe, bei denen das Eindringen in ein IT-System nur erfolgte, um Informationen für einen Angriff auf das eigentliche Zielsystem (eines völlig anderen Unternehmens) zu erbeuten. Die Masse der Angriffe war erfolgreich, weil seitens der Nutzer elementare Sicherheitsvorkehrungen nicht beachtet wurden. So konnten beispielsweise aufgrund nachlässigen Patch-Managements bereits lange vom Hersteller geschlossene Schwachstellen ausgenutzt werden.

Ernstzunehmende Angriffe mit Schadenswirkung auf das Funktionieren des Staates sowie kritischer Infrastrukturen waren im vergangenen Jahr, anders als in anderen Staaten, nicht zu verzeichnen. Durch die immer weiter steigende Abhängigkeit einer modernen Gesellschaft von der Informationstechnik werden die mit solchen Angriffen verbundenen Risiken allerdings ansteigen. Die im November 2011 durchgeführte LÜKEX-Übung hat dies eindrucksvoll bestätigt.

Zusammenfassend lassen sich zwei Ergebnisse festhalten:

- Die Beobachtung von Sicherheitsvorfällen und die daraus abgeleitete Gefährdungslage wird immer mehr unverzichtbare Voraussetzung der IT-Sicherheitsgestaltung. Eine enge Zusammenarbeit der Sicherheitsbehörden ist hierbei zwingend. Ein frühzeitiger Informationsaustausch zwischen den Akteuren ist grundlegende Voraussetzung für ein konsequentes und – unter Nutzung der jeweiligen Kompetenzen in präventiven und repressiven Bereichen – wirksames Vorgehen im Schadensfall.
- Durch mit vertretbarem Aufwand erreichbare Mindestsicherheitsstandards lassen sich bereits 80 Prozent der beobachteten Angriffe abwehren (Pareto-Prinzip).

2 Besondere Cyber-Angriffe

2.1 S[redacted]

Das Eindringen in die Systeme von S[redacted] und die Veröffentlichung mehrerer Millionen Kundendatensätze zeigt, dass selbst Global Player im IT-Markt betroffen sein können. Nachdem S[redacted] zwei Hacker verklagt hatte, da diese den Kopierschutz der S[redacted] umgangen hatten, wurden als Gegenreaktion durch die Hacktivismusgruppe „Anonymous" eine Reihe von S[redacted] Websites durch DDoS-Angriffe lahmgelegt. Darüber hinaus gelang es Hackern, in das S[redacted]- und das S[redacted] sowie in den Musikdienst Qriocity einzudringen und rund 100 Millionen Kundendaten zu stehlen. Hiervon waren etwa 5 Millionen deutsche Nutzer betroffen, zum Teil sogar mit Kontodaten. S[redacted] war dem Angriff auf seine Datenbanken zunächst hilflos ausgeliefert und musste zeitweise seine Nutzerangebote abschalten. Verantwortlich machte S[redacted] auch für diese Angriffe die Gruppe „Anonymous", die dies allerdings bestritt. Leidtragende waren später jedoch die Kunden von S[redacted], die dem Risiko ausgesetzt waren, dass ihre Daten von Kriminellen missbraucht werden.

Das Image von S[redacted] hat durch einen unzureichenden Schutz seiner Dienste mit diesem Vorfall nachhaltigen Schaden genommen.

2.2 Duqu

Das Bekanntwerden der Schadsoftware „Duqu" zeigt, dass Stuxnet kein Einzelfall war. Nach den Erkenntnissen des Nationalen Cyber-Abwehrzentrums handelt es sich bei Duqu um ein Schadprogramm, das große Teile des Stuxnet-Codes enthält. Betroffen waren bisher nicht näher bezeichnete Unternehmen im Sudan, Iran, Frankreich, Niederlande, Ungarn, Schweiz und Indonesien. Die Auswahl der Branchen, die angegriffen wurden, lässt darauf schließen, dass Duqu zur Angriffsvorbereitung bzw. Aufklärung eingesetzt wurde.

Von Duqu ist auch der KRITIS-Bereich potenziell gefährdet. Da Duqu vermehrt bei Herstellern von SCADA[1]-Systemen aufgetreten ist, kann vermutet werden, dass der Angreifer gezielt Informationen zu solchen Systemen erhalten wollte. Grundsätzlich könnten die abgeflossenen Informationen zu SCADA dazu genutzt werden, die Systeme anzugreifen, die auch in KRITIS Unternehmen im Einsatz sein könnten. Sofern die kritischen Prozesse der KRITIS Unternehmen von den betroffenen SCADA-Systemen (stark) abhängig sind bzw. durch diese erbracht werden, könnte es im Falle eines Angriffes zu einer relevanten Beeinträchtigung oder dem Ausfall der Versorgung mit dem Service der jeweiligen KRITIS führen. Dies wäre verbunden mit entsprechenden Auswirkungen auf die Bevölkerung, auf staatliche Stellen und auf die Wirtschaft.

2.3 DigiNotar

Der Angriff auf DigiNotar erfolgte, um im Nachgang Dritte anzugreifen. Mit dem Einbruch bei DigiNotar und der Erzeugung von SSL-Zertifikaten war es möglich, die vertrauliche, verschlüsselte Kommunikation von Internetnutzern auszuspähen. Außerdem verursachte der Vorfall enorme Kosten für die niederländische Regierung, da diese die Zertifikate für die Absicherung von Regierungswebseiten und -diensten komplett austauschen musste. Zeitweise mussten sogar einige Online-Regierungsdienste abgeschaltet werden, zum Beispiel die elektronische Abgabe der Lohnsteuererklärung. Betroffen waren aber weit mehr Fachverfahren der niederländischen Regierung.

Da es sich bei SSL um einen internationalen Standard handelt, werden auch im deutschen Behördennetz SSL-Zertifikate an vielen verschiedenen Stellen zur Absicherung der Kommunikation eingesetzt. Das deutsche Netz ist daher für einen Angriff wie den oben beschriebenen prinzipiell genauso anfällig wie das niederländische. Der Vorfall bei DigiNotar steht dabei sogar nur für einen von mehreren erfolgreichen Angriffen auf Zertifizierungsstellen in allen Teilen der Welt im Jahr 2011. Das BSI hat daher eine Projektgruppe eingesetzt, um eine technische Lösung für dieses Problem zu erarbeiten.

---

[1] Supervisory Control and Data Acquisition (SCADA)-Systeme dienen zum Überwachen und Steuern technischer Prozesse.

Unternehmen und Einrichtungen aus dem KRITIS-Bereich können in derselben Weise wie nicht-KRITIS Unternehmen und Einrichtungen betroffen sein - sowohl als Nutzer/Anwender als auch als Diensteanbieter. Dies wäre im KRITIS-Kontext insbesondere dann relevant, wenn z.B. kritische Prozesse von der Verfügbarkeit einer vertrauenswürdigen, TLS/SSL-gesicherten Kommunikationsinfrastruktur abhängig sind. Der Angriff auf DigiNotar oder ähnlich gelagerte IT-Sicherheitsvorfälle könnten im KRITIS-Bereich zu Beeinträchtigungen und Störungen führen. So wäre es beispielsweise möglich, dass manipulierte Softwareprodukte, die mit validen Zertifikaten signiert wurden, in der Folge eingesetzt werden, um an Informationen und Unternehmensdaten zu gelangen bzw. durch Sabotage Betriebsabläufe zu stören. In Bezug auf diesen konkreten Fall gibt es keine Hinweise darauf, dass KRITIS in Deutschland betroffen war. Vorrangig waren verschiedenen Anwendungen der Niederländischen Regierung sowie iranische Nutzer betroffen.

2.4 PATRAS

Der „Einbruch" in das GPS-basierte Zielverfolgungssystem „PATRAS" blieb nicht ohne Auswirkungen auf die Ermittlungsarbeit deutscher Sicherheitsbehörden. Die mit Hilfe dieses Systems durchgeführten Lokalisierungsdienste mussten für einen kurzen Zeitraum unterbrochen werden. Grundsätzlich ist auch nicht auszuschließen, dass Kriminelle (vornehmlich aus dem Bereich des Menschen- und Drogenhandels) durch Veröffentlichung der ermittelten Bewegungsprofile davon Kenntnis erlangten, Ziel einer staatlichen Überwachungsmaßnahme gewesen zu sein.

Verursacht wurde der Zwischenfall durch eine Kette von Fehlern auf verschiedenen Ebenen, die allesamt sehr leicht vermeidbar gewesen wären und die schließlich durch einen Unberechtigten ausgenutzt wurden.

Der PATRAS-Fall war die erste Bewährungsprobe für das Nationale Cyber-Abwehrzentrum. Der Vorfall ereignete sich nicht nur kurz nach dessen offizieller Eröffnung, es waren darüber hinaus auch zwei der beteiligten Behörden unmittelbar betroffen. Im Rahmen mehrerer anlassbezogener Treffen und Vollversammlungen des Cyber-Abwehrzentrums konnte der Vorfall analysiert werden. In der Folge hat die Bundespolizei ihre IT-Prozesse optimiert.

2.5 [redacted]

Der Vorfall bei dem Unternehmen [redacted] zeigt anschaulich, dass die Angriffsszenarien komplexer geworden und Angriffe immer häufiger mehrstufig aufgebaut sind. In diesem Fall wurde zunächst durch einen Einbruch im März 2011 in die IT-Systeme der Firma [redacted] technologisches Wissen erbeutet, das dazu verwendet werden konnte, das von [redacted] vertriebene SecurID-Einmalpasswort-System zu schwächen.

Einige Monate später wurde mit den beim [redacted]-Angriff gewonnenen Informationen das Rüstungsunternehmen L[redacted] angegriffen.

Die Kommunikationspolitik der Firma [redacted] trug dabei zur Aufklärung des Falles wenig bei. Nachdem anfangs von Unternehmensseite noch die Ansicht vertreten wurde, die Sicherheit des SecurID-Systems sei nicht beeinträchtigt, gab man nach und nach zu, dass man sich seiner Sache doch nicht ganz sicher sei. Angesichts der Tatsache, dass weltweit etwa 40 Millionen SecurID-Hardware-Tokens verkauft wurden und dazu noch einmal schätzungsweise 250 Millionen Software-ID-Generatoren kommen, ist diese Zurückhaltung aus wirtschaftlichen Erwägungen zwar verständlich, aus Kundensicht jedoch nicht. Knapp 300 Millionen Nutzer darüber im Unklaren zu lassen, dass ihre Zugangsdaten vermutlich kompromittiert wurden, ist unter Sicherheitsaspekten nicht zu verantworten. Erst knapp drei Monate nach dem Vorfall begann das Unternehmen [redacted] damit, einen Teil der Hardware-Tokens auszutauschen. Und erst im Dezember 2011 berichtete [redacted] der Bundesverwaltung detailliert über den genauen Ablauf des Angriffs.

Auch Unternehmen und Einrichtungen aus dem KRITIS-Bereich, die die SecureID Lösung von [redacted] einsetzen, könnten betroffen sein. Zum einen ist eine direkte Folge für Unternehmen, die die möglicherweise kompromittierte Lösung einsetzen, in erster Linie in der ggf. notwendigen Evaluierung bzw. dem Ersatz/Austausch des 2-Faktor Authentifizierungsverfahrens zu sehen. Zum anderen könnte der vorliegende IT-Sicherheitsvorfall im KRITIS-Bereich zu Beeinträchtigungen und Störungen führen, wenn sich die Täter durch das kompromittierte SecureID System mit geringerem Aufwand Zugang zu relevanten Systemen der KRITIS verschaffen können. In diesem Fall sind nach aktuellen Kenntnissen Unternehmen und Einrichtungen aus dem KRITIS-Bereich in Deutschland nicht betroffen. Unternehmen und Einrichtungen aus dem KRITIS-Bereich könnten aber sowohl durch das Angriffsmuster des primären Vorfalls ([redacted], Eindringen in Systeme zur Informationsbeschaffung) als auch durch das Angriffsmuster des sekundären Vorfalls ([redacted] Angriff unter Verwendung zuvor gewonnener Informationen) betroffen sein.

2.6 Miner Bot-Net

Mit Hilfe von Bot-Netzen versuchten Angreifer im vergangenen Jahr, Geld von verschiedenen Website-Betreibern zu erpressen und drohten diesen damit, ihre Website mittels eines DDoS-Angriffes lahmzulegen. Es handelt sich also um die digitale Entsprechung der herkömmlichen Schutzgelderpressung. Ein Spezialfall war das „Miner-Bot-Net", welches sich durch die verwendete Kommunikationsstruktur sehr resistent gegenüber Gegenmaßnahmen zeigte. Es nutzte keine zentralen Steuerungssysteme, sondern verteilte seine Angriffsbefehle über Peer-to-Peer-Kommunikation[2]. Im Visier der Angreifer standen zunächst Pizzabringdienste, später kamen größere Unternehmen der Immobilienbranche und weitere Sektoren (vereinzelt auch Behörden) als

[2] Viele Bot-Netze verwenden eine Kommunikationsstruktur, bei der die einzelnen Bots Befehle von übergeordneten „Command-and-Control"-Servern erhalten. Gelingt es, die Hoheit über die „Command-and-Control"-Server zu erhalten oder diese abzuschalten, kann ein davon abhängiges Bot-Netz in der Regel unschädlich gemacht werden. In einem „Peer-to-Peer-Netz" sind alle Computer gleichberechtigt und können sowohl Dienste in Anspruch nehmen, als auch zur Verfügung stellen. Es existieren keine „Command-and-Control"-Server. Das Netz organisiert sich selbst. Die Bekämpfung ist daher wesentlich aufwändiger.

Angriffsziele hinzu. Die strafrechtliche Verfolgung ist inzwischen von den Polizeien übernommen worden.

3 Grundsätzliche Schlussfolgerungen

Die geforderte und anzustrebende Cyber-Sicherheit ist kein statischer Zustand, sondern ein kontinuierlicher Prozess, der die Risiken des Cyber-Raums und die erforderlichen und angemessenen Gegenmaßnahmen in ein effektives und tragbares Verhältnis zueinander stellt.

Da der Cyber-Raum essentielle Bedeutung für alle Akteure erlangt hat, müssen sich Staat, Wirtschaft, Wissenschaft und Bevölkerung weiterhin stark engagieren.

- Aktives Beobachten und Analysieren der Bedrohungslage ist unverzichtbare Voraussetzung für die Cybersicherheitsgestaltung.
- Es besteht eine Diskrepanz zwischen öffentlich gewordenen Cyber-Angriffen und sich im Internet darstellenden Angriffspotenzial.
- 80:20-Regel: Durch konsequentes Umsetzen von Standardsicherheitsmaßen ist die Masse der Cyber-Angriffe beherrschbar.
- Für die 20 Prozent hochwertiger Angriffe werden verbesserte Sicherheitskonzepte und Lösungen benötigt (dies gilt insbesondere für den Bereich KRITIS).
- Die Ermittlung von Tätern (Attributierung) auf Basis eines erfolgten Cyber-Angriffs ist schwierig.

□

Referat IT3
OAR Treib

03.05. 2012
Tel.: 2355

[redacted]

Ziel der Behandlung: *Strategische Ausrichtung der Internationalen Zusammenarbeit zur Cyber-Außenpolitik einschließlich –Sicherheit.*

Problem: *AA betrachtet diese Thematik als ureigenes Kompetenzfeld und lehnt Abstimmung im Cyber-SR grundsätzlich ab. Die Entwicklung/Vorstellung einer Strategie wurde bilateral zugesagt. → Sie sollten betonen, dass politische Abstimmung im Cyber-SR erfolgen soll.*

Sachstand

Gem. Ergebnisprotokoll der zweiten Sitzung des Cyber-SR am 18. Oktober 2011 wurde AA beauftragt, ein Grundsatzpapier zu Zielen und Strategien der internationalen Zusammenarbeit im Bereich Cyber-Sicherheit in Abstimmung mit den betroffenen Ressorts zu erstellen.

Im Ergebnis steht ein Papier, das hauptsächlich das aus politischer Zugehörigkeit resultierende DEU-Engagement in internationalen Gremien/Foren reflektiert (EU, NATO, VN, OSZE, EUROPARAT; OECD); insoweit liegt eine gute/umfangreiche Status Quo-Beschreibung vor, insb. auf Grundlage der Zulieferungen seitens BMVg, BMJ und BMI.

AA wird voraussichtlich die Vorstellung des Papiers nutzen, um für eine zusammenfassende Darstellung der derzeit auf EU-Ebene laufenden Initiativen zum Thema „Cyber-Security" zu werben um ein Gesamtbild hierzu zu erhalten und möglicherweise auch eine gemeinsame Linie für die Begleitung dieser Initiativen zu erarbeiten. Hintergrund sind die diversen Initiativen auf EU-Ebene und die innerhalb der Bundesregierung verteilten Zuständigkeiten.

Ein richtungsweisendes, strategisches Konzept wird nur im Ansatz geliefert.

Vorliegendes Arbeitspapier orientiert sich am unter FF des BMI für die Quad-Konsultationen in 2011 entwickelten Non-Paper „Norms of State Behavior". Bereits das Non-Paper geht über reine Sicherheitsthemen hinaus, denn Sicherheit und netzpol. Ziele wie Freiheit, Offenheit usw. müssen national wie international ausbalanciert werden.

Gesprächsführungsvorschlag (aktiv):

- Dank an AA und die an der Erarbeitung des Papiers beteiligten Ressorts.
- Das Papier beschreibt zutreffend den politischen Rahmen, die Ausgangslage und gegenwärtige Ziele für das DEU-Engagement im EU- bzw. internationalen Bereich.
- Unter der Überschrift „Prinzipien" wird deutlich, dass Ziele und Strategie der internationalen Zusammenarbeit im Bereich Cyber-Sicherheit nicht ohne weiteres losgelöst von einer allgemeinen Cyber-Außenpolitik betrachtet werden können. Zutreffend werden im vorliegenden Arbeitspapier unter „Prinzipien" wesentliche Grundlinien der BReg. wie Offenheit, Transparenz und Freiheit im Cyber-Raum benannt, die im Spannungsfeld zu Sicherheitsfragen stehen.
- Bei dieser Sachlage rege ich an, unsere Diskussion entsprechend auszuweiten und **in einem nächsten Schritt** ein nach außen zu vertretendes ganzheitliches strategisches **Konzept für einen globalen, ungeteilten Cyber-Raum der Freiheit und des Rechts** zu entwickeln.
- „Norms of State Behavior in Cyberspace" bilden insoweit den Kern der Bemühungen (konsise Vorstellungen wurden auf Arbeitsebene für die Quad-Konsultationen mit USA, FRA und UK bereits entwickelt; darüber hinaus müssten m.E. auch noch Ideen zur Weiterentwicklung des Völkerrechts abgestimmt werden –etwa Verantwortung der Staaten für Gefahren, die von ihrem Territorium ausgehen[1]-.
- Bei dieser Sachlage plädiere ich für folgenden **Dreischritt**:
    1. Formulierung einheitlicher **Definitionen** sowie eines gemeinsamen, ressortübergreifenden Verständnisses bezüglich Cyber-Außenpolitik und Cyber-Sicherheit als Voraussetzung dafür, dass mit internationalen Gesprächspartnern ein gemeinsames Verständnis entwickelt werden kann.
    2. **Prioritäten** setzen. Mit Blick auf Zielkonflikte sollten gegenpolige Aspekte nach Wichtigkeit und Dringlichkeit unterschieden werden (z.B. Freiheit, Offenheit, Transparenz im Internet vs. Repression oder präventive/aktive Cybersicherheit).
    3. Geopolitisch **„SMART Ziele"**[2] setzen, d.h. ein aus den Prioritäten abgeleitetes Engagement der BReg in der EU und in internationalen

[1] Keine Neuschöpfungen, sondern Anleihen z.B. im Weltraum-/Umweltrecht
[2] SMART ist ein Akronym für „Specific Measurable Accepted Realistic Timely"

Foren formulieren sowie aufgrund der Interessenlage Möglichkeiten der bilateralen Ansprache verschiedener Akteure/Länder eruieren[3] (z.B. mit gleichgesinnten EU-Staaten sowie USA, aber nicht zuletzt auch mit Blick auf bevölkerungsreiche aufstrebende in der Orientierung schwankende digital entwicklungsfähige Regionen und Länder).

- Dazu **beispielhaft** drei **praktische Denkanstöße**:
  1. **Afrika** ist offenbar weltweit am stärksten digital entwicklungsfähig. Afrikanische Länder sind über internationale Foren so gut wie nicht an das westl. Lager angebunden; mal abgesehen vom letztjährigen Internet Governance Forum **(IGF)** in Nairobi. Wenn die westl. Welt in dieser Region keine Kontakte knüpft, werden andere Staaten, deren Maßstäbe wir nicht teilen (RUS/CHN), das Vakuum ausfüllen. Deshalb kämen m.E. Gespräche und vielleicht ein „Coaching" eines ausgesuchten Staates in der Region in Frage (Vermittlung der Denkart + netzpol. Grundsätze, Muster für strategische Sicherheitsaufstellung, Awareness Raising Materialien zur Verfügung stellen, Sicherheit made in Germany?.....). Als strategisch wichtig könnte mglw. **Südafrika** angesehen werden (BRICS-Staat, vermutlich aufgeschlossen, relativ stabil, als Multiplikator geeignet...). Südafrika gehört auch zu den Ländern, mit denen OECD verstärkt zusammenarbeiten will (Synergie?).
  2. **Südamerika!** Von den südamerikanischen Staaten gehören Chile und Mexiko bereits der OECD an; sie dürften damit relativ westl. ausgerichtet sein. **Brasilien** als noch wichtiger „BRICS-Staat" hingegen steht bisher nur als Partner für verstärkte Zusammenarbeit im Fokus der OECD. Aus strategischen geopolitischen Gründen (Multiplikator, Vorzeigeland, ansonsten wie oben Südafrika) wäre daran zu denken, mit Brasilien ins Gespräch zu kommen.
  3. **„Problemstaaten"**
     Speziell auf Cyber Sicherheit gerichtete bilaterale Gespräche mit RUS und CHN intensivieren. Netzpol. Fragen müssten zugunsten eher konsensfähiger Aspekte (Wirtschaft, Pol./Mil, Menschenrechte, digitale Entwicklungshilfe) hintangestellt werden.

Reaktiv:

[3] z.B BRICS-Staaten

- Den Vorschlag des AA, die derzeit auf EU-Ebene laufenden vielfältigen Initiativen zum Thema Cyber-Security innerhalb der Bundesregierung zu erheben und möglicherweise darauf aufbauend eine gemeinsame Linie zu entwickeln, teile ich uneingeschränkt. Gern greife ich insoweit auch den Vorschlag des AA auf, sich in der kommenden Sitzung des Cybersicherheitsrates verstärkt dem EU-Thema zu widmen.
- Das BMI wird sich gern an der für Mitte September dJ geplanten 2. Berliner Cyber-Konferenz mit Schwerpunkt auf den Menschenrechten im Internet beteiligen und sowohl seine IT-Kompetenz als auch seine verfassungsrechtliche Expertise einbringen.

CCC
Chinese Compulsory certification
Sicherh.-prod. müssen

Auswärtiges Amt **ressortabgestimmter Entwurf, Stand: 07.02.2012**

Internationale Zusammenarbeit zur Cyber-Sicherheit

Arbeitspapier für den Cyber-Sicherheitsrat

Inhaltsverzeichnis

Hinweis zur Formatierung:
Im nachstehenden Dokument sind Positionen der Bundesregierung unterstrichen, *Zitate* kursiv und **Schlüsselbegriffe** fett hervorgehoben. In der Übersicht relevanter internationaler Organisationen (Kapitel 4) sind außerdem die **Gremien** jeweils fett unterstrichen.

1. Der politische Rahmen

In der im Februar 2011 beschlossenen Cyber-Sicherheitsstrategie für Deutschland definiert die Bundesregierung als neues Politikfeld eine ***„Cyber-Außenpolitik"***, die *„deutsche Interessen und Vorstellungen in Bezug auf Cyber-Sicherheit in internationalen Organisationen wie den Vereinten Nationen, der OSZE, dem Europarat, der OECD und der NATO koordiniert und gezielt verfolgt"*.[1]
Die internationale Zusammenarbeit zum Thema Cyber-Sicherheit hat sich in den letzten Monaten erheblich verdichtet mit dem Ziel, zunächst eine grundsätzliche Verständigung für **verantwortliches staatliches Verhalten im Cyberraum** zu erreichen.
Dabei gibt es entgegengesetzte Vorstellungen: Die Bemühungen der westlichen Staaten richten sich auf politisch verbindliche Verhaltensnormen auf der Basis bestehenden Völkerrechts sowie gemeinsamer Interessen und Werte; diese sind - neben dem Aspekt der Sicherheit - die Freiheit, Offenheit und Zuverlässigkeit des Netzes. Demgegenüber gibt es eine Gruppe von Staaten um Russland und China, die den über Cyber-Sicherheit hinausgehenden Begriff Informationssicherheit verwenden, und diesen auch über Kontrolle der Inhalte im Netz und des Zugangs zu Informationen definieren. Wir befinden uns somit noch in einer Phase der internationalen Diskussion, in der die Teilnehmer um ein gemeinsames Verständnis von Begriffen und Definitionen ringen und ideologische Verwerfungen im Grundverständnis zu überbrücken sind. Deshalb werden global akzeptierte Vereinbarungen nur mittel- bis langfristig zu erreichen sein. Die Internationale Cyber-Sicherheitskonferenz im Auswärtigen Amt am 13./14. Dezember mit Teilnahme von 24 Staaten und Internationalen Organisationen hat immerhin gezeigt, dass sich zwischen den Hauptakteuren eine Bereitschaft abzeichnet, gemeinsam auf vertrauens- und sicherheitsbildende Maßnahmen zur Vermeidung von Instabilitäten, Fehleinschätzungen und Eskalationsrisiken hinzuarbeiten.

Die Bundesregierung setzt sich dafür ein, Cyber-Außenpolitik nicht auf den Bereich der Sicherheit zu verengen, sondern die Ziele Offenheit, Transparenz und Freiheit des Cyberraums gleich zu gewichten. Zum einen sind ungehinderter Zugang zum Internet (Verfügbarkeit und Netzneutralität) und fairer Wettbewerb unverzichtbar für unsere Gesellschaften und Ökonomien geworden. Zum anderen müssen Grund- und Menschenrechte wie Meinungs-, Rede- und Versammlungsfreiheit im Internet genau so geschützt sein wie in der realen Welt. Allerdings ist das Internet zur universellen Durchsetzung dieser Rechte ebenso nutzbar wie als Instrument der Repression. Es gilt daher, die Authentizität und Vertraulichkeit der übertragenen Daten zu gewährleisten.

---

1) Cyber-Sicherheitsstrategie, S. 11

Für die Befassung des Cyber-Sicherheitsrates soll mit dem vorliegenden Papier **in einem ersten Schritt** skizziert werden, **welchen Beitrag die Außen- und Europapolitik in den verschiedenen Foren zur Cyber-Sicherheit leisten kann.** Dabei stehen im Mittelpunkt die Bemühungen um einen *„Kodex für staatliches Verhalten im Cyber-Raum (Cyber-Kodex), der auch vertrauens- und sicherheitsbildende Maßnahmen umfasst."*[2]
Cyber-Außenpolitik ist nicht auf die Cyber-Sicherheit beschränkt. Das vorliegende Papier ist daher nur ein Element einer umfassenden Cyber-Außenpolitik, welche die Bundesregierung unter Federführung des Auswärtigen Amts und unter Einbeziehung der sicherheitspolitischen, der menschenrechtlichen und der wirtschaftlich-entwicklungspolitischen Dimensionen erarbeitet.

2. Ausgangslage und Ziele

Netzsicherheit ist eine primär nationale Verantwortung. Zugleich ist *„Sicherheit im globalen Cyber-Raum nur durch ein abgestimmtes Instrumentarium auf nationaler und internationaler Ebene zu erreichen"*.[3] Daraus erwächst die Notwendigkeit einer engeren Abstimmung und Zusammenarbeit mit Partnern in der EU und der NATO auf diplomatischen, militärpolitischen und technischen Kanälen. Ebenso wichtig ist indes die multi- und bilaterale Einbeziehung anderer Staaten und regionaler Zusammenschlüsse.

Eine wachsende Sorge gilt der Möglichkeit von Cyberattacken, die die kritische Infrastruktur beeinträchtigen können. Hier ist Raum für gefährliche Missverständnisse: Schädigendes Verhalten mit Cybermitteln kann in vielen Fällen nicht oder erst nach aufwendigen Ermittlungen („Forensik") einem staatlichen oder nichtstaatlichen Akteur zugeordnet werden. Dementsprechend schwer ist es im konkreten Fall zu entscheiden, ob eine Gefährdung der inneren oder der äußeren Sicherheit vorliegt.
Des Weiteren besteht das Risiko, dass Cyberverteidigungsstrategien von Staaten oder Bündnissen als offensive Aufrüstung verstanden werden können.
Gleichzeitig stehen bisher keine Instrumente der Vertrauens- und Sicherheitsbildung zur Verfügung, wie wir sie aus der herkömmlichen Rüstungskontrolle kennen.

Ziele:

- Durch aktive und ausgewogene Diplomatie Transparenz schaffen und Vertrauen aufbauen.
- Internationale Verpflichtungen zur Zusammenarbeit bei der Aufdeckung und Rückverfolgung von Angriffen etablieren.

---

2) Cyber-Sicherheitsstrategie, S. 11
3) Cyber-Sicherheitsstrategie, S. 11

- Konkrete internationale Zusammenarbeit beim Schutz von Netzen und bei der Bekämpfung von organisierter Cyber-Kriminalität, Cyber-Spionage oder Cyber-Terrorismus ausbauen.
- Kommunikationskanäle für Krisensituationen schaffen, die im Falle simulierter oder tatsächlicher Angriffe, die Dritten zugeschoben werden könnten, genutzt werden können.[4]

Prinzipien:
Staatliches Verhalten im Cyberraum sollte sich an folgenden Prinzipien und Zielen orientieren:

- Offenheit, Transparenz und Freiheit des Cyberraums
- Schutz der Meinungsfreiheit und des Informationsinteresses der Menschen
- Gebrauch des Netzes zu friedlichen Zwecken[5]
- Verfügbarkeit / Zugang, Vertraulichkeit, Integrität und Authentizität
- Entwicklung einer Cyber-Sicherheitskultur
- Verpflichtung zum Schutz kritischer Informationsinfrastrukturen
- Verpflichtung zur Bekämpfung von Schadprogrammen und von Missbrauch des Cyberraums für kriminelle und terroristische Zwecke
- Zusammenarbeit von Regierungen bei der Rückverfolgung von Cyber-Attacken

Vorschläge / Maßnahmen:
Um Staaten in ihrem Verhalten näher an die Beachtung der oben aufgeführten Prinzipien heranzuführen, hat die Bundesregierung im G8-Rahmen **Vorschläge für vertrauensbildende Maßnahmen** eingebracht, die in die G8-Erklärung von Deauville eingeflossen und weiter Gegenstand der internationalen Diskussion sind:

- Austausch von nationalen Strategien und „best practices"
- Austausch nationaler Standpunkte zu internationalen rechtlichen Normen
- Einrichtung und Notifizierung von Ansprechpartnern („points of contact")
- Frühwarnmechanismen und die Stärkung von Zusammenarbeit u. a. zwischen Computer Emergency Response Teams (CERTs)[6]
- Herstellung von Krisenkommunikationsverbindungen zur Erfassung von Cyber-Zwischenfällen

---

4) Zur Weiterentwicklung dieses Gedankens hat das AA einen Projektvorschlag zur Finanzierung im Rahmen der Europäischen Sicherheitsforschung eingebracht.
5) Diese Formulierung schließt die Nutzung des Cyberraums bei völkerrechtlich legitimierten militärischen Operationen nicht aus.
6) Computer Emergency Response Teams (CERT) werden von Regierungen, aber auch von Branchen unterhalten, um z. B. bei Bekanntwerden neuer Sicherheitslücken oder neuartiger Virenverbreitung Warnungen herauszugeben und Lösungsansätze anzubieten. CERT der Bundesregierung ist seit dem 1. September 2001 das CERT-Bund des Bundesamts für Sicherheit in der Informationstechnik (BSI).

- Entwicklung von technischen Empfehlungen zur Einrichtung robuster und sicherer globaler Cyber-Infrastruktur
- Verantwortung zur Bekämpfung von Terrorismus einschl. Austausch von Vorgehensweisen und verbesserter Kooperation beim Umgang mit nichtstaatlichen Akteuren
- Unterstützung von Fähigkeiten in Entwicklungsländern
- Cyber-Sicherheitsunterstützung für Großereignisse, z. B. Olympische Spiele

Die Bundesregierung verfolgt dabei einen schrittweisen, pragmatischen Ansatz, der mit Transparenzmaßnahmen und Vertrauensbildung beginnt. Zunächst ist über Prinzipien und Maßnahmen zu verhandeln, die politisch in einer möglichst großen Zahl von relevanten Staaten vermittelbar sind. Darauf aufbauend sollen möglichst weiterreichende konkrete Verpflichtungen vereinbart werden. Der Ansatz, alle Aspekte in einem umfassenden Regelwerk zu erfassen, erscheint zum gegenwärtigen Zeitpunkt wenig erfolgversprechend.

3. Deutsches Engagement im internationalen Diskurs

Die internationale Berliner Cyber-Sicherheitskonferenz hatte als weiteres Ergebnis, dass es für den notwendigen internationalen Diskurs keinen Königsweg im Sinne eines einzigen, ideal geeigneten Forums gibt.
Die Bundesregierung hat die o. g. Vorschläge für vertrauens- und sicherheitsbildende Maßnahmen (VSBM) außer in den G8 auch im 1. Ausschuss der VN-Generalversammlung und in der OSZE eingebracht. Die Bundesregierung unterstützt ebenso wie die USA das auf der Londoner Cyber-Konferenz (1./2. Nov. 2011) erklärte Ziel, binnen eines Jahres erste Ergebnisse zur Vereinbarung von VSBM zu erzielen und dazu die Kräfte gleichgesinnter Staaten zu bündeln, die unser Verständnis von Offenheit, Transparenz, Freiheit und Sicherheit im Cyberraum teilen. Zugleich muss nach Auffassung der Bundesregierung die Debatte von Anfang an unter Einbindung aller wichtigen Akteure geführt werden. Dazu gehören neben den Zivilgesellschaften auch die Regierungen der Staaten, die eine andere Auffassung von Freiheit und Sicherheit im Cyberraum vertreten.

Vor diesem Hintergrund wird die Bundesregierung

- sich weiterhin, und im engen Schulterschluss besonders mit den USA, Großbritannien und Frankreich, für die Herausbildung von Normen und Regeln für verantwortliches staatliches Verhalten im Cyberraum sowie für VSBM für den Cyberraum engagieren; wir arbeiten aktiv in der OSZE mit und setzen uns weiter für die rasche Schaffung einer OSZE-Cyber-AG ein, stellen 2012 erneut ein Mitglied in der Gruppe der Regierungsexperten in den Vereinten Nationen (VN) und setzen die Impulse der Internationalen

Berliner Cyber-Sicherheitskonferenz u. a. durch Folgeprojekte mit dem VN-Forschungsinstitut für Abrüstung zur Schaffung internationaler Transparenz über militärische Cyberfähigkeiten um;

- den Dialog mit anderen wichtigen Akteuren suchen; nach den drei Treffen im Quad-Rahmen (Deutschland, USA, Frankreich, Großbritannien) und den bilateralen Cyber-Konsultationen mit den USA, die bereits 2011 stattgefunden haben, sollen im 1. Quartal 2012 bilaterale Cyber-Konsultationen mit Russland und im 2. Quartal mit China stattfinden;
- regelmäßige Konsultationen zu Cyber-Sicherheit mit anderen Schlüsselstaaten, wie Indien, Brasilien und Südafrika, anstreben;
- sich an der Diskussion um das Für und Wider völkerrechtlich verbindlicher Regelungen beteiligen. So ist das Übereinkommen des Europarates über Computerkriminalität Beleg dafür, dass ein völkerrechtliches Instrument bestimmte Fragen der Cyberthematik erfolgreich regeln kann. Demgegenüber sind völkerrechtliche Verträge nach dem Muster der Abrüstung und Rüstungskontrolle für den Cyberraum nicht erfolgversprechend, schon weil die Implementierungs- und Verifikationsprobleme derzeit kaum lösbar erscheinen;
- den Dialog mit Wirtschaft und Zivilgesellschaft fortsetzen.

4. Schlussfolgerungen für unsere Positionierung in zwischenstaatlichen und internationalen Organisationen

4.1. Europäische Union

Der Grundsatz, dass nationale Eigenverantwortung keinen Widerspruch zu verstärkter grenzübergreifender Zusammenarbeit und Harmonisierung darstellt, gilt im besonderen Maße für die EU. Die EU verfügt - anders als die NATO - über Mechanismen, technische Standards in Bezug auf die Industrie verbindlich zu vereinbaren. Dies kann auch der Rahmen sein, um künftige internationale Verhaltensstandards in Kooperation mit der Industrie EU-weit zur Anwendung zu bringen. Dies gilt nicht nur mit Blick auf die Netzsicherheit, sondern auch mit Blick auf IT-Infrastrukturen, Interoperabilität, Produktsicherheit, Datenschutz, Urheberrechte. Die Bundesregierung begrüßt, dass die EU im Vorfeld der Londoner Konferenz vom 2. November mit der Abstimmung gemeinsamer Grundpositionen für den Cyberraum begonnen hat.

Die Bundesregierung setzt sich in der EU dafür ein, dass

- Cyber-Themen weiterhin grundsätzlich in den fachlich zuständigen Direktionen und Ratsausschüssen diskutiert werden; zugleich muss der wachsenden sicherheitspolitischen Bedeutung im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik und durch den Europäischen Auswärtigen Dienst (EAD) adäquat Rechnung getragen werden.

- die Zuständigkeiten innerhalb der EU-Strukturen gebündelt und besser sichtbar gemacht werden;

- das Mandat der europäischen IT-Sicherheitsagentur ENISA maßvoll erweitert wird, nicht nur mit Blick auf den Schutz der EU-Netze, sondern auch, damit ENISA sich stärker für gemeinsame Übungen der EU-MS (ggf. mit Partnern) engagieren und einzelnen Mitgliedstaaten auf Anfrage Hilfe leisten kann.

- die EU ihre aktive Rolle in der transatlantischen Zusammenarbeit ausbaut. Sie begrüßt, dass EU und USA am 3. November 2011 eine erste gemeinsame Cyber-Sicherheits-Übung[7] unter Beteiligung von 20 Mitgliedstaaten der EU durchgeführt haben.

---

7) „Cyber Atlantic 2011" ist ein Element der EU-US Arbeitsgruppe zu Cyber-Sicherheit und Kriminalität, die beim EU-US-Gipfel im November 2010 eingerichtet worden war.

- dass der Transatlantische Wirtschaftsrat (TEC) im Rahmen seines Schwerpunktbereichs Informations- und Kommunikationstechnik (IKT) gemeinsame Standards im Internet für Unternehmen festlegt. Eine frühzeitige transatlantische Einigung auf Mindesterfordernisse bei Sicherheit und Datenschutz soll zudem neue nichttarifäre Handelshemmnisse vermeiden helfen

4.2. NATO

Die **NATO** identifiziert Cyber-Sicherheit in ihrem 2010 beschlossenen Strategischen Konzept als eine der wesentlichen neuen sicherheitspolitischen Herausforderungen. Im Kreis der internationalen Organisationen ist die Allianz mit der im Juni 2011 verabschiedeten "NATO Cyber Defence Policy" und dem seit September 2011 in Umsetzung befindlichen Aktionsplan vergleichsweise weit fortgeschritten. Dabei genießt die Verbesserung des Schutzes der NATO-Netzwerklandschaft (bündniseigene und daran angeschlossene nationale Netze) vor Cyber-Angriffen oberste Priorität. Zur langfristigen Verbesserung der Cyber-Sicherheit sieht die "Cyber Defence Policy" eine Zusammenarbeit mit anderen internationalen Organisationen und Partnerstaaten der NATO vor. Ein erstes Treffen zum Thema Cyber-Sicherheit mit einigen ausgewählten Partnerstaaten, die auf vergleichbarem technischen Niveau liegen, gemeinsame Werte und Herangehensweisen an Cyber-Sicherheit mit den Verbündeten teilen und Interesse an einer Zusammenarbeit bekundet haben, fand im November 2011 statt.

Die Bundesregierung setzt sich dafür ein, dass

- der NATO "Cyber Defence Action Plan" zügig umgesetzt wird;
- die Praxis der NATO-Cyber-Übungen verstetigt, auf alle Verbündeten, geeignete Partnerstaaten sowie die EU ausgeweitet und vertieft wird;
- die NATO ihre Partnerschaftspolitik nutzt, um zur Vertrauensbildung im Cyber-Raum beizutragen;
- das NATO Cooperative Cyber Defence Centre of Excellence in Tallinn verstärkt genutzt und entspr. den Bedürfnissen der beitragenden Nationen fortentwickelt wird.

4.3. Vereinte Nationen

4.3.1. Im Rahmen des **1. Ausschusses der VN-Generalversammlung** hat Deutschland seine Kandidatur für die Gruppe der Regierungsexperten für Cyber-Sicherheit 2012 frühzeitig angemeldet und wurde bereits vom VN-Generalsekretär aufgefordert, wie bereits 2005 und 2010 auch 2012 einen der 15 Experten zu stellen. Diese Expertengruppe hatte 2010 einen u. a. zwischen USA, Russland und China abgestimmten Kompromissbericht verabschiedet. Daher besteht die Hoffnung, in diesem Gremium weitergehende Verständigungen auf dem Wege zu VSBM zu erzielen.

4.3.2. Im **VN-Sicherheitsrat** (SR) haben viele Mitgliedstaaten grundsätzliche Vorbehalte gegen SR-Befassung mit Themen, die in Ausschüssen der Generalversammlung behandelt werden. Die Bundesregierung wird jedoch weiter sondieren, welche Aspekte des Themas sich für eine thematische Debatte des SR eignen.

4.3.3. Die Bundesregierung beteiligt sich aktiv an den Arbeiten der **VN-Verbrechensverhütungskommission**. Die 1. Sitzung der 2010 im VN-Rahmen beschlossenen Expertengruppe für Computerkriminalität hat zunächst eine Studie über Art und Ausmaß internetbasierter Verbrechen in Auftrag gegeben. Nach Auffassung der Bundesregierung sollen Ansätze für neue Regelungswerke dort entwickelt werden, wo tatsächlich Regelungsbedarf festgestellt wird. Die Bundesregierung ist daher weiterhin skeptisch gegenüber Bestrebungen seitens Russlands und mehrerer Entwicklungs- bzw. Schwellenländer, eine VN-Konvention zu Computerkriminalität ins Leben zu rufen. Das umfassende Übereinkommen über Computerkriminalität des Europarats deckt alle bislang operationalisierbaren Aspekte ab und ist offen für einen Beitritt auch nicht-europäischer Staaten.

4.3.4. Im Nachgang zu dem von den VN unterstützten **Weltgipfel zur Informationsgesellschaft** (WSIS) wird derzeit die „Tunis-Agenda" abgearbeitet und mit jährlichen Fortschrittsberichten dokumentiert. Der Wirtschafts- und Sozialrat **ECOSOC** hat dabei der "Commission on Science and Technology for Development" (CSTD) und der 2006 gegründeten "United Nations Group on the Information Society (UNGIS) koordinierende Funktionen zugewiesen. Das durch den WSIS initiierte jährliche **Internet Governance Forum** (IGF) ermöglicht lebhaften Austausch zwischen Regierungen, internationalen Organisationen, Verbänden, NGOs, Wissenschaftlern, engagierten Bürgerinnen und Bürgern und der Wirtschaft.

Die Bundesregierung nimmt ressortübergreifend am IGF teil. Der Multistakeholder-Prozess bietet eine gute Möglichkeit, allgemeine und aktuelle Themen auch der Cybersicherheit mit anderen Staaten, Unternehmen, NGOs,

Wissenschaftlern und engagierten Bürgern aus aller Welt zu erörtern. Der offene, innovative und diskussionsorientierte Ansatz des IGF sollte erhalten bleiben. Zurückhaltend verhält sich die Bundesregierung gegenüber Bestrebungen, die zentrale Funktion der "Internet Corporation for Assigned Names and Numbers" (ICANN) bei der Internetverwaltung zu relativieren. Das bestehende System der Verwaltung durch eine Nichtregierungsorganisation mit einem Regierungsbeirat (Governmental Advisory Committee) hat sich als effizient bewährt.

4.3.5. Die **Internationale Fernmeldeunion (ITU)** beschäftigt sich als VN-Sonderorganisation mit 193 Mitgliedsstaaten mit Fragen der Standardisierung, der internationalen Koordinierung von Funkfrequenzen und der Entwicklungszusammenarbeit im Bereich der Telekommunikation. Traditionell ermöglicht die ITU auch die Mitgliedschaft privater Unternehmen aber auch wissenschaftlichen Einrichtungen. Sie stellt Entwicklungsländern best-practice Modelle für Cyber-Sicherheit zur Verfügung. Das Thema Cyber-Sicherheit wird u. a. in der Studiengruppe 17 bearbeitet, wo unter Beteiligung der europäischen IT-Sicherheitsagentur ENISA ein Fahrplan zur Verbesserung der Sicherheitsstandards bei der Informations- und Telekommunikationstechnologie fortgeschrieben wird. Hier geht es um Fachthemen wie "Lücken in Standards zur Widerstandsfähigkeit von Kommunikationsnetzwerken" und Empfehlungen für künftige Standardisierungsaktivitäten.
Die Bundesregierung unterstützt die wichtige Rolle der ITU hinsichtlich der technischen Aspekte von Cyber-Sicherheit, besonders durch Setzen von Standards; sie ist jedoch, gemeinsam mit vielen europäischen Ländern und den USA, grundsätzlich gegen eine Aufgabenausweitung der ITU nicht nur auf Internet-Governance, sondern auch auf Fragen der Cyber-Sicherheit, die über das technisch geprägte Mandat hinausgehen. Danach sollten etwa Fragen der Internetkriminalität, zu Internetinhalten oder zur nationalen Verteidigung grundsätzlich nicht im Rahmen der ITU behandelt werden.

4.4. Internationales Komitee des Roten Kreuzes und Völkerrechtskommission

Das **Internationale Komitee des Roten Kreuzes (IKRK)** hat im Rahmen der 31. gemeinsamen Konferenz mit dem Roten Halbmond Ende November 2011 **die Anwendbarkeit des humanitären Völkerrechts auf den Cyberraum** thematisiert. Hierzu hat das IKRK der Konferenz einen Bericht unter dem Titel "International Humanitarian Law and the challenges of contemporary armed conflicts" (Humanitäres Völkerrecht und die Herausforderungen moderner bewaffneter Konflikte) vorgelegt, dessen Kapitel über Methoden und Mittel der Kriegsführung einen besonderen Schwerpunkt auf Cyberoperationen legt. Das Auswärtige Amt unterstützt diese Meinungsbildung durch Förderung eines Projekts des VN-Instituts für Abrüstungsforschung (UNDIR).

Die Frage der **Staatenverantwortlichkeit für die Cyberangriffe von Privatpersonen** ist noch nicht abschließend geklärt. Die Bundesregierung hält es für sinnvoll, dass die **Völkerrechtskommission (ILC)** sich mit dieser Thematik befasst.

4.5. OSZE

Die Konferenz der **Organisation für Sicherheit und Zusammenarbeit in Europa** (OSZE) zur Cyber-Sicherheit im Mai 2011 zeigte, dass zahlreiche Staaten die OSZE mit ihren Erfahrungen in blockübergreifender Rüstungskontrolle und Vertrauensbildung als geeigneten Rahmen sehen, VSBM auch für den Cyber-Raum zu entwickeln. Allerdings bestehen innerhalb der 56 OSZE-Teilnehmerstaaten sehr unterschiedliche Auffassungen über das Spannungsfeld zwischen Netzsicherheit und Informationsfreiheit. Ein geplanter Beschluss des OSZE-Ministerrats in Wilna (06./07.12.2011), der eine Arbeitsgruppe "Cyber-Sicherheit" begründen sollte, um eine Liste möglicher VSBM zu erarbeiten, scheiterte an Definitionsfragen, denen letztlich entgegengesetzte Interessen besonders der USA und Russland zu Grunde lagen ("Informationssicherheit", Nicht-Einmischung).
Die Bundesregierung wird sich dafür einsetzen, dass die Arbeiten im Rahmen der OSZE fortgeführt werden, auch mit Blick auf einen möglichen Modellcharakter für globale Regelungen.

Konkret sollen folgende Maßnahmen vorangebracht werden:

1) Transparenzmaßnahmen:
- Informationsaustausch zu anwendbarem Völkerrecht;
- Informationsaustausch zu Organisationsstrukturen, Strategien und Ansprechpartnern;
- Austausch von Weißbüchern, evtl. Doktrinen im Cyberbereich

2) Risikoverminderungs- und Stabilitätsmaßnahmen:
- Krisenkommunikationskanäle einrichten oder verstärken;
- Zusammenarbeit von CERTs[8] (Computer Emergency Response Teams) einrichten;
- Gemeinsame Übungen zu simulierten Cybervorfällen durchführen.

8) vgl. Fußnote 5)

4.6. Europarat

Das wegweisende Übereinkommen des Europarats (EuR) über Computerkriminalität, dem auch Nicht-Mitgliedstaaten des EuR beitreten können, wurde bislang von 32 Staaten ratifiziert und weiteren 15 gezeichnet. Ca. 100 Staaten nutzen es als Modell für ihre nationale Gesetzgebung. Der EuR erarbeitet zudem Völkerrechtsnormen und politische Handlungsempfehlungen zum Schutz der Menschenrechte sowie zur Achtung rechtsstaatlicher und demokratischer Prinzipien im Internet.
Die Bundesregierung setzt sich aktiv dafür ein, dass die vom EuR entwickelten Völkerrechtsnormen von möglichst vielen Staaten ratifiziert und implementiert werden.
Derzeit wird eine Strategie zu "Internet Governance" abgestimmt, die alle Maßnahmen des Europarats für den Zeitraum 2012 - 2015 bündelt. Sie soll im Januar 2012 vom Ministerkomitee beschlossen werden. Im Fokus stehen Maßnahmen wie die Entwicklung eines Rechtsinstruments zum Zugang zum Internet, einer Charta mit Rechten für Internet-Nutzer und, in Zusammenarbeit mit der EU, die Modernisierung des Übereinkommens zum Datenschutz.

4.7. OECD

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) hat neben Grundsätzen und Empfehlungen für die Wirtschaft im Bereich der Informations- und Kommunikationstechnologien auch solche für Netzpolitik erarbeitet. Der dafür zuständige Fachausschuss (Committee for Information, Computer and Communications Policy, CICCP), hat eine Arbeitsgruppe "Working Party on Information Security and Privacy" beauftragt, sich neben Datenschutzrechtlichen Aspekten auch mit Cyber-Sicherheit zu befassen. Diese Arbeitsgruppe entwickelt Modelle zur Stärkung des Vertrauens in die Internetwirtschaft. Dies betrifft derzeit insbesondere Fragen des Schutzes der kritischen Informationsinfrastrukturen, des Identitätsmanagements, der Abwehr von Schadsoftware, des Schutzes Minderjähriger online, von Sensornetzwerken sowie Fragen des Datenschutzes. Die Bundesregierung unterstützt das besondere Anliegen der OECD, dass Verbesserungen der Cybersicherheit nicht dazu führen dürfen, dass die globalen offenen Netze eingeschränkt werden oder protektionistischen Absichten Vorschub geleistet wird.

Referat IT3
Dr. Pilgermann (-1527)

22.05.2012

[redacted]

Ziel der Behandlung: *Sicherung der Unterstützung der Ressorts beim weiteren Vorgehen, da BMI sich in koordinierender Funktion beim KRITIS-Schutz grdsl. im Kompetenzbereich der Fachressorts bewegt; insb. Stimmungsbild bzgl. gesetzlicher Regelungen einfangen und Boden für entsprechende Verhandlungen bereiten.*

Sachstand

Mit Sitzung des CyberSR vom 18.11. wurde mittels Zustimmung zu einem Grundsatzpapier des BMI diesem eine koordinierende Funktion eingeräumt. Die Ergebnisse der letzten Sitzung wurden folgendermaßen abgearbeitet:

- Branchenübergreifende IT-Sicherheitsstandards sind allgemein bekannt; als Mindeststandard ist etwas Vergleichbares in Deutschland jedoch nicht gesetzlich festgeschrieben. IT Grundschutz, ISO-Normen 27001
- Die Verfügbarkeit/Umsetzung branchenspezifischer Mindestsicherheits-anforderungen sowie gesetzl. Verankerung in Aufsichtsnormen wurde von BMI gemeinsam mit den Ressorts aufgearbeitet. Die äußerst unterschiedlichen Niveaus über die Branchen führen nicht zuletzt zur Notwendigkeit, dies im ITSG (s.u. und Sz. Sonstiges) mit abzubilden.
- Die Sektoren-/Branchenübersicht mit Zuordnung entsprechender Bundesaufsichtsbehörden und zuständiger Ressorts wird im Rahmen der Ressortabstimmungen kontinuierlich weiterentwickelt und dient auch als Grundlage für die Mitwirkung von Ressorts bei den Ministergesprächen (s.u.).

In konkreter Ausgestaltung treibt BMI den IT-Schutz Kritischer Infrastrukturen folgendermaßen voran:

- Herr Minister Dr. Friedrich entschied im März 2012, selbst Gespräche mit Betreibern Kritischer Infrastrukturen und deren Verbänden zu führen. Die Ressorts wurden zeitnah auf Arbeitsebene informiert; zudem werden jeweils zeitgleich mit den Einladungsschreiben von Herr Minister an die Wirtschaftsvertreter von Fr. Stn Rogall-Grothe Schreiben an die zuständigen Staatssekretäre in den Fachressorts mit der Bitte um Mitwirkung bei den Gesprächen versendet.

- Bei der Erarbeitung von Optionen für ein IT-Sicherheitsgesetz ist der IT-Schutz Kritischer Infrastrukturen ein elementares Modul, welches nach aktuellem Stand 3 Bestandteile haben sollte:
    - Einrichtung des BSI als zentrale Stelle in der Bundesregierung für Fragen IT-Schutz KRITIS
    - Festschreibung Mindestanforderungen an IT-Sicherheit
    - Verpflichtung der Betreiber zur Meldung schwerer Vorfälle und Ausbau von Meldewegen.
- Aktiv wird die Kooperation im Rahmen des Umsetzungsplan KRITIS (UPK) weiterentwickelt:
    - Eine eigens dafür eingerichtete Unter-Arbeitsgruppe (UAG) schreibt den inzw. 5 Jahre alten UPK im Hinblick zur inhaltlichen aber auch organisatorischen Weiterentwicklung bis Ende 2012 fort. Deutlich wird bereits, dass in Zukunft der KRITIS-Schutz ganzheitlich im UPK bearbeitet (neben Hauptschwerpunkt IT-Schutz auch physischer Schutz) und die Struktur schlanker und agiler gemacht werden soll.
    - Um die strategische Ausweitung des Teilnehmerkreises belastbar durchzuführen, wurden Aufnahme-Kriterien für den UPK erarbeitet und auf der Sitzung der Arbeitsgruppen des UPK Mitte Mai verabschiedet. Auf dieser Basis wird nun die Abdeckung über die Branchen mittels Aufnahme neuer Mitglieder in naher Zukunft sichergestellt.

Regelmäßig (alle 2-3 Monate) führt BMI Ressort-Abstimmungen zu IT-Schutz KRITIS auf Arbeitsebene durch. In diesem Rahmen wurde Ende März u.a. der Anstoß für die Anbindung der Aufsichtsbehörden auf Bundesebene an das CyberAZ getätigt.

Gesprächsführungsvorschlag:

1) Sensibilisierung für das Thema

- verschärfte Bedrohungslage
    - Verweis auf Vortrag Hr. Hange; zudem jüngste Ausfälle: Anfang 2012 Mobilfunknetz von V[redacted] für mehrere Tage zu weiten Teilen ausgefallen; KW21 massive Störung bei S-Bahn Berlin zurückzuführen auf IT-Probleme (ohne Angriff))
- Weitreichende Abhängigkeiten zwischen den Kritischen Infrastrukturen:
    - Aufarbeitung im Rahmen einer Studie aktuell im UPK im Abschluss; demnach höchstgradigste Abhängigkeit von Energie- und IKT-Versorgung
    - Folge ist enorme Verschachtelung und Komplexität, bei welchen sich keiner mehr für Sicherheit des Gesamtsystems verantwortlich fühlt (Bsp.: Liberalisierung bei Energieversorgung, wo organisatorische Trennung von Erzeugung und Transport explizit gefordert wird)
- Schutz Kritischer Infrastrukturen als Priorität in Cybersicherheitsstrategie und regelmäßig auf CyberSR-Agenda

2) Rückblick auf Aktivitäten

- Kooperation im UPK aktiv vorangetrieben und weiterentwickelt:
    - Mit kürzlich erfolgter Verabschiedung von Aufnahmekriterien wird nun strategische Ausweitung um unterrepräsentierte Branchen umgesetzt.
    - Arbeiten der UAG Fortschreibung halten an; Ergebnisse bis Ende 2012 erwartet – hohe Motivation aller Teilnehmer zur Fortführung und Mitgestaltung des neuen UPK
- Cybersicherheitslage erfordert Adressierung des KRITIS-Schutzes auf höchster Ebene; Minister-Entscheidung, selbst Gespräche mit Betreibern und Verbänden zu führen:
    - Geplant insges. 6 Gespräche mit 7 Sektoren (~~Termine in~~ Ressorts bekannt)
    - Minister lädt Vorstandsvorsitzende der Betreiber und entsprechende Vertreter aus den Verbänden unter Bezug auf entsprechend beigefügtes Diskussionspapier ein; Diskussionspapier als Erstaufschlag, welcher in Diskussionen weiterentwickelt werden soll

- Gespräche gemeinsam mit den verantwortlichen Hausleitungen der Fachressorts (Schreiben Frau Stn Rogall-Grothe jeweils im Vorfeld mit konkreten Informationen)
- Bislang zwei Gespräche (Finanzen/Versicherungen und IKT) geführt: offene, konstruktive Diskussion; am Ende Bitte von Herr Minister zur schriftlichen Stellungnahme einer jeden Branche zum Diskussionspapier

3) Ausblick / weiteres Vorgehen

- Abschluss der Gespräche mit den Betreibern bis Ende August
- Im Anschluss: Abarbeitung und Fortentwicklung des Diskussionspapiers im UPK
- Parallel: Evaluierung der Regelungsgrundlagen gemäß Auftrag Cybersicherheitsstrategie hält unter Einbindung der Fachressorts an; Minister behält sich Entscheidung für nach den Gesprächen im Herbst 2012 vor
  - Verweis auf TOP Sonstiges mit weiteren Informationen zum Thema

Man sollte schon jetzt ändern, dass wir die Wirtschaft sehr unterschiedlich antgestellt sehen und im Jahr 5 nach Beschluss UP KRITIS schon zweifel haben, ob die freiwillige Kooperation reicht. USA ist zu dem Schluss gekommen, dass das nicht reicht.

musste. **Die TCG hat eine neue Version entwickelt und beabsichtigt diese im Laufe des Jahres 2013 als ISO-Standard zu veröffentlichen.** Alle in der TCG zusammengeschlossen Unternehmen haben bekundet, die TPMs nach diesem neuen Standard herzustellen und in die Geräte einzubauen. Dies bedeutet, dass in Zukunft Geräte mit einem aktivierten TPM auf den Markt kommen werden.

2010 stellte M[redacted] eine end-to-end-trust-Vision vor. Basis dieser Verbindungen sind sichere Authentifizierungen, wie z. B. mit dem nPA und dem neuen TPM. Sollte es M[redacted] auf dieser Basis gelingen, vertrauenswürdige Umgebungen aufzubauen, **könnte** dies der **weltweite Durchbruch für die TC-Technologie sein**. Bisher erfolgt zwar ein großflächiger Einbau der TPMs aber es gibt, abgesehen von einigen unternehmensinternen Netzen, keine größeren Anwendungen.

Mit der neuen Version gehen mit dem potentiellen Sicherheitsgewinn allerdings **Kontrollverluste für den Nutzer** einher. Mit Unterstützung des TC-Moduls können Hersteller Rechner so einrichten, dass das Ausführen anderweitiger (z.B. herstellerfremder) Programme unterbunden wird. Das bisher verfolgte Prinzip des Universal-Computers würde aufgegeben, Systeme für bestimmte Einsatzzwecke könnten eingeführt werden.

Letztinstanzlich unterliegen aber auch immer alle Daten auf einem IT-Gerät primär der Kontrolle desjenigen, der festlegen kann welche Software läuft. Wenn also Geräte-Eigentümer **nicht die volle Oberhoheit über ihre Informationstechnik** besitzen, also nicht bestimmen können, mit welcher Software auf die Daten zugegriffen wird, so verlieren die Eigentümer auch die Oberhoheit über die auf diesen Systemen verarbeiteten und gespeicherten Daten.

Für die **Bundesverwaltung** sind IT-Systeme, die über die Spezifikationen in der neuen Version verfügen, **nicht akzeptabel**. Die Bundesverwaltung muss weiterhin allein darüber entscheiden, was mit ihren Daten passiert. Dies gilt auch für den **Betrieb von kritischen Infrastrukturen**. Es ist fraglich, inwiefern diese Zielgruppe auch in Zukunft ausreichend Marktmacht innehat, um entsprechende IT-Systeme zu angemessenen Preisen erstehen zu können.

Secunet-Module

Für eine Vielzahl der kleinen und mittelständischen Unternehmen (**KMU**) und der **Bürger** könnten Systeme, die unter den Bedingungen der neuen Spezifikation arbeiten, ein Zugewinn an Sicherheit bedeuten. Es wird deutlich, dass die von diesem Personenkreis zurzeit umgesetzten IT- Sicherheitsmaßnahmen den Bedrohungen – insb. mit Blick auf zukünftige Entwicklungen – nicht angemessen begegnen können. Mit der neuen Version könnten die IT- Systeme perspektivisch sicherer gestaltet werden, weil sich Sicherheitsfunktionalitäten auf einen standardmäßig aktivierten **hardwareseitigen Sicherheitsanker** verlassen könnten. So würde es z. B. Hackern schwerer fallen, die IT-Systeme in ein Botnetz zu übernehmen.

Aus diesen Gründen war es notwendig, die Eckpunkte aus 2007 auf die neue Version der Spezifikation zu aktualisieren. **Die Bedeutung der Einflussnahme der Bundesregierung ist heute noch wichtiger als vor 4 Jahren, weil abzusehen ist, dass sich die Verwendung der TC-Technik über kurz oder lang in alle Bereiche der Informationstechnik ausbreiten wird.**

Im Gegensatz zum Eckpunktepapier 2007 ist jetzt eine **differenzierte Betrachtung** der TC-Technik notwendig. Es ist dabei zu **unterscheiden** zwischen einem **Privatanwender/ KMU** und der **öffentlichen Verwaltung/Kritische Infrastrukturen**. Der Einsatz für Privatanwender wird **begrüßt**, weil dadurch ein **Sicherheitsgewinn** erzielt werden kann. Für die **öffentliche Verwaltung lehnen** wir die Verwendung **ab**, weil durch die Verwendung des aktivierten TPMs die Kontrolle über die sich auf den Rechnern befindlichen Daten nicht mehr der alleinigen Kontrolle des Eigentümers befindet.

Das vorliegende Eckpunktepapier befindet sich in der Ressortabstimmung. Letzte Abstimmungen erfolgen derzeit. Als Anlage ist das Eckpunktepapier in der zur Abstimmung versandten Ausgangsversion beigefügt.

Gesprächsführungsvorschlag:

- Neue Spezifikationen der TCG werden in naher Zukunft veröffentlicht werden.
- Die hardwarebasierte Sicherheitstechnik der TCG wird **grundsätzlich begrüßt**.
- 2004 und 2007 wurde bereits Eckpunkte veröffentlicht, die von der TCG akzeptiert wurden.
- Kernpunkte des Eckpunktepapiers 2007:

  - Anforderungen an einen zu veröffentlichenden Standard (Verfügbarkeit, offen, für die Forschung geeignet),
  - Zertifizierung des TPM,
  - Entscheidungsfreiheit über den Einsatz und
  - internationale Zusammenarbeit.
- Durch die neuen Spezifikationen ist jetzt eine **Aktualisierung des Eckpunktepapiers** notwendig geworden.
- Kernpunkte des neuen Eckpunktepapiers sind:
  - Transparenz beim Privatanwender
  - Trennung der Interessenlage zwischen Privatanwender/KMU und öffentlicher Verwaltung/KRITIS
- Die neuen Versionen der TC-Technik haben sicherheits- und wirtschaftspolitische Implikationen; daher Diskussion des Eckpunktepapiers im Cyber-Sicherheitsrat
- **Sicherheitsbedenken** beim Einsatz in der Bundesverwaltung und Kritischen Infrastrukturen
  - **Bundesverwaltung** kann Rechner, die über ein eingeschaltetes TPM verfügen nicht einsetzen, weil
    - damit ein **Kontrollverlust** über ihre Daten einhergeht und
    - die **Verwendung anderer als der vom Hersteller vorgesehenen Software** eingeschränkt ist (siehe insbesondere Punkte 3, 4, 13, 14 und 15 des Eckpunktepapiers).
  - **Wirtschaftlicher Aspekt:** Wenn diese Versionen für den Massenmarkt produziert werden, wird Bundesverwaltung evtl. zum **Nischennachfrager**. Dies könnte dazu führen, dass der Einkauf eines Nischenproduktes **teurer** wird als der Einkauf eines Rechners aus dem Massenmarkt. Hier ist die Zusammenarbeit der öffentlichen Verwaltung gefragt, um genügend Nachfrage zu generieren. (z. B. durch Beschaffungsamt).
- **Wirtschaftspolitische Implikationen:** Auch im neuen Eckpunktepapier sind die Eckpunkte enthalten, die der deutschen Wirtschaft den Zugang zu und die Verwendung des Standards sichern werden. Dies ist umso wichtiger als in Zukunft damit zu rechnen ist, dass ein aktiviertes TPM in jedem Gerät vorhanden sein wird.
- Verbesserungen bei der IT-Sicherheit bei **Bürgern und KMU** durch Nutzung des TPM und der Verschlüsselungsmöglichkeiten **aber** absolute Transparenz und Hinweis auf die Konsequenzen hinsichtlich des Verlusts der alleinigen Verfügungsgewalt über die auf solcher Informationstechnik verarbeiteten und

gespeicherten Daten notwendig (siehe insbesondere Punkte 3, 5, 9, 10, 13, 14 und 17 des Eckpunktepapiers)

- Letzte Arbeiten im Rahmen der **Ressortabstimmung** werden vorgenommen
- Vorgesehen: Vorstellung des neuen Eckpunktepapiers im **IT-Rat** und im **IT-PLR**

VS-NfD

Eckpunktepapier „Trusted Computing" der Bundesregierung

April 2012

1. Begriffsbestimmung

Die Bundesregierung versteht unter „Trusted Computing" die Architekturen, Implementierungen, Systeme und Infrastrukturen, die auf den Standards der Trusted Computing Group (TCG) basieren oder diese nutzen. Zur Vermeidung von Missverständnissen wird eine darüber hinausgehende, allgemeinere Verwendung des Begriffs „Trusted Computing" stets besonders gekennzeichnet.

2. Erhöhung der IT-Sicherheit

Die Bundesregierung begrüßt und unterstützt eine Erhöhung des Niveaus der IT-Sicherheit auf IT-Plattformen von Unternehmen, öffentlicher Verwaltung und Privatanwendern durch die Einführung von „Trusted Computing"-Lösungen auf Grundlage der Standards der TCG, soweit beide die hier aufgeführten Eckpunkte erfüllen.

3. Oberhoheit des Geräte-Eigentümers

Ein Geräte-Eigentümer muss über die vollständige Kontrolle (Steuerbarkeit und Beobachtbarkeit) der gesamten „Trusted Computing"-Sicherheitssysteme seiner Geräte verfügen. Der Geräte-Eigentümer kann im Rahmen seiner Oberhoheit entscheiden, inwieweit er diese Kontrolle an seine Nutzer oder Administratoren delegiert. Muss der Geräte-Eigentümer diese Kontrolle vor einer Nutzung beim Erwerb oder später, teilweise oder ganz, an andere Dritte (Hardware- oder Software-Komponenten des Geräts oder dem Geräte-Hersteller) delegieren oder abtreten, so erfolgt dies ausschließlich im Rahmen einer bewussten und informierten Entscheidung (also u. a. in voller Kenntnis der möglichen Einschränkungen der Verfügbarkeit durch Maßnahmen dieser Dritter).

4. Öffentliche Verwaltung, nationale und öffentliche Sicherheitsinteressen

Der Betrieb und die Verfügbarkeit von Geräten in der öffentlichen Verwaltung und im Bereich der nationalen und öffentlichen Sicherheit bedingen die alleinige Kontrolle des Eigentümers über deren „Trusted Computing"-Sicherheitssysteme. Aufgrund der öffentlichen und nationalen Sicherheitsinteressen darf in keinem Fall der Eigentümer gezwungen werden, die Kontrolle eines „Trusted Computing"- Sicherheitssystems, in Gänze oder auch nur in Teilen, an andere Dritte außerhalb des Einflussbereichs der öffentlichen Verwaltung abzutreten.

5. Privater Bereich

Die Bundesregierung fordert Hersteller von „Trusted Computing"-Geräten und Komponenten (sowohl Software als auch Hardware) nachdrücklich auf, auch für den privaten Bereich solche Geräte und Komponenten anzubieten, die jederzeit dem Eigentümer die volle Kontrolle über das „Trusted Computing"-Sicherheitssystem einräumen.

6. Verfügbarkeit der Standards

Alle geltenden Standards zu „Trusted Computing" müssen unabhängig von einer Mitgliedschaft in der TCG für jedermann jederzeit kostenfrei und vollständig verfügbar sein. Ebenso müssen ggf. vorhandene erläuternde, konkretisierende oder

abgrenzende Sekundärdokumente der TCG jedem Interessierten frei zur Verfügung stehen.

7. **Offene Standards**
Unabhängig von einer Mitgliedschaft in der TCG müssen alle Standards zu „Trusted Computing" von jedermann vollständig zur Umsetzung in Architekturen, Implementierungen, Systemen und Infrastrukturen verwendet werden können. Für die Anwendungen der Standards dürfen keine Lizenzgebühren (z. B. aus Patentansprüchen) erhoben werden.

8. **Freiheit der Forschung**
Standards zu „Trusted Computing" sind so zu gestalten, dass die akademische Forschung zu „Trusted Computing"-basierten Lösungen und deren Zusammenspiel mit Alternativen nicht behindert wird. Die Bundesregierung fördert die unabhängige akademische Forschung zur Technik des „Trusted Computing" und deren Folgen.

9. **Interoperabilität**
Bei der Realisierung sicherer Plattformen muss der interoperable Einsatz von „Trusted Computing"-Lösungen mit alternativen Ansätzen jederzeit im Vordergrund stehen. Für den Einsatz in der Bundesverwaltung muss gewährleistet sein, dass „Trusted Computing"-Produkte sowohl mit anderen „Trusted Computing"-basierten als auch mit alternativen Lösungen interoperabel sind.

10. **Transparenz**
Sämtliche Standards, Lösungen und deren Erarbeitung im Bereich „Trusted Computing" sind transparent im Hinblick auf ihren tatsächlichen Zweck, ihre funktionalen Eigenschaften und verwendete kryptographische Techniken zu erstellen.

11. **Zertifizierung**
Jede „Trusted Computing"-Lösung auf Basis der Standards der TCG soll transparent, nachvollziehbar und für unterschiedliche Sicherheitsniveaus zertifizierbar sein. Das Trusted Plattform Module (TPM) als grundlegende Komponente muss mindestens eine Zertifizierung nach Common Criteria EAL4+ („resistant against moderate attack potential") aufweisen. Zertifizierungsansätze sollen dabei weder zum Ausschluss von Unternehmen, der akademischen Forschung oder Lösungen unter freien Lizenzen führen.

12. **Nationale IT-Industrie**
Die Bundesregierung sieht durch die „Trusted Computing"-Technik sowohl nationale Sicherheitsinteressen als auch die Wettbewerbsfähigkeit der deutschen IT-Sicherheitsindustrie betroffen. Die Bundesregierung fordert daher faire, transparente Wettbewerbsbedingungen für alle IT-Sicherheitsunternehmen und ruft deutsche Unternehmen auf, Produkte auf Basis der Standards der TCG anzubieten, sofern die Forderungen dieses Eckpunktepapiers erfüllt sind.

13. **Entscheidungsfreiheit**
Geräte-Eigentümer müssen in der Lage sein, aufgrund der vorausgesetzten technischen und inhaltlichen Transparenz von „Trusted Computing"-Lösungen eigenverantwortliche Entscheidungen zur Produktauswahl, Inbetriebnahme, Konfiguration, Anwendung und Stilllegung zu treffen. Eine Deaktivierung darf keine

negativen Einflüsse auf die Funktionalität der Hard- und Software haben, die nicht die Funktion der „Trusted Computing"-Technik nutzen.

14. **Gewährleistung der IT-Sicherheit**
„Trusted Computing" bietet aus Sicht der Bundesregierung einen wesentlichen Schritt zur Erreichung der IT-Sicherheitsziele, wie Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität. Jede eingesetzte „Trusted Computing"-Lösung ist auf die Einhaltung dieser geforderten Sicherheitsziele zu prüfen. Insbesondere darf die Verfügbarkeit nicht zwangsweise externer Kontrolle unterliegen und die Vertraulichkeit nicht durch unzureichende Verfügungsgewalt über eigene Schlüssel kompromittiert werden. Im Interesse der für die Beurteilung der IT-Sicherheit erforderlichen Transparenz ist es in jedem Fall wichtig, dass keine undokumentierten Funktionen enthalten sind, sowie eine Beeinflussung der TPM-Funktionalität durch andere Hardware-Komponenten oder -funktionalitäten ausgeschlossen ist. Insbesondere für den Einsatz in sicherheitskritischen Netzen (z. B. in der öffentlichen Verwaltung) können ausschließlich zertifizierte TPM zum Einsatz kommen. Diese Voraussetzung sieht die Bundesregierung derzeit lediglich bei diskreten TPM gegeben.

15. **Verfügbarkeit von Kritischen Infrastrukturen**
Der Einsatz von „Trusted Computing"-Lösungen bei Betreibern Kritischer Infrastrukturen muss so erfolgen, dass sich daraus keine zusätzlichen Risiken für kritische Prozesse ergeben – dies gilt insbesondere für das Sicherheitsziel Verfügbarkeit. Eine schnelle Infrastrukturwiederherstellung selbst im Rahmen von Krisen- und Katastrophenbewältigung muss unbehindert und flexibel erfolgen können.

16. **Schutz digitaler Werke**
Die Bundesregierung sieht eine wesentliche Funktionalität von „Trusted Computing" in einem nachhaltigen Schutz der mittels Informationstechnik (IT) gespeicherten, verarbeiteten und übertragenen digitalen Werke für jedermann. Dieser Schutz ist unter einer ausgewogenen, fairen Berücksichtigung der Interessen von Rechteinhabern und Besitzern (d. h. Nutzern) von Daten und den Geräten, auf denen diese verarbeitet werden, zu realisieren.

17. **Datenschutz**
Der Schutz personenbezogener Daten ist eine wichtige Voraussetzung für die Steigerung der Sicherheit im IT-Bereich. Daher sind die Bestimmungen des Datenschutzes bei „Trusted Computing"-Anwendungen zu berücksichtigen und haben aufgrund ihrer Ableitung aus grundgesetzlich verbrieften Rechten immer Vorrang vor wirtschaftlichen Interessen.

18. **Standardisierung**
Für einen breiten Einsatz der „Trusted Computing"-Technik ist es essentiell, diese zu standardisieren. Dies ist hauptsächlich eine Aufgabe der beteiligten Unternehmen. Darüber hinaus gestaltet die Bundesregierung den Standardisierungsprozess mit und achtet darauf, dass der Zugang zur Erstellung der Standards für deutsche Unternehmen, Forschungseinrichtungen und Interessengruppen fair, offen, angemessen und diskriminierungsfrei gestaltet wird. Die Beteiligung deutscher Organisationen wird unterstützt.

19. Internationale Zusammenarbeit

Nationale Alleingänge sind im Zeitalter der Globalisierung, insbesondere in Bezug auf die Informations- und Kommunikationstechnik, wenig Erfolg versprechend. Aus diesem Grund fordert die Bundesregierung deutsche Unternehmen und Organisationen zum Engagement in den Projekten zu „Trusted Computing", insbesondere aber in der TCG auf. Darüber hinaus arbeitet die Bundesregierung international aktiv mit staatlichen und nicht-staatlichen Organisationen zu Fragen des „Trusted Computing" zusammen, insbesondere um die in diesem Eckpunktepapier festgelegten Anforderungen an das „Trusted Computing"-Konzept zu realisieren. Die Bundesregierung bringt darüber hinaus die besonderen IT-Sicherheits-Anforderungen des öffentlichen Sektors in die TCG und andere Projekte und Initiativen zur „Trusted Computing"-Technik ein.

Loose, Katrin

Von: Spatschke, Norman
Gesendet: Freitag, 25. Mai 2012 17:23
An: [redacted]; Achatz, Reinhold, Dr.
Cc: [redacted]org'; Dürig, Markus, Dr.; StRogall-Grothe_; Engel, Simone
Betreff: TOP 5 der TO der 3. Sitzung des Cyber-SR am 31.5.2012
Anlagen: 120416_Eckpunktepapier TC_Ausgangsversion.doc

Sehr geehrte assoziierte Wirtschaftsvertreter im Cyber-SR,

im Auftrag von Frau Staatssekretärin Rogall-Grothe übersende ich Ihnen anliegend für den Hintergrund zu TOP 5 der Sitzung des Cyber-SR am 31.5. das Eckpunktepapier der Bundesregierung mit der Bitte um Kenntnisnahme.

Freundliche Grüße,
N. Spatschke
BMI - IT 3; -2045

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

VS-NfD

Eckpunktepapier „Trusted Computing" der Bundesregierung

April 2012

1. Begriffsbestimmung
Die Bundesregierung versteht unter „Trusted Computing" die Architekturen, Implementierungen, Systeme und Infrastrukturen, die auf den Standards der Trusted Computing Group (TCG) basieren oder diese nutzen. Zur Vermeidung von Missverständnissen wird eine darüber hinausgehende, allgemeinere Verwendung des Begriffs „Trusted Computing" stets besonders gekennzeichnet.

2. Erhöhung der IT-Sicherheit
Die Bundesregierung begrüßt und unterstützt eine Erhöhung des Niveaus der IT-Sicherheit auf IT-Plattformen von Unternehmen, öffentlicher Verwaltung und Privatanwendern durch die Einführung von „Trusted Computing"-Lösungen auf Grundlage der Standards der TCG, soweit beide die hier aufgeführten Eckpunkte erfüllen.

3. Oberhoheit des Geräte-Eigentümers
Ein Geräte-Eigentümer muss über die vollständige Kontrolle (Steuerbarkeit und Beobachtbarkeit) der gesamten „Trusted Computing"-Sicherheitssysteme seiner Geräte verfügen. Der Geräte-Eigentümer kann im Rahmen seiner Oberhoheit entscheiden, inwieweit er diese Kontrolle an seine Nutzer oder Administratoren delegiert. Muss der Geräte-Eigentümer diese Kontrolle vor einer Nutzung beim Erwerb oder später, teilweise oder ganz, an andere Dritte (Hardware- oder Software-Komponenten des Geräts oder dem Geräte-Hersteller) delegieren oder abtreten, so erfolgt dies ausschließlich im Rahmen einer bewussten und informierten Entscheidung (also u. a. in voller Kenntnis der möglichen Einschränkungen der Verfügbarkeit durch Maßnahmen dieser Dritter).

4. Öffentliche Verwaltung, nationale und öffentliche Sicherheitsinteressen
Der Betrieb und die Verfügbarkeit von Geräten in der öffentlichen Verwaltung und im Bereich der nationalen und öffentlichen Sicherheit bedingen die alleinige Kontrolle des Eigentümers über deren „Trusted Computing"-Sicherheitssysteme. Aufgrund der öffentlichen und nationalen Sicherheitsinteressen darf in keinem Fall der Eigentümer gezwungen werden, die Kontrolle eines „Trusted Computing"- Sicherheitssystems, in Gänze oder auch nur in Teilen, an andere Dritte außerhalb des Einflussbereichs der öffentlichen Verwaltung abzutreten.

5. Privater Bereich
Die Bundesregierung fordert Hersteller von „Trusted Computing"-Geräten und Komponenten (sowohl Software als auch Hardware) nachdrücklich auf, auch für den privaten Bereich solche Geräte und Komponenten anzubieten, die jederzeit dem Eigentümer die volle Kontrolle über das „Trusted Computing"-Sicherheitssystem einräumen.

6. Verfügbarkeit der Standards
Alle geltenden Standards zu „Trusted Computing" müssen unabhängig von einer Mitgliedschaft in der TCG für jedermann jederzeit kostenfrei und vollständig verfügbar sein. Ebenso müssen ggf. vorhandene erläuternde, konkretisierende oder

abgrenzende Sekundärdokumente der TCG jedem Interessierten frei zur Verfügung stehen.

7. **Offene Standards**
Unabhängig von einer Mitgliedschaft in der TCG müssen alle Standards zu „Trusted Computing" von jedermann vollständig zur Umsetzung in Architekturen, Implementierungen, Systemen und Infrastrukturen verwendet werden können. Für die Anwendungen der Standards dürfen keine Lizenzgebühren (z. B. aus Patentansprüchen) erhoben werden.

8. **Freiheit der Forschung**
Standards zu „Trusted Computing" sind so zu gestalten, dass die akademische Forschung zu „Trusted Computing"-basierten Lösungen und deren Zusammenspiel mit Alternativen nicht behindert wird. Die Bundesregierung fördert die unabhängige akademische Forschung zur Technik des „Trusted Computing" und deren Folgen.

9. **Interoperabilität**
Bei der Realisierung sicherer Plattformen muss der interoperable Einsatz von „Trusted Computing"-Lösungen mit alternativen Ansätzen jederzeit im Vordergrund stehen. Für den Einsatz in der Bundesverwaltung muss gewährleistet sein, dass „Trusted Computing"-Produkte sowohl mit anderen „Trusted Computing"-basierten als auch mit alternativen Lösungen interoperabel sind.

10. **Transparenz**
Sämtliche Standards, Lösungen und deren Erarbeitung im Bereich „Trusted Computing" sind transparent im Hinblick auf ihren tatsächlichen Zweck, ihre funktionalen Eigenschaften und verwendete kryptographische Techniken zu erstellen.

11. **Zertifizierung**
Jede „Trusted Computing"-Lösung auf Basis der Standards der TCG soll transparent, nachvollziehbar und für unterschiedliche Sicherheitsniveaus zertifizierbar sein. Das Trusted Plattform Module (TPM) als grundlegende Komponente muss mindestens eine Zertifizierung nach Common Criteria EAL4+ („resistant against moderate attack potential") aufweisen. Zertifizierungsansätze sollen dabei weder zum Ausschluss von Unternehmen, der akademischen Forschung oder Lösungen unter freien Lizenzen führen.

12. **Nationale IT-Industrie**
Die Bundesregierung sieht durch die „Trusted Computing"-Technik sowohl nationale Sicherheitsinteressen als auch die Wettbewerbsfähigkeit der deutschen IT-Sicherheitsindustrie betroffen. Die Bundesregierung fordert daher faire, transparente Wettbewerbsbedingungen für alle IT-Sicherheitsunternehmen und ruft deutsche Unternehmen auf, Produkte auf Basis der Standards der TCG anzubieten, sofern die Forderungen dieses Eckpunktepapiers erfüllt sind.

13. **Entscheidungsfreiheit**
Geräte-Eigentümer müssen in der Lage sein, aufgrund der vorausgesetzten technischen und inhaltlichen Transparenz von „Trusted Computing"-Lösungen eigenverantwortliche Entscheidungen zur Produktauswahl, Inbetriebnahme, Konfiguration, Anwendung und Stilllegung zu treffen. Eine Deaktivierung darf keine

negativen Einflüsse auf die Funktionalität der Hard- und Software haben, die nicht die Funktion der „Trusted Computing"-Technik nutzen.

14. **Gewährleistung der IT-Sicherheit**
„Trusted Computing" bietet aus Sicht der Bundesregierung einen wesentlichen Schritt zur Erreichung der IT-Sicherheitsziele, wie Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität. Jede eingesetzte „Trusted Computing"-Lösung ist auf die Einhaltung dieser geforderten Sicherheitsziele zu prüfen. Insbesondere darf die Verfügbarkeit nicht zwangsweise externer Kontrolle unterliegen und die Vertraulichkeit nicht durch unzureichende Verfügungsgewalt über eigene Schlüssel kompromittiert werden. Im Interesse der für die Beurteilung der IT-Sicherheit erforderlichen Transparenz ist es in jedem Fall wichtig, dass keine undokumentierten Funktionen enthalten sind, sowie eine Beeinflussung der TPM-Funktionalität durch andere Hardware-Komponenten oder -funktionalitäten ausgeschlossen ist. Insbesondere für den Einsatz in sicherheitskritischen Netzen (z. B. in der öffentlichen Verwaltung) können ausschließlich zertifizierte TPM zum Einsatz kommen. Diese Voraussetzung sieht die Bundesregierung derzeit lediglich bei diskreten TPM gegeben.

15. **Verfügbarkeit von Kritischen Infrastrukturen**
Der Einsatz von „Trusted Computing"-Lösungen bei Betreibern Kritischer Infrastrukturen muss so erfolgen, dass sich daraus keine zusätzlichen Risiken für kritische Prozesse ergeben – dies gilt insbesondere für das Sicherheitsziel Verfügbarkeit. Eine schnelle Infrastrukturwiederherstellung selbst im Rahmen von Krisen- und Katastrophenbewältigung muss unbehindert und flexibel erfolgen können.

16. **Schutz digitaler Werke**
Die Bundesregierung sieht eine wesentliche Funktionalität von „Trusted Computing" in einem nachhaltigen Schutz der mittels Informationstechnik (IT) gespeicherten, verarbeiteten und übertragenen digitalen Werke für jedermann. Dieser Schutz ist unter einer ausgewogenen, fairen Berücksichtigung der Interessen von Rechteinhabern und Besitzern (d. h. Nutzern) von Daten und den Geräten, auf denen diese verarbeitet werden, zu realisieren.

17. **Datenschutz**
Der Schutz personenbezogener Daten ist eine wichtige Voraussetzung für die Steigerung der Sicherheit im IT-Bereich. Daher sind die Bestimmungen des Datenschutzes bei „Trusted Computing"-Anwendungen zu berücksichtigen und haben aufgrund ihrer Ableitung aus grundgesetzlich verbrieften Rechten immer Vorrang vor wirtschaftlichen Interessen.

18. **Standardisierung**
Für einen breiten Einsatz der „Trusted Computing"-Technik ist es essentiell, diese zu standardisieren. Dies ist hauptsächlich eine Aufgabe der beteiligten Unternehmen. Darüber hinaus gestaltet die Bundesregierung den Standardisierungsprozess mit und achtet darauf, dass der Zugang zur Erstellung der Standards für deutsche Unternehmen, Forschungseinrichtungen und Interessengruppen fair, offen, angemessen und diskriminierungsfrei gestaltet wird. Die Beteiligung deutscher Organisationen wird unterstützt.

19. **Internationale Zusammenarbeit**

Nationale Alleingänge sind im Zeitalter der Globalisierung, insbesondere in Bezug auf die Informations- und Kommunikationstechnik, wenig Erfolg versprechend. Aus diesem Grund fordert die Bundesregierung deutsche Unternehmen und Organisationen zum Engagement in den Projekten zu „Trusted Computing", insbesondere aber in der TCG auf. Darüber hinaus arbeitet die Bundesregierung international aktiv mit staatlichen und nicht-staatlichen Organisationen zu Fragen des „Trusted Computing" zusammen, insbesondere um die in diesem Eckpunktepapier festgelegten Anforderungen an das „Trusted Computing"-Konzept zu realisieren. Die Bundesregierung bringt darüber hinaus die besonderen IT-Sicherheits-Anforderungen des öffentlichen Sektors in die TCG und andere Projekte und Initiativen zur „Trusted Computing"-Technik ein.

Loose, Katrin

Von:	Spatschke, Norman
Gesendet:	Freitag, 25. Mai 2012 16:17
An:	StRogall-Grothe_
Cc:	Dürig, Markus, Dr.; Dimroth, Johannes, Dr.
Betreff:	WG: Gesetzgebung CyberSicherheit US

Liebe Kollegen,
wie in heutiger R. erbeten übersende ich den anliegenden Vermerk zur Gesetzgebung in US.

12-02-21
zgebung Cybe

Freundliche Grüße,
N. Spatschke
BMI - IT 3; -2045

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

Referat IT 3
IT 3 606 000 - 2/3#2
Refl: Dr. Dürig
Ref: Dr. Dimroth

Berlin, den 21. Februar 2012
Hausruf: 1374/1993

Frau Stn Rogall-Grothe

über

Herrn IT D
Herrn SV IT D

Betr.: US-Gesetzentwurf zu Cyber-Sicherheit

1. Votum

Kenntnisnahme des og Entwurfs und Kurzbewertung hierzu.

2. Sachverhalt

Senatoren aus beiden Parteien haben in der 7. KW Woche ihren lang erwarteten umfassenden Gesetzentwurf zu Cybersicherheit vorgelegt. Herzstück des Entwurfs ist eine Regelung, wonach das Heimatschutzministerium (DHS) in einem mehrstufigen Verfahren in Zusammenarbeit mit Unternehmen festlegen soll, welche Teile der Infrastruktur als kritisch einzustufen. Für diese soll DHS sodann Sicherheitsanforderungen festlegen. Für Unternehmen, die diesen Anforderungen nicht entsprechen und nicht bereits Aufsichtsbehörden oder Industriestandards unterliegen, würde das DHS zusammen mit den Unternehmen Standards entwickeln. Unternehmen, die diese Erfordernisse nach einem Evaluierungsprozess weiterhin nicht erfüllen würden, könnten Geldstrafen auferlegt

werden. Auf der anderen Seite sollen Unternehmen, die die festgelegten Standards erfüllen, im Falle eines Angriffs von der Haftung befreit sein.

Folgende weitere Elemente sind im Gesetzgebungsvorschlag enthalten:

- Regelungen für einen verbesserten Informationsaustausch zu IT-Sicherheitsbedrohungen zwischen Behörden und der Wirtschaft. Vorgesehen ist, dass Unternehmen, bei denen ein Ausfall oder eine Störung der IT Systeme massive Folgen für die die Sicherheit der USA und ihrer Bevölkerung oder die US-Wirtschaft hätten, Regierungsstellen über Cyber-Vorfälle unterrichten müssen. Im Gegenzug sollen DHS, Verteidigungsministerium und Geheimdienst (DNI) relevante Bedrohungsinformationen in Echtzeit an die Unternehmen geben.
- Verbesserung der IT-Sicherheit im Bereich der Administration durch eine Reform des "Federal Information Security Act (FISMA)". DHS soll insoweit das Recht erhalten, im Falle eines Angriffs in Netze einzugreifen, auch wenn diese einer privaten Firma gehören.
- Bestimmungen zur Förderung von Forschung und Entwicklung im Bereich IT-Sicherheit.

Im Rahmen einer Anhörung am 16. Februar 2012 im Senatsausschuss für Homeland-Security and Government Affairs wurde deutlich, dass der Entwurf von Teilen der Republikaner aber auch von angehörten Sachverständigen insgesamt skeptisch beurteilt wird. Insbesondere wurde auf die drohenden Kosten für die Wirtschaft, auf die fehlende Eignung des DHS zur Abwehr von Cyberangriffen und auf datenschutzrechtliche Probleme hingewiesen.

3. Stellungnahme

Der Entwurf enthält einige Regelungsvorschläge, welche auch Gegenstand der hiesigen Überlegungen zu einem IT-Sicherheitsgesetz (IT-SiG) sind. Dies gilt insbesondere für den verbesserten Schutz der IT-Sicherheit im Bereich KRITIS und die insoweit vorgesehene enge Einbindung der betroffenen Branchen in die Erarbeitung der konkreten Vorgaben. Auch die Verbesserung des Informationsaustauschs soll grundsätzlich im IT-SiG

aufgegriffen werden. Überdenkens wert erscheint hierbei die Idee, auch die Behörden ihrerseits zu verpflichten, relevante Informationen an die Unternehmen zu geben. Regelungen zu behördlichen Befugnissen zum regelnden Eingriff in privat betriebene Netze sind hingegen für das IT-SiG wegen der hierzu noch offenen Fragen und wegen der besonderen Sensibilität solcher Vorschläge derzeit nicht vorgesehen.

Der weitere Fortgang des Gesetzgebungsverfahrens wird am Ende davon abhängen, ob sich Haus und Senat einigen. Entscheidend wird auch sein, ob es gelingt, die Internet-Community davon zu überzeugen, dass diese Gesetzesentwürfe grundsätzlich verschieden sind von den nach massiven Protesten auf Eis gelegten Gesetzentwürfe zum Schutz geistigen Eigentums (SOPA /PIPA).

In Vertretung

Dr. Dimroth

Kroll, Simone

Von: Spatschke, Norman
Gesendet: Dienstag, 29. Mai 2012 18:42
An: StRogall-Grothe_
Cc: ITD_; SVITD_; Engel, Simone; Dürig, Markus, Dr.; Mantz, Rainer, Dr.; IT3_
Betreff: Cyber-Sicherheitsrat, hier: aktualisierte Sz

Lieber Herr Franßen,
im Nachgang meiner Mail von Freitag übersende ich anliegende Informationen bzw. Sprechzettel mit der Bitte um Austausch in der Mappe.

Sprechzettel P-BSI (Kernpunkte des Vortrags), Bitte Fach 2 der Mappe zuordnen.
Hintergrund: Herr Hanebeck hatte BSI am Fr. gebeten, Kernpunkte des Vortrags an Frau Rogall zu übersenden. Eine Überarbeitung des Vortrags wurde nicht erbeten.

120531_3. yber-Sicherheitsrat.

Im Gesprächsführungsvorschlag geringfügig modifizierter Sz zu Cyber-Außenpolitik (Bitte Fach 3 zuordnen).
Hintergrund: AA hat auf Arbeitsebene Pläne zu 2. Cyber-Konferenz im September mitgeteilt. Zudem werde StS Haber für nächste Sitzung des Cyber-SR vorschlagen, die derzeitigen KOM-Bemühungen für mehr Cybersicherheit in den Fokus zu rücken.

TOP 2 Cyber Außenpolitik.docx

Bitte in Fach 5 den urspr. Sz ersetzen (war in R. so erbeten)

120529 Trusted Computing.docx

Zu TOP 6 (CERT-Strukturen der Länder):
Wie erbeten hat entsprechendes Telefonat mit HE (Hr. Jurk) stattgefunden. Die Länder begrüßen dieses TOP ausdrücklich und werden zu TOP 6 wie folgt vortragen:
- Hr. Zinell zu den CERT-Aktivitäten + Bemühungen des IT-PLR,
- Hr. Jurk zu IMK-Länder AG „Cybersicherheit" und Erfahrungen aus der Lükex vorstellen, die den Aufbau entsprechender Strukturen erforderlich scheinen lassen.

Freundliche Grüße,
N. Spatschke
BMI - IT 3; -2045

Helfen Sie Papier zu sparen! Müssen Sie diese E-Mail tatsächlich ausdrucken?

Von: Spatschke, Norman
Gesendet: Freitag, 25. Mai 2012 17:56
An: StRogall-Grothe_
Cc: ITD_; SVITD_; Dürig, Markus, Dr.; Engel, Simone
Betreff: Informationspunkte IT 3 nach heutiger R. bei Frau StnRG

Lieber Hanebeck,
nach heutiger R. bei Frau Rogall sollte IT 3 folgenden Punkten nachgehen:

* In Bezug auf KRITIS-TOP Übersendung Vermerk Gesetzgebung USA → bereits erledigt

* Formelle Benennung des BW-Vertreters Dr. Zinell als Ländervertreter im Cyber-SR → Anruf in BW ergab, dass dieser Punkt für TO der CdS am 14.6. angemeldet worden ist. Dr. Zinell ist also zum Zeitpunkt der Sitzung „nur" vorläufiger Ländervertreter.

* TN B[redacted] → Für [redacted] wird „aller Voraussicht" nach [redacted] teilnehmen (übrigens auch Mitglied in AG 4)

* TN HE → Herr Viktor Jurk ist amtierender Leiter der Abteilung VII (E-Government und Verwaltungsinformatik) des Hessischen Innenministeriums. Er vertritt Herrn St Koch, der aufgrund der Anwesenheitspflicht bei der Plenarsitzung im Hessischen Landtag und der Teilnahme von Herrn Minister Rhein an der zeitgleich stattfindenden Innenministerkonferenz verhindert ist.

* Cyber-SR im BT-Innenausschuss → Cyber-SR stand auf TO des IA am 25.5.2011. Wie vorhin ausgeführt, wurde im Rahmen der IA-Sitzung jährliche Berichterstattung an IA angeregt (siehe Kurzbericht über Sitzung und Bericht über Arbeit des Cyber- SR in Anlage).

In Bezug auf Ihr avisiertes Telefonat mit Frau Feyerbacher zum Vortrag des P-BSI: Sie rief vorhin bei mir an und fragte zur beabsichtigten Übersendung des Berichts des Cyber-AZ an Mitglieder des Cyber-SR. Ich habe sie darüber informiert, dass Fr. Rogall entschieden hat, den Bericht dem Protokoll beizufügen. Er wird nicht ausliegen und auch nicht vorher übersandt. BSI wird Bericht bei Patras glätten und nach der Sitzung neue Fassung übersenden.
Ich habe zudem erwähnt, dass Sie sich bei ihr bzgl. des Vortrags von P-BSI melden wollen und dieser „strategischer" werden soll.

< Nachricht: WG: Bericht über 41. Sitzung des Innenausschusses am 25.5. >> < Datei: 17(4)262 BMI - Bericht - Arbeit des Nationalen Cyber-Sicherheitsrates.pdf >>
Beste Grüße+Schöne Pfingsten,
N.Spatschke

Referat IT3
ORR Dr. Dimroth

15.05. 2012

[redacted]

Ziel der Behandlung: *Darstellung gesetzgeberischer Maßnahmen als mögliche Reaktion auf das Ergebnis der derzeit laufenden Ministergespräche mit den Betreibern kritischer Infrastrukturen.*

Sachstand

BM Dr. Friedrich hat im Februar dieses Jahres entschieden, dass in Umsetzung des in der Cybersicherheitsstrategie insoweit enthaltenen Prüfauftrages ein IT-Sicherheitsgesetz mit folgenden Kerninhalten vorbereitet werden soll:

- Pflicht zur Erfüllung von Mindestanforderungen an IT-Sicherheit für Betreiber kritischer Infrastrukturen,
- Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle für Betreiber kritischer Infrastrukturen,
- Ressortübergreifend verpflichtende und einheitliche Vorgaben zur IT-Sicherheit für die Bundesverwaltung,
- Pflicht zur Erfüllung von Mindestanforderungen an IT-Sicherheit für Telekommunikationsanbieter und Telemediendiensteanbieter,
- Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle für Telekommunikationsanbieter,
- Pflicht zur Information der Nutzer über Schadprogramme für Telekommunikationsanbieter,
- Recht für Telemediendiensteanbieter Nutzungsdaten zur Störungsbeseitigung zu verwenden,
- Erweiterung der Zuständigkeiten des BKA auf bestimmte Fälle von Cybercrime und
- Erweiterung der Katalogstraftaten iSv § 100a StPO (Telekommunikationsüberwachung) auf bestimmte Fälle von Cybercrime.

Entsprechende Formulierungsvorschläge wurden zwischenzeitlich erarbeitet und werden derzeit finalisiert, um im Anschluss eine Leitungsentscheidung dazu einzuholen.

In Bezug auf die Kommunikation hat BM entschieden,

- zunächst (nach außen) zu kommunizieren, dass die **Ergebnisse** der derzeit laufenden **Ministergespräche abgewartet** würden und er im Anschluss je nach Ergebnis der Gespräche über die Erforderlichkeit gesetzgeberischer Maßnahmen entscheiden werde und, dass
- im Rahmen der Sitzung des Cyber-SR im Mai 2012 das Thema IT-Sicherheitsgesetzgebung als **eine mögliche Option** angesprochen und diskutiert werden solle.

Gesprächsführungsvorschlag:

- In der Cybersicherheitsstrategie haben wir uns darauf geeinigt, die Frage möglichen Gesetzgebungsbedarfs zu evaluieren. Diesbezüglich sollten die derzeit laufenden Ministergespräche mit den Betreibern kritischer Infrastrukturen zunächst abgewartet werden. Soweit hier erhebliche Defizite hinsichtlich der IT-Sicherheit offenbar werden, müssen wir auch über gesetzgeberische Maßnahmen nachdenken. Ein entsprechender Prüfauftrag ist auch in der Cybersicherheitsstrategie enthalten.
- Frage an die Ressort- und Ländervertreter: Gibt es in Ihren Häusern/Ländern zur Frage bestehenden Gesetzgebungsbedarfs zur Erhöhung der IT-Sicherheit im Kritis-Bereich und/oder auch darüber hinaus Überlegungen? Wie stehen Sie beispielsweise zu einer Verpflichtung von Betreibern kritischer Infrastrukturen, erhebliche IT-Sicherheitsvorfälle an eine zentrale Bundesstelle zu melden?
- Frage an Wirtschaftsvertreter: Gibt es in den Verbänden schon Überlegungen hierzu?
- Der Cyber-Sicherheitsrat als politisch zuständiges Gremium wird seitens BMI eng in den weiteren Prozess eingebunden werden.

Referat IT3
AR Spatschke

24.5. 2012

[redacted]

Ziel der Behandlung: *Abstimmung über den nächsten thematischen Schwerpunkt in der nächsten Sitzung des Cyber-SR.*

Sachstand

Das im Rahmen der ersten Sitzung des Cyber-SR am 3.5.2011 abgestimmte Schwerpunktepapier bis 2013 (Anlage) sieht insgesamt 5 Punkte vor, von denen Punkt 1 und 5 intensiv erörtert worden.

Ein weiter Schwerpunkt ist unter Ziffer 2 die *„Koordinierung von Maßnahmen zur Verbesserung der Sicherheit von IT-Systemen in Deutschland"*. Dies korrespondiert mit dem strategischen Ziel 2 der Cyber-Sicherheitsstrategie der BuReg („Sichere IT-Systeme in Deutschland").

Der Statusbericht des Cyber-AZ stellt u.a. fest, dass die Hauptbetroffenen der durch das Cyber-AZ von April 2011 bis März 2012 registrierten ca. 500 IT-Sicherheitsvorfälle überwiegend Privatanwender waren.

Es besteht trotz vielfältiger Initiativen (nPA, ABBZ, DE-Mail, DsIN) anhaltender Handlungsbedarf beim Schutz der IT-Systeme der Bürger. Die kriminelle Schattenwirtschaft hat sich zu einer ausdifferenzierten, weltweit agierenden Industrie entwickelt:

- Es agieren nicht mehr nur hochspezialisierte Einzeltäter, sondern Kriminelle, die international bestens vernetzt sind und arbeitsteilig zusammenwirken.
- In den Foren der Undergroundeconomy kann jedes beliebige Schadprogramm samt notwendiger Infrastruktur per Mausklick geordert werden.
- Alle zwei Sekunden wird ein neues Schadprogramm programmiert – sei es ein Virus, ein Wurm oder Trojanisches Pferd.
- Um die Zwanzigtausend Webseiten werden täglich mit Schadprogrammen infiziert und wirken damit als Ansteckungspunkte.

- Die Internetkriminalität entwickelt sich hochdynamisch. Sowohl die Zahl der begangenen Straftaten als auch die verursachten Schäden steigen in Deutschland stetig an:
    - 2010 wurden 19% mehr Fälle von IuK-Kriminalität gemeldet als 2009.
    - Die registrierten Schäden sind im selben Zeitraum um fast 70% gestiegen. Sie beliefen sich im Jahr 2010 auf über 61 Mio. Euro.
    - Nichtamtliche Umfragen und Schätzungen gehen von Schäden in Milliardenhöhen aus.

Gesprächsführungsvorschlag:

- Verweis auf Vortrag von P-BSI zur Bedrohungslage
- Trotz verstärkter Bemühungen von Staat und Wirtschaft, z.B. nPA, ABBZ, DsiN, DE-Mail) sind Privatanwender nach wie vor die Hauptbetroffenen von Cyberangriffen.
- **Wirtschaft, Staat und Gesellschaft** sind gemeinsam gefordert, einerseits, die **Chancen zu nutzen**, die sich uns durch Informations- und Kommunikationstechnologie bieten. Andererseits müssen die Risiken der zunehmenden Vernetzung im Cyberraum so gering wie möglich gehalten werden.
- Der **Staat** kann nur den **Rahmen** und die **Grundlagen** schaffen. Für die Gewährleistung von **Cyber-Sicherheit** sind wir auf die **Mitwirkung** von **Wirtschaft** und **Nutzer** angewiesen.
- **Frage und Einladung zur Diskussion an Mitglieder**:
    - Welchen Impuls könnte der Cyber-SR als politisch-strategisches Gremium setzen?
    - Sollte eine konzertierte Awarenesskampagne aller Ressorts initiiert werden? Vorbereitung dann zur nächsten Sitzung.

Referat IT3
AR Spatschke

23.5. 2012

[redacted]

Ziel der Behandlung: *Information der Mitglieder des Cyber-SR über die Thematik strukturierter Informations- und Meldewege zwischen den CERTS der Länder und dem BSI. Ggf. sollten die anwesenden Ländervertreter die IMK-AG „Cybersicherheit" informieren.*

Sachstand

Eine knappe Aufstellung zu BSI-Erkenntnissen des BSI zum aktuellen Planungsstand bzw. der Existenz von CERTs in den Bundesländern findet sich in der Anlage wieder. Eine formale, von den Ländern bestätigte Erhebung ist nicht existent.

In Bezug auf den **VerwaltungsCERT-Verbund** fand Anfang Mai die „erste Lesung" der Kooperationsvereinbarung im Rahmen der Kooperationsgruppe „Leitlinie Informationssicherheit des IT-Planungsrats" mit den Ländern statt. Ein Zeitpunkt für die Verabschiedung ist derzeit nicht absehbar.

Das BSI bereitet derzeit mit Mitteln des IT-Planungsrats eine Schulungsmaßnahme für den Aufbau eines LandesCERTs vor.

Sechs Länder (Sachsen, Sachsen-Anhalt, Thüringen, Berlin, Brandenburg, Mecklenburg-Vorpommern) treffen sich auf eigene Initiative auf Arbeitsebene, um sich untereinander zum Aufbau eines LandesCERTs auszutauschen und voneinander zu lernen. Das BSI CERT-Bund unterstützt

Probleme zeichnen sich insbesondere beim Ressourcenmangel (Finanzen, Personal) in einigen Bundesländern ab. Aufgrund fehlender Beteiligung an LÜKEX-Prozess fehlen teilweise wichtige Zusammenhänge und Erfahrungen, die in der Folge zu unterschiedlichen Geschwindigkeiten und Mehraufwand führen werden.

Gesprächsführungsvorschlag:

- Mitglieder des Cyber-SR kurz über Thematik strukturierter Informations- und Meldewege zwischen den CERTS der Länder und dem BSI informieren.
- Ländervertreter sollten IMK-AG „Cybersicherheit" informieren.

AG IT-Pl Rat

- **Aber:** Thematik wird bereits durch die Kooperationsgruppe „Leitlinie Informationssicherheit des IT-Planungsrats" mit der Verhandlung der Kooperationsvereinbarung zum VerwaltungsCERT-Verbund bearbeitet.
- Eine Doppelbefassung beider AGs ist nicht zielführend → Konsentierung der Informationen muss auf Länderebene erfolgen.

Anlage

Tabelle1

Sachstand / Einschätzung CERT-Strukturen der Länder

Land	Status	Geringe Erkenntnisse im BSI	Kommentar
Baden-Württemberg	ja		auch im CERT-Verbund, „virtuelles CERT"= Mitarbeiter mit Teilaufgabe
Bayern	ja		auch im CERT-Verbund
Berlin	im Aufbau		erste Schritte eingeleitet
Brandenburg	nein	x	erste Überlegungen laufen; sehr frühes Stadium
Bremen	nein	x	über Dienstleister „Dataport" Grundzüge gegeben
Hamburg	im Aufbau		erste Schritte eingeleitet, über Dienstleister „Dataport" Grundzüge gegeben
Hessen	im Aufbau		erste Schritte eingeleitet
Mecklenburg-Vorpommern	im Aufbau		erste Schritte eingeleitet; über Dienstleister „Dataport" Grundzüge gegeben
Niedersachsen	nein	x	Konzept vorhanden, kein Team, sehr frühes Stadium
Nordrhein-Westfalen	ja		auch im CERT-Verbund
Rheinland-Pfalz	ja		auch im CERT-Verbund
Saarland	nein	x	erste Überlegungen laufen; sehr frühes Stadium
Sachsen	im Aufbau		erste Schritte eingeleitet
Sachsen-Anhalt	im Aufbau		erste Schritte eingeleitet
Schleswig-Holstein	nein	x	über Dienstleister „Dataport" Grundzüge gegeben
Thüringen	im Aufbau		erste Schritte eingeleitet

Dieses Blatt ersetzt die Seiten 137 - 165

Die Entnahme erfolgte mangels Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss

Dieses Blatt ersetzt die Seiten 166 - 186

Die Entnahme erfolgte mangels Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss

Dieses Blatt ersetzt die Seiten 187 - 223

Die Entnahme erfolgte mangels Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss

Koch, Theresia

Von: Spatschke, Norman
Gesendet: Dienstag, 29. Mai 2012 18:42
An: StRogall-Grothe_
Cc: ITD_; SVITD_; Engel, Simone; Dürig, Markus, Dr.; Mantz, Rainer, Dr.; IT3_
Betreff: Cyber-Sicherheitsrat, hier: aktualisierte Sz

Lieber Herr Franßen,
im Nachgang meiner Mail von Freitag übersende ich anliegende Informationen bzw. Sprechzettel mit der Bitte um Austausch in der Mappe.

Sprechzettel P-BSI (Kernpunkte des Vortrags), Bitte Fach 2 der Mappe zuordnen.
Hintergrund: Herr Hanebeck hatte BSI am Fr. gebeten, Kernpunkte des Vortrags an Frau Rogall zu übersenden. Eine Überarbeitung des Vortrags wurde nicht erbeten.

120531_3. ber-Sicherheit...

Im Gesprächsführungsvorschlag geringfügig modifizierter Sz zu Cyber-Außenpolitik (Bitte Fach 3 zuordnen).
Hintergrund: AA hat auf Arbeitsebene Pläne zu 2. Cyber-Konferenz im September mitgeteilt. Zudem werde StS Haber für nächste Sitzung des Cyber-SR vorschlagen, die derzeitigen KOM-Bemühungen für mehr Cybersicherheit in den Fokus zu rücken.

TOP 2 Cyber Außenpolitik.docx

Bitte in Fach 5 den urspr. Sz ersetzen (war in R. so erbeten)

120529 Trusted Computing.docx

TOP 6 (CERT-Strukturen der Länder):
Wie erbeten hat entsprechendes Telefonat mit HE (Hr. Jurk) stattgefunden. Die Länder begrüßen dieses TOP ausdrücklich und werden zu TOP 6 wie folgt vortragen:
- Hr. Zinell zu den CERT-Aktivitäten + Bemühungen des IT-PLR,
- Hr. Jurk zu IMK-Länder AG „Cybersicherheit" und Erfahrungen aus der Lükex vorstellen, die den Aufbau entsprechender Strukturen erforderlich scheinen lassen.

Freundliche Grüße,
N. Spatschke
BMI - IT 3; -2045

Von: Spatschke, Norman
Gesendet: Freitag, 25. Mai 2012 17:56
An: StRogall-Grothe_
Cc: ITD_; SVITD_; Dürig, Markus, Dr.; Engel, Simone
Betreff: Informationspunkte IT 3 nach heutiger R. bei Frau StnRG

Lieber Hanebeck,
nach heutiger R. bei Frau Rogall sollte IT 3 folgenden Punkten nachgehen:

* In Bezug auf KRITIS-TOP Übersendung Vermerk Gesetzgebung USA → bereits erledigt

* Formelle Benennung des BW-Vertreters Dr. Zinell als Ländervertreter im Cyber-SR → Anruf in BW ergab, dass dieser Punkt für TO der CdS am 14.6. angemeldet worden ist. Dr. Zinell ist also zum Zeitpunkt der Sitzung „nur" vorläufiger Ländervertreter.

* TN [redacted] → Für [redacted] wird „aller Voraussicht" nach [redacted] teilnehmen (übrigens auch Mitglied in AG 4)

* TN HE → Herr Viktor Jurk ist amtierender Leiter der Abteilung VII (E-Government und Verwaltungsinformatik) des Hessischen Innenministeriums. Er vertritt Herrn St Koch, der aufgrund der Anwesenheitspflicht bei der Plenarsitzung im Hessischen Landtag und der Teilnahme von Herrn Minister Rhein an der zeitgleich stattfindenden Innenministerkonferenz verhindert ist.

* Cyber-SR im BT-Innenausschuss → Cyber-SR stand auf TO des IA am 25.5.2011. Wie vorhin ausgeführt, wurde im Rahmen der IA-Sitzung jährliche Berichterstattung an IA angeregt (siehe Kurzbericht über Sitzung und Bericht über Arbeit des Cyber- SR in Anlage).

In Bezug auf Ihr avisiertes Telefonat mit Frau Feyerbacher zum Vortrag des P-BSI: Sie rief vorhin bei mir an und fragte zur beabsichtigten Übersendung des Berichts des Cyber-AZ an Mitglieder des Cyber-SR. Ich habe sie darüber informiert, dass Fr. Rogall entschieden hat, den Bericht dem Protokoll beizufügen. Er wird nicht ausliegen und auch nicht vorher übersandt. BSI wird Bericht bei Patras glätten und nach der Sitzung neue Fassung übersenden.
Ich habe zudem erwähnt, dass Sie sich bei ihr bzgl. des Vortrags von P-BSI melden wollen und dieser „strategischer" werden soll.

< Nachricht: WG: Bericht über 41. Sitzung des Innenausschusses am 25.5. >> < Datei: 17(4)262 BMI - Bericht - Arbeit des Nationalen Cyber-Sicherheitsrates.pdf >>
Beste Grüße+Schöne Pfingsten,
N.Spatschke

3. Cyber-Sicherheitsrat am 31. Mai 2012
Kernbotschaften P BSI

I. Wo stehen wir heute?

Kernbotschaft 1 (Gesamtlage): Die IT-Durchdringung und IT-Vernetzung steigern die Attraktivität für Cyber-Angriffe verschärfen die Gefährdungslage.

- Die IT ist aus unserem Alltag nicht mehr wegzudenken: Sie durchdringt alle Lebensbereiche und ist Bestandteil wesentlicher (Geschäfts-)Prozesse.
- Die Durchdringung ist so weit fortgeschritten, dass die administrative Handlungsfähigkeit und die wirtschaftliche Leistungsfähigkeit von einer gut funktionierenden und sicheren IT abhängen.
- Quer durch alle Branchen ist die Hälfte der deutschen Unternehmen schon heute vom Internet abhängig.
- Eine fast durchgängige Vernetzung verbindet fast alle IT mit dem Internet, sodass sich IT-Sicherheit zur Cyber-Sicherheit entwickelt.

Kernbotschaft 2 (aktuelle Gefährdungslage): Die Angriffsmethodiken sind ausgeklügelt und individuell auf bestimmte Ziele zugeschnitten (Stichwort zweistufige Angriffe/APT).

- Im letzten Jahr haben wir beobachtet, dass die Quantität und Qualität der Angriffe weiter zunimmt. Aktuelle Fälle wie etwa DigiNotar bzw. RSA zeigen, dass sogar Unternehmen im (IT-)Sicherheitsbereich, also Unternehmen, die sich aufgrund ihrer unternehmerischen Ausrichtung mit dem Thema (IT-)Sicherheit intensiv befassen, getroffen werden können.
- Qualitativ sind insbesondere die zweistufigen Angriffe (Einstieg und „Nachladen") hervorzuheben.
- So z.B. im Fall DigiNotar: Der Angriff auf eine niederländische Zertifizierungsstelle war nur die erste Stufe des Angriffs. Mit den dort entwendeten Zertifikaten konnten sich die Angreifer in den Internetverkehr einklinken und so Daten abgreifen.
- Das Beispiel DigiNotar ist nicht nur wegen der Angriffsmethodik von besonderer Bedeutung. Es zeigt auch: Das Internet wird nicht nur als Transportinfrastruktur für Angriffe genutzt (z.B. DDoS-Angriffe), es ist auch als Infrastruktur selbst gefährdet.

3. Cyber-Sicherheitsrat am 31. Mai 2012
Kernbotschaften P BSI

- Wir, die Bundesverwaltung verzeichnen täglich 2.500 Infektionsversuche (ungezielte Angriffe). Trotz hoch entwickelter Virenscanner und Firewalls finden wir weiterhin eine Infektion pro Woche auf einem PC in der Bundesverwaltung.
- Darüber hinaus verzeichnen wir täglich 5 gezielte Angriffe auf Bundesverwaltung mit manipulierten Mails.
- Auf der Seite der Angreifer beobachten wir zugleich, dass mit den so genannten „Hacktivisten" ein neuer Typus von Angreifer agiert. Seine Motivationslage ist unterschiedlich und auch die Angriffsfähigkeiten bewegen sich auf unterschiedlichstem Niveau.
- Aus unserer Zusammenarbeit mit der Wirtschaft wissen wir, dass diese Gefährdungslage die Wirtschaft gleichermaßen trifft bzw. sie ebenfalls dieser ausgesetzt ist.

Wohin führt der (technische) Trend?

Kernbotschaft 3 (Trendaussagen): Neue Technologien bzw. technische Entwicklungen (z.B. Smartphones, Cloud Computing, VoIP) forcieren die IT-Durchdringung und IT-Vernetzung weiter. Die Gefährdungslage wird sich – auch in der Breite - weiter verschärfen.

- Neue Technologien bzw. technische Entwicklungen forcieren die IT-Durchdringung und IT-Vernetzung weiter. Hierzu gehören insbesondere die Trends im Mobilsektor als auch das Cloud Computing.
- Allein die Zahlen belegen, der Trend ist schon da. Die Prognose für Deutschland 2012 im Mobilsektor ist: Verkauf von 28,9 Millionen Handys, davon 15,9 Millionen Smartphones. Beim Cloud Computing 2012 in D erwarteter Umsatz: 5,3 Mrd. €.
- Zugleich sind Smartphones mit Sicherheitsmechanismen schwach ausgestattet (bestimmte für den Kunden attraktive Services sind dadurch auch erst möglich). Unter dem Motto „Bring your own Device" erfolgt eine Durchmischung dienstlicher und privater Nutzung von IT. Informationen und Daten werden in Clouds ohne vereinbarte Sicherheitsstandards ausgelagert.

3. Cyber-Sicherheitsrat am 31. Mai 2012
Kernbotschaften P BSI

Was können wir tun?

Kernbotschaft 4 (Handlungsschwerpunkte aus BSI-Sicht): Eine Reihe von Aktivitäten bringt die Cyber-Sicherheit in der Breite voran.

- Eigeninitiatives melden und systematisches Erfassen von Sicherheitsvorfällen (auch in anonymisierter Form) für Aktualisierung der Gefährdungslage und Verbesserung der Prävention (Stichwort für TOP 6 für CERT-Strukturen).
- Konzept der Mindestanforderungen ist fachlich in die Breite und durch Good Practise fortzuentwickeln.
- Aktives Zugehen auf Kritis-Sektoren (Stichwort für nachfolgenden TOP 3).
- Übergreifende nationale Kooperation ist auszubauen → Allianz: Anwender/Nutzer, Hersteller, Diensteanbieter.
- Die Analysefähigkeit von Sicherheitsvorfällen ist bei allen Handelnden auszubauen.

Kernbotschaft 5 (Fazit): Erstes Jahr war insbesondere vom Aufbau der Zusammenarbeit geprägt. Zur weiteren inhaltlichen Vertiefung der Zusammenarbeit sollen Projektgruppen gegründet werden.

- Das erste Jahr des Cyber-Abwehrzentrums war insbesondere vom Aufbau der Zusammenarbeit geprägt (Zusammenarbeit des Nukleus ab März 2011; ab Juni 2011 Einbindung der assoziierten Behörden; Kommunikationswege etabliert etc.).
- Ein weiterer Schwerpunkt im ersten Jahr war zudem das Zusammenspiel bei der Vorfallsbewertung zwischen den Behörden.
- Um die weitere inhaltliche Zusammenarbeit weiter zu vertiefen, planen wir die Einrichtung von Projektgruppen, die sich mit unterschiedlichen Themen wie etwa dem Hacktivismus beschäftigen sollen. Hierzu befinden wir uns jedoch derzeit noch in der Abstimmung mit den beteiligten Behörden.

Referat IT3
OAR Treib

03.05. 2012
Tel.: 2355

3. Sitzung des Cyber-SR am 31. Mai 2012
TOP 2: Cyber-Außenpolitik

Ziel der Behandlung: *Strategische Ausrichtung der Internationalen Zusammenarbeit zur Cyber-Außenpolitik einschließlich –Sicherheit.*
Problem: *AA betrachtet diese Thematik als ureigenes Kompetenzfeld und lehnt Abstimmung im Cyber-SR grundsätzlich ab. Die Entwicklung/Vorstellung einer Strategie wurde bilateral zugesagt. → Sie sollten betonen, dass politische Abstimmung im Cyber-SR erfolgen soll.*

Sachstand

Gem. Ergebnisprotokoll der zweiten Sitzung des Cyber-SR am 18. Oktober 2011 wurde AA beauftragt, ein Grundsatzpapier zu Zielen und Strategien der internationalen Zusammenarbeit im Bereich Cyber-Sicherheit in Abstimmung mit den betroffenen Ressorts zu erstellen.
Im Ergebnis steht ein Papier, das hauptsächlich das aus politischer Zugehörigkeit resultierende DEU-Engagement in internationalen Gremien/Foren reflektiert (EU, NATO, VN, OSZE, EUROPARAT; OECD); insoweit liegt eine gute/umfangreiche Status Quo-Beschreibung vor, insb. auf Grundlage der Zulieferungen seitens BMVg, BMJ und BMI.
AA wird voraussichtlich die Vorstellung des Papiers nutzen, um für eine zusammenfassende Darstellung der derzeit auf EU-Ebene laufenden Initiativen zum Thema „Cyber-Security" zu werben um ein Gesamtbild hierzu zu erhalten und möglicherweise auch eine gemeinsame Linie für die Begleitung dieser Initiativen zu erarbeiten. Hintergrund sind die diversen Initiativen auf EU-Ebene und die innerhalb der Bundesregierung verteilten Zuständigkeiten.
Ein richtungsweisendes, strategisches Konzept wird nur im Ansatz geliefert. Vorliegendes Arbeitspapier orientiert sich am unter FF des BMI für die Quad-Konsultationen in 2011 entwickelten Non-Paper „Norms of State Behavior". Bereits das Non-Paper geht über reine Sicherheitsthemen hinaus, denn Sicherheit und netzpol. Ziele wie Freiheit, Offenheit usw. müssen national wie international ausbalanciert werden.

Gesprächsführungsvorschlag (aktiv):

- Dank an AA und die an der Erarbeitung des Papiers beteiligten Ressorts.
- Das Papier beschreibt zutreffend den politischen Rahmen, die Ausgangslage und gegenwärtige Ziele für das DEU-Engagement im EU- bzw. internationalen Bereich.
- Unter der Überschrift „Prinzipien" wird deutlich, dass Ziele und Strategie der internationalen Zusammenarbeit im Bereich Cyber-Sicherheit nicht ohne weiteres losgelöst von einer allgemeinen Cyber-Außenpolitik betrachtet werden können. Zutreffend werden im vorliegenden Arbeitspapier unter „Prinzipien" wesentliche Grundlinien der BReg. wie Offenheit, Transparenz und Freiheit im Cyber-Raum benannt, die im Spannungsfeld zu Sicherheitsfragen stehen.
- Bei dieser Sachlage rege ich an, unsere Diskussion entsprechend auszuweiten und **in einem nächsten Schritt** ein nach außen zu vertretendes ganzheitliches strategisches **Konzept für einen globalen, ungeteilten Cyber-Raum der Freiheit und des Rechts** zu entwickeln.
- „Norms of State Behavior in Cyberspace" bilden insoweit den Kern der Bemühungen (konsise Vorstellungen wurden auf Arbeitsebene für die Quad-Konsultationen mit USA, FRA und UK bereits entwickelt; darüber hinaus müssten m.E. auch noch Ideen zur Weiterentwicklung des Völkerrechts abgestimmt werden –etwa Verantwortung der Staaten für Gefahren, die von ihrem Territorium ausgehen[1]-.
- Bei dieser Sachlage plädiere ich für folgenden **Dreischritt**:
    1. Formulierung einheitlicher **Definitionen** sowie eines gemeinsamen, ressortübergreifenden Verständnisses bezüglich Cyber-Außenpolitik und Cyber-Sicherheit als Voraussetzung dafür, dass mit internationalen Gesprächspartnern ein gemeinsames Verständnis entwickelt werden kann.
    2. **Prioritäten** setzen. Mit Blick auf Zielkonflikte sollten gegenpolige Aspekte nach Wichtigkeit und Dringlichkeit unterschieden werden (z.B. Freiheit, Offenheit, Transparenz im Internet vs. Repression oder präventive/aktive Cybersicherheit).
    3. Geopolitisch **„SMART Ziele"**[2] setzen, d.h. ein aus den Prioritäten abgeleitetes Engagement der BReg in der EU und in internationalen

[1] Keine Neuschöpfungen, sondern Anleihen z.B. im Weltraum-/Umweltrecht
[2] SMART ist ein Akronym für „Specific Measurable Accepted Realistic Timely"

Foren formulieren sowie aufgrund der Interessenlage Möglichkeiten der bilateralen Ansprache verschiedener Akteure/Länder eruieren[3] (z.B. mit gleichgesinnten EU-Staaten sowie USA, aber nicht zuletzt auch mit Blick auf bevölkerungsreiche aufstrebende in der Orientierung schwankende digital entwicklungsfähige Regionen und Länder).

- Dazu **beispielhaft** drei **praktische Denkanstöße**:
    1. **Afrika** ist offenbar weltweit am stärksten digital entwicklungsfähig. Afrikanische Länder sind über internationale Foren so gut wie nicht an das westl. Lager angebunden; mal abgesehen vom letztjährigen Internet Governance Forum **(IGF)** in Nairobi. Wenn die westl. Welt in dieser Region keine Kontakte knüpft, werden andere Staaten, deren Maßstäbe wir nicht teilen (RUS/CHN), das Vakuum ausfüllen. Deshalb kämen m.E. Gespräche und vielleicht ein „Coaching" eines ausgesuchten Staates in der Region in Frage (Vermittlung der Denkart + netzpol. Grundsätze, Muster für strategische Sicherheitsaufstellung, Awareness Raising Materialien zur Verfügung stellen, Sicherheit made in Germany?.....). Als strategisch wichtig könnte mglw. **Südafrika** angesehen werden (BRICS-Staat, vermutlich aufgeschlossen, relativ stabil, als Multiplikator geeignet...). Südafrika gehört auch zu den Ländern, mit denen OECD verstärkt zusammenarbeiten will (Synergie?).
    2. **Südamerika!** Von den südamerikanischen Staaten gehören Chile und Mexiko bereits der OECD an; sie dürften damit relativ westl. ausgerichtet sein. **Brasilien** als noch wichtiger „BRICS-Staat" hingegen steht bisher nur als Partner für verstärkte Zusammenarbeit im Fokus der OECD. Aus strategischen geopolitischen Gründen (Multiplikator, Vorzeigeland, ansonsten wie oben Südafrika) wäre daran zu denken, mit Brasilien ins Gespräch zu kommen.
    3. **„Problemstaaten"**
       Speziell auf Cyber Sicherheit gerichtete bilaterale Gespräche mit RUS und CHN intensivieren. Netzpol. Fragen müssten zugunsten eher konsensfähiger Aspekte (Wirtschaft, Pol./Mil, Menschenrechte, digitale Entwicklungshilfe) hintangestellt werden.

Reaktiv:

[3] z.B BRICS-Staaten

- Den Vorschlag des AA, die derzeit auf EU-Ebene laufenden vielfältigen Initiativen zum Thema Cyber-Security innerhalb der Bundesregierung zu erheben und möglicherweise darauf aufbauend eine gemeinsame Linie zu entwickeln, teile ich uneingeschränkt. Gern greife ich insoweit auch den Vorschlag des AA auf, sich in der kommenden Sitzung des Cybersicherheitsrates verstärkt dem EU-Thema zu widmen.
- Das BMI wird sich gern an der für Mitte September dJ geplanten 2. Berliner Cyber-Konferenz mit Schwerpunkt auf den Menschenrechten im Internet beteiligen und sowohl seine IT-Kompetenz als auch seine verfassungsrechtliche Expertise einbringen.

3. Sitzung des Cyber-SR am 31. Mai 2012
TOP 5: Trusted Computing

Ziel der Behandlung: *Information des Cyber-Sicherheitsrat über die Entwicklung eines neuen Standards und deren Auswirkung auf die IT- und Cyber-Sicherheit*

Sachstand

Das Ziel, das die Trusted Computing Group (TCG) mit der Entwicklung und Produktion des Trusted Platform Moduls (TPM) verfolgt, ist, einen Beitrag zur Sicherheit von Informationssystemen zu leisten. Auf diesem Chip (TPM) können Schlüssel zur Verschlüsselung, Zertifikate oder andere sicherheitsrelevante Informationen sicher gespeichert und somit geschützt werden.

Die TCG wurde 2003 durch Adaption der Trusted Computing Platform Alliance gegründet. Die Zielsetzung der TCG ist die Entwicklung und Förderung offener, herstellerunabhängiger Industriestandard-Spezifikationen für plattformübergreifende Trusted Computing Bausteine und Software-Schnittstellen. Neben diesen Zielen richtet sich das Interesse der TCG auch auf den Schutz von Urheber- und Patentrechten. Nur eine in allen Funktionen nicht manipulierbare Plattform bietet Gewähr, dass weitere Sicherheitsmaßnahmen und Sicherheitsmechanismen auf der Ebene des Betriebssystems und auf den Anwendungsebenen nicht ausgehebelt werden können. Zu solchen Sicherheitsmaßnahmen gehören Lösungen wie Kopierschutz, Rechteverwaltung, Lizenzprüfung und Quellenangaben.

Durch die Maßnahmen des BMI und des BMWi gemeinsam ist es gelungen, den ursprünglichen closed shop der amerikanischen Industrie auch für andere Institutionen zu öffnen. So sind heute auch u. a. das BSI, deutsche Hersteller und Wissenschaftsinstitute dabei. Insgesamt sind in der TCG zurzeit ca. 200 Unternehmen und staatliche Organisationen (NSA/NIST (USA), CESG (GB) und ANSSI (Frankreich)) organisiert.

Warum muss sich der CyberSR mit diesem technischen System auseinandersetzen?

Seit Jahren werden in nahezu **jedes Gerät**, ob Rechner oder Mobil-Telefon, die TPMs eingebaut. Derzeit sind in etwa **150 Mio. Geräten** das TPM eingebaut. In anderen **zukunftsweisenden Gebieten**, wie im Automotiv-Bereich und smart Grids ist der Einsatz des TPM ohne weiteres vorstellbar. Damit ist die Grundlage dafür gelegt, dass die **TC-Technik zu einer Basis- Sicherheitsstruktur** wird, an der niemand mehr vorbei kommt und auf der alle anderen Sicherheitsmechanismen aufbauen.

Dadurch wird deutlich, dass es notwendig ist, dass der Cyber-Sicherheitsrat sich mit so einem grundlegenden Sicherheitssystem befasst und Einfluss auf die weitere Entwicklung der neuen und absehbaren Standards nimmt.

2004 ist es uns gelungen, eine Öffnung der Mitarbeit zugunsten der deutschen Industrie, Wissenschaft und staatlichen Stellen ausländischer Staaten zu erreichen. Wir haben die deutsche Position in Diskussionen mit der TCG eingebracht. Beispiel hierfür ist die Zertifizierung von TPM aufgrund von Prüfkriterien, die die TCG entwickelt hat. Das BSI ist die wichtigste Zertifizierungsstelle weltweit. Da die Zertifizierung nur bei diskreten TPM und nicht bei integrierten TPM möglich ist, ergibt sich durch die Zertifizierungsanforderungen /-möglichkeiten ein Wettbewerbsvorteil für Infineon als Weltmarktführer von diskreten TPM.

Hieran wird deutlich, dass die **Einflussnahme der Bundesregierung sowohl aus sicherheits- als auch wirtschaftspolitischer Sicht von Bedeutung war**, weil damit die Weltmarktführerschaft von Infineon und damit ein deutscher Hersteller und vertrauenswürdiger Lieferant des Sicherheitschips erhalten blieb.

BMI und BMWi haben sich frühzeitig um die Entwicklung bei der TCG gekümmert und ein Eckpunktepapier veröffentlicht. Wesentlicher Inhalt des Eckpunktepapiers 2007 bezog sich auf Anforderungen an einen zu veröffentlichenden Standard (Verfügbarkeit, offen, für die Forschung geeignet), auf die Zertifizierung des TPM, die Entscheidungsfreiheit über den Einsatz und die internationale Zusammenarbeit.

Warum jetzt Überarbeitung des Eckpunktepapiers?

Die aktuelle Version 1.2 der TC-Spezifikation ist als ISO-Standard veröffentlicht. Sie sah vor, dass der Anwender das TPM, sofern er es benutzen wollte, aktiv einschalten

musste. **Die TCG hat eine neue Version entwickelt und beabsichtigt diese im Laufe des Jahres 2013 als ISO-Standard zu veröffentlichen.** Alle in der TCG zusammengeschlossen Unternehmen haben bekundet, die TPMs nach diesem neuen Standard herzustellen und in die Geräte einzubauen. Dies bedeutet, dass in Zukunft Geräte mit einem aktivierten TPM auf den Markt kommen werden.

2010 stellte Microsoft seine end-to-end-trust-Vision vor. Basis dieser Verbindungen sind sichere Authentifizierungen, wie z. B. mit dem nPA und dem neuen TPM. Sollte es Microsoft auf dieser Basis gelingen, vertrauenswürdige Umgebungen aufzubauen, **könnte** dies der **weltweite Durchbruch für die TC-Technologie** sein. Bisher erfolgt zwar ein großflächiger Einbau der TPMs aber es gibt, abgesehen von einigen unternehmensinternen Netzen, keine größeren Anwendungen.

Mit der neuen Version gehen mit dem potentiellen Sicherheitsgewinn allerdings **Kontrollverluste für den Nutzer** einher. Mit Unterstützung des TC-Moduls können Hersteller Rechner so einrichten, dass das Ausführen anderweitiger (z.B. herstellerfremder) Programme unterbunden wird. Das bisher verfolgte Prinzip des Universal-Computers würde aufgegeben, Systeme für bestimmte Einsatzzwecke könnten eingeführt werden.

Letztinstanzlich unterliegen aber auch immer alle Daten auf einem IT-Gerät primär der Kontrolle desjenigen, der festlegen kann welche Software läuft. Wenn also Geräte-Eigentümer **nicht die volle Oberhoheit über ihre Informationstechnik** besitzen, also nicht bestimmen können, mit welcher Software auf die Daten zugegriffen wird, so verlieren die Eigentümer auch die Oberhoheit über die auf diesen Systemen verarbeiteten und gespeicherten Daten.

Für die **Bundesverwaltung** sind IT-Systeme, die über die Spezifikationen in der neuen Version verfügen, **nicht akzeptabel**. Die Bundesverwaltung muss weiterhin allein darüber entscheiden, was mit ihren Daten passiert. Dies gilt auch für den **Betrieb von kritischen Infrastrukturen**. Es ist fraglich, inwiefern diese Zielgruppe auch in Zukunft ausreichend Marktmacht innehat, um entsprechende IT-Systeme zu angemessenen Preisen erstehen zu können.

Für eine Vielzahl der kleinen und mittelständischen Unternehmen (**KMU**) und der **Bürger** könnten Systeme, die unter den Bedingungen der neuen Spezifikation arbeiten, ein Zugewinn an Sicherheit bedeuten. Es wird deutlich, dass die von diesem Personenkreis zurzeit umgesetzten IT- Sicherheitsmaßnahmen den Bedrohungen – insb. mit Blick auf zukünftige Entwicklungen – nicht angemessen begegnen können. Mit der neuen Version könnten die IT- Systeme perspektivisch sicherer gestaltet werden, weil sich Sicherheitsfunktionalitäten auf einen standardmäßig aktivierten **hardwareseitigen Sicherheitsanker** verlassen könnten. So würde es z. B. Hackern schwerer fallen, die IT-Systeme in ein Botnetz zu übernehmen.

Aus diesen Gründen war es notwendig, die Eckpunkte aus 2007 auf die neue Version der Spezifikation zu aktualisieren. **Die Bedeutung der Einflussnahme der Bundesregierung ist heute noch wichtiger als vor 4 Jahren, weil abzusehen ist, dass sich die Verwendung der TC-Technik über kurz oder lang in alle Bereiche der Informationstechnik ausbreiten wird.**

Im Gegensatz zum Eckpunktepapier 2007 ist jetzt eine **differenzierte Betrachtung** der TC-Technik notwendig. Es ist dabei zu **unterscheiden** zwischen einem **Privatanwender/ KMU** und der **öffentlichen Verwaltung/Kritische Infrastrukturen**. Der Einsatz für Privatanwender wird **begrüßt**, weil dadurch ein **Sicherheitsgewinn** erzielt werden kann. Für die **öffentliche Verwaltung lehnen** wir die Verwendung **ab**, weil durch die Verwendung des aktivierten TPMs die Kontrolle über die sich auf den Rechnern befindlichen Daten nicht mehr der alleinigen Kontrolle des Eigentümers befindet.

Das vorliegende Eckpunktepapier befindet sich in der Ressortabstimmung. Letzte Abstimmungen erfolgen derzeit. Als Anlage ist das Eckpunktepapier in der zur Abstimmung versandten Ausgangsversion beigefügt.

Gesprächsführungsvorschlag:

- Neue Spezifikationen der TCG werden in naher Zukunft veröffentlicht werden.
- Die hardwarebasierte Sicherheitstechnik der TCG wird **grundsätzlich begrüßt**.
- 2004 und 2007 wurde bereits Eckpunkte veröffentlicht, die von der TCG akzeptiert wurden.
- Kernpunkte des Eckpunktepapiers 2007:

- Anforderungen an einen zu veröffentlichenden Standard (Verfügbarkeit, offen, für die Forschung geeignet),
- Zertifizierung des TPM,
- Entscheidungsfreiheit über den Einsatz und
- internationale Zusammenarbeit.

- Durch die neuen Spezifikationen ist jetzt eine **Aktualisierung des Eckpunktepapiers** notwendig geworden.
- Kernpunkte des neuen Eckpunktepapiers sind:
  - Transparenz beim Privatanwender
  - Trennung der Interessenlage zwischen Privatanwender/KMU und öffentlicher Verwaltung/KRITIS
- Die neuen Versionen der TC-Technik haben sicherheits- und wirtschaftspolitische Implikationen; daher Diskussion des Eckpunktepapiers im Cyber-Sicherheitsrat
- **Sicherheitsbedenken** beim Einsatz in der Bundesverwaltung und Kritischen Infrastrukturen
  - **Bundesverwaltung** kann Rechner, die über ein eingeschaltetes TPM verfügen nicht einsetzen, weil
    - damit ein **Kontrollverlust** über ihre Daten einhergeht und
    - die **Verwendung anderer als der vom Hersteller vorgesehenen Software** eingeschränkt ist (siehe insbesondere Punkte 3, 4, 13, 14 und 15 des Eckpunktepapiers).
  - **Wirtschaftlicher Aspekt:** Wenn diese Versionen für den Massenmarkt produziert werden, wird Bundesverwaltung evtl. zum **Nischennachfrager**. Dies könnte dazu führen, dass der Einkauf eines Nischenproduktes **teurer** wird als der Einkauf eines Rechners aus dem Massenmarkt. Hier ist die Zusammenarbeit der öffentlichen Verwaltung gefragt, um genügend Nachfrage zu generieren. (z. B. durch Beschaffungsamt).
- **Wirtschaftspolitische Implikationen:** Auch im neuen Eckpunktepapier sind die Eckpunkte enthalten, die der deutschen Wirtschaft den Zugang zu und die Verwendung des Standards sichern werden. Dies ist umso wichtiger als in Zukunft damit zu rechnen ist, dass ein aktiviertes TPM in jedem Gerät vorhanden sein wird.
- Verbesserungen bei der IT-Sicherheit bei **Bürgern und KMU** durch Nutzung des TPM und der Verschlüsselungsmöglichkeiten **aber** absolute Transparenz und Hinweis auf die Konsequenzen hinsichtlich des Verlusts der alleinigen Verfügungsgewalt über die auf solcher Informationstechnik verarbeiteten und

gespeicherten Daten notwendig (siehe insbesondere Punkte 3, 5, 9, 10, 13, 14 und 17 des Eckpunktepapiers)

- Letzte Arbeiten im Rahmen der **Ressortabstimmung** werden vorgenommen
- Vorgesehen: Vorstellung des neuen Eckpunktepapiers im **IT-Rat** und im **IT-PLR**

239

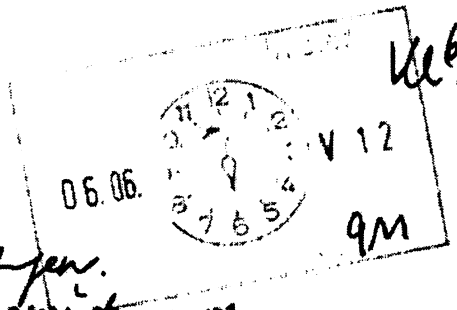
Referat IT 3

IT 3 - 606 000-2/112#18

Refl: MR Dr. Dürig/MR Dr. Mantz
Sb: AR Spatschke

Berlin, den 4. Juni 2012

Hausruf: 2045

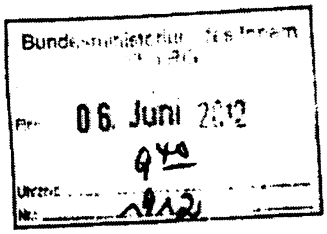


LMB:
Rat vorgesehen.
Mit Dank zurück

Herrn Minister

über

Frau Staatssekretärin Rogall-Grothe
Herrn IT-Direktor
Herrn SV IT-Direktor



AR Spatschke z.w.V.

Betr.: Gespräch mit [redacted] / Sitzung der AG 4 des IT-Gipfels am 11.6.2012

Anlage: - 1 Mappe -

1. Votum

Anliegend werden die sitzungsvorbereitenden Unterlagen mit der Bitte um Kenntnisnahme vorgelegt.

2. Sachverhalt

Die Tagesordnung der am 11. Juni 2012 von 13:00 – 15:00 Uhr stattfindenden 2. AG 4-Sitzung sieht neben einer Unterrichtung zum aktuellen Planungsstand des Gipfels (einschl. Podiumsdiskussion und Veranstaltungskonzept Vortag) eine inhaltliche Diskussion zum Thema Providerverantwortung vor.

Vorgeschaltet findet von 12:00 bis 13:00 Uhr ein Treffen mit Vertretern der Geschäftsführung von [redacted] statt, in dem neben einer Ein-

tragung in das Gästebuch und einer Führung in der Banknotengalerie ein ca. halbstündiges Fachgespräch zu fachspezifischen Themen stattfinden soll.

Zu beiden Veranstaltungen werden Sie durch Hrn. ITD, Hrn. Dr. Dürig und Hrn. Spatschke (IT 3) begleitet.

Der diesjährige IT-Gipfel findet am 13.November 2012 in Essen statt.

3. Stellungnahme

Entfällt.

Dr. Mantz

Spatschke

Dieses Blatt ersetzt die Seiten 241 - 247

Die Entnahme erfolgte mangels Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss

Referat IT 3
AR Spatschke

4. Juni 2012

Sitzung der AG 4 des IT-Gipfels
„Vertrauen, Datenschutz und Sicherheit im Internet"
am 11. Juni 2012

TOP 2: Bericht zu den Sachständen in den Unterarbeitsgruppen **Reaktiv**

Bei TOP 2 steht die Berichterstattung zur bisherigen Tätigkeit der UAGs durch die Vorsitzenden im Vordergrund. Die Thematik „Providerverantwortung" wird unter TOP 3 vertieft erörtert.
Sie sollten den Vorsitzenden für die geleistete Arbeit danken.

Sachstand

UAG 1: Sicheres Cloud Computing (Vorsitz [redacted]) → [redacted] trägt vor

- Baut auf die durch die beiden UAGs „Recht und Technik" der AG 4 in 2011 geleisteten Vorarbeiten sowie das „Eckpunktepapier zur Sicherheit in der Cloud" des BSI auf.
- UAG will gemeinsames Verständnis und möglichst industrieweiten Konsens erarbeiten, was eine "Sichere Cloud" in der Praxis auszeichnet.
- Anwendern sollen konkrete Orientierung bzw. Empfehlungen geboten werden (z.B. Zertifizierungen oder Gütesiegel).
- UAG soll Plattform für die Zusammenführung der Ergebnisse sowie Aktivitäten der Cloud-Projekte, Initiativen sowie Unterarbeitsgruppen der anderen IT-Gipfel-Arbeitsgruppen sein.
- Bisherige Arbeitsergebnisse „überschaubar": keine Präsenzsitzung bisher – UAG 1 tagt heute am 11.6. erstmals in Bonn.

UAG 2: Sichere Identitäten (Vorsitz BSI) → Hr. Flätgen vor

- Zum letzten Gipfel hatte die vormals durch BMI geführte UAG zehn Mindestandards für die Anbieter elektronischer Identitäten (Identitätsprovider) erarbeitet, die in den nächsten 2 Jahren durch die in der AG 4 vertretenen Unternehmen umgesetzt werden sollen.
- In Abhängigkeit des Evaluationsergebnisses soll ggf. eine Selbstverpflichtung der Wirtschaft angestrebt werden.

- UAG 2 wird nun in 2 Schritten Evaluierungskriterien sowie ein Erhebungs- und Auswertungskonzept erarbeiten.
- Evaluierungskriterien wurden in Präsenzsitzung am 4.6. erörtert.
- Das Erhebungs- und Auswertungskonzept wird anschl. erarbeitet und voraus sichtlich durch das BSI mit externer Unterstützung erarbeitet.
- Die Evaluierung bezieht sich dann zum Einen auf den IST-Zustand in den Unternehmen/Institutionen der AG4-Mitglieder. Erfasst werden soll im Vorfeld auch der jeweils individuelle Umsetzungsgrad des Anforderungskatalogs (inkl. der Informationen über die Zeitdauer einer bereits bestehenden Umsetzung), da dies die Grundlage für eine Evaluierung bildet.

UAG 3: Providerverantwortung (Vorsitz [redacted] → [redacted] trägt vor.

- UAG wird nach wie vor von eco geführt. Einrichtung der UAG trägt dem Umstand Rechnung, dass ISPs eine große Verantwortung für die Sicherheit der Endkundensysteme zukommt.
- [redacted] sieht die UAG als erfolgreiche Plattform bereits bestehender Maßnahmen wie Anti-Botnet-Beratungszentrum, DNS-Changer und Webseitencheck für KMU (Aktion min finaz. Unterstützung des BMWi), und darin auch deutlichen Mehrwert zu anderen UAGs.
- Nach BMI- Verständnis sollte UAG aber aus sich heraus Maßnahmen anstoßen und nicht nur Plattform ohnehin bereits bestehender Initiativen darstellen.
- Darüber hinausgehende Maßnahmen (Port 25-Sperre in Routern) werden zwar durch BMI/BSI forciert, jedoch nur zögerlich angenommen.
- Bislang hat es eine Telko und eine Präsenzsitzung am 22.5. gegeben.

UAG 4: Mobile Sicherheit (Vorsitz [redacted] → [redacted] trägt vor.

- UAG hat sich die Erhöhung der Sicherheit bei Betrieb mobiler Endegräte zum Ziel gesetzt.
- Zunächst wurde ein Fragebogen für eine Anwenderstudie (ca. 1.100 Privatnutzer) erarbeitet, die vor kurzem durchgeführt wurde (an den Kosten beteiligt sich BMI mit ca. 1.000 EUR). In Bälde wird dann eine Umfrage unter Businessanwendern durchgeführt.
- Ergebnisse werden durch UAG unterjährig pressewirksam platzieren (im Sommer in [redacted] Hauptstadtforum) und daraus ableitend einen Kriterienkatalog für

Sicherheitsarchitekturen entwickeln. Anbieter- und Anwenderworkshops sollen hierbei helfen.

- UAG ist im Vergleich zu anderen 3 UAGs gesehen sehr weit, Telkos und Präsenzsitzungen haben stattgefunden.

Referat IT 3
AR Spatschke

5. Juni 2012

Sitzung der AG 4 des IT-Gipfels
"Vertrauen, Datenschutz und Sicherheit im Internet"
am 11. Juni 2012

Teilnehmerliste

Dr. Hans-Peter Friedrich	BMI
[redacted]	[redacted] GmbH
Martin Schallbruch	BMI
Dr. Markus Dürig	BMI
Norman Spatschke	BMI
[redacted]	[redacted] GmbH
[redacted]	[redacted] AG
Horst Flätgen	BSI
[redacted]	[redacted]
Dr.Waldemar Grudzien	Bundesverband deutscher Banken
[redacted]	[redacted]
[redacted]	D[redacted] AG
[redacted]	[redacted] e.V.
Heike Troue	DsiN e.V.
[redacted]	[redacted] Germany
[redacted]	[redacted]
[redacted]	[redacted] AG
[redacted]	M[redacted] GmbH
[redacted]	e[redacted]

[redacted] (B[redacted] ist kurzfristig verhindert. B[redacted] prüft Alternativen.

Keine Rückmeldung:

V[redacted] V[redacted]

V[redacted] (zum wiederholten Mal)

Bundesministerium
des Innern

[redacted]

POSTANSCHRIFT Bundesministerium des Innern, 11014 Berlin

Bundesministerium des Innern
Dr. Hans-Peter Friedrich
Bundesminister des Innern
Mitglied des Deutschen Bundestages
minister@bmi.bund.de

HAUSANSCHRIFT
Alt-Moabit 101 D
10559 Berlin
POSTANSCHRIFT
11014 Berlin
TEL +49(0)30 18 681-1000
FAX +49(0)30 18 681-1014

[redacted] GmbH
Vorsitzender der Geschäftsführung
[redacted]com
HAUSANSCHRIFT
[redacted]
POSTANSCHRIFT
[redacted]
TEL
FAX [redacted]

An die
Mitglieder der AG 4
- Nur per E-Mail -

DATUM Berlin, den 22. Mai 2012

Sehr geehrte Damen und Herren,

Sehr geehrte Damen und Herren,

nach unserer ersten hochrangigen Sitzung 2012 auf der CeBIT freuen wir uns, Sie nunmehr zur zweiten Sitzung nach München einladen zu können. Diese findet statt am

Montag, 11. Juni 2012, 13.00 – 15.00 Uhr
bei [redacted]

Folgende Agenda sehen wir vor:

1. Überblick zum aktuellen Planungsstand des IT-Gipfels (einschl. Podiumsdiskussion und Veranstaltungskonzept für den Vortag)

Bundesministerium
des Innern

[redacted]

2. Bericht zu den Sachständen in den Unterarbeitsgruppen
3. Diskussion Thema „Providerverantwortung"
4. Sonstiges.

Wir freuen uns darauf, Sie am 11. Juni zahlreich in [redacted] begrüßen zu dürfen. Bitte bestätigen Sie Ihre Teilnahme bis möglichst 1. Juni gegenüber [redacted] ([redacted].com) und dem Bundesministerium des Innern (Norman.Spatschke@bmi.bund.de) und führen am Sitzungstag Ihren Personalausweis mit.

Wir freuen uns auf interessante Diskussionen.

Mit freundlichen Grüßen

Dr. Hans-Peter Friedrich
(Bundesminister des Innern)

[redacted]
(Vorsitzender der Geschäftsführung)

Referat IT 3
RR'n Gitter

4. Juni 2012

Sitzung der AG 4 des IT-Gipfels
"Vertrauen, Datenschutz und Sicherheit im Internet"
am 11. Juni 2012

TOP 3: Stärkung Providerverantwortung	**Aktiv**

Ziel dieses TOPs ist, die inhaltliche Diskussion zur Frage der Providerverantwortung und möglichen Regelungserfordernissen anzustoßen.

Ziel der Behandlung ist es, im Vorfeld möglicher Regelungsvorhaben in einem IT-Sicherheitsgipfel die Thematik mit allen Providern zu erörtern. Wichtige Provider (Telekom, Vodafone, 1&1) sind in der AG 4.

Sachstand

Bedrohungslage

- Die Anzahl neuer Schadprogramme nimmt weiterhin stark zu. Täglich werden etwa 13 neue Schwachstellen in Standardsoftware entdeckt, die durch Mutationen für 60.000 Schadprogramme und 20.000 manipulierte Webseiten missbraucht werden können.
- Signifikante Bedrohungen gehen immer mehr von Botnetzen aus, in denen – häufig über Ländergrenzen hinweg – eine Vielzahl durch Schadsoftware „gekaperte" Rechner zusammengeschaltet und ferngesteuert werden, um Angriffe gegen Dritte zu fahren. Beobachtet werden insbesondere Erpressungsversuche, bei denen solche Angriffe angedroht werden.
- Ein weiterer bedeutender Angriffsweg ist die Infizierung einzelner Rechner durch den Besuch mit Schadprogrammen manipulierter Webseiten. Diese sog. Drive-by-exploits dürften mittlerweile einen Großteil von Infektionen ausmachen.
- Im IT-Gipfelprozess der AG 4 hat der eco-Verband mit technischer Unterstützung des BSI das „Anti-Botnet Beratungszentrum" (ABBZ) initiiert. Das BMI unterstützte die erfolgreiche Initiative aus Mitteln des IT-Investitionsprogramms mit einer Anschubfinanzierung i.H.v. ca. 1,6 Mio. EUR. Problem: Unzureichende Beteiligung der Provider. Im Endeffekt war nur United Internet ([redacted], [redacted] und [redacted]) engagiert.
- Verfahren zur Erkennung und Abwehr von Malware bzw. Spam werden wahrscheinlich von einzelnen TK-Providern in unterschiedlichem Umfang bereits genutzt.

- Einzelne Provider informieren betroffene Kunden, vereinzelt sind auch Sperrungen einzelner Dienste (bspw. E-Mail) bzw. des Internetzugangs üblich.
- Im Einzelnen ist das Vorgehen der Provider sehr uneinheitlich. Zur Erkennung der Angreifer und Angriffsmuster müssen IP-Adressen und weitere Verbindungsdaten einige Zeit gespeichert werden. Derzeitige Regelung in § 100 TKG lässt dies aber nicht eindeutig für einen bestimmten Zeitraum zu.

Regelungsvorschläge zur Stärkung der Providerverantwortlichkeit im IT-SicherheitsG:

- Einheitliche Mindestanforderungen an die Gewährleitung von Sicherheit in den eigenen Netzen (TK-Provider) und bei Internetdiensten (Telemedien).
- Korrespondierend angemessene Rechte zur Durchführung von Schutzmaßnahmen und zur Detektion von Angriffen
- Stärkung der Kooperation zwischen Providern und Sicherheitsexperten durch einheitliche Meldewege und -pflichten (analog zu existierenden Regelungen für den Datenschutz)
- Konsequente Information und ggf. Unterstützung der Nutzer durch entsprechende Technik (Firewalls), um deren Handlungsfähigkeit und –willen zu stärken.

Gesprächsführungsvorschlag:

- **Die Gewährleistung von Sicherheit im Cyber-Raum ist zu einer existenziellen Herausforderung des 21. Jahrhunderts geworden.**
- **Cybersicherheit (die Sicherheit der IT-Infrastruktur und die sichere Nutzung dieser Infrastruktur) muss in erster Linie durch Prävention geleistet werden. Hierzu sind alle Beteiligten (Staat, Wirtschaft, private Nutzer) aufgefordert.**
- **Aufgabe des Staates ist es, den notwendigen Rahmen für Maßnahmen der Beteiligten zur Verfügung stellen.**
- **Freiwilliges Engagement einiger Provider etwa im Rahmen der Anti-Botnetz-Initiative zeigt den richtigen Weg auf. Wir müssen aber alle Provider stärker in die Verantwortung nehmen und – wo notwendig – auch die notwendigen Voraussetzungen für einen wirksamen Schutz des Cyber-Raums schaffen.**

- Im Einzelnen könnte hierfür eine Anpassung der gesetzlichen Rahmenbedingungen in TKG und TMG erforderlich erscheinen:
  - Durch einheitliche Mindestanforderungen an die Provider zur Gewährleistung von IT-Sicherheit,
  - zur Information und ggf. technische Unterstützung der Nutzer

  könnten Wettbewerbsvoraussetzungen für die Anbieter angeglichen und die IT-Sicherheit insgesamt erhöht werden.
- Korrespondierend muss für Provider Rechtssicherheit bestehen, dass die Durchführung von Schutzmaßnahmen und Maßnahmen zur Erkennung von Angriffen in angemessenem Umfang zulässig sind (z.B. sollte die Speicherung von Verkehrs- und Nutzungsdaten zum Erkennen und Beheben von Angriffen – wo erforderlich – zulässig sein).
- Kooperation zwischen Providern und Sicherheitsexperten muss ggf. durch die Schaffung einheitlicher Meldewege (analog zu existierenden Regelungen für den Datenschutz) gestärkt werden.

Referat IT3
ORR Dr. Dimroth

5.6. 2012

2. Sitzung der AG 4 am 11. Juni 2012

hier: IT-Sicherheitsgesetz

Sachstand

- BM hat im Februar dJ entschieden, dass in Umsetzung des in der Cybersicherheitsstrategie insoweit enthaltenen Prüfauftrages ein IT-Sicherheitsgesetz mit folgenden Kerninhalten vorbereitet werden soll:

  - Pflicht zur Erfüllung von Mindestanforderungen an IT-Sicherheit für Betreiber kritischer Infrastrukturen,
  - Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle für Betreiber kritischer Infrastrukturen,
  - Ressortübergreifend verpflichtende und einheitliche Vorgaben zur IT-Sicherheit für die Bundesverwaltung,
  - Pflicht zur Erfüllung von Mindestanforderungen an IT-Sicherheit für Telekommunikationsanbieter und Telemediendiensteanbieter,
  - Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle für Telekommunikationsanbieter,
  - Pflicht zur Information der Nutzer über Schadprogramme für Telekommunikationsanbieter,
  - Recht für Telemediendiensteanbieter Nutzungsdaten zur Störungsbeseitigung zu verwenden,
  - Erweiterung der Zuständigkeiten des BKA auf bestimmte Fälle von Cybercrime und
  - Erweiterung der Katalogstraftaten iSv § 100a StPO (Telekommunikationsüberwachung) auf bestimmte Fälle von Cybercrime.

- Entsprechende Formulierungsvorschläge wurden zwischenzeitlich erarbeitet und werden derzeit finalisiert, um im Anschluss eine Leitungsentscheidung dazu einzuholen und die Hausabstimmung einzuleiten.

- Darüber hinaus prüfen wir derzeit ob noch weitere Regelungsinhalte in den Gesetzentwurf übernommen werden sollten:

  - Mindestanforderungen an IT-Sicherheit für die gesamte Wirtschaft über entsprechende Regelungen im Wirtschaftsrecht (AktG; GmbHG; HGB).
  - Aufgabe und Befugnis des BSI zur Untersuchung von Hard- und Softwarekomponenten zur Förderung der IT-Sicherheit und Befugnis zur Veröffentlichung der hierbei erzielten Ergebnisse.
  - Regelungsinhalte die derzeit in den USA im Rahmen dortiger Gesetzesinitiativen zur Cybersicherheit diskutiert werden.
  - Jährliche Berichtspflicht des BSI auch zur Aufklärung der Öffentlichkeit (diesbezüglich ist allerdings fraglich, ob in Ermangelung der Betroffenheit personenbezogener Daten eine gesetzliche Regelung erforderlich ist).

- In Bezug auf die Kommunikation hat BM entschieden, zunächst (nach außen) zu kommunizieren, dass die **Ergebnisse** der derzeit laufenden **Ministergespräche abgewartet** würden und er im Anschluss je nach Ergebnis der Gespräche über die Erforderlichkeit gesetzgeberischer Maßnahmen entscheiden werde.

Referat IT 3
AR Spatschke

4. Juni 2012

Sitzung der AG 4 des IT-Gipfels
„Vertrauen, Datenschutz und Sicherheit im Internet"
am 11. Juni 2012

TOP 4: Sonstiges, Termine
Verabschiedung durch Hrn. Minister und [redacted]

- Wünsche / Anregungen zu diesem TOP erfragen.
- Hinweis auf nächste Sitzung der AG 4 am **27.9. von 14 – 16 Uhr**, dann wieder in Berlin. Die offizielle Einladung erfolgt rechtzeitig vor der Sitzung.

Dieses Blatt ersetzt die Seiten 260 - 272

Die Entnahme erfolgte mangels Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss

Bundesministerium des Innern

Referat IT 3

IT 3 – 606 000-2/112#18

Ergebnisprotokoll

Thema:	**Sitzung der AG 4 des IT-Gipfels „Vertrauen, Datenschutz und Sicherheit im Internet"**		
Ort: CeBIT Hannover	**Datum:** 6.3.2012	**Beginn:** 16.00 Uhr	**Ende:** 18.00 Uhr
Verfasser: AR Spatschke			**Seite:** 1 von 5

Teilnehmer:	
BM Dr. Hans-Peter Friedrich	Heike Troue (DSiN)
[redacted]	Michael Hange (BSI)
Martin Schallbruch (BMI)	[redacted]
Dr. Markus Dürig (BMI)	[redacted]
Norman Spatschke (BMI)	[redacted]
Vicky Radunz (BMI)	[redacted]
[redacted]	[redacted]
[redacted] (FhG AISEC)	Dr. Ibrahim Karasu (BdB)
Peter Schaar (BfDI)	[redacted]
[redacted]	[redacted]
Dr. Rainer Metz (BMELV)	[redacted]
[redacted]	[redacted]
[redacted]	
Abwesend: [redacted]	

Tagesordnung:

TOP 1: Begrüßung
TOP 2: Vorstellung /Verabschiedung der neuen AG-Struktur
TOP 3: Diskussion zum Thema „Cloud Computing"
TOP 4: Diskussion zum Thema „Mobile Sicherheit"
TOP 5: Diskussion zum Datenschutz
- Vorschläge KOM und Positionierung Deutschlands

TOP 6: Sonstiges, Termine

TOP 1

BM Dr. Friedrich und [redacted] eröffnen die Sitzung und begrüßen die Teilnehmer.
BM Dr. Friedrich betont, dass der IT-Gipfel in München im Rückblick gut verlaufen sei, insbesondere das durch die AG 4 verantwortete Forum „Cybersicherheit als Standortvorteil für Deutschland" habe interessante und fruchtbare Diskussionen ermöglicht.
Im Fokus der heutigen AG 4 – Sitzung stehe insbesondere die Weichenstellung der Arbeit der AG 4 im Jahr 2012. Es gibt keine Anmerkungen zur Tagesordnung.

Bundesministerium des Innern

TOP 2

BM Dr. Friedrich stellt einleitend die Veränderung in der Struktur der Unterarbeitsgruppen (UAG) der AG 4 dar. Die an den bisherigen Themenschwerpunkten „Cloud Computing" und „Sichere Identitäten" orientierten UAGs hätten ihre Arbeit zum Teil erfolgreich abgeschlossen und wichtige Zwischenziele erreicht. Daher solle die UAG-Struktur gestrafft und modifiziert werden. Folgende vier UAGs der AG 4 sollen in Zukunft tätig sein: *UAG 1 „Cloud Computing"*, *UAG 2 „Anforderungen an Sichere Identitäten"*, *UAG 3 „Providerverantwortung stärken"* und *UAG 4 „Mobile Sicherheit"*.

BM Dr. Friedrich betont, dass sich nach seinem Verständnis jedes Mitglied der AG 4 aktiv in mindestens eine UAG einbringen solle.

Die Themen „Cloud Computing" und „Mobile Sicherheit" werden separat erörtert, daher stellen die Vorsitzenden von UAG 2 und UAG 3 kurz die Aufgaben und Ziele ihrer jeweiligen UAGs vor.

Hr. Hange stellt die **UAG 2** vor, deren Vorsitz das BSI vom BMI übernommen habe. Mit dem vorgelegten und zum IT-Gipfel veröffentlichten Katalog an Mindestanforderungen für Identitätsprovider sei ein wichtiges Zwischenziel erreicht. In der sich nun anschließenden zweijährigen Evaluierungsphase gelte es, in einem 1. Schritt Evaluierungskriterien zu entwickeln und anhand dieser in einem 2. Schritt die Akzeptanz und den Mehrwert der Maßnahme festzustellen. Ziel sei es, eine Selbstverpflichtung der Wirtschaft anzustreben.

[redacted] weist darauf hin, dass eine Synchronisation mit den Aktivitäten der Forschungsunion hilfreich sein könnte.

[redacted] informiert über die **UAG 3**. Die ISPs wollten demnach Aufmerksamkeit und Sensibilität der Nutzer für das Thema Schutz und Sicherheit weiter stärken. So habe die DTAG soeben ihre Geschäftskunden auf die Botnetzproblematik und das ABBZ aufmerksam gemacht.

BM Dr. Friedrich erläutert, dass dem Thema „Providerverantwortung" aus seiner Sicht eine besondere Bedeutung zukomme. Das ABBZ spiele dabei eine wichtige Rolle, jedoch seien weiterführende und koordinierte Maßnahmen der Provider nötig, um die Kunden bei der Absicherung ihrer Systeme zu unterstützen. Je mehr freiwillige Maßnahmen Provider zum Schutz ihrer Kunden ergreifen würden, desto weniger seien entsprechende Aktivitäten des Gesetzgebers erforderlich. Dies könne auch einen Wettbewerbsvorteil für Provider generieren.

[redacted] betont, dass die Rolle des Providers die des „Helfers" und nicht die des „Aufpassers" sein müsse. [redacted] habe im Zusammenhang mit der DNS-Changer-Problematik ca. 4.000 Kunden angeschrieben, die trotz verstärkter Öffentlichkeitsarbeit bis dahin nicht aktiv geworden waren. Die Folge dieser Unterstützungsleistung wäre ein überwiegend positives Feedback seitens der Kunden gewesen.

TOP 3

[redacted] führt in die Thematik ein und erläutert, dass es zum „Cloud Computing" bereits sehr viele Initiativen und Papiere gäbe. Daher sei es seine Erwartung an diese UAG, eine gewisse Konvergenz herbeizuführen und nicht zu divergieren.

Im Folgenden stellt [redacted] die Ergebnisse der UAG „Rechtliche Anforderungen an Cloud Computing" dar, die bis dato unter dem Vorsitz des BdB gestanden hat. Die UAG

habe die allgemein gültigen rechtlichen Rahmenbedingungen für die Nutzung und das Angebot von Cloud-Dienstleistungen anhand der drei Beispielbranchen Versicherungswirtschaft, Kreditwirtschaft und Telekommunikation untersucht und schlage Rechtsänderungen in verschiedenen Bereichen vor, z.B.: Flexibilisierung des AGB-Rechts, Modernisierung des Datenschutzrechts, Zulassung weiterer elektronischer Unterschriftsmechanismen.

[redacted] als Vorsitzender der UAG „Definition von technischen Anforderungen zur Nutzung von Cloud-Services" stellt darauf hin die Ergebnisse dieser UAG vor. Man habe zusammen mit dem BSI – aufbauend auf dem entsprechenden BSI-Eckpunktepapier – ein mehrstufiges Modell verschiedener Sicherheitsanforderungen entwickelt. Als nächste Schritte schlägt er die Erarbeitung technischer Richtlinien vor, die als Grundlage einer Zertifizierung dienen sollten.
[redacted] erwähnt in diesem Zusammenhang den Zertifizierungsantrag des GdV an das BSI zur Zertifizierung der „Trusted German Insurance Cloud".
Hr. Hange warnt davor, zu hohe Standards bei der Beschreibung des Schutzbedarfs zu setzen, da dann möglicherweise keine Geschäftsmodelle entwickelt werden könnten. **Dr. Ottenberg** unterstützt dies und schlägt ein pragmatisches Vorgehen vor.
Hr. Schaar hinterfragt den Ansatz einer „deutschen Cloud" kritisch und hebt die Vorzüge einer europäischen Lösung hervor.
Hr. Clemens betont demgegenüber die Bedeutung der Stärkung des Standortes Deutschland. Es sei für den Kunden wesentlich, Transparenz herzustellen und ihm die Verunsicherung zu nehmen. Die Kunden müssten die Unterschiedlichkeit von Angeboten erkennen und die richtigen Schlüsse für sich ableiten können.
[redacted] empfiehlt, die in Deutschland bestehenden hohen Standards auch in Europa zu setzen und verweist in diesem Zusammenhang auf die Arbeiten von SAP und Roland Berger („European Gold Standard"). [redacted] unterstützt die Forderungen nach Zertifikaten und verleiht seiner Sorge Ausdruck, dass der Mittelstand bei der Thematik „Cloud Computing" abgehängt wird.
BM Dr. Friedrich verweist zur Frage vermehrter europäischer Standardisierung auf sein am heutigen Tage stattgefundenes Gespräch mit Neelie Kroes. Die EU-KOM sei sehr engagiert, jedoch rate er zu einem Zweischritt: Zum einen sei es erforderlich, verstärkt deutsche Standards zu setzen. Parallel müsse Europa unterstützt werden.

Die Frage der Veröffentlichung der durch die UAGs erarbeiteten Papiere wurde nicht diskutiert. Sie sollen jedoch in die Arbeit der neuen, unter Leitung der D[redacted] stehenden UAG mit einfließen.

TOP 4
[redacted] stellt eingangs fest, dass die Einführung einer neuen Infrastruktur das Thema IT-Sicherheit um mindestens zehn Jahre zurückwerfe. Smartphones entwickelten sich zu den beliebtesten Angriffszielen von Hackern überhaupt. Neben der Gerätesicherheit stünde auch die Sicherheit und Vertrauenswürdigkeit von Anwendungen (Apps) im Vordergrund. Die Etablierung dieser UAG sei daher im besonderen Interesse der AG 4 und des IT-Gipfelprozesses insgesamt.
[redacted] verweist auf die aktuelle Kooperation von V[redacted] und [redacted] für die Realisie-

rung innovativer Sicherheitslösungen auf Basis von Standard-SIM-Karten. Zudem plädiert er dafür, nicht das Bedrohungsszenario in den Vordergrund zu stellen, sondern die Thematik als Chance zu begreifen.
[redacted] fragt, ob angesichts bereits bestehender Lösungen tatsächliche neue Ansätze entwickelt werden müssten. [redacted] betont, dass bestehende Ansätze weiter entwickelt würden, der Blick jedoch auf die Massenvermarktbarkeit gerichtet werden müsse. **Hr. Schallbruch** informiert über den bereits im Sherpakreis erörterten Ansatz, demzufolge Sicherheitsanforderungen definiert werden müssten, die unterschiedlichen Anbieter unterbreitet werden könnten. Die kürzlich seitens BMI mit Apple geführten Gespräche hätten ein solches Interesse an Sicherheitsanforderungen bestätigt.
[redacted] hinterfragt, warum aus Ressourcengründen die Behandlung der Thematik „Sicherheit mobiler Netze" unterbleiben solle. Sie verweist in diesem Zusammenhang auf Hacks von Mobiltelefonen, die sie im Rahmen der CeBIT gesehen habe. Aus Verbrauchersicht seien bestehende Sicherheitsrisiken und die Identifikation etwaiger Strukturen ein nicht zu vernachlässigendes Thema.
In der sich hieran anschließenden Diskussion betonen [redacted], **Hr. Schallbruch** und **Hr. Hange** übereinstimmend, dass es allgemein bekannt sei, dass der GSM-Standard unsicher sei und sich zahlreiche (internationale) Gremien mit diesen Fragen auseinandersetzen. Auch das BSI beteilige sich an der Diskussion. Für die sichere Regierungskommunikation würden solche Erkenntnisse berücksichtigt und zusätzliche Sicherheitsfeatures etabliert. Dieser Ansatz sei aber für die Endanwender zu aufwendig.
[redacted] hält neben der – bereits geführten – technologischen Diskussion die Frage der Verbraucheraufklärung als wesentlich an. Hier solle DSiN eine bedeutendere Rolle spielen.
[redacted] unterstreicht, dass das Thema „Vertrauen" eine noch zu geringe Rolle spiele.
[redacted] sieht in der Aufklärung der Verbraucher ebenfalls einen wichtigen Ansatz.

TOP 5
BM Dr. Friedrich informiert über die Pläne der EU-KOM zur Reformierung des EU-Datenschutzes. Demnach habe die KOM Anfang Januar 2012 den Entwurf eines Datenschutz-Pakets vorgelegt, das aus zwei Rechtsakten besteht. Die Richtlinie 95/46/EG solle durch eine Verordnung, KOM(2012) 11, ersetzt werden, während an die Stelle des Rahmenbeschlusses im Polizei- und Justizbereich eine Richtlinie, KOM(2012) 10, treten solle.

BM Dr. Friedrich begrüßt den Ansatz der KOM, die Reform des europäischen Datenschutzrechts anzustreben. Dies sei der wichtigsten und zugleich herausforderndsten Themen unserer Informationsgesellschaft. Das geltende Datenschutzrecht stamme aus der Zeit vor dem Internet. Damals herrschten gänzlich andere Voraussetzungen als heute: Die private Nutzung von sozialen Netzwerken ließe sich nicht mit der staatlichen Volkszählung von einst vergleichen. Dasselbe gelte für andere Alltäglichkeiten des Internets, wie Mails, Blogs, Foren oder zahlreiche mobile Anwendungen. Der Nutzer begreife das Internet zunehmend als einen Ort der freien Entfaltung. **BM Dr. Friedrich** schlussfolgert, dass sich daraus ein „Recht auf Datenverarbeitung" ableiten ließe. Diesem berechtigten Anliegen müsse unser Datenschutzrecht Rechnung tragen.
Punktuelle Regelungen, die den Neuerungen der Informationsgesellschaft gerecht werden, reichen aus seiner Sicht nicht aus. Vielmehr müssten grundsätzliche Fragen neu gestellt

werden. So würden beispielsweise zahlreiche Dienste des Internets (z.B. Blogs, Twitter) inzwischen presseähnlichen Charakter aufweisen. Den Aspekt der Meinungs- und Informationsfreiheit ebenso wie der Pressefreiheit berücksichtige die Verordnung viel zu wenig und laufe somit Gefahr, damit die Freiheit des Internets einzuschränken.

BM Dr. Friedrich kritisiert weiter, dass der Entwurf nicht innovationsoffen und differenziert genug sei. So unterliege die automatisierte Buchhaltung eines kleinen Unternehmens grundsätzlich den gleichen Regelungen wie F[redacted] und G[redacted] Zudem sehe der Verordnungsentwurf eine Reihe materieller Verschärfungen und zusätzlicher Verpflichtungen für die Wirtschaft vor, die dadurch in erheblichem Umfang zusätzlich belastet würde.

Erschwerend sei darüber hinaus, dass künftig eine Abstimmung mit allen 27 Mitgliedsstaaten erforderlich sein könnte, da der Verordnungsvorschlag bei 91 Artikeln insgesamt 45 Ermächtigungen an die Kommission für weitergehende Durchführungsbestimmungen vorsehe. Hier müsse man fragen, ob mehr Detailregelungen und mehr Ermächtigungen an die Kommission immer einen besseren Schutz bedeuten.

BM Dr. Friedrich appelliert abschließend an die Mitglieder der AG 4, die Bemühungen des BMI gegenüber der KOM zu unterstützen, und sich in die datenschutzrechtliche Debatte einzubringen.

Hr. Schaar betont die außerordentliche Bedeutung der Thematik, begrüßt das Engagement des Herrn Ministers, teilt aber die meisten vorgebrachten Kritikpunkte nicht. Er hält den Entwurf für eine grundsätzlich sinnvolle Weiterentwicklung des Datenschutzrechts, sieht aber noch Verbesserungsbedarf. So müssten z.B. technologische Aspekte (privacy by default) weiter entwickelt und konkretisiert werden. Auch sei es nicht sinnvoll, das Handeln von Privatpersonen, die etwa in sozialen Netzwerken aktiv sind, generell der Aufsicht der Datenschutzbehörden zu unterstellen.

[redacted] begrüßt den Ansatz der Internationalisierung und Harmonisierung des Entwurfs. Er sieht durch den Entwurf jedoch eine massive Einengung der deutschen und europäischen Wirtschaft. So überhöhe beispielsweise der Verordnungsentwurf das Prinzip der Einwilligung, was – aufgrund des Charakters der Angebote - grundsätzlich Playern wie Google, Apple und Facebook entgegen komme, kleine und mittlere Unternehmen in Deutschland und Europa jedoch benachteilige. Aus diesem Grund sei eine gemeinsame Industriepolitik erforderlich. [redacted]e und [redacted] unterstützen diese Aussagen und befürchten ein Monopol der genannten Unternehmen für neue Services, anderen Unternehmen drohe der Verlust von Geschäftsmodellen. Es sei daher sei eine „Datenstandortpolitik" als ein wichtiger Impuls des IT-Gipfels nötig.

TOP 6

BM Dr. Friedrich und [redacted] beenden die Sitzung mit dem Hinweis, dass die nächste Sitzung der AG 4 am 11. Juni 2012 von 13:00 – 15:00 Uhr in München bei [redacted] stattfinden soll. Der diesjährige IT-Gipfel soll am 13. November 2012 in Essen stattfinden.

Im Hinblick auf diesen frühen Termin sollten alle vier Unterarbeitsgruppen nunmehr zeitnah ihre Arbeit aufnehmen und - soweit noch nicht geschehen – das Arbeitsprogramm im Kreis der UAG-Mitglieder abstimmen.

Verteiler: Mitglieder und „Sherpas" der AG 4

gez. Spatschke

Besuch des Bundesinnenministers Dr. Hans-Peter Friedrich, MdB

G&D München, 11. Juni 2012

Uhrzeit	Ablauf	Teilnehmer:
12:00 Uhr	**Begrüßung** (Haupteingang Prinzregentenstraße 159) **Photo** **Eintragung Gästebuch**	BM Herr Dr. Hans-Peter Friedrich [redacted](Gesellschafterin) [redacted]CEO) Herr Schallbruch, Herr Dr. Dürig, Herr Spatschke (BMI) [redacted]
12:10 Uhr	Besichtigung Banknotengalerie	BM Dr. Hans-Peter Friedrich [redacted](Gesellschafterin) [redacted]Geschäftsführer B[redacted]
12:30 Uhr	Besprechung zu [redacted]echnologiethemen (Raum 708-09) - Mobiltelefon als nPA-Leser - Zusammenarbeit Bundesdruckerei	[redacted](CEO) [redacted]Gesellschafterin) [redacted](Geschäftsführer G[redacted] [redacted]Geschäftsführer B[redacted] Herr Schallbruch, Herr Dr. Dürig, Herr Spatschke (BMI) [redacted]
12:55 Uhr	Ende und Wechsel in den Konferenzbereich [redacted]	
13:00 Uhr	Sitzung der AG 4 des IT-Gipfels	Leitung: Herr BM Dr. Hans-Peter Friedrich Herr Dr. Karsten Ottenberg
15:00 Uhr	Ende der Sitzung und Verabschiedung	

[redacted]

Spatschke, Norman

Von: Schallbruch, Martin
Gesendet: Mittwoch, 25. April 2012 13:50
An: IT3_
Cc: IT4_; IT1_; IT5_; ITD_
Betreff: WG: 11. Juni 2012 - BM Teilnahme / Leitung der Sitzung der AG 4 des IT-Gipfels

(Gemeint ist 12:00 Uhr [redacted] und 13:00 AG 4)

1) IT 1, IT 4, IT 5 z.K.
2) IT 3, bitte federführende Vorbereitung; bitte IT 4 und IT 5 zu [redacted] einbinden (bitte vor allem Komplexe Pass/nPA/Bundesdruckerei und S[redacted] vorbereiten); ich begleite He. Minister bei beiden Terminen
3) Bitte Ausdruck zTe, TÜL, Reiseplanung

Schallbruch

Von: Strahl, Claudia
Gesendet: Mittwoch, 25. April 2012 13:10
An: Schallbruch, Martin
Betreff: WG: 11. Juni 2012 - BM Teilnahme / Leitung der Sitzung der AG 4 des IT-Gipfels

---

Von: Körner, Bianca
Gesendet: Mittwoch, 25. April 2012 12:46
An: ITD_; Spatschke, Norman
Cc: PStSchröder_; Kuczynski, Alexandra; StRogall-Grothe_; Kluge, Barbara; Schlatmann, Arne; Radunz, Vicky; Weinhardt, Cornelius
Betreff: 11. Juni 2012 - BM Teilnahme / Leitung der Sitzung der AG 4 des IT-Gipfels

Sehr geehrter Herr Schallbruch, sehr geehrter Herr Spatschke,

am 11. Juni um 12:00 Uhr wird BM Dr. Friedrich an der nächsten AG 4 Sitzung des IT-Gipfels in München bei [redacted] teilnehmen. Im Vorfeld der Sitzung wird BM um 12:00 Uhr einen Termin mit Vertretern der Geschäftsführung von [redacted] wahrnehmen, bei dem BM über BMI-relevante Technologien des Unternehmens informiert werden soll. Ein kurzer Programmablauf ist dieser Mail beigefügt. Bitte senden Sie die Vorbereitung und ggf. einen Vorschlag für die fachliche Begleitung bis zum 4. Juni an das Ministerbüro.

Vielen Dank.

Mit freundlichen Grüßen

i.A.

Bianca Körner
Ministerbüro
Dr. Hans-Peter Friedrich MdB
Bundesministerium des Innern
Alt-Moabit 101 D
10559 Berlin
Tel: 030-186811002
Fax: 030-18681-1014

Fv bis 6.6.
u. W. in M6
f 30.5.

280

BMI

IT3-M-601 000-9/3#5

Refl: MinR Dr. Mantz
Ref: RRn Otte

Berlin, den 5. Juni 2012
Hausruf: 1374/2808

IT3

1. Fr. Otte cl. Übersandt
2. Ø Vorlage f. Leerlaufvermerk
3. Wv Ø 30.1.2013
4. Zdh

Herrn Minister

07.06

über

Abdruck:
Herrn St Fritsche
G I 2

Frau Stn Rogall-Grothe
Herrn IT-D
Herrn SV IT-D

Bundesministerium des Innern
SLRG
07. Juni 2012
1929

1) Ø SV ITD n.R.
2) IT3

Betr.: Überarbeitung von Außenwirtschaftsgesetz (AWG) und Außenwirtschaftsverordnung (AWV); Kompromissvorschlag zur Investitionsprüfung

Bezug: Ministervorlage vom 06.09.2011; Az. IT3-606 000-2/14#1
Vorlage Stn Rogall-Grothe vom 14.02.2012; Az. IT3-M-601 000-9/3#5

Anlage: - 1-

RR'n Otte z.d.V.

1. Votum

Billigung, die Forderung zur Verankerung eines Vorkaufsrechts zurückzustellen, falls BMWi zugesteht, die Investitionsprüfung gemäß den BMI-Forderungen anzupassen.

2. Sachverhalt

Wie von Herrn Minister gebilligt (Vorlage vom 06.09.2011) und von Frau Staatssekretärin bestätigt (Vorlage vom 14.02.2012), hat sich Referat IT 3 im Rahmen der derzeitigen Überarbeitung von AWG und AWV für eine Anpassung der Investitionsprüfung nach § 7 Abs. 2 Nr. 5 AWG eingesetzt. Nach § 7 Abs. 2 Nr. 5 AWG kann der Erwerb von gebietsansässigen Her-

stellern von Kryptosystemen zur Gewährleistung wesentlicher Sicherheitsinteressen der Bundesrepublik beschränkt werden. Hintergrund der BMI-Forderungen zur Anpassung der Investitionsprüfung sind aktuelle technische Entwicklungen sowie Schwachstellen und Lücken, die in den bisherigen AWG-Verfahren aufgetreten sind. Die Änderungen haben primär klarstellenden Charakter und dienen der Präzisierung der geltenden Rechtslage, um die Intention, die der Gesetzgeber mit der Einführung der Norm 2004 verfolgt hat, zu wahren. Nach Anpassung würde die Zahl der von der Investitionsprüfung erfassten Unternehmen von 25 auf 39 steigen (s. Anlage).
Ergänzend hat IT 3 im Vorgriff auf die Gründung einer Beteiligungsgesellschaft (zuletzt Ministervorlage vom 15.03.2012; Az. IT 3- 606 000-2/41#19) die Verankerung eines Vorkaufsrechts angestrebt, um zu gewährleisten, dass keines der vertrauenswürdigen Unternehmen, die Produkte mit IT-Sicherheitsfunktionen herstellen, infolge der Anordnung von Beschränkungen oder Handelspflichten nach § 7 Abs. 2 Nr. 5 AWG seine Tätigkeit einstellen muss, weil es nicht an die betriebswirtschaftlich erforderlichen frischen Kapitalmittel kommt.

BMWi hat zunächst sowohl eine Ausweitung der Investitionsprüfung auf Unternehmen, die ihre Produktion von zugelassenen IT-Sicherheitsprodukten eingestellt haben, aber noch über das Know-How verfügen bzw. deren Produkte noch im Einsatz in der Bundesverwaltung sind („hergestellt haben"), als auch das Vorkaufsrecht abgelehnt.

Jetzt hat BMWi Bereitschaft signalisiert, alle Forderungen bezüglich der Investitionsprüfung zu übernehmen ("Produkte mit IT-Sicherheitsfunktionen" statt „Kryptoprodukte", „zur Verarbeitung" statt „zur Übertragung", Einbeziehung wesentlicher Komponenten der IT-Sicherheitsprodukte und Aufnahme von „hergestellt haben"). Das Vorkaufsrecht wird jedoch weiter abgelehnt.

3. Stellungnahme

Der Verzicht auf das Vorkaufsrecht bei Übernahme aller Forderungen zur Investitionsprüfung ist ein für BMI guter Kompromiss.
Damit wäre es gelungen, alle wesentlichen Forderungen zur IT-Sicherheit zu verankern und die Investitionsprüfung als wirksames Instrument zu erhalten. Die Übernahme der Forderungen hinsichtlich der Investitionsprüfung stellt ein deutliches Zugeständnis des BMWi dar. Bisher wurde die Forderung unter Verweis auf den Auftrag aus dem Koalitionsvertrag, das Außenwirtschaftsrecht zu entschlacken, strikt abgelehnt.

Die Verankerung des Vorkaufsrechts ist zwar weiter wünschenswert. Vor vor dem Hintergrund, dass die Bestrebungen zur Gründung einer Beteiligungsgesellschaft jedoch nicht ausreichend fortgeschritten sind, die Finanzierung noch fraglich ist und eine staatliche Beteiligung an Unternehmen auch ohne Verankerung im AWG möglich wäre, kann die Forderung aber zunächst zurückgestellt und auf einen späteren Zeitpunkt verschoben werden.

auf dem wieder auf die TO, wenn wir sowas sind!
Thema für Koal Verh. in 2013

Dr. Mantz

Otte

Anlage

Unternehmen, die zugelassene Kryptosysteme herstellen oder hergestellt haben

Hersteller	Kurzinformation
D[redacted]AG	
A[redacted]GmbH	Ethernet Verschlüsselungssystem
B[redacted]	
b[redacted]	OSCI Kommunikationssoftware, Software zur Dateiverschlüsselung und -signierung
C[redacted]	Verschlüsselungslösung für mobile IT (z.B. Notebooks)
C[redacted]s GmbH	Kryptoboxen
C[redacted]GmbH	Kryptographisches E-Mail-PlugIn für Microsoft Outlook mit smartcard.
E[redacted]	Produkt zur Trennung von Netzen mit unterschiedlichen Einstufungen, Abstrahlgeräte
G[redacted]	Firewall mit VPN-Funktionalität (IPSec).
L[redacted]	
N[redacted]GmbH	Mobiler Zugang zum IVBB
O[redacted]AG	Produkte im Rahmen von SAR-Lupe und SATCOM BW, Gallileo
[redacted]	Militärisches Funkgerät
[redacted]GmbH	Sprach-Verschlüsselung im GSM-Netz.
S[redacted]GmbH	Kryptosystem mit S2M-Schnittstelle für verschlüsselte Kommunikation in ISDN-Netzen.
S[redacted]AB	
S[redacted]AG	Verschlüsselungssysteme
S[redacted]	Mobilfunktelefon mit Sprachverschlüsselung, SNS-Karte
S[redacted]	Realisierung eines sicheren Kommunikationskanals für TCP/IP-basierte Client/Server-Anwendungen.
S[redacted]	Herstellung abstrahlgeschützter Hardware
S[redacted]	
T[redacted]GmbH	Lösung zur mobilen Datensynchronisation
T[redacted] (T[redacted], T[redacted] Defence)	Tragbarer Schlüsselmittelspeicher mit Schnittstellen RS 232, DS 101 und DS 102 zur Nutzung im Schlüsselmittelverteilsystem VESUV.
T[redacted] (jetzt: [redacted]	Kryptosystem zur Verschlüsselung von Daten im analogen Netz mit V.24-Schnittstelle (Kryptomodem).
V[redacted]	Kryptogerät für Satellitenkommunikation.

Anlage

Hersteller von IT-Sicherheitsprokuten bzw. Systemen zur Übertragung von Verschlusssachen, die durch die Neufassung zusätzlich erfasst würden

Hersteller	Kurzinformation
C[redacted]GmbH, Karlsruhe	Projekt RMCDE-Übergänge für das MILRADNET
I[redacted]	Produkt zur Trennung von Netzen mit unterschiedlichen Einstufungen
K[redacted]	Datenlöschgerät für magnetische Datenträger
U[redacted]AG	Software für Zugangskontrolle und Festplatten-Verschlüsselung insbesondere auf Notebooks.
Z[redacted]	Datenlöschgerät für magnetische Datenträger

Hersteller wesentlicher Komponenten, die möglicherweise durch die Neufassung zusätzlich erfasst würden

Hersteller	Kurzinformation
C[redacted]GmbH	Hersteller abstrahlgeschützter Hardware
D[redacted]GmbH, Bremen	Projekt Euro Hawk: Entwicklung add-on German crypto system
E[redacted]GmbH	Hersteller abstrahlgeschützter Hardware
G[redacted]GmbH	Hersteller abstrahlgeschützter Hardware
[redacted]	micro-SD Karte für SNS
I[redacted]AG	Hersteller von Smartcards, die als Langzeitspeichermedium für Schlüssel in Frage kommen
I[redacted]Stuttgart	Hersteller von Krypto-Asics, insbesondere in älteren, aber noch im Gebrauch befindlichen Geräten wie das ED 6.2
[redacted]	Hersteller von Smartcards, die als Langzeitspeichermedium für Schlüssel in Frage kommen
T[redacted]Ulm	Projekt SVFuA, Wellenform MAHRS/TIGER

Radunz, Vicky

Von: Radunz, Vicky
Gesendet: Montag, 11. Juni 2012 19:12
An: ITD_; Schallbruch, Martin
Cc: SVITD_; Batt, Peter; IT3_; Mantz, Rainer, Dr.; Franßen-Sanchez de la Cerda, Boris; StRogall-Grothe_; StFritsche_; Hübner, Christoph, Dr.; GI2_; KabParl_; Schlatmann, Arne; Kluge, Barbara; Weinhardt, Cornelius
Betreff: Vorlage Überarbeitung Außenwirtschaftsgesetz, Kompromissvorschlag zur Investitionsprüfung

Lieber Herr Schallbruch,

anliegend vorab z.K. der Rücklauf der Vorlage zur Überarbeitung des Außenwirtschaftsgesetzes und der Außenwirtschaftsverordnung von IT 3. Zur Stellungnahme Vorverkaufsrecht die Bemerkung des Ministers auf S. 3 z.K.:

„muss dann wieder auf die TO, wenn wir soweit sind! Thema für Koa(litions)Verhandlungen in 2013"

Beste Grüße
Vicky Radunz

Ministerbüro
Bundesministerium des Innern
Telefon: 0049 30 18 681-1075
Fax: 0049 30 18 681-1018
E-Mail: vicky.radunz@bmi.bund.de

Von: Fax 1018
Gesendet: Montag, 11. Juni 2012 15:41
An: Radunz, Vicky
Betreff: 5 Seite(n) empfangen. (MID=939037)

939037_FAX_1206
11-154105.TIF

Dieses Blatt ersetzt die Seiten 286 - 294

Die Entnahme erfolgte mangels Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss

Dieses Blatt ersetzt die Seiten 295 - 300

Die Entnahme erfolgte mangels Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss

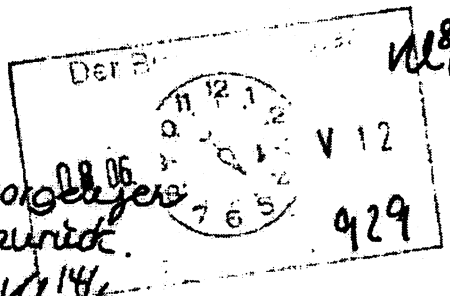
4660
301

BMI

IT3-606 000-9/31#1

Refl: Dr. Dürig/Dr. Mantz
Ref: Dr. Pilgermann/RRn Otte

Berlin, den 07. Juni 2012
Hausruf: 1374/1527/2808

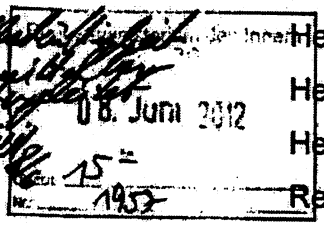


LHB:
Hat BM vorgelegen
Mit Dank zurück.

Herrn Minister

über

Frau Stn Rogall-Grothe
Herrn IT-D
Herrn SV IT-D



Abdrucke:

Herrn PSt Dr. Bergner;
Herrn St Fritsche;
Herren LLS, AL ÖS und AL KM;
Referate Presse und Z 9

IT 3
Dr. Pilgermann e.a.V.

Betr.: IT-Schutz kritischer Infrastrukturen; Vorbereitung Ministerspräch mit Vertretern des Energie-Sektors

Bezug: Ministervorlage vom 17. April 2012; Az. IT3-606 000-9/31#1

Anlage: Vorbereitungsmappe

Zur Vorbereitung Ihres Gesprächs mit Vertretern des Energie-Sektors am 13. Juni 2012 erhalten Sie anliegende **Vorbereitungsmappe**.

Nach den bereits geführten Gesprächen:

- 9. Mai mit Vertretern des Finanz- und Versicherungswesens, sowie
- 23. Mai mit Vertretern des IKT-Sektors

findet am 13. Juni 2012 der dritte Termin der Gesprächsreihe mit Vertretern des Energie-Sektors statt. Ziel ist es, gemeinsam mit Vorständen und Verbänden der betroffenen Branchen den IT-Schutz Kritischer Infrastruktu-

ren zu stärken und umfassende und flächendeckende IT-Sicherheitsstandards und Meldewege zu etablieren.

Teilnehmer: Bisher haben 21 Teilnehmer aus der Wirtschaft zugesagt. Teilnehmen wird zudem Herr Staatssekretär Kapferer, BMWi (s. Teilnehmerliste, **Fach 1**).

Hinweis Ministerbüro: Eine aktualisierte Teilnehmerliste wird rechtzeitig zum Termin vorgelegt.

Dr. Düwig / Dr. Mantz

elektr. ger.
Dr. Pilgermann / Otte

Ministergespräch IT-Schutz kritischer Infrastrukturen

Energie-Sektor

BMI, Raum 1.071, 13. Juni 2012, 15-17 Uhr

➢ Agenda und Teilnehmerliste	**Fach 1**
➢ Gesprächsführungsvorschlag Begrüßung	**Fach 2**
➢ Gesprächsleitfaden Cybersicherheit aus fachspezifischer Sicht	**Fach 3**
➢ Gesprächsleitfaden und Unterlagen Cybersicherheitslage	**Fach 4**
➢ Gesprächsleitfaden und Diskussionspapier Anforderungen an IT-Schutz aus Sicht BMI	**Fach 5**
➢ Gesprächsleitfaden Diskussion der Anforderungen	**Fach 6**
➢ Gesprächsleitfaden Zusammenfassung / Ausblick	**Fach 7**
➢ Potentielle Fragen der Wirtschaft (und Antworten)	**Fach 8**
➢ Hintergrundinformationen KRITIS Allgemein	**Fach 9**
➢ Hintergrundinformationen KRITIS im Energie-Sektor	**Fach 10**
➢ Cybersicherheitsstrategie	**Fach 11**

Bundesministerium des Innern

Agenda

IT-Schutz kritischer Infrastrukturen im Energie-Sektor

13. Juni 2012, 15-17 Uhr, Raum 1.071

Bundesministerium des Innern, Alt-Moabit 101D, 10559 Berlin

15:00 – 15.07 **Begrüßung und Einführung**
Dr. Hans-Peter Friedrich, Bundesminister des Innern

15:07 – 15:10 **Cybersicherheit/IT-Sicherheit im Energie-Sektor aus fachspezifischer Sicht**
Stefan Kapferer, Staatssekretär im Bundesministerium für Wirtschaft und Technologie

15:10 – 15:20 **Cybersicherheitslage in Deutschland**
Michael Hange, Präsident des BSI
Möglichkeit zu Rückfragen zur Gefährdungslage

15:20 – 15:25 **Energieversorgung und Aufgaben des BBK**
Ralph Tiesler, Vizepräsident des BBK

15:25 – 15:30 **Anforderungen an den IT-Schutz kritischer Infrastrukturen aus Sicht des BMI**
Martin Schallbruch, IT-Direktor im Bundesministerium des Innern

15:30 – 16:50 **Diskussion der Anforderungen an den IT-Schutz kritischer Infrastrukturen und der getroffenen Maßnahmen**
Diskussionsleitung: Dr. Hans-Peter Friedrich, Bundesminister des Innern

16:50 – 17:00 **Zusammenfassung und Ausblick**
Dr. Hans-Peter Friedrich, Bundesminister des Innern

Stand: 13. Juni 2012

Ministergespräche IT-Schutz kritischer Infrastrukturen

Teilnehmerliste Energie

Teilnehmer Wirtschaft

Strom – Erzeuger

1. [redacted], Vorstand, R[redacted]
2. [redacted], Leiter Konzernsicherheit, R[redacted]
3. [redacted], Vorstand, E[redacted] AG
4. [redacted], Director Business Information Office Production IT, V[redacted] AG
5. [redacted] Mitglied des Vorstandes, E[redacted]

Strom – Netzbetreiber

6. [redacted], Geschäftsführer Märkte und Systembetrieb,
7. [redacted], Leiter Systemführung,
8. [redacted] Geschäftsführer, T[redacted] GmbH
9. [redacted], Vorsitzender der Geschäftsführung, T[redacted] GmbH
10. [redacted] Leiter Netzführung, T[redacted] GmbH
11. [redacted], Technischer Geschäftsführer, A[redacted]
12. [redacted] Leiter Systemführung Netze Brauweiler, A[redacted] GmbH

Gas – Handel (und Speicher)

13. [redacted] Sprecher der Geschäftsführung, W[redacted]
14. [redacted], Abteilungsleiterin Information Management, W[redacted]

Gas - Netzbetreiber

15. [redacted], Geschäftsführer Business Services, O[redacted] GmbH
16. [redacted] Head of IT-Management, O[redacted] GmbH

Stand: 13. Juni 2012

Mineralöl

17. [redacted], Vorstand, B[redacted]

Verbände

18. [redacted]H, stellvertretener Geschäftsführer,
B[redacted]e. V.

19. [redacted] Fachgebietsleiter Beschaffung, Logistik, IT
Bu[redacted]t e. V.

20. [redacted] Geschäftsführer,
V[redacted]e. V.

21. [redacted]orsitzender des Vorstandes,
[redacted]e. V.

Staatliche Teilnehmer

22. **Herr Stefan KAPFERER**, Staatssekretär
Bundesministerium für Wirtschaft und Technologie

23. **Herr Michael SCHULTZ**, Referatsleiter,
Bundesministerium für Wirtschaft und Technologie

BMI

24. **Herr Martin SCHALLBRUCH**, IT-Direktor

25. **Herr Arne SCHLATMANN**, Leiter Leitungsstab

26. **Frau Barbara KLUGE**, Leiterin Ministerbüro

27. **Frau Dr. Barbara SLOWIK**, Leiterin ÖS II 1

28. **Herr Stefan VON HOLTEY**, Leiter KM 4

29. **Herr Dr. Rainer Mantz**, Leiter IT 3

30. **Herr Dr. PILGERMANN**, Referat IT 3

Geschäftsbereich

31. **Herr Michael HANGE**, Präsident, BSI

32. **Herr Ralph TIESLER**, Vizepräsident, BBK

33. **Herr Jürgen MAURER**, Vizepräsident, BKA

34. **Herr Frank SASSENSCHEIDT-GROTE**, Referatsgruppenleiter 4A, BfV

Referat IT 3
Verfasser RRn Otte

5. Juni 2012
Hausruf 2808

Ministergespräche IT-Schutz kritischer Infrastrukturen
Gesprächsführungsvorschlag Begrüßung

Begrüßung teilnehmende Wirtschaftsvertreter,
Herr **Kapferer** (Staatssekretär, Bundesministerium für Wirtschaft und Technologie)

Die Gewährleistung von IT-Sicherheit ist eine der zentralen Fragen unserer Zeit.

- In unserer **global vernetzten Welt** sind Staat, Wirtschaft und Bevölkerung auf das **verlässliche Funktionieren** von **Informations- und Kommunikationstechnologie** und des **Internets** angewiesen.
  Wir profitieren als **Industrienation**: Die **rasante Fortentwicklung** der IT und die zunehmende Vernetzung eröffnen **Chancen** und schaffen Innovationen. Sie sind ein wichtiger Baustein für Produktivität, **wirtschaftliches Wachstum und Wohlstand**.

- Gleichzeitig steigen mit der Abhängigkeit die **Risiken**: **IT-Ausfälle** stellen eine **reale Gefahr** dar.
  Dies zeigten zuletzt die Angriffe mit **infizierten E-Mails auf Betreiber von Gas-Pipelines in den USA** im Frühjahr des Jahres. Das Schadprogramm **Stuxnet** 2010 war ein Weckruf und hat gezeigt, dass selbst vom Internet abgekoppelte Prozesse und Systeme angreifbar sind und aufgrund des weitverbreiteten Einsatzes gleicher Systeme (hier SCADA) weitreichende Folgen haben können.
  Seit wenigen Wochen kursiert ein weiteres Schadprogramm namens **Flame** durch Fachkreise und auch Medien – Herr **Hange**, der **Präsident** des Bundesamtes für die Sicherheit in der

Informationstechnik, wird im Anschluss einen **Überblick über die Gefährdungslage** geben.

- Die **Gefährdungslage ist real** und **Anlass** für mich, **Sie heute einzuladen.** Lassen Sie uns **gemeinsam** überlegen, wie wir uns **besser aufstellen** können. Ihnen kommt als **Vertreter der großen Unternehmen** und **Verbände** der **Energiebranche** in Deutschland eine **unverzichtbare wirtschaftliche und gesellschaftliche Rolle** zu.

Schutz kritischer Infrastrukturen: Daseinsvorsorge des 21. Jahrhunderts

- Als Bundesminister der Innern ist mir der Schutz der für unsere Gesellschaft elementaren **Infrastrukturen** ein **besonderes Anliegen. Widerstandsfähige Infrastrukturen** und ein sicheres, verfügbares und vertrauliches Internet über nationale Grenzen und Rechtssysteme hinweg sind das **Rückgrat unserer globalisierten Welt.** Es ist Aufgabe des Staates, die **Grundversorgung sicherzustellen** und kritische Infrastrukturen zu schützen (Daseinsvorsorge und Gefahrenabwehr).

- Dabei geht es um das **robuste Funktionieren** und die **permanente Verfügbarkeit der für die Bevölkerung elementaren Dienstleistungen.**

- **Energie ist die Basisinfrastruktur. Auf Energie und insbesondere auf Elektrizität sind alle anderen Infrastrukturen** (IKT, Banken und Versicherungen, Wasserversorgung, Medien etc.) **sowie auch die Bevölkerung, der Staat und die Gesamtwirtschaft angewiesen.** Die **Folgen** einer längeren Unterbrechung können für Bevölkerung, Staat und Wirtschaft **katastrophal** sein.

- **Zudem ist die Energieversorgung von einer dezentralen Versorgungstruktur geprägt. Ich möchte gleich vorwegnehmen, dass entsprechende Äußerungen meinerseits Ende Mai in einem Interview (sog. Madsack-Gespräch) nicht überall korrekt wiedergegeben wurden. Ohne Frage besteht eine hohe Abhängigkeit der Gesellschaft von Energie und die Strukturen erfordern besondere Maßnahmen – Umsetzungsstand und alles Weitere wollen wir jedoch heute erörtern.**

Rolle und Aufgabe BMI

- Die Bundesregierung hat den IT-Schutz der kritischen Infrastrukturen mit der **Cyber-Sicherheitsstrategie** (Februar 2011) in den Mittelpunkt ihrer Maßnahmen zur Cyber-Sicherheit gestellt.

- Hiermit habe ich auch den Auftrag erhalten, **gesetzgeberische Maßnahmen zu prüfen**. Dies entspricht der **internationalen Diskussion**. Ich war gerade in den **USA**, wo entsprechende Gesetzesvorschläge zur Cyber-Sicherheit im Kongress intensiv beraten werden.

- Ich bin der Auffassung, dass wir auch in **Deutschland bundesweit einheitliche Mindestanforderungen und Meldewege** brauchen und dass der Weg der USA auch für uns eine Möglichkeit ist. Dabei sollten wir auf Vorhandenes aufbauen. Die Finanz- und IKT-Branche sind hier schon sehr weit und auch für die **Energiebranche gibt es bereits solide Regeln** (§ 11 Abs. 1a EnWG).

- Für den Schutz kritischer Infrastrukturen spielt der Ausbau der Zusammenarbeit im **Umsetzungsplan KRITIS** eine wesentliche Rolle. Hier haben wir seit 2007 ein Gremium der **Zusammenarbeit**

etabliert. Dieses Erfolgsmodell wollen wir weiter voranbringen und stärken.

- Zudem haben wir mit dem **Cyber-Abwehrzentrum** die Basis für die operative Zusammenarbeit der zuständigen Bundesbehörden geschaffen und bringen **Know-how und Sachverstand** zusammen. Hiervon kann und soll auch die Wirtschaft profitieren.

Sicherheit kann nur gemeinsam gelingen

- Der **Staat** kann jedoch nur den **Rahmen** und die **Grundlagen** schaffen. Für die **Gewährleistung der Cyber-Sicherheit** sind wir auf Ihre Mitwirkung angewiesen. Sie sind als Betreiber in der Pflicht. **Nur gemeinsam** und in enger Kooperation können wir die Versorgungssicherheit und die Wettbewerbsfähigkeit in Deutschland sicherstellen.

- Das Gespräch heute mit Ihnen ist mir besonders wichtig. Die Energieversorgung steht nicht nur im Mittelpunkt aller kritischen Infrastrukturen. Mit der **Einführung von Smart Metern** stehen wir aktuell vor neuen Herausforderungen.

- Dabei **engagieren** gerade Sie als **große Konzerne** in der Energieversorgung sich seit Jahren **für die IT-Sicherheit**. So wurden mit dem BDEW-Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme" branchenintern wichtige Grundlagen gelegt.

- Den im UP KRITIS vertretenen Konzernen möchte ich für die engagierte und gute Zusammenarbeit danken.

Ziel der Gespräche: IT-Schutz flächendeckend stärken

- Unser heutiges Gespräch ist der **dritte Termin** in einer Reihe. Zu den kritischen Infrastrukturen zählen auch das Finanzwesen, IKT, Wasser, Verkehr, Gesundheitswesen, die Ernährungswirtschaft sowie Medien und Kultur. Mit Vertretern der Finanz- und IKT-Sektoren habe ich bereits gesprochen.
  (Die kritischen Infrastrukturen in Staat und Verwaltung können wir mit Strukturen wie dem IT-Rat in anderer Form schützen.)

- Ich möchte mit Ihnen **gemeinsam überlegen**, wo wir **weiter tätig** werden müssen, wo **Lücken** bestehen und **wie wir die IT-Sicherheit kritischer Infrastrukturen bundesweit flächendeckend gewährleisten** können. Was aus meiner Sicht grundlegend für den IT-Schutz kritischer Infrastrukturen ist, habe ich Ihnen mit der Einladung übermittelt (**Diskussionspapier** liegt aus). Bevor wir nachher in die Diskussion einsteigen, wird **Herr Schallbruch**, der IT-Direktor in meinem Haus, Ihnen **unsere Überlegungen vorstellen**.

- Ich möchte dieses Dokument **gemeinsam mit Ihnen weiterentwickeln.** Sie wissen selbst am besten, was gebraucht wird. **RWE** hat bereits **vor dem Gespräch umfassende Anmerkungen zu dem Papier übermittelt,** für die ich mich **bedanken** möchte. Auch die anderen Anwesenden möchte ich einladen, mir **im Nachgang** Ihre **Überlegungen** zum Dokument und zur Diskussion **schriftlich zukommen zu lassen** – Vertreter anderer Branchen haben sich zum Beispiel zu diesem Zweck auch zusammengefunden und gemeinsame Papiere abgestimmt.

Überleitung zu weiteren Vorträgen und zur Diskussion ⇒ Fach 3

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 07.06.2012
Hausruf: 1527

2. Cybersicherheit im Energie-Sektor aus fachspezifischer Sicht

Herr St. Kapferer (BMWi) wurde mit Einladungsschreiben von Stn. Rogall-Grothe um Vorbereitung eines kurzen Beitrags gebeten.

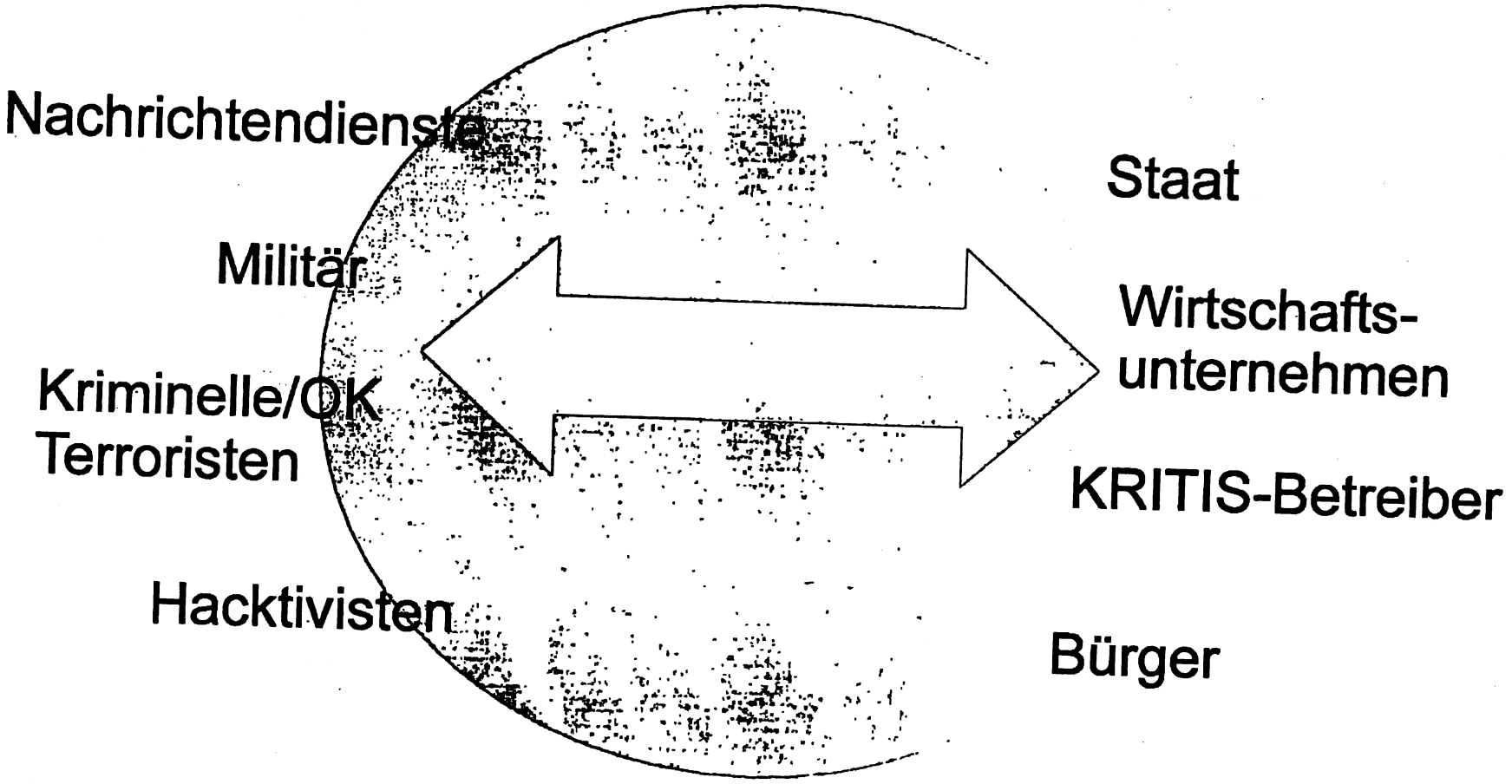
I. Sprechempfehlung

- Darstellung der gemeinsamen Vorgehensweise zw. Innenminister als KRITIS-Koordinierer und Fachressorts mit sektorspezifischer Kompetenz
- Hinweis auf die nunmehr verankerte IT-Sicherheit in der Aufsichtspflicht über den Energie-Sektor (EnWG); zudem Mitwirkung von BMWi und BNetzA im UPK
- Verweis auf Herrn St. Kapferer für einen Beitrag „Cybersicherheit im Energie-Sektor aus fachspezifischer Sicht"

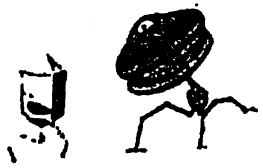
II. Aktueller Sachstand

- BMWi ist seit Beginn der Arbeiten im UPK (ab 2005) Teil der Kooperation mit der Wirtschaft. Die Aufsichtsbehörde BNetzA nimmt ebenfalls an den Sitzungen der Arbeitsgruppen teil.

Cyberangriffe und Cyber-Abwehr ein permanenter Wettlauf

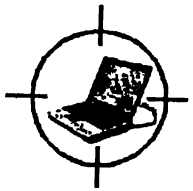


Gefährdungen



Ungezielte Angriffe

- Verfügbarkeit, Sabotage, Betrug
- Unspezifische Zielgruppen
- **Conficker**

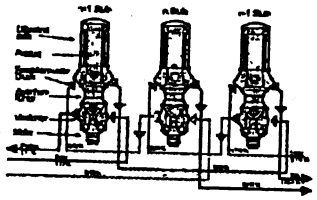


Gezielte Angriffe

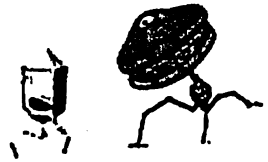
- Spionage, Sabotage, Identitätsdiebstahl
- Spezielle Zielgruppen
- **RSA**

Skalpellartige Angriffe

- Manipulation und Sabotage mit großem Schadensausmaß
- Komplexe, langwierige Vorbereitung
- **DigiNotar**
- **Duqu**



Gefährdungen



Ungezielte Angriffe

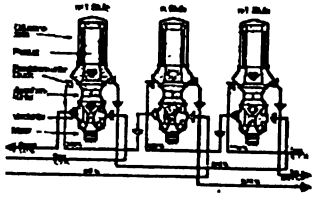
- USA 03: Virus legt Stromversorgung lahm
- Australien 09: Virenausbruch in Verwaltungsnetzwerk eines Stromversorgers

Gezielte Angriffe

- ICS-CERT (04/2012): Warnung vor gezielten Angriffen auf Gasversorger
- DHS 02/2012: Starker Anstieg der Anzahl der Angriffe auf KRITIS-Systeme innerhalb eines Jahres (von 11 auf 86)

Skalpellartige Angriffe

- **Stuxnet**



Bundesamt
für Sicherheit in der
Informationstechnik

Gefährdungslage

Michael Hange
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

13. Juni 2012

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 13.06.2012
Hausruf: 1527

3. Cybersicherheitslage in Deutschland

Herr P BSI Hange hat (in Abstimmung mit BKA / BfV) einen kurzen Vortrag zur Cyber-Bedrohungslage vorbereitet – Übergabe an diesen
Herr VP BBK Tiesler hat in Ergänzung einen Vortrag zu Auswirkungen aus Sicht BBK vorbereitet

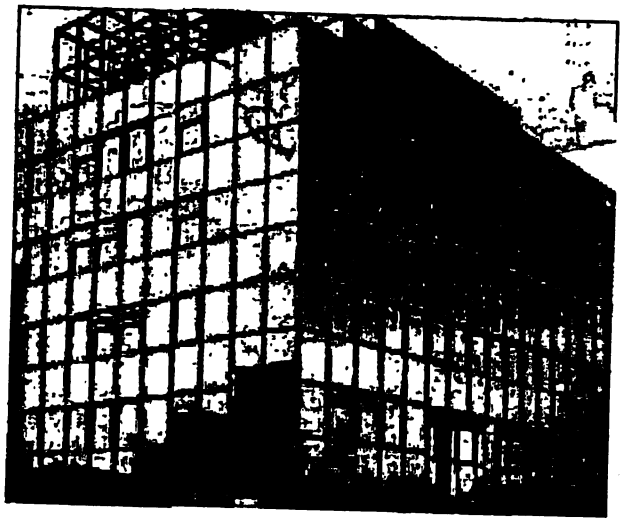
I. Sprechempfehlung

- Einführung zu Stuxnet als Schadprogramm, welches Ende 2010 mit seinen potentiellen Auswirkungen auf Atomkraftwerke das Thema Cybersicherheit endgültig auf die Tagesordnung aller Entscheider gesetzt hat
- Erinnerung an letzte LÜKEX-Übung von Nov. 2011, bei welcher im Bereich Kritischer Infrastrukturen breitflächige Ausfälle ein Bestandteil waren.
- Verweis an P BSI Herr Hange m.d.B. um einen Einblick in die Bedrohungslage im Cyberspace
-
- *(nach Vortrag P BSI)* Verweis an VP BBK Tiesler m.d.B. um Ergänzung aus der Perspektive Bevölkerungsschutz- und Katastrophenhilfe

II. Aktueller Sachstand

- Angespannte IT-Sicherheitslage, weil Abhängigkeit der Gesellschaft von Kritischen Infrastrukturen – hier insb. Energie und IKT erheblich gestiegen ist und die Angreifer sich professionalisiert haben
- BBK mit vergleichsweise hoher Kompetenz bei Kritischen Infrastrukturen im Energiesektor

Kontakt



Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Michael Hange
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-0
Fax: +49 (0)22899-10-9582-0

Michael.Hange@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de

VS – NUR FÜR DEN DIENSTGEBRAUCH
Ministergespräch KRITIS am 13. Juni 2012
Vorfälle

Konkrete KRITIS-relevante IKT-Vorfälle unmittelbar aus dem Energie-Sektor sind dem BSI nicht bekannt und wurden nicht gemeldet.

Folgende Vorfälle sind überwiegend IKT-Vorfälle im eigentlichen Sinne. Ähnliche Vorfälle könnten grundsätzlich aber auch durch gezielte Angriffe auf die eingesetzten IKT-Systeme (hier: Systeme zur Netzsteuerung (Vorfälle 1+3) bzw. zum Stromhandel (2)) ausgelöst werden. Vorfälle 1 und 2 sind auf den Vortragsfolien des Präsidenten des BSI aufgeführt.

Vorfall 1, Elektrizitätsversorgung: Stromausfall in Europa am 4. November 2006

- Teile von Deutschland, Frankreich, Belgien, Italien, Österreich, Spanien waren bis zu 120 Minuten ohne Strom
- Auslöser: Kurzfristige Abweichungen von der Planung für eine Abschaltung einer Höchstspannungsübertragungsleitung über die Ems und weitere Fehler führten zur zeitweisen elektrotechnischen Spaltung des europäischen Übertragungsnetzes in drei unabhängige Teile
- In unterversorgten Netzbereichen kam es durch sogenannten Lastabwurf zu Stromausfällen.
- Bundesnetzagentur hat den Vorfall eingehend untersucht.

Vorfall 2, Elektrizitätsversorgung: Stromhandel beeinträchtigt – fast – Netzstabilität

- Das deutsche Elektrizitätsnetz war Anfang Februar 2012 mehrfach an Stabilitätsgrenze.
- Auslöser: Zu gering eingekaufte Strommengen mussten durch Regelenergie kompensiert werden; dadurch fehlte Regelenergie für Zwecke der Netzstabilisierung.
- Bundesnetzagentur prüft, ob hier Verschulden einzelner Bilanzkreisverantwortlicher vorliegt.
- Vorfall wird vielfach von der Presse aufgegriffen (Schlagzeilen wie „Stromhändler zocken fast bis zum Blackout").

VS – NUR FÜR DEN DIENSTGEBRAUCH
Ministergespräch KRITIS am 13. Juni 2012
Vorfälle

Vorfall 3, Gasversorgung: Gedrosselte Gaslieferung nach Europa führt zur Abschaltung von Gaskraftwerken, und begünstigt Vorfall 2

- Durch die Anfang Februar 2012 von Russland um 30 Prozent gedrosselten Gaslieferungen nach Europa fehlte auch Gas in Süddeutschland, sodass Gaskraftwerke heruntergefahren werden mussten.
- Der Mangel an verfügbarer elektrischer Leistung wurde verschärft und begünstigte ggf. durch die weitere Verknappung von Erzeugungsleistung die im Vorfall 2 geschilderten Vorgänge am Strommarkt.

Vorfall 4, Gasversorgung: Pressemeldungen zu IT-Angriffen auf US-Pipelines

- Betreiber von Gas-Pipelines in den USA wurden gezielt *in der Bürokommunikationsumgebung* angegriffen. Diese kann Ausgangspunkt für Angriffe auf Steuerungssysteme (Projektierung von Anlagen, Vorbereitung des „Sprungs über die Luftschnittstelle) sein oder konkurrenzrelevante Informationen (Explorationsplanung, Fördermengen, ...) enthalten
- Laut Pressemeldungen konnten die Angreifer dadurch in einzelnen Fällen auch den Zugang zu Steuerungssystemen erreichen.
  (Wir vermuten bei Stuxnet auch den Sprung vom Büronetz ins Steuerungsnetz.)
- Nach Einschätzung des BSI handelt es sich hier um einen – in diesem Fall ggf. gelungenen – Angriff, wie er auch alle anderen Sektoren, aber auch Behörden betrifft, und im Regierungsnetz nahezu täglich abgewehrt wird. (vgl. VS-NfD-Bericht des BSI zu diesem Vorfall)
- Von diesem Fall unabhängig gibt es Hinweise auf gezielte Angriffe im Sektor Energie auch in DE.

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 07.06.2012
Hausruf: 1527

5. Diskussion der Anforderungen an den IT-Schutz

Diskussionspapier aus 4) war Wirtschaftsvertretern in Vorbereitung zur Verfügung gestellt worden

Moderation: Minister (entlang Diskussionspapier)

(Vorgeschlagener Fragesteller (Min/StnRG/ITD) jeweils in Klammern; **prioritäre Fragen fett)**

I. Sprechempfehlung

(Min) **Allgemeine Fragen:**

- Einschätzung zum Sachstand des IT-Schutzes der Kritischen Infrastrukturen im Sektor insgesamt
- **Kompatibilität von Auflagen und Rahmenbedingungen in Deutschland mit denen in anderen Ländern?**
- Erfahrungen aus der Zusammenarbeit im UPK seit 2007?

Fragen zu den Punkten aus dem Diskussionspapier:

1) *Mehr Transparenz schaffen*

(Die kritischen Geschäftsprozesse müssen identifiziert; die Abhängigkeit dieser Prozesse von IKT bekannt sein.)

- *StnRG:* **Besteht bei den IKT-Unternehmen übergreifend Transparenz bzgl. der Anforderungen, die andere Unternehmen (kritische Infrastrukturen) auf Grund ihrer Abhängigkeiten an diese stellen?** (Bezug auf Aussage der Banken vom 09.05. mit enormer Abhängigkeit von IKT und Energie).
- *ITD:* **Wie werden Risiken für die Gesellschaft im Risikomanagement prominent abgebildet?** (Bezug: eine im UPK erstellte Studie zu Abhängigkeiten von Kritischen Infrastrukturen bestätigt bereits jetzt die herausragende Bedeutung von Energieversorgern; explizit in allen 3 bekannten Branchen Strom, Gas und auch Mineralöl. Auch der TAB-Bericht des wissenschaftliches Dienstes des Bundestages hat die hohe Bedeutung noch einmal herausgearbeitet)

2) *Robuste Grundlagen*

(Mindeststandards müssen definiert sein. Regelmäßige Überprüfungen (Audits) verifizieren deren Umsetzung.)

Mindeststandards

- *StnRG:* **EnWG setzt Standards nur für Bereiche des Energie-Sektors (ausgenommen: Erzeuger und Händler sowie die gesamte Mineralölbranche): wie wird Erreichung mindestens dieses Niveaus in den nicht-regulierten Bereichen sichergestellt?**

Audits

- *ITD:* Wie groß ist inzwischen der Anteil von IT-Anforderungen in den regelmäßigen Audits (intern oder auch durch Externe)?
- *ITD:* Wie könnte in diesem Bereich eine Zusammenarbeit mit dem BSI aussehen?

3) *Kritische Prozesse autonom gestalten*

(Kritische Prozesse dürfen weder mit dem Internet verbunden sein noch von dessen Funktionstüchtigkeit abhängen.)

- *StnRG:* **Können zentrale IT-Systeme (zur Aufrechterhaltung der eigenen, zentralen Prozesse) unabhängig vom öffentlichen Internet fortbetrieben werden?**

4) *Produkt- und Dienstleistungssicherheit*

(Für besonders sensible Bereiche kommen zertifizierte Produkte zum Einsatz; IT-Sicherheit fließt von Anfang an mit in Planung von IKT-Diensten ein.)

- *Min:* **In BReg besondere Zulassungsverfahren für IT in sensiblen Bereichen. Gibt es vergleichbare Vorkehrungen zum Einsatz ausschließlich zertifizierter Systeme in den kritischen Bereichen?**

5) *Lagefortschreibung und Frühwarnung*

(Alle Unternehmen sind über die Warn- und Alarmierungsmechanismen des UPK an das BSI angeschlossen.)

- Min: Dank an Mitwirkende im UPK aus dem Sektor und Einrichtung von Meldekontakten und –mechanismen. **Was fehlt den Organisationen, um umfassend Meldekontakte einzurichten und in einem zweiten Schritt die Kommunikation mittels Einrichtung branchenspezifischer SPOCs zu bündeln?**

- *StnRG:* Vergleichsweise **geringes Meldeaufkommen über UPK-Strukturen** im Vergleich zur Lage in der Bundesverwaltung. Wie ist großer Unterschied zu erklären?

6) *Regelmäßige Übungen*

(Mit regelmäßigen Übungen werden aufgebaute Strukturen überprüft.)

- *ITD:* LÜKEX als erste nationale IT-Übung (Bund, Länder, KRITIS) Ende 2011 ein Erfolg – welche Formate des gemeinsamen Übens werden gebraucht?
- *ITD:* Wie ergänzen die Branchen die übergreifenden regelmäßigen Übungen aus dem UPK sektorspezifisch?

7) *Institutionalisierte Kooperation*

(Alle Branchen müssen im UPK vertreten sein. Darüber hinaus muss das Thema Cybersicherheit auch in allen Branchen intern in einer institutionalisierten Zusammenarbeit aufgearbeitet werden.)

- Min: **Herausragenden Dank an Mineralölwirtschaftsverband, welcher einen der beiden AG-Leiter für den UPK stellt: *Herr* [redacted] Dieser macht eine hervorragende Arbeit und hat maßgeblich zum Zusammenerhalt und Erfolg der UPK beigetragen.** Wie können die Unternehmen aus der gesamten Branche „Mineralöl" besser an den Mechanismen partizipieren?
- Hinweis auf hohen Organisationsgrad des Energie-Sektors im UPK – Frage, wie sich in Zukunft die Kooperation der komplexen Unternehmensstruktur (Erzeuger, Händler, Netzbetreiber auf verschiedenen Ebenen) unter dem Dach des UPK gestalten kann?

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 07.06.2012
Hausruf: 1527

4. Anforderungen an den IT-Schutz KRITIS aus Sicht BMI

Herr ITD Schallbruch hat einen Vortrag zur Vorstellung des Diskussionspapiers vorbereitet

I. Sprechempfehlung

- mit verschärfter Bedrohungslage Notwendigkeit zum sektorübergreifenden, koordinierten Vorgehen
- alle Betreiber in allen Sektoren müssen ein gewisses Mindestmaß an KRITIS-Schutz gewährleisten
- BMI hat dies in 7 Kernforderungen in einem Diskussionspapier zusammengefasst und mit der Einladung übersandt
- Verweis an ITD zur Vorstellung der konkreten Forderungen aus Sicht BMI

II. Aktueller Sachstand

- BMI hat Diskussionspapier „IT-Schutz Kritischer Infrastrukturen in Deutschland" mit 7 grundlegenden Forderungen zum IT-Schutz KRITIS erarbeitet
- An Wirtschaftsvertreter übersandt im Rahmen der Einladungsschreiben von Herr Minister

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 08.06.2012
Hausruf: 1527

IT-Schutz KRITIS im Energiesektor

I. Hintergrundinformationen

Der KRITIS-Sektor „Energie" (IKT) ist in folgende Branchen aufgeteilt:
- Elektrizität
- Mineralöl
- Gas

Marktsituation und Branchenorganisation

Innerhalb einer jeden Branche grdsl. Aufteilung in Erzeugung und Verteilung, welche von der (europäischen) Regulierung in jüngster Vergangenheit auch explizit in separate Unternehmen gezwungen wurden. Dies hat am Markt zu einiger Bewegung geführt (jüngstes Beispiel 18. Mai 2012: E.on verkauft Gasnetz für 3,2 Mrd. € an Finanzinvestoren).
Verteilung bei Elektrizität und Strom ist netzgebunden (mit entsprechenden Kritikalitäten); Mineralölversorgung bedient sich zur Verteilung grdsl. des Verkehrssektors. Für die Branchen Gas und Mineralöl komplettieren auf Grund der Speicherbarkeit auch noch Speicherbetreiber das Bild.

- Elektrizität: 4 große Übertragungsnetzbetreiber (für die großen Distanzen): T[redacted] GmbH ([redacted]ochter), [redacted] (vormals V[redacted]), A[redacted]GmbH (vormals [redacted] und T[redacted] GmbH (Tochter von [redacted]); eine Vielzahl von Erzeugern
- Gas: 12 große Fernnetzbetreiber; Erzeugung kaum in DE (> 85% Import)
- Mineralöl: Förderung kaum in DE (ca. 3%), 13 Raffinerien zur Weiterverarbeitung des Rohöls – zudem Handel und Tankstellen.

Verbandstechnisch erscheint für Gas und Elektrizität insb. der BDEW[1] relevant, der auch in Angelegenheiten der IKT-Sicherheit aktiv ist. Für die

[1] Bundesverband der Energie- und Wasserwirtschaft

Stadtwerke agiert zudem der VKU[2] als Ansprechpartner. Die Mineralölbranche ist im MWV[3] organisiert.

Aufsichtssituation

Energiewirtschaftsgesetz erlegt Netzbetreibern (Verteilung) Pflichten – auch explizit zur IT-Sicherheit – auf. Von diesem nicht abgedeckt ist die Branche Mineralöl; für diese existieren aus internationalen Verträgen sowie EU-Vorgaben im Grunde nur Auflagen zur Bevorratung.

Auch die Erzeugung wird nicht direkt mit Auflagen von der Regulierung bedacht; Auflagen werden hier vielmehr von den Netzbetreibern im Rahmen von Anschlussbedingungen auferlegt.

Aufsicht über Elektrizitäts- und Gasversorgung obliegt der Bundesnetzagentur (BNetzA). Diese erstellt (gemäß dem neuen EnWG nun erstmalig) unter Beteiligung des BSI einen Katalog von Sicherheitsanforderungen.

IKT-Abhängigkeit

Steuerung im Energiebereich (die gesamte Verteilung) wird auch heute weitgehend IT-basiert abgebildet; BSI geht jedoch von geeigneter Abschottung aus – die Steuerung der Versorgungsnetze selbst sei demnach sogar vom Internet getrennt.

Besondere Relevanz kommt den Betreibern aus dem Energie-Sektor zu, weil neben der Bereitstellung von Dienstleistungen an die Gesellschaft auch andere KRITIS-Sektoren hochgradig von Services aus diesem Sektor abhängig sind (so auch dargestellt von Vertretern aus Finanzsektor im Minister-Gespräch am 09. Mai).

Schutzniveau und Lücken

Die großen Marktteilnehmer sind sich ihrer Verantwortung bewusst und beschäftigen sich seit Jahren aktiv mit der IT-Sicherheit ihrer Infrastrukturen.

---

[2] Verband kommunaler Unternehmen
[3] Mineralölwirtschaftsverband

Lücken: Die gesetzlich festgeschriebenen Anforderungen greifen nur für einen Teil des Energie-Sektors (Mineralöl ausgeklammert).

Organisationsgrad

Bei dem Energiesektor kann für den UPK noch nicht von einer umfassenden Repräsentierung ausgegangen werden, obgleich im letzten Jahr eine Ausweitung stattgefunden hat. Von den eingeladenen Organisationen sind nicht im UPK vertreten: V[redacted] AG, T[redacted] GmbH, [redacted] GmbH, W[redacted], B[redacted], V[redacted]

Branchenspezifisch wird das Thema aufgegriffen (von den großen Marktteilnehmern auch sehr aktiv). Bislang partizipiert BSI jedoch nicht an diesen Strukturen; über eine Verstärkung dieser Zusammenarbeit hinaus sollte für die Zukunft auf eine Verzahnung mit dem branchenübergreifenden UPK hingearbeitet werden.

Zudem stellt der Mineralölwirtschaftsverband mit [redacted] einen der beiden AG-Leiter für den UPK.

Aktuelle Entwicklungen

- EU KOM (DG HOME) evaluiert in Zusammenarbeit mit den MS aktuell die EKI-Richtlinie (Europ. Kritische Infrastrukturen) von 2008, die Teil des Europ. Programms zum Schutz Kritischer Infrastrukturen (EPSKI) ist. In der Richtlinie wurden nur Regelungen für Energie und Transport/Verkehr getroffen. Die Evaluierung, die bis Ende 2012 angelegt ist, ist ergebnisoffen. Eine denkbare Zukunftsoption ist die Ausweitung auf andere Sektoren; im Vordergrund steht dabei die IKT. DE hält die bestehende Richtlinie für verfehlt und lehnt eine Ausweitung ab.
- Sicherheitskatalog zur detaillierten Ausgestaltung von Anforderungen aus dem EnWG befindet sich aktuell in Erarbeitung bei BNetzA unter Einbindung des BSI.

[redacted]

Zusagen	Absagen	Ablage	Wegiegen
16. Mai 2012			
Antwort	R	WV	

[redacted]
Vorsitzender des Vorstandes
Chief Executive Officer

Herrn
Bundesminister des Inneren
Dr. Hans-Peter Friedrich
Platz der Republik 1
11011 Berlin

Bundesministerium des Inneren
St'n RG
Eing. 22. Mai 2012
Uhrzeit 10⁰⁰
Nr.: ___/

Essen, 14. Mai 2012

Sehr geehrter Herr Minister Friedrich,

herzlichen Dank für Ihr Schreiben vom 16. April 2012 und Ihre Einladung, am 13. Juni 2012 in Ihr Ministerium zur Diskussion der Cybersicherheit von Kritischen Infrastrukturen zu kommen.

[redacted]st sich seiner besonderen Verantwortung zur Cybersicherheit der eingesetzten Informations- und Kommunikationstechnologien bewusst. Aus diesem Grund hat die Cybersicherheit im Konzern einen hohen Stellenwert. In diesem Zusammenhang begrüßen wir die Cybersicherheitsstrategie der Bundesregierung vom Februar 2011 ausdrücklich.

Dem hohen Stellenwert der Cybersicherheit begegnen wir im Konzern mit einer einheitlichen Steuerung, nachvollziehbaren und messbaren Maßnahmen sowie einer kooperativen Zusammenarbeit mit Ihrem Ministerium und den Ihnen unterstellten Bundesämtern BSI und BBK. Ergänzend möchte ich anfügen, dass der Konzern in der Vergangenheit wie auch aktuell auf nationaler und internationaler Ebene aktiv an Projekten zur Definition und Implementierung von Branchenstandards zur Cybersicherheit mitwirkt.

Unsere Konzeption zur Cybersicherheit sowie Anregungen an die Bundesregierung hierzu entnehmen Sie bitte der Anlage zu diesem Schreiben. Darin finden Sie auch den Umsetzungsstand im [redacted]-Konzern. Ich habe mir erlaubt, zu einigen Punkten von uns identifizierte Verbesserungspotenziale aufzuzeigen. An der weiteren Diskussion und Ausgestaltung möchten wir uns gerne weiterhin aktiv beteiligen.

Leider kann ich selber am 13. Juni wegen eines seit langem feststehenden Termins nicht zu Ihnen nach Berlin kommen. [redacted], der als Personalvorstand der [redacted] für die Sicherheit im Konzern verantwortlich ist, kommt aber gerne Ihrer Einladung nach.

[redacted]

[redacted]

...

Wenn Sie einverstanden sind, würde [redacted] zusammen mit [redacted] dem Leiter Konzernsicherheit der [redacted], mit Ihnen über den Stand der Cybersicherheit sowie das Diskussionspapier „IT-Schutz Kritischer Infrastrukturen" diskutieren.

Mit besten Grüßen

Jürgen Schaar

Anlage
Feedback zum Diskussionspapier
"IT-Schutz Kritischer Infrastrukturen in Deutschland, 25. Januar 2012"

Aktivitäten von [redacted]

- [redacted]rbeitet eng mit dem Bundesinnenministerium sowie den Bundesbehörden BKA, BSI und BBK zusammen. Insbesondere engagieren wir uns aktiv im UP KRITIS. Bei Ausgestaltung unserer Konzeption zur Cybersicherheit nutzen wir intensiv die Arbeitsergebnisse des UP KRITIS. Dieses gilt insbesondere für die Ausgestaltung unserer Mechanismen zur Früherkennung und Bewältigung von IT-Krisen sowie für IT-Notfall und Krisenübungen.
- Bei der Gestaltung unserer Sicherheitsmaßnahmen haben wir eine Übereinstimmung mit existierenden Standards und Normen im Fokus. Bestandteil unserer Strategie zur Cybersicherheit ist die Konformität unserer Sicherheitsmaßnahmen zum „Stand der Technik". Konkret bedeutet dieses, dass wir unser konzernweites Managementsystem zur Cybersicherheit an der ISO 27000 Reihe ausrichten.
- [redacted]at eine eigene Security-Organisation, vergleichbar mit anderen Konzernen. Wir verfügen über ein integriertes Security-Konzept. Die Steuerung aller sicherheitsrelevanten Aktivitäten wurde in der Konzernsicherheit gebündelt. Es wird ein unternehmerischer Ansatz verfolgt, d.h. Risiken und Prävention werden hinsichtlich der wirtschaftlichen Wirkungen bewertet, aus welchem Schutzniveau und Maßnahmen abgeleitet werden.
- Seit 2009 beinhaltet die Security-Organisation auch die Verantwortung für die Informationssicherheit. Diese Verantwortung umfasst auch die Cybersicherheit. In der Informationssicherheit verfolgen wir dabei einen umfassenden und integrierten Ansatz. Dieser Ansatz umfasst den Schutz aller Informationen, unabhängig wann und in welchem Medium (Papier, elektronisch) sie vorliegen. Des Weiteren umschließt unsere Konzeption alle digitalen Technologien (klassische IT, Telekommunikation, Prozesssteuerung / Prozessdatenverarbeitung, Medien- und Gebäudetechnik). Kriterium für die Definition der notwendigen Schutzmaßnahmen ist der jeweilige Schutzbedarf. Dieser wird durch Bedrohungsanalyse und Risikobewertung ermittelt. Hierfür existiert eine konzernweite Methodik.
- In unserem Vorgehensmodell zur Implementierung von neuen ITK Systemen und Infrastrukturen ist die Cybersicherheit verankert. Durch Schulungen und Awareness-Maßnahmen sensibilisieren wir unsere Mitarbeiter für die Notwendigkeit zur Informationssicherheit.
- Unseren Lieferanten von ITK Produkten und Dienstleistungen machen wir genaue Vorgaben zur Cybersicherheit. Hier legen wir den gleichen Standard an wie für uns selbst.
- Regelmäßig führen wir Krisen- und Notfallübungen durch. Unsere ITK Systeme und Infrastrukturen unterziehen wir regelmäßigen Penetrationstests.
- Transparenz über Status und Verbesserungspotenziale in unserer Cybersicherheit erhalten wir über ein gestuftes Berichtssystem. Alle Konzerngesellschaften berichten regelmäßig und bei Bedarf Ad-hoc ihren Umsetzungsstand zu den konzernweiten festgelegten Initiativen und Maßnahmen sowie existierenden Risiken und Sicherheitsvorfällen in der Cybersicherheit. Die Konzernsicherheit konsolidiert und bewertet dieses Reporting und er-

stellt einen Übersichtsbericht für den Konzernvorstand sowie die Compliance Organe des Konzerns.

- Unsere Konzeption zur Cybersicherheit und die Umsetzung prüfen wir regelmäßig durch interne und externe Reviews und Audits. Erkannte Abweichungen und Verbesserungspotenziale arbeiten wir in unserem kontinuierlichen Verbesserungsprozess ab.
- Wir arbeiten seit mehreren Jahren in verschiedenen Institutionen und Gremien aktiv und teilweise federführend an der Weiterentwicklung von Standards zur Cybersicherheit in der Energieversorgung mit. Dieses gilt insbesondere für die KRITIS relevanten Teile unseres Unternehmens (z.B. BDEW Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme", VGB PowerTech Richtlinie „IT-Sicherheit für Erzeugungsanlagen, DIN SPEC 27009:12-04 „Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002", BSI Schutzprofil für SmartMeter).
- Dem BSI gegenüber ist ein Regel- sowie Notfallkontakt (24/7) benannt. Bei KRITIS-relevanten Sicherheitsvorfällen wird das BSI Lagenzentrum informiert. Gleiches gilt für KRITIS-relevante Anfragen zu einzelnen Fällen wie z.B. eingesetzte Produkte mit aktuell bekannten Schwachstellen usw.
- Die Zusammenarbeit mit dem BKA, BSI, BBK sowie dem BMI beurteilen wir als kooperativ und gewinnbringend für beide Seiten. Dieses leiten wir auch aus Anfragen zur Beteiligung an Veranstaltungen Ihres Ministeriums bzw. Ihnen unterstellten Behörden ab, denen wir mit großer Freude nachgekommen sind (Beitrag auf dem BSI Kongress 2011 und Behördenleitungstag 2011, SPOC für das BKA).
- Wir sind grundsätzlich an einer Vertiefung der Partnerschaft zur Cybersicherheit zwischen Staat und Wirtschaft interessiert. Wir haben die Cybersicherheit in den letzten Jahren aus eigener unternehmerischer sowie KRITIS-Verantwortung und aus Fürsorgepflicht gegenüber den Mitarbeitern erheblich vorangebracht. Diesen Weg werden wir fortsetzen.

Forderungen an die Bundesregierung

- Unserer Einschätzung und Beobachtung nach geht die größte Bedrohung auf KRITIS relevante ITK Infrastrukturen heutzutage von s.g. Advanced Persistent Threats (ATP) aus. Solche Angriffe setzen einen hohen Ressourcenaufwand, ein sehr spezifisches Know-how sowie eine mehrmonatige Vorbereitung voraus (vgl. Stuxnet). Diese Voraussetzungen können in der Regel nur staaten- oder länderübergreifend operierende terroristische Gruppierungen erfüllen. Schutz gegen Cyber-Terrorismus und auch Cyber-War ist daher ebenso grundsätzlich Aufgabe des Staates wie die Terrorismusbekämpfung und die Landesverteidigung. Die Kosten für Schutzmaßnahmen gegen solche Angriffe müssen daher von der Allgemeinheit getragen werden.
- Ein höheres Schutzniveau erfordert meistens kostspielige Präventivmaßnahmen zur Verbesserung des Schutzes gegen Cyber-Terrorismus und Cyber-War. Bei der Anreizregulierung für den Netzbereich können jedoch keine Kosten für „Terror-Prävention" in den Netzentgelten berücksichtigt werden. Wir brauchen daher ein wettbewerbsneutrales Um-

lagesystem über den Strompreis, bei dem die sicherheitsrelevanten Mehraufwendungen weitergewälzt werden können, z.B. im Rahmen der Netzentgelte.

- Die Politik sollte die Zuständigkeiten und die Zusammenarbeit der Behörden auf Bundes- und Länderebene besser ordnen: dabei sollte die Zusammenarbeit der beiden Ministerien BMI, BMJ und BMWi und den jeweils unterstellten Bundesbehörden (BSI, BBK, Bundesnetzagentur, Bundesdatenschutzbeauftragter) verbessert werden. Die Ministerien haben die Angewohnheit, beliebig parallel und unabgestimmt zu agieren.

- Die existierenden Initiativen auf Bundes- und Landesebene zur Cybersicherheit sollten konsolidiert werden und eine gemeinsame Steuerung erhalten. Bestandteil dieser übergreifenden Steuerung sollte die Ressourcenoptimierung und Vermeidung von Doppelarbeit sein.

- Vertrauenswürdigkeit und Verlässlichkeit des Personals spielt für uns eine große Rolle. Durch vertrauenswürdiges und verlässliches Personal wird ein erheblicher Beitrag zur Cybersicherheit geleistet. KRITIS-Unternehmen müssen Instrumentarien an die Hand bekommen, um die Vertrauenswürdigkeit und Verlässlichkeit ihres Personals, insbesondere bei Neueinstellungen, nachvollziehen zu können. Aus unserer Sicht war das „alte" BDSG ausreichend und derzeit wird die Novelle regelmäßig angepasst und ist seit geraumer Zeit im Geschäftsgang. Um rechtssichere und praktikable Regelungen für die Korruptions- und Kriminalitätsbekämpfung in Unternehmen zu schaffen, benötigen z.B. Unternehmen der Kritischen Infrastrukturen praktikable Lösungen. Das Führungszeugnis als „altes" bewährtes Mittel und Einstellungsvoraussetzung, welches auch dem Resozialisierungsgedanken der Bundesrepublik Rechnung trägt, soll nun kontraproduktiv und an unpraktikable Vorrausetzungen angebunden werden. In diesem Zusammenhang verweisen wir auf das ASW Eckpunktepapier zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes (Beschäftigtendatenschutzgesetz) vom 25. August 2010

- Der UP KRITIS ist konsequent in eine Plattform zum gegenseitigen Erfahrungsaustausch und zur gemeinsamen Bewertung von Bedrohungen und Vorfällen der Cybersicherheit auszubauen. Die Dominanz in der Leitung des UP KRITIS durch das BSI ist in eine eigene Moderation durch die KRITIS-Unternehmen umzuwandeln. Der UP KRITIS bzw. die KRITIS-Unternehmen sollten in die Arbeit des Cyberabwehrzentrums in geeigneter und angemessener Weise einbezogen werden.

Anlage
Umsetzungsstand IT-Schutz Anforderungen,
Bezug zum Diskussionspapier "IT-Schutz Kritischer Infrastrukturen in Deutschland"

1 Mehr Transparenz schaffen

> [redacted]at in den vergangenen Jahren flächendeckend im Rahmen seiner Business Continuity Vorsorge s.g. BIA's (Business Impact Analysen) über alle relevanten Geschäftsprozesse durchgeführt. In Abhängigkeit der Kritikalität der Prozesse wurden Maßnahmen zur Aufrechterhaltung definiert und - wo notwendig - Redundanzen vorgesehen.	**Business Impact Analysen im Rahmen des Business Continuity Managements definieren Kritikalität der Prozesse**
> Unsere Konzernsicherheit erstellt zweimal im Jahr eine umfassende Bedrohungsanalyse zur Cybersicherheit. Gegenstand ist die Bewertung der für die Cybersicherheit aktuell existierenden Bedrohungen für den Konzern. Diese Bedrohungsanalyse wird allen Konzerngesellschaften als Input zur Durchführung eigenständiger Risikobewertungen zur Verfügung gestellt. *Die Bedrohungsanalyse I 2011 ist dem BSI zur Verfügung gestellt worden und ist als Input in die Erstellung des BSI Bedrohungskatasters eingegangen.*	**Konzernweite Analyse der Cyberbedrohungen als Ausgangspunkt zur gesellschaftsspezifischen Risikoanalyse**
> Die von den Konzerngesellschaften erstellten Risikobewertungen zur Cybersicherheit gehen quartalsweise sowohl in das Risikomanagementsystem der Gesellschaft als auch in das Risikoreporting des Konzerns (nach KonTraG) ein. Hierzu werden die einzelnen Risikobewertungen der Konzerngesellschaften von der Konzernsicherheit geprüft, konsolidiert und ggf. um gesellschaftsübergreifende Risiken ergänzt.	**Integriertes, durchgängiges Risikoreporting im Rahmen des Risikomanagements**
> Der Status der Cybersicherheit sowie ggf. aufgetretene Sicherheitsvorfälle werden quartalsweise durch die Gesellschaften an die Konzernsicherheit berichtet. Die Konzernsicherheit erstellt einen Sicherheitsbericht für den Konzernvorstand. Dieser Bericht geht auch an das Compliance Board des Konzerns. Im Fall von aufgetretenen Sicherheitsvorfällen wird ein Überblick über die ergriffenen und noch zu ergreifenden Korrekturmaßnahmen angefügt. Bei Notwendigkeit wird dieses Regelreporting durch eine Ad-hoc-Berichterstattung mit gleicher Verfahrensweise ergänzt.	**Konzerweites Berichtswesen zum Status sowie von Sicherheitsvorfällen**
> Jahresweise ist der Status der Informationssicherheit / Cybersicherheit Bestandteil der Prüfung des Jahresabschlusses des Konzerns. Der durch die Hauptversammlung bestellte Wirtschaftsprüfer des Jahresabschlusses lässt sich durch die Konzernsicherheit über Systematik, Umsetzungsstand, Risiken und Maßnahmen zur Cybersicherheit berichten. Des Weiteren lässt sich der Prüfungsausschuss der [redacted] AG durch die Konzernsicherheit regelmäßig über den Stand und die Maßnahmen zur Cybersicherheit berichten.	**Regelmäßige Prüfung der Maßnahmen durch die Aufsichtsorgane**

Anlage
Umsetzungsstand IT-Schutz Anforderungen,
Bezug zum Diskussionspapier "IT-Schutz Kritischer Infrastrukturen in Deutschland"

2 Robuste Grundlagen durch ein standardisiertes und übergreifendes Sicherheitsniveau

> Der Konzern verfügt seit 2001 über einheitliche, standardisierte Vorgaben und Prozesse zur IT-Sicherheit. Im Jahre 2008 wurden diese Standards den aktuellen Anforderungen und technischen Veränderungen angepasst. Nicht technische Aspekte des Schutzes von Prozessen und Daten (Kommunikationssicherheit) wurden mit berücksichtigt. Diese Standards sind Bestandteil des Konzernregelwerkes.

Etablierte Standards zur IT- und Informationssicherheit

> Seit 2009 migriert der Konzern seine Standards zur Informationssicherheit in ein ISMS nach ISO 27000. Die Implementierung eines ISMS erfolgt in allen Konzerngesellschaften und bezieht alle digitalen Technologien (klassische IT, Telekommunikation Prozesssteuerung/Prozessleittechnik, Medien-/Gebäudetechnik) mit ein.

Implementierung eines konzernweiten Information Security Management Systems (ISMS)

> Besonderer Bedeutung misst der Konzern der Akzeptanz und Einhaltung der Standards zur Cybersicherheit durch das Personal (eigene Mitarbeiter wie auch Fremddienstleister) bei. Insbesondere in Zeiten von erhöhter Arbeitsbelastung und steigendem Kostendruck müssen Maßnahmen zur Cybersicherheit der Betrachtung auf Sinnhaftigkeit, Einhaltbarkeit und Praxisnähe standhalten.

Besondere Bedeutung der Einhaltung von Maßnahmen zur Cybersicherheit

Aus diesem Grund hat der Konzern ein Review seines Regelwerkes für Nutzer von ITK Systemen zur Cybersicherheit durchgeführt. Dieses mit der Zielsetzung, höhere Akzeptanz bei den Mitarbeitern zu erreichen und unnötige ggf. veraltete Regelungsbestandteile zu eliminieren, aber auch um Lücken im Regelwerk zu schließen bzw. fehlende Präzisierungen zu ergänzen.

> Der Konzern ist traditionell sehr engagiert bei der Erarbeitung und Definition von Standards und Normen in seinem Umfeld. Dieses gilt auch für die Cybersicherheit.

Intensive Mitarbeit bei der Definition von nationalen und internationalen Standards und Normen

Z.B:

- *Arbeitsergebnisse UP KRITIS*
  „Früherkennung und Bewältigung von IT-Krisen",
  „IT-Notfall- und Krisenübungen in Kritischen Infrastrukturen"
- *BDEW Whitepaper*
  „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme"
- *VGB PowerTech Richtlinie*
  „IT-Sicherheit für Erzeugungsanlagen"
- *DIN SPEC 27009:12-04*
  „Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002"
- *BSI Schutzprofil für SmartMeter).*

> Die interne Revision des Konzerns überprüft im Rahmen ihrer Prüfungshandlungen auch die Einhaltung und Wirk-

Routinemäßige Prüfungen durch interne Revision

Anlage
Umsetzungsstand IT-Schutz Anforderungen,
Bezug zum Diskussionspapier "IT-Schutz Kritischer Infrastrukturen in Deutschland"

samkeit der Maßnahmen zur Cybersicherheit in den Konzerngesellschaften.

> Über das Konzernregelwerk sind alle Konzerngesellschaften verpflichtet, jahresweise s.g. Penetrationstests auf besonders kritische Systeme und Infrastrukturkomponenten durchzuführen

Verpflichtung zur Durchführung von Penetrationstests

3 Kritische Prozesse autonom gestalten

> Wir stimmen zu, dass besonders kritische Prozesse einer genauen Risikobewertung bedürfen, um daraus die geeigneten Sicherheitsmaßnahmen abzuleiten.

Allerdings halten wir die pauschale Forderung nach einer grundsätzlichen Trennung vom „Internet" sowie „öffentlichen Netzen" gleichermaßen für unrealistisch wie auch finanziell mit erheblichen Mehrbelastungen verbunden.

„Abschottung" war unserer Einschätzung nach noch nie ein wirksames Mittel zur Abwehr von Bedrohungen und Angriffen. Dieses hat auch der s.g. Stuxnet Vorfall gezeigt. Wie Ihnen bekannt sein dürfte, wurde hier der Angriff über externe Speichermedien (USB-Sticks) geführt.

Grundsätzlicher Verzicht von „Internet" und „öffentlichen Netzen" gleichermaßen unrealistisch wie wirtschaftlich nicht zielführend.

> Anstelle einer pauschalen Forderung zum Verzicht auf Internet und öffentliche Netze halten wir es für besser, gemeinsam branchenspezifisch Schutzziele und Schutzniveau zu definieren (d.h. gegen welche Bedrohungen ist sich zu schützen und auf welchem Level ist der Schutz sicherzustellen. Die Definition der jeweiligen notwendigen und richtigen Sicherheitsmaßnahmen hat sich am Stand der Technik sowie den Business-Anforderungen zu orientieren und ist jeweils spezifisch durch die Prozess- und Technologieexperten zu realisieren.

Dieser Ansatz bietet den Vorteil, nicht im Vorhinein auf einzelne Technologien/Technologiebereiche zu verzichten, nur weil diese subjektiv als nicht sicher angesehen werden. Ebenso erlaubt dieser Ansatz neue, innovative Technologien sicher zu nutzen.

Es existieren heute ausreichend technische sowie organisatorische Maßnahmen, um internetbasierende Dienste oder öffentliche Netzwerke sicher in die eigene ITK Infrastrukturen zu integrieren.

Definition von Schutzzielen und Schutzniveau erscheint zielführender als globaler Verzicht auf einzelne ausgewählte Technologien

4 Produkt- und Dienstleistungssicherheit gewährleisten

> Wir unterstützen den Ansatz des „Security by Design".

Aus diesem Grund sind IT-Sicherheitsaspekte sowohl im hauseigenen Projektvorgehensmodell für IT-Projekte wie auch im Beschaffungsprozess verankert.

Security by Design ist richtiger Ansatz

Die Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. als Interessenvertretung für die Belange der betrieblichen Kriminalprävention und Unternehmenssicherheit in der

Vertrauenswürdiges und verlässliches Personal

deutschen Wirtschaft begrüßt das Anliegen der Bundesregierung, den Arbeitnehmerdatenschutz im Rahmen des Bundesdatenschutzgesetzes klarzustellen und gleichzeitig rechtssichere und praktikable Regelungen für die Korruptions- und Kriminalitätsbekämpfung in Unternehmen zu schaffen. Eine Analyse des Beschäftigtendatenschutzgesetzes aus Sicht der Unternehmenssicherheitsbereiche zeigt jedoch, dass es in verschiedenen Bereichen zu maßgeblichen (negativen) Auswirkungen auf die betriebliche Praxis bei der Verhinderung und Bekämpfung von betriebsinterner Kriminalität in der deutschen Wirtschaft kommt.

Das Führungszeugnis als Einstellungsvoraussetzung bzw. Einsatzvoraussetzung von Dienstleistern im Bereich von Kritischen Infrastrukturen muss generell möglich bleiben und nicht an unpraktikable Bedingungen geknüpft sein.

vgl. hierzu: ASW-Eckpunkte zum Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes (Beschäftigtendatenschutzgesetz) vom 25. August 2010.

5 Durch Lagefortschreibung und Frühwarnung Gefahren vorbeugen

> [redacted]hat für Warn- und Alarmierung gegenüber dem BSI bereits seit 2009 einen 24/7 Kontakt eingerichtet.

Benannter 24/7 Warn- und Alarmierungskontakt sowie intensive Zusammenarbeit mit dem BSI

Bei relevanten Vorfällen der Cybersicherheit wurde und wird das Lagezentrum im BSI entsprechend informiert.

Die Zusammenarbeit mit dem BSI erfolgt aus unserer Sicht zielorientiert und kollegial. Dieses schließt auch die Information des BSI über Sicherheitsvorfälle und den Know-how-Austausch dazu ein.

> Cybersicherheit bedeutet auch immer schnelles informieren und reagieren. Hier sehen wir noch Nachholbedarf auf Seiten des BSI.

Verbesserungen auf Seiten des BSI hinsichtlich Geschwindigkeit von Information und Frühwarnung notwendig.

Unseren Anforderungen nach erfolgt die Information zu vorhandenen Schwachstellen oder Angriffen durch die Medien bzw. spezialisierte Dienstleister heute deutlich schneller (bis zu drei Tage) als über das BSI. Der Monatsbericht zur IT-Sicherheitslage des BSI erfolgt nicht zeitnah genug (Berichtsmonat erst zum Ende des Folgemonats) als das er sein Potenzial entfalten könnte. Hier muss unserer Einschätzung nach eine deutliche Entbürokratisierung erfolgen.

> Eine allgemeine Verpflichtung zur Meldung von Sicherheitsvorfällen erscheint uns als wenig zielführend.

Allgemeine Meldeverpflichtung für Sicherheitsvorfälle nicht zielführend

Zum einen sind ITK Infrastrukturen und eingesetzte Systeme zwischen den KRITIS Sektoren und einzelnen KRITIS Unternehmen zu heterogen bzw. zu verschieden ausgeprägt/konfiguriert als das sich singuläre Vorfälle auf allgemeine Bedrohungen abstrahieren ließen.

Zum anderen sind wir der Überzeugung, dass Sicherheitsvorfälle wie auch Bedrohungen einer intensiven Diskussion im Kreis der KRITIS Unternehmen/Branchen bedürfen, um

Anlage
Umsetzungsstand IT-Schutz Anforderungen,
Bezug zum Diskussionspapier "IT-Schutz Kritischer Infrastrukturen in Deutschland"

aus ihnen allgemeine Rückschlüsse zu ziehen. Ein schlichtes Meldeverfahren würde lediglich einen zusätzlichen Bürokratismus aufbauen, der wenig Mehrwert, aber einen erhöhten Aufwand und letztlich Kosten bedeuten würde.

> Unserer Einschätzung und Beobachtung nach geht die größte Bedrohung auf KRITIS ITK Infrastrukturen heutzutage von s.g. Advanced Persistent Threats (ATP) aus. Angriffe, die einen hohen Ressourcenaufwand voraussetzen sowie sehr spezifisches Know-how verlangen sowie eine mehrmonatige Vorbereitung benötigen (vgl. Stuxnet). Diese Voraussetzungen können in der Regel nur staaten- oder länderübergreifend operierende terroristische Gruppierungen erfüllen

Abwehr von Cyber-War und Cyberterrorismus ist Staatsaufgabe

Für die Abwehr solcher Angriffe sind daher die gleichen Verantwortlichkeiten, Aufklärungs- und Reaktions-Mechanismen anzuwenden wie für physikalische Angriffe.

6 Mit Übungen auf den Ernstfall vorbereiten

> Elementarer Bestandteil der Konzern BCM Systematik ist die Durchführung von Notfall- und Krisenübungen auf Ebene der Geschäftsprozesse, aber auch im IT Umfeld.

Regelmäßige Durchführung von Krisenübungen

Insbesondere im Bereich Verteilnetz Strom werden solche Übungen gemeinsam mit Telekommunikationsanbietern sowie den Gemeinden und Kreisen durchgeführt.

> Der Konzern war an der Bundessonderlage IT im Rahmen der LÜKEX 2010 beteiligt. Dieses sowohl mit der Einspielung eines Szenarios in die Sonderlage als auch mit einem umfangreichen eigenen Szenario im Verteilnetzbereich.

Beteiligung an der Bundessonderlage IT im Rahmen der LÜKEX 2010

Eine Beteiligung des Sektors Energieversorgung im Rahmen der LÜKEX 2012 war seitens der Übungsplanung / -steuerung nicht vorgesehen.

> Der Konzern beteiligt sich aktiv an den Übungen zur Krisenbewältigung des UP KRITIS und hat an der Entwicklung der Verfahrensweisen des UP KRITIS zur Krisenbewältigung mitgearbeitet.

Beteiligung an Übungen des UP KRITIS

7 Durch Kooperationen an Know-how und Stärken gewinnen

> Wir haben dem BMI gegenüber im Oktober/ November letzten Jahres vorgeschlagen, eine Gruppe Cybersicherheit - unter Einbezug des BSI - innerhalb der bestehenden AK Stromversorgung des BBK zu implementieren. Hierzu hat es zwischen [redacted]G) sowie den Mitarbeitern des BMI Herrn Dr. Dürig und Herrn Dr. Pilgermann am 11.11.2011 ein Gespräch gegeben. Ergebnis des Gespräches war es, diesen Ansatz mit BBK und BSI abzustimmen. Den mir vorliegenden Informationen nach ist diese Abstimmung derweil herbeigeführt. [redacted]hat zwischenzeitlich auch einen Vorschlag zur inhaltlichen Ausges-

[redacted]vorschlag zur Implementierung einer Gruppe Cybersicherheit innerhalb der AK Stromversorgung des BBK

Anlage
Umsetzungsstand IT-Schutz Anforderungen,
Bezug zum Diskussionspapier "IT-Schutz Kritischer Infrastrukturen in Deutschland"

taltung gegenüber dem BMI vorgelegt.

An der weiteren Ausgestaltung dieser Gruppe Cybersicherheit arbeitet [redacted] gerne weiterhin federführend mit und begrüßt eine zeitnahe Umsetzung.

> [redacted] versteht das Ansinnen des BMI, alle KRITIS Sektoren und Branchen im UP KRITIS vertreten zu sehen.

Organisatorische Neugestaltung des UP KRITIS notwendig

Gleichzeitig möchte [redacted] aber aufzeigen, dass schon heute durch die große Anzahl von vertretenen Personen eine wirkungsvolle, inhaltliche Arbeit nur mehr begrenzt möglich ist. Dieses liegt in der Natur von Gruppen größer 30 Personen.

Aus Sicht [redacted] ist eine neue Arbeitsweise für den UP KRITIS notwendig. Hierbei wäre ein angepasstes organisatorische Modell notwendig, möglicherweise mehrstufig ausgeprägt (Branche / Sektor / gesamt).

> Die vom UP KRITIS abzudeckenden Aufgabenbereiche sollten überdacht und neu definiert werden. Hierbei sollten die Schwerpunkte zukünftig liegen auf:

Neudefinition der Aufgaben des UP KRITIS und Festlegung der Verantwortlichkeiten notwendig

- *Erfahrungsaustausch zu Good Practice der Cybersicherheit*
- *Diskussion von aktuellen Gefährdungen der Cybersicherheit und Erstellung von gemeinsamen Risikobewertungen*
- *Erstellen von Positionspapieren zu Bedrohungen und Sicherheitsvorfällen und Ableitung von Handlungsrichtlinien*

Stand: 29.05.2012

KRITIS-Sektor „Energie“

Teilnehmende Unternehmen

Name	Aktien-Index	Umsatz in Mrd. (2011)	Mitarbeiter (2011)	Hauptsitz	Mitglied UPK (Bezug Nr. 5)	Übungs-beteiligung (Bezug Nr.6)	Kurzbeschreibung
[redacted]	DAX	52	72068	[redacted]	Ja	Ja	[redacted] ist einer der größten Energieversorgungskonzerne Europas und gemessen am Umsatz der zweitgrößte Deutschlands.
[redacted]	DAX	113	78889	[redacted]	Ja	Ja	[redacted] ist der größte private Energiekonzern der Welt, der hauptsächlich im europäischen Gas- und Elektrizitätsgeschäft tätig ist.
V[redacted]AG		0,14	20980	[redacted]	*Nein*	*Nein*	Hauptaktionär der V[redacted] ist zu 100 Prozent der schwedische Mutterkonzern V[redacted] Die V[redacted]AG ist der viertgrößte Stromversorger Deutschlands.
E[redacted]AG	-	19	20296	[redacted]	Ja	Ja	[redacted] ist das drittgrößte Energieunternehmen in Deutschland
T[redacted]GmbH	-	8	750	[redacted]	*Nein*	*Nein*	Die T[redacted] ist eine Tochter des niederländischen Stromnetzbetreibers T[redacted] und Betreibt in Deutschland ein Hochspannungsnetz, welches 40 Prozent der Fläche in Deutschland abgedeckt.Damit werden 20 Mio. Menschen indirekt mit Strom versorgt.

Stand: 29.05.2012

Name	Aktien-Index	Umsatz in Mrd. (2011)	Mitarbeiter (2011)	Hauptsitz	Mitglied UPK (Bezug Nr. 5)	Übungs-beteiligung (Bezug Nr.6)	Kurzbeschreibung
[redacted]GmbH	-	4	608	[redacted]	*Nein*	*Nein*	Das Unternehmen betreibt das Hochspannungsnetz im Osten Deutschlands sowie im Raum Hamburg. Damit deckt es 30 Prozent der Fläche Deutschlands ab und bedient mehr als 18 Mio. Menschen indirekt mit Strom.
A[redacted]GmbH	-	0,6	816	[redacted]	Ja	Ja	A[redacted]betreibt das längste Übertragungsnetz in Deutschland und ist als Teil des [redacted]-Konzerns entstanden. Das Netzgebiet liegt schwerpunktmäßig im Westen und Südwesten von Deutschland.
[redacted]	-	3,4	200	[redacted]	Ja	Ja	Das Unternehmen betreibt das Übertragungsnetz in BW und ist eine Tochter des [redacted]
O[redacted]GmbH	-		1600	[redacted]	Ja	Ja	Das Unternehmen ist eine Erdgastransportgesellschaft und betreibt in Deutschland das größte Ferngasleitungsnetz.
W[redacted]	-	9	367	[redacted]	*Nein*	*Nein*	W[redacted] handelt und vertreibt Erdgas an Stadtwerke, regionale Versorger, Industriebetriebe und Kraftwerke in Deutschland und im europäischen Ausland.
B[redacted]	-	44	5100	[redacted]	Ja	Ja	Die [redacted] ist mit ihrem Tankstellennetz und im Schmierstoffhandel in Deutschland führend und besitzt das zweigrößte Raffineriesystem in Deutschland.
W[redacted]GmbH	-	12	>2000	[redacted]	*Nein*	*Nein*	Die W[redacted] GmbH ist eine 100 Prozentige Tochter der [redacted] und ist der größte Deutsche Erdöl- und Erdgasproduzent.

Stand: 29.05.2012

Teilnehmende Verbände

Name	Angeschlossene Institutionen	Beschäftigte der angeschlossenen Institutionen	Hauptsitz	Mitglied UPK (Bezug Nr. 5)	Übungs-beteiligung (Bezug Nr. 6)	Kurzbeschreibung
B[redacted]	1800	-	[redacted]	*Nein*	*Nein*	Der [redacted] vertritt laut Eigenangaben rund 1800 Unternehmen, die rund 90 Prozent des Stromabsatzes, gut 60 Prozent des Nah- und Fernwärmeabsatzes, 90 Prozent des Erdgasabsatzes sowie 80 Prozent der Trinkwasser-Förderung und 60 Prozent der Abwasser-Entsorgung in Deutschland repräsentieren
M[redacted]	11	-	[redacted]	Ja	Ja	Mitglied im [redacted] sind Unternehmen mit Sitz in Deutschland, die Rohöl in eigenen oder konzernverbundenen Raffinerien verarbeiten sowie Mineralölprodukte über eine eigene oder konzernverbundene Vertriebsorganisation in Deutschland vertreiben.
V[redacted]	1400	240000	[redacted]	*Nein*	*Nein*	Der [redacted] vertritt die Interessen der kommunalen Wirtschaft in den Bereichen Energie- und Wasserversorgung, Entsorgung und Umweltschutz.

487#02
342

Referat IT 3
IT3-606 000-9/7#6

Berlin, den 11. Juni 2012
Hausruf: 1374/2308/1584

Refl: Dr. Dürig / Dr. Mantz
Ref: Dr. Gitter

18.06. V I 7 18/6 968

Bundesministerium des Innern St'n RG
Eing.: 13. Juni 2012
Uhrzeit: 15
Nr.: 2002

Herrn Minister 14/6

über

Abdruck:
Herrn St F ✓
LS

Frau St'in Rogall-Grothe 15/6
Herrn IT D
Herrn SV IT D 12/6.

JT3
1. Dr. Mantz 2k Mo 10/7
2. Verlage an VI2+VI4 Rücklauf b.g. 22/6
3. Fr. Dr. Gitter, bitte nächste Prüfschritte und vorschlagen, mitteilen

1) SV ITD m.R.
2) IT3 Mo 2/7

Referate VI2 und VI4 haben mitgezeichnet.

25 10/7

Betr.: Aktive Netzverteidigung

Bezug: Aktuelle Medienberichterstattung zu staatlich gesteuerten operativen IT-Maßnahmen

Anlagen: (1) Presseartikel zur „Operation Olympic Games" (Auswahl)
(2) Presseartikel zur Errichtung der Abt. CNO (Auswahl)
(3) MV v. 29.Mai 2012 – IT3-606 000-2/72#16
(4) BSI-Lagemeldung v. 11. Juni 2012 zu möglicher Verbindung zwischen Schadprogrammen Stuxnet und Flame
(5) Bericht des BMVg an den Verteidigungsausschuss des Dt. BT zum Themenkomplex „Cyber Warfare" v. 13. April 2012

1. Votum

Kenntnisnahme und Billigung der nächsten Schritte.

2. Sachverhalt

Die Möglichkeit eines staatlich gesteuerten Einsatzes von IT zur Durchführung operativer Maßnahmen im Cyberraum wird derzeit in den Medien breit diskutiert. Anlass ist zum einen ein seitens der US-Regierung nicht dementierter Artikel in der New York Times v. 1. Juni 2012, dessen Autor behauptet, Belege dafür zu haben, dass der Einsatz des 2010 entdeckten Schadprogramms „Stuxnet" zur Zerstörung der Zentrifugen in iranischen Atomanlagen durch Präs. Obama angeordnet wurde (Operation „Olympic Games", s. **Anlagenkonvolut 1**).

Am. 5. und 6. Juni berichteten deutsche Medien unter Berufung auf einen schriftlichen Bericht des BMVg an den BT-Verteidigungsausschuss zum Themenkomplex „Cyber Warfare" zudem u.a. über den Aufbau der Abteilung Computernetzwerkoperationen (CNO) beim Kommando Strategische Aufklärung (KSA) der Bundeswehr (**Anlagenkonvolut 2**).

Die Berichterstattung steht zudem im Zusammenhang mit dem aktuellen Bekanntwerden des hochkomplexen Schadprogramms „Flame", das umfassende Funktionalitäten zum Ausspähen digitaler Dokumente aufweist und dessen Verbreitung vornehmlich im Nahen Osten nachgewiesen wurde (S. MV v. 29. Mai 2012, **Anlage 3**). Durch die aktuelle Meldung des IT-Sicherheits-Unternehmens Kaspersky zu Verbindungen zwischen den Schadprogrammen „Stuxnet" und Flame" (s. Lagebericht des BSI v. 11. Juni 2012, **Anlage 4**; hierzu erfolgt gesonderte Vorlage) wird das Thema voraussichtlich weiter im Fokus der öffentlichen Berichterstattung bleiben.

Bei dem nun bekannt gewordenen Bericht an den Verteidigungsausschuss (als **Anlage 5** beigefügt) handelt es sich um die leicht aktualisierte Fassung eines bereits im Juni 2011 unter Beteiligung des BMI erstellten und an den Verteidigungsausschuss übersandten Berichts der Bundesregierung zum Thema „Cyber Warfare".

3. Stellungnahme

Die aktuelle Medienberichterstattung stellt unter dem Schlagwort „Cyberwar" operative IT-Maßnahmen als staatliche Handlungsform überzeichnet dar.

Tatsächlich werden Cyber-Angriffe von unterschiedlichen Akteuren mit verschiedensten Motivlagen durchgeführt. Hierbei ist vermehrt eine neue Qualität von komplexeren und zielgerichteten Angriffen zu beobachten. Herkunft und der Hintergrund der einzelnen Angriffe lassen sich jedoch in den meisten Fällen nicht eindeutig identifizieren. Eine Unterscheidung zwischen staatlichen und nichtstaatlichen Angriffen kann daher im Einzelfall regelmäßig nicht mit absoluter Sicherheit vorgenommen werden. Dies gilt auch für die in den Medien jeweils hervorgehobenen hochkomplexen Schadprogramme Duqu (als sog. „Stuxnet-Nachfolger") und Flame. Die aktuellen Behauptungen zum Ursprung von „Stuxnet" werden hingegen auf diesbezügliche konkrete Informationen aus Regierungskreisen gestützt. Aufgrund der großen Verletzlichkeit der umfassend vernetzten Industriegesellschaften könnten IT-Angriffe mit vergleichbarer Wirkung auch von zivilen Gruppen mit unterschiedlicher Motivationslage durchgeführt werden.

Der Begriff „Cyberwar" ist deshalb weder sachlich noch rechtlich geeignet, um die sicherheitspolitischen Herausforderungen einer nahezu vollständig vernetzten Gesellschaft angemessen zu beschreiben. Dies wird auch in dem von den Medien zitierten BMVg-Bericht an den Verteidigungsausschuss klargestellt. Die unter federführender Gesamtverantwortung des BMI erstellte Cyber-Sicherheitsstrategie der Bundesregierung umfasst daher alle Arten von IT-Angriffen und behandelt das Thema Internetsicherheit schwerpunktmäßig unter einem zivilen Gesichtspunkt.

IT-Sicherheit muss primär durch Maßnahmen zum präventiven und reaktiven Schutz der eigenen IT-Systeme und –Infrastruktur gewährleistet werden. Dazu gehören die Maßnahmen

- zum Schutz der Informationssysteme des Bundes und der kritischen Infrastrukturen, die federführend vom Bundesamt für Sicherheit in der Informationstechnik (BSI) koordiniert werden,
- polizeiliche Maßnahmen zur Bekämpfung krimineller Cyberangriffe, für die – soweit der Bund zuständig ist – BKA die Federführung hat, und
- Maßnahmen der Spionageabwehr, für die - soweit der Bund zuständig ist - das Bundesamt für Verfassungsschutz federführend ist.

Auch mit den im Entwurf eines IT-SicherheitsG vorgeschlagenen Regelungen für KRITIS-Betreiber und Internet-Provider sollen präventive und reaktive Schutzmaßnahmen gestärkt werden. Die in dem Bericht an den Verteidigungsausschuss beschriebenen Maßnahmen der Bundeswehr im Bereich der Cybersicherheit dienen weitestgehend dem Schutz eigener IT-Systeme und lassen sich daher ebenfalls in diesen Rahmen einordnen.

Daneben geht der Bericht an den Verteidigungsausschuss in einem kurzen Abschnitt auf operative Maßnahmen in gegnerischen Netzwerken ein, die ausdrücklich als militärisches Wirkmittel bezeichnet werden. Die Bezeichnung Computer Netzwerk Operationen (Cyber Network Operations, CNO) ist im militärischen Kontext für (staatliche) Maßnahmen in fremden Netzen gebräuchlich, nämlich in Abgrenzung zu dem Begriff der „Cyber (network) defense" als Bezeichnung für IT-Maßnahmen im eigenen Herrschaftsbereich. Cyber-Operationen der Bundeswehr sind im Kontext eines militärischen Einsatzes zur Verteidigung (Art. 87 a Absatz 2 GG) sowie im Rahmen und nach den Regeln eines Systems gegenseitiger kollektiver Sicherheit i.S.d. Art. 24 Absatz 2 GG möglich.
Die Bundeswehr hat mit dem Ziel, mittelfristig ebensolche operativen Maßnahmen in einem militärischen Kontext vornehmen zu können, bereits 2006 mit dem Aufbau der Abteilung Computernetzwerkoperationen bei dem Kommando Strategische Aufklärung (KSA, eigener Verband innerhalb des Streitkräfteunterstützungskommandos) begonnen. Dieses Vorhaben ist öffentlich bekannt, die besondere Medienaufmerksamkeit, ausgehend von einem Artikel in der FTD v. 5. Juni 2012 (s. Anlage 1), dürfte im Zusammenhang mit den weiteren aktuellen Vorkommnissen stehen.

Dennoch verdeutlichen die aktuell öffentlich diskutierten Sicherheitsvorfälle, bei denen komplexe Schadprogramme Anwendung fanden, Handlungsbedarf zur Abwehr von schweren IT-Angriffen durch Maßnahmen im Ausland in einem zivilen Kontext:
Innerhalb Deutschlands dürften die klassischen Eingriffsbefugnisse nach StPO und ergänzend allgemeine polizeirechtliche Instrumente grundsätzlich ausreichen, um kurzfristig einem Cyber-Angriff zu begegnen.

Aufgrund der grenzüberschreitenden Struktur des Internet muss jedoch davon ausgegangen werden, dass auch bei schwerwiegenden Cyber-Angriffen Server zumindest teilweise im Ausland belegen sind. Die existierenden Mittel im zwischenstaatlichen Rechtsverkehr (insbs. Rechtshilfeersuchen, einschließlich vereinfachter/beschleunigter Verfahren zwischen einzelnen Staaten z.B. nach der Cybercrime Convention des Europarats) sind bereits aufgrund der technisch bedingten besonderen Eilbedürftigkeit zur Abwehr eines Cyber-Angriffs zur Gefahrenabwehr bzw. zur Schadensbegrenzung nicht geeignet. Zur Abwehr einer schweren unmittelbar drohenden Gefahr bzw. zur Schadensbegrenzung (etwa bei einem Cyber-Angriff auf kritische Infrastrukturen) könnten daher aktive IT-Maßnahmen, die im Ausland Wirkung entfalten, erforderlich sein.

Solche operative Maßnahmen zur Abwehr von Cyber-Angriffen im Ausland bedürfen aus verfassungsrechtlichen Gründen einer gesetzlichen Eingriffsbefugnis. Die völkerrechtliche Bewertung einer solchen staatlichen Maßnahme hängt von den Umständen im Einzelfall ab. Bislang gibt es weder völkervertragliche noch völkergewohnheitsrechtliche Regelungen spezifisch zur Abwehr von Cyber-Angriffen. Diskutiert wird, inwieweit Staaten nach allgemeinem Völkergewohnheitsrecht Duldungspflichten gegenüber aktiven IT-Maßnahmen haben könnten, die sich auf ihrem Territorium auswirken könnten. Allerdings werden derzeit in fast allen Industriestaaten Überlegungen angestellt, wie dieser fehlenden Rechtssicherheit begegnet werden kann.

Eine Einigung über die völkerrechtliche Zulässigkeit von aktiven Maßnahmen zur Verteidigung gegen schwerwiegende IT-Angriffe in fremden Netzen wäre zumindest dann wünschenswert, wenn ein Staat die von seinem Territorium ausgehenden IT-Angriffe nicht in angemessenem Zeitrahmen unterbindet. ~~Wir werden daher~~ im internationalen und europäischen Kontext die Diskussion aufnehmen/fortsetzen werden, ~~darauf hinwirken, eine~~ Regelung für Maßnahmen der aktiven Netzverteidigung in schwerwiegenden zeitkritischen Fällen auf bi- oder multilateraler Ebene zu erreichen (z.B. Recht zur „Nacheile" im Cyberraum und eine korrespondierende Duldungspflicht des betroffenen Staates). Dies wird voraussichtlich jedoch nur in einem langwierigen Prozess gelingen, zumal eine Reihe von völker- und verfassungsrechtlichen Fragen der Klärung bedürfen. Dennoch sollte < >

Des Weiteren soll u.a. in Zusammenarbeit mit Abt. V, in Umsetzung des in Ziffer 10 der Cyber-Sicherheitsstrategie enthaltenen Prüfauftrags, eine vertiefte Prüfung zu folgenden rechtlichen Gesichtspunkten erfolgen (s. i.e. Anlage 6)

- Klärung der nationalen Zuständigkeiten für aktive Gefahrenabwehrmaßnahmen gegen schwerwiegende IT-Angriffe,
- Klärung der verfassungsrechtlichen Voraussetzungen für hoheitliche IT-Maßnahmen im Ausland,
- weitergehende Prüfung der Erheblichkeitsschwelle für eine völkerrechtliche Relevanz von IT-Maßnahmen,
- Beobachtung der aktuellen Diskussion über die Anwendung und Entwicklung des Völkerrechts bzgl. der Zulässigkeit von aktiven Verteidigungsmaßnahmen und den Duldungspflichten von Staaten gegenüber solchen Maßnahmen.

Elektr. gez.
Dr. Dürig Dr. Mantz Dr. Gitter

Anlagenkonvolut 1

WELT ONLINE

7. Jun. 2012
Diesen Artikel finden Sie online unter
http://www.welt.de/106407109

Die Welt ¦ 02.06.12

US-Präsident befahl Angriff mit Stuxnet-Virus

Enthüllungsbuch: Programm ließ Zentrifugen des iranischen Atomprogramms explodieren. Neue Dimension im Cyberkrieg *Von Ansgar Graw*

Das Geheimnis um den Computervirus Stuxnet ist gelöst. Die US-Regierung hat gemeinsam mit Israel den Virus entwickelt, der iranische Atomanlagen wirkungsvoll attackierte und durch einen Programmierfehler 2010 ins Internet ausbrechen konnte. Das berichtet die "New York Times" unter Berufung auf nicht genannte Regierungsoffizielle in den USA, Israel und Europa. Washington und Jerusalem wurden von Teheran und Fachleuten in der gesamten Welt bereits seit Längerem verdächtigt, Stuxnet entwickelt zu haben. Washington betrieb die Operation unter dem Codewort "Olympische Spiele".

Stuxnet hat den Cyberwar, also die Kriegsführung gegen fremde Computernetze, auf eine neue Ebene gebracht. Erstmals wurde nicht nur die Software anderer Rechner beschädigt, sondern physischer Schaden an nahezu 1000 von 5000 iranischen Zentrifugen angerichtet. Der lange Zeit den iranischen Wissenschaftlern verborgen gebliebene Stuxnet-Wurm befahl den Zentrifugen in der Anreicherungsanlage Natans plötzliche Beschleunigungen oder Verlangsamungen. Dadurch seien etliche Zentrifugen explodiert.

Präsident Barack Obama sei sich der Gefahr bewusst gewesen, den Cyberwar qualitativ zu steigern, schreibt "New York Times"-Autor David E. Sanger, der zu diesem Thema nächste Woche ein Buch veröffentlicht. Wenn die USA, die regelmäßig Cyberattacken von dritter Seite geächtet haben, als Drahtzieher bekannt würden, könnten andere Länder, Terroristen oder Hacker damit ähnliche Aktionen rechtfertigen. Doch weil Obama keinen anderen Weg sah, einen israelischen Militärschlag gegen das iranische Atomprogramm mit unvorhersehbaren Folgen für die Gesamtregion zu verhindern, habe er an dem von seinem Vorgänger George W. Bush initiierten Projekt festgehalten. Die USA hätten damit "den Rubikon überschritten", sagt der frühere CIA-Chef Michael Hayden.

Da die Computer in Natans aus Sicherheitsgründen nicht mit dem Internet verbunden sind, musste ein "Burggraben" überwunden werden. Der Artikel suggeriert, dies sei durch einen unwissenden iranischen Mitarbeiter geschehen, dessen USB-Stick mit dem Virus verseucht wurde. Denkbar ist aber ebenso der Einsatz eines Überläufers.

Als Stuxnet im Sommer 2010 über den Laptop eines iranischen Wissenschaftlers ins Internet ausbrechen und sich dort unzählige Male vervielfachen konnte, fragte Obama seine Mitarbeiter: "Sollen wir das Ding beenden?" Dann aber entschloss er sich zur Fortsetzung. Besondere Ironie: Stuxnet ließ sich nur an den vom Iran verwendeten, technisch weitgehend überholten P-1-Zentrifugen aus pakistanischer Produktion ausprobieren. Die USA verfügten über dieses Testmaterial dank Muammar al-Gaddafi. Der vergangenes Jahr in einem von Washington unterstützten Volksaufstand getötete libysche Diktator hatte P-1-Zentrifugen bei der Beendigung seines Nuklearprogramms 2003 den USA übergeben. Sie lagern in einem Großlabor in Tennessee und dienten dort als Trainingslager für die "Olympischen Spiele".

WELT ONLINE

7. Jun. 2012
Diesen Artikel finden Sie online unter
http://www.welt.de/106406191

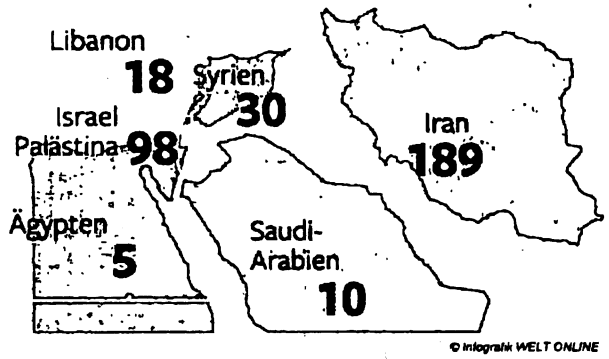
Meinung 02.06.12 Computerviren

Willkommen in der Ära des Cyberkriegs!

Der Einsatz des Computervirus Stuxnet markiert den Beginn einer neuer Art der Kriegsführung. Ob Barack Obamas öffentliches Bekenntnis dazu den USA nutzt oder schadet, wird sich noch zeigen. *Von Clemens Wergin*

Verbreitung des Spionage-Virus

Anzahl der Viren



© Infografik WELT ONLINE

So verteilt sich die Anzahl der Viren auf die Länder im Nahen Osten

Bis Freitag war es ein gut informiertes Gerücht, nach einem Enthüllungsbericht der New York Times darf es nun als bestätigt gelten: Der Computerwurm Stuxnet, der die Steuerungscomputer der iranischen Urananreicherungsalage in Natans befallen hatte, war ein Projekt der amerikanischen Regierung, an dem auch Israel mitgearbeitet hat. Die Amerikaner haben die erste digitale Bombe der Geschichte gezündet.

Der Autor des Times-Artikels scheint privilegierten Zugang zu hochranigen Quellen in der US -Regierung bekommen zu haben. Das Weißen Haus hat offenbar ein Interesse daran, Barack Obama im Wahlkampf als Präsidenten darzustellen, der entschlossen und unkonventionell handelt, wenn es um nationale Sicherheitsinteressen geht.

Der "Cyberwar" ist die Waffe des 21. Jahrhunderts und man wird davon ausgehen können, dass Russland, China und andere Staaten längst mitmischen in diesem Schattenkrieg. Die USA sind aber nun die ersten, die – wenn auch nicht mit Klamamen – zugeben, in diesem Kneg die erste digitale Bombe benutzt zu haben. Denn solch einen ausgefeilten Virus zur Beschädigung kritischer Infrastruktur eines verfeindeten Landes hatte es bis dato nicht gegeben.

Mehr Zeit für Diplomatie

Stuxnet ist auch der erste Virus, der nicht nur Computer auspäht oder lahmlegt, sondern der echte physische Zerstörung angenchtet hat, weil er iranische Uranzentnfugen zur Explosion brachte. Leider hat der Virus das iranische Atomprogramm nur verlangsamt, aber nicht entscheidend behindert

Es gibt gute und vertretbare Gründe für den Einsatz von Stuxnet Der Virus sollte Obama mehr Zeit für Diplomatie verschaffen. Er richtete sich gegen eine Anlagensteuerung, die Teheran sich illegal beschafft hatte. Und er beschädigte einen Teil des Nuklearprogramms, welches der Iran zunächst illegal und im Geheimen begonnen hatte und nach seiner Öffentlichwerdung gegen den Willen des UN-Sicherheitsrates weiter betrieb

Es ist auch allemal besser, ein fnedensbedrohendes Land wie den Iran mit einem Computervirus anzugreifen, als mit echten Bomben. Aber ein quasi kriegerischer Akt ist es eben doch.

Neue Ära im Cyberwar

Und so markiert der Einsatz von Stuxnet den Moment, an dem die Welt faktisch in die Ära des Cyberkriegs eingetreten (Link: http://www.welt.de/106389042) ist. Das ist vergleichbar mit Technologiesprüngen wie dem ersten Einsatz von Schießpulver, der Erfindung des Panzers oder dem Abwurf der ersten Atombombe. Eine erneute Büchse des Pandora ist geöffnet worden

Die US-Regierung muss sich nun aber fragen lassen, ob es nicht besser gewesen wäre, den Ursprung der Attacke und seine Details im Vagen zu lassen, statt sich damit zu brüsten (Link, http://www.welt.de/106402529) . Das hätte Obama vielleicht weniger Imagepunkte gebracht. Der Sicherheit Amerikas wäre es aber dienlicher gewesen.

Denn da Amerika nun als Cyberangreifer enttarnt ist, senkt das die Hemmschwelle für Feinde des Landes, ihrerseits Cyberangriffe gegen Amerika zu versuchen. Obama hat den Cyber-Damm eingerissen. Es wird schwer sein, ihn nach dem Quasi-Eingeständnis in der New York Times wieder aufzurichten.

Die erstaunlich detaillreichen Leaks sind aber auch inhaltlich gefährlich. Sie helfen dem Iran, zu rekonstruieren, was in Natans tatsächlich passiert ist und sich besser gegen zukünftige Attacken zu wappnen. Und sie können als Blaupause dienen für andere Staaten, wie man einen erfolgreichen Cyberangriff durchführt. Gegen wen auch immer.

Die US-Regierung wollte mit den Enthüllungen die Meriten von Barack Obama als sicherheitspolitischem Hardliner herausstreichen. Tatsachlich hat sie aber gezeigt, dass ihr das Image des Präsidenten zur Not wichtiger ist als die Sicherheitsinteressen des Landes.

WELT ONLINE

7. Jun. 2012
Diesen Artikel finden Sie online unter
http://www.welt.de/106409040

Welt am Sonntag | 03.06.12

Barack Obama führt den Krieg der Zukunft

Der Präsident im Cyber-War: Er soll Computerangriffe gegen den Iran mit Viren wie Stuxnet befohlen haben *Von Ansgar Graw*

Der Cyber-War begann im Nahen Osten, und sein erster Krieger war Agent.btz Ein US-Soldat fand auf seinem Parkplatz einen USB-Stick und schob ihn leichtfertig in seinen dienstlichen Laptop. Das aktivierte einen Virus, der blitzschnell ins Netz des Pentagon eindrang und sich zu den als "geheim" klassifizierten Dokumenten durchwühlte.

Agent.btz, wie der "Pentagon-Wurm" nach seiner Entdeckung genannt wurde, spionierte Code-Wörter aus, kopierte Dateien, verlangsamte die Rechner und entwickelte sich zu einer veritablen Bedrohung für die Verteidigungsfähigkeit der Vereinigten Staaten. Erst eine viele Monate Zeit, Geld und Energie kostende Abwehrschlacht, die "Operation Buckshot Yankee", konnte Agent btz stoppen.

Die USA, im Jahr 2008 Ziel dieses Angriffs mit immer noch unbekanntem Absender, sind inzwischen zur Attacke übergegangen. Stuxnet, ein Computer-Virus, der iranische Atomanlagen massiv beschädigt hat, wurde von Washington und Jerusalem gemeinsam entwickelt, hat die "New York Times" enthüllt. Autor David E. Sanger berichtet, dass schon der vormalige Präsident George W. Bush 2006 Vorbereitungen für einen Viren-Angriff gegen die iranischen Aufbereitungsanlagen befahl. Sein Nachfolger Barack Obama rüstete das geheime Programm unter dem Code-Wort "Olympische Spiele" weiter auf Obama führte den Krieg im Netz auf eine neue Ebene.

Denn Stuxnet ist der erste Virus, der nicht nur die Software anderer Rechner beschädigt, sondern physische Zerstörung an rund 1000 von 5000 iranischen Zentrifugen angerichtet hat. Der Computer-Wurm nistete sich gezielt und ausschließlich in die Siemens-Steuerungsanlagen ein und befahl den Zentrifugen plötzliche Beschleunigungen oder Verlangsamungen ihrer Operationen. Die Maschinen explodierten förmlich - wie bei einem Bombenangriff.

Die USA hätten mit diesem weiterentwickelten Computer-Virus "den Rubikon überschritten", sagt der frühere CIA-Chef Michael Hayden. Erst als Stuxnet durch einen Programmierfehler im Juni 2010 aus dem geschlossenen Computersystem der iranischen Atomanlage Natans ins Internet ausbrechen konnte, wurde der Virus als Ursache der bis dahin mysteriösen Havarien identifiziert. Die USA und Israel wurden sofort als die Initiatoren verdächtigt. Das hat der vom Weißen Haus nicht dementierte Artikel nun bestätigt.

Barack Obama, der mächtige Warlord 2.0. und zugleich das hoch gefährdete nächste Opfer des Cyber-War. Kein Land ist Viren-Attacken so schutzlos ausgeliefert wie die durch und durch computerisierten USA, deren Kraftwerke, Bankensysteme, Frischwasserzuleitungen und Aufzüge in unzähligen Wolkenkratzern allesamt über oft vernetzte Rechner gesteuert werden. Viren, selbst so komplexer Art wie Stuxnet, dessen Entwicklung rund 10.000 Arbeitsstunden gekostet haben dürfte, sind stets leichter auszutüfteln als Anti-Viren-Programme. Es ist wie bei Mörsern oder Raketen: Angriff ist leichter als Verteidigung.

Die Journalisten in Washington rätseln um die Hintergründe der Enthüllung. Dass Sanger seine Informationen, die teilweise aus dem innersten Zirkel des Präsidenten stammen, von einem verräterischen Maulwurf bekam, ist unwahrscheinlich. Wollte sich also der Wahlkämpfer Obama profilieren als entschlossener Hightech-Krieger? Doch bei einer Pressekonferenz im Weißen Haus widersprach Sprecher Josh Earnest entschieden der These, die Informationen aus Obamas innerstem Zirkel seien gezielt weitergegeben worden. "Es gibt einen Grund dafür, dass Informationen (als geheim) klassifiziert sind", sagte Earnest Ihre Publizierung bedeute "eine signifikante Bedrohung der nationalen Sicherheit".

Obama war sich bewusst, dass eine Aufdeckung der amerikanischen Rolle gefährliche Konsequenzen haben würde. Andere Länder, Terroristen, Geheimdienste oder Hacker könnten ähnliche Aktionen als legitim darstellen, würden die USA, die regelmäßig mögliche Cyber-Attacken als "kriegerischen Akt" ächten, als Initiatoren von Stuxnet entlarvt werden.

Davor warnte der Präsident mehrfach im kleinen Kreis. Nunmehr stehen die USA als erstes Land der Welt fest, das Cyber-Waffen eingesetzt hat. Gemessen an den eigenen Grundsätzen ist das eine Kriegserklärung.

Washingtons Entschluss, eine Cyber-Schlacht gegen den Iran zu starten, resultierte aus dem Drängen Israels nach einem Militärschlag gegen den Iran 2008 wurde Jerusalem bei Bush vorstellig und bat um die Überlassung spezieller bunkerbrechender Bomben. Der Präsident lehnte energisch ab, versicherte aber zugleich, die Entwicklung des Sabotage-Virus mit Hochdruck voranzutreiben. Daran arbeiteten der amerikanische Inlandsgeheimdienst NSA und die israelische Spezialeinheit des Militärs, Unit 8200, gemeinsam.

Stuxnet wurde zur genialen Waffe Doch auch ihre Wirkung blieb begrenzt. Warum konnte der Virus nicht alle Zentrifugen zerstören? Warum wurde er entdeckt? Dass er im Iran immerhin Schaden anrichtete, aber gegen Nordkorea gar nicht erst eingesetzt wurde, hat andere Gründe: Pjöngjang ist kaum vernetzt und selbst die dortigen Rüstungsingenieure verfügen nur selten über private Laptops. Im Iran soll hingegen ein leichtsinniger Wissenschaftler seinen vom amerikanischen oder israelischen Geheimdienst mit Stuxnet infizierten USB-Stick in das geschlossene Computer-Netz von Natans gesteckt haben - so wie damals der US-Soldat beim Agenten btz. Der Mensch bleibt die Schwachstelle bei der Abwehr von Computer-Viren

Ein neuer Rüstungswettlauf hat begonnen. "Flame" heißt der jüngste Virus, der Ende Mai auf Rechnern vor allem im Iran, aber auch in Israel und anderen Ländern des Nahen Ostens entdeckt wurde. Er verfügt über deutlich mehr Fähigkeiten als Stuxnet, spioniert nicht nur Siemens-Systeme aus, lässt sich aus der Ferne steuern, liefert Screenshots von infizierten Computern, kann angeblich sogar die Mikrofone von Handys oder Blackberrys einschalten, um Gespräche zu belauschen, und auf Befehl zerstört er sich bis zur Spurlosigkeit.

Israel verweist auf infizierte Computer im eigenen Land und bestreitet die Verantwortung für Flame. Washington schweigt.

The New York Times

June 1, 2012

Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER

WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.

At a tense meeting in the White House Situation Room within days of the worm's "escape," Mr. Obama, Vice President Joseph R. Biden Jr. and the director of the Central Intelligence Agency at the time, Leon E. Panetta, considered whether America's most ambitious attempt to slow the progress of Iran's nuclear efforts had been fatally compromised.

"Should we shut this thing down?" Mr. Obama asked, according to members of the president's national security team who were in the room.

Told it was unclear how much the Iranians knew about the code, and offered evidence that it was still causing havoc, Mr. Obama decided that the cyberattacks should proceed. In the following weeks, the Natanz plant was hit by a newer version of the computer worm, and then another after that. The last of that series of attacks, a few weeks after Stuxnet was detected around the world, temporarily took out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium.

This account of the American and Israeli effort to undermine the Iranian nuclear program is based on interviews over the past 18 months with current and former American, European and Israeli officials involved in the program, as well as a range of outside experts. None would allow their names to be used because the effort remains highly classified, and parts of it continue to this day.

These officials gave differing assessments of how successful the sabotage program was in slowing Iran's progress toward developing the ability to build nuclear weapons. Internal Obama administration estimates say the effort was set back by 18 months to two years, but some experts inside and outside the government are more skeptical, noting that Iran's enrichment levels have steadily recovered, giving the country enough fuel today for five or more weapons, with additional enrichment.

Whether Iran is still trying to design and build a weapon is in dispute. The most recent United States intelligence estimate concludes that Iran suspended major parts of its weaponization effort after 2003, though there is evidence that some remnants of it continue.

Iran initially denied that its enrichment facilities had been hit by Stuxnet, then said it had found the worm and contained it. Last year, the nation announced that it had begun its own military cyberunit, and Brig. Gen. Gholamreza Jalali, the head of Iran's Passive Defense Organization, said that the Iranian military was prepared "to fight our enemies" in "cyberspace and Internet warfare." But there has been scant evidence that it has begun to strike back.

The United States government only recently acknowledged developing cyberweapons, and it has never admitted using them. There have been reports of one-time attacks against personal computers used by members of Al Qaeda, and of contemplated attacks against the computers that run air defense systems, including during the NATO-led air attack on Libya last year. But Olympic Games was of an entirely different type and sophistication.

It appears to be the first time the United States has repeatedly used cyberweapons to cripple another country's infrastructure, achieving, with computer code, what until then could be accomplished only by bombing a country or sending in agents to plant explosives. The code itself is 50 times as big as the typical computer worm, Carey Nachenberg, a vice president of Symantec, one of the many groups that have dissected the code, said at a symposium at Stanford University in April. Those forensic investigations into the inner workings of the code, while picking apart how it worked, came to no conclusions about who was responsible.

A similar process is now under way to figure out the origins of another cyberweapon called Flame that was recently discovered to have attacked the computers of Iranian officials, sweeping up information from those machines. But the computer code appears to be at least five years old, and American officials say that it was not part of Olympic Games. They have declined to say whether the United States was responsible for the Flame attack.

Mr. Obama, according to participants in the many Situation Room meetings on Olympic Games, was acutely aware that with every attack he was pushing the United States into new territory, much as his predecessors had with the first use of atomic weapons in the 1940s, of intercontinental missiles in the 1950s and of drones in the past decade. He repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons — even under the most careful and limited circumstances — could enable other countries, terrorists or hackers to justify their own attacks.

"We discussed the irony, more than once," one of his aides said. Another said that the administration was resistant to developing a "grand theory for a weapon whose possibilities they were still discovering." Yet Mr. Obama concluded that when it came to stopping Iran, the United States had no other choice.

If Olympic Games failed, he told aides, there would be no time for sanctions and diplomacy with Iran to work. Israel could carry out a conventional military attack, prompting a conflict that could spread throughout the region.

A Bush Initiative

The impetus for Olympic Games dates from 2006, when President George W. Bush saw few good options in dealing with Iran. At the time, America's European allies were divided about the cost that imposing sanctions on Iran would have on their own economies. Having falsely accused Saddam Hussein of reconstituting his nuclear program in Iraq, Mr. Bush had little credibility in publicly discussing another nation's nuclear ambitions. The Iranians seemed to sense his vulnerability, and, frustrated by negotiations, they resumed enriching uranium at an underground site at Natanz, one whose existence had been exposed just three years before.

Iran's president, Mahmoud Ahmadinejad, took reporters on a tour of the plant and described grand ambitions to install upward of 50,000 centrifuges. For a country with only one nuclear power reactor — whose fuel comes from Russia — to say that it needed fuel for its civilian nuclear program seemed dubious to Bush administration officials. They feared that the fuel could be used in another way besides providing power: to create a stockpile that could later be enriched to bomb-grade material if the Iranians made a political decision to do so.

Hawks in the Bush administration like Vice President Dick Cheney urged Mr. Bush to consider a military strike against the Iranian nuclear facilities before they could produce fuel suitable for a weapon. Several times, the administration reviewed military options and concluded that they would only further inflame a region already at war, and would have uncertain results.

For years the C.I.A. had introduced faulty parts and designs into Iran's systems — even tinkering with imported power supplies so that they would blow up — but the sabotage had had relatively little effect. General James E. Cartwright, who had established a small cyberoperation inside the United States Strategic Command, which is responsible for many of America's nuclear forces, joined intelligence officials in presenting a radical new idea to Mr. Bush and his national security team. It involved a far more sophisticated cyberweapon than the United States had designed before.

The goal was to gain access to the Natanz plant's industrial computer controls. That required leaping the electronic moat that cut the Natanz plant off from the Internet — called the air gap, because it physically separates the facility from the outside world. The computer code would invade the specialized computers that command the centrifuges.

The first stage in the effort was to develop a bit of computer code called a beacon that could be inserted into the computers, which were made by the German company Siemens and an Iranian manufacturer, to map their operations. The idea was to draw the equivalent of an electrical blueprint of the Natanz plant, to understand how the computers control the giant silvery centrifuges that spin at tremendous speeds. The connections were complex, and unless every circuit was understood, efforts to seize control of the centrifuges could fail.

Eventually the beacon would have to "phone home" — literally send a message back to the headquarters of the National Security Agency that would describe the structure and daily rhythms of the enrichment plant. Expectations for the plan were low; one participant said the goal was simply to "throw a little sand in the gears" and buy some time. Mr. Bush was skeptical, but lacking other options, he authorized the effort.

Breakthrough, Aided by Israel

It took months for the beacons to do their work and report home, complete with maps of the electronic directories of the controllers and what amounted to blueprints of how they were connected to the centrifuges deep underground.

Then the N.S.A. and a secret Israeli unit respected by American intelligence officials for its cyberskills set to work developing the enormously complex computer worm that would become the attacker from within.

The unusually tight collaboration with Israel was driven by two imperatives. Israel's Unit 8200, a part of its military, had technical expertise that rivaled the N.S.A.'s, and the Israelis had deep intelligence about operations at Natanz that would be vital to making the cyberattack a success. But American officials had another interest, to dissuade the Israelis from carrying out their own pre-emptive strike against the Iranian nuclear facilities. To do that, the Israelis would have to be convinced that the new line of attack

was working. The only way to convince them, several officials said in interviews, was to have them deeply involved in every aspect of the program.

Soon the two countries had developed a complex worm that the Americans called "the bug." But the bug needed to be tested. So, under enormous secrecy, the United States began building replicas of Iran's P-1 centrifuges, an aging, unreliable design that Iran purchased from Abdul Qadeer Khan, the Pakistani nuclear chief who had begun selling fuel-making technology on the black market. Fortunately for the United States, it already owned some P-1s, thanks to the Libyan dictator, Col. Muammar el-Qaddafi.

When Colonel Qaddafi gave up his nuclear weapons program in 2003, he turned over the centrifuges he had bought from the Pakistani nuclear ring, and they were placed in storage at a weapons laboratory in Tennessee. The military and intelligence officials overseeing Olympic Games borrowed some for what they termed "destructive testing," essentially building a virtual replica of Natanz, but spreading the test over several of the Energy Department's national laboratories to keep even the most trusted nuclear workers from figuring out what was afoot.

Those first small-scale tests were surprisingly successful: the bug invaded the computers, lurking for days or weeks, before sending instructions to speed them up or slow them down so suddenly that their delicate parts, spinning at supersonic speeds, self-destructed. After several false starts, it worked. One day, toward the end of Mr. Bush's term, the rubble of a centrifuge was spread out on the conference table in the Situation Room, proof of the potential power of a cyberweapon. The worm was declared ready to test against the real target: Iran's underground enrichment plant.

"Previous cyberattacks had effects limited to other computers," Michael V. Hayden, the former chief of the C.I.A., said, declining to describe what he knew of these attacks when he was in office. "This is the first attack of a major nature in which a cyberattack was used to effect physical destruction," rather than just slow another computer, or hack into it to steal data.

"Somebody crossed the Rubicon," he said.

Getting the worm into Natanz, however, was no easy trick. The United States and Israel would have to rely on engineers, maintenance workers and others — both spies and unwitting accomplices — with physical access to the plant. "That was our holy grail," one of the architects of the plan said. "It turns out there is always an idiot around who doesn't think much about the thumb drive in their hand."

In fact, thumb drives turned out to be critical in spreading the first variants of the computer worm; later, more sophisticated methods were developed to deliver the malicious code.

The first attacks were small, and when the centrifuges began spinning out of control in 2008, the Iranians were mystified about the cause, according to intercepts that the United States later picked up. "The thinking was that the Iranians would blame bad parts, or bad engineering, or just incompetence," one of the architects of the early attack said.

The Iranians were confused partly because no two attacks were exactly alike. Moreover, the code would lurk inside the plant for weeks, recording normal operations; when it attacked, it sent signals to the Natanz control room indicating that everything downstairs was operating normally. "This may have been the most brilliant part of the code," one American official said.

Later, word circulated through the International Atomic Energy Agency, the Vienna-based nuclear watchdog, that the Iranians had grown so distrustful of their own instruments that they had assigned people to sit in the plant and radio back what they saw.

"The intent was that the failures should make them feel they were stupid, which is what happened," the participant in the attacks said. When a few centrifuges failed, the Iranians would close down whole "stands" that linked 164 machines, looking for signs of sabotage in all of them. "They overreacted," one official said. "We soon discovered they fired people."

Imagery recovered by nuclear inspectors from cameras at Natanz — which the nuclear agency uses to keep track of what happens between visits — showed the results. There was some evidence of wreckage, but it was clear that the Iranians had also carted away centrifuges that had previously appeared to be working well.

But by the time Mr. Bush left office, no wholesale destruction had been accomplished. Meeting with Mr. Obama in the White House days before his inauguration, Mr. Bush urged him to preserve two classified programs, Olympic Games and the drone program in Pakistan. Mr. Obama took Mr. Bush's advice.

The Stuxnet Surprise

Mr. Obama came to office with an interest in cyberissues, but he had discussed them during the campaign mostly in terms of threats to personal privacy and the risks to infrastructure like the electrical grid and the air traffic control system. He commissioned a major study on how to improve America's defenses and announced it with great fanfare in the East Room.

What he did not say then was that he was also learning the arts of cyberwar. The architects of Olympic Games would meet him in the Situation Room, often with what they called the "horse blanket," a giant foldout schematic diagram of Iran's nuclear

production facilities. Mr. Obama authorized the attacks to continue, and every few weeks — certainly after a major attack — he would get updates and authorize the next step. Sometimes it was a strike riskier and bolder than what had been tried previously.

"From his first days in office, he was deep into every step in slowing the Iranian program — the diplomacy, the sanctions, every major decision," a senior administration official said. "And it's safe to say that whatever other activity might have been under way was no exception to that rule."

But the good luck did not last. In the summer of 2010, shortly after a new variant of the worm had been sent into Natanz, it became clear that the worm, which was never supposed to leave the Natanz machines, had broken free, like a zoo animal that found the keys to the cage. It fell to Mr. Panetta and two other crucial players in Olympic Games — General Cartwright, the vice chairman of the Joint Chiefs of Staff, and Michael J. Morell, the deputy director of the C.I.A. — to break the news to Mr. Obama and Mr. Biden.

An error in the code, they said, had led it to spread to an engineer's computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world. Suddenly, the code was exposed, though its intent would not be clear, at least to ordinary computer users.

"We think there was a modification done by the Israelis," one of the briefers told the president, "and we don't know if we were part of that activity."

Mr. Obama, according to officials in the room, asked a series of questions, fearful that the code could do damage outside the plant. The answers came back in hedged terms. Mr. Biden fumed. "It's got to be the Israelis," he said. "They went too far."

In fact, both the Israelis and the Americans had been aiming for a particular part of the centrifuge plant, a critical area whose loss, they had concluded, would set the Iranians back considerably. It is unclear who introduced the programming error.

The question facing Mr. Obama was whether the rest of Olympic Games was in jeopardy, now that a variant of the bug was replicating itself "in the wild," where computer security experts can dissect it and figure out its purpose.

"I don't think we have enough information," Mr. Obama told the group that day, according to the officials. But in the meantime, he ordered that the cyberattacks continue. They were his best hope of disrupting the Iranian nuclear program unless economic sanctions began to bite harder and reduced Iran's oil revenues.

Within a week, another version of the bug brought down just under 1,000 centrifuges. Olympic Games was still on.

A Weapon's Uncertain Future

American cyberattacks are not limited to Iran, but the focus of attention, as one administration official put it, "has been overwhelmingly on one country." There is no reason to believe that will remain the case for long. Some officials question why the same techniques have not been used more aggressively against North Korea. Others see chances to disrupt Chinese military plans, forces in Syria on the way to suppress the uprising there, and Qaeda operations around the world. "We've considered a lot more attacks than we have gone ahead with," one former intelligence official said.

Mr. Obama has repeatedly told his aides that there are risks to using — and particularly to overusing — the weapon. In fact, no country's infrastructure is more dependent on computer systems, and thus more vulnerable to attack, than that of the United States. It is only a matter of time, most experts believe, before it becomes the target of the same kind of weapon that the Americans have used, secretly, against Iran.

This article is adapted from "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power," to be published by Crown on Tuesday.

Gitter, Rotraud, Dr.

Von: Nimke, Anja
Gesendet: Montag, 4. Juni 2012 16:04
An: Andris, Ekkehard; Dimroth, Johannes, Dr.; Dürig, Markus, Dr.; Gitter, Rotraud, Dr.; Kurth, Wolfgang; Mantz, Rainer, Dr.; Otte, Kathrin; Pilgermann, Michael, Dr.; Spatschke, Norman; Treib, Heinz Jürgen; Welsch, Günther, Dr.
Betreff: WG: 15:46 Antivirus-Unternehmen leitet Flame-Virus auf eigene Server um

-----Ursprüngliche Nachricht-----
Von: IDD, Platz 2
Gesendet: Montag, 4. Juni 2012 15:50
An: IT3_
Cc: ITD_; OESIII3_; OESII4_; IDD, Platz 3
Betreff: dpa: 15:46 Antivirus-Unternehmen leitet Flame-Virus auf eigene Server um

bdt0460 3 pl 338 dpa 0983

Computer/Sicherheit/Nahost/Iran/
Antivirus-Unternehmen leitet Flame-Virus auf eigene Server um =

Zur Analyse des neu entdeckten Computer-Virus Flame hat das russische Antivirus-Unternehmen Kaspersky eine Grube für den Schädling aufgestellt. Ein «Sinkhole» fängt nun Daten auf, die Flame eigentlich an seine kriminellen Schöpfer schicken sollte.

Moskau/Berlin (dpa) - Im Kampf gegen den Computer-Virus Flame haben Fachleute des russischen Antivirus-Unternehmens Kaspersky Lab nun eine virtuelle Quarantäne eingerichtet, in der von Flame ausspionierte Daten landen. In Zusammenarbeit mit dem US-amerikanischen Internet-Provider GoDaddy und dem Dienst OpenDNS werden die Zieladressen von Flame in ein «Sinkhole» (Senkgrube) umgeleitet, um den Forschern die Analyse des Computer-Schädlings zu ermöglichen, kündigte Kaspersky am Montag an.

Die Zieladressen (Domains) der sogenannten «C&C-Server» (Command-and-Control-Server) von Flame seien durchweg unter gefälschten Identitäten angemeldet worden, sagte Virenanalyst Magnus Kalkuhl der Nachrichtenagentur dpa.

Flame war in den vergangenen Monaten von Kaspersky Lab entdeckt worden. Das Schadprogramm kann das Mikrofon des Rechners einschalten und Gespräche belauschen, Bildschirminhalte und Tastatureingaben aufzeichnen sowie das Datennetzwerk ausspähen. Den regionalen Schwerpunkt machte Kaspersky im Iran, Nahen Osten und Nordafrika aus. «Die Komplexität und Funktionalität der neu entdeckten Schadsoftware übersteigt die aller bislang bekannten Cyber-Bedrohungen», sagte Firmen-Chef Eugene Kaspersky. Er setzte Flame in eine Reihe mit dem Schädling Stuxnet, der bestimmte Industrieanlagen-Module von Siemens angreift und vermutlich zur Sabotage der Atomprogramme im Iran eingesetzt wurde.

Ein erster Vergleich mit dem «kleinen Stuxnet-Bruder» Duqu habe ergeben, dass Flame sehr unterschiedlich programmiert worden sei, sagte Kalkuhl. Daher stamme Flame vermutlich aus einer anderen Quelle als Duqu. Die Angriffe mit dem Computerwurm Stuxnet auf iranische Atomanlagen sollen nach einem Bericht der «New York Times» vom amerikanischen Präsidenten Barack Obama angeordnet worden sein. In diesem Zusammenhang war auch darüber spekuliert worden, ob nicht auch Flame im staatlichen Auftrag programmiert und in Umlauf gebracht worden ist.

dpa-Notizblock

Internet
- [Blog-Eintrag Secure-List](http://dpaq.de/FnybK)

* * * *

Die folgenden Angaben sind nicht zur Veröffentlichung bestimmt

dpa-Kontakte

- Autor: Christoph Dernbach, +49 30 285232150, <netzwelt@dpa.com>
- Redaktion: Peter Zschunke, +49 30 285232150, <netzwelt@dpa.com>
- Foto: Newsdesk, +49 30 2852 31515, <foto@dpa.com>

dpa chd yyon n1 pz

041546 Jun 12

Anlage 2

05.06.2012, 07:14

Elektronische Aufrüstung:

Bundeswehr bedingt bereit für den Cyberkrieg

Jahrelang rüstete die Bundeswehr virtuell auf - inzwischen hat sie die "Anfangsbefähigung" erreicht, um gegnerische PC und Server zu attackieren. Das zeigen Unterlagen, die der FTD vorliegen. Vor einem Einsatz sind noch Rechtsfragen zu klären. von *Thomas Steinmann Berlin* und *Max Borowski Jerusalem*

Die Bundeswehr ist nach jahrelanger virtueller Aufrüstung inzwischen zu Angriffen auf Computernetze und Server in der Lage. Die Streitkräfte hätten eine "Anfangsbefähigung" für Attacken in "gegnerischen Netzen" erreicht, heißt es in Unterlagen des Verteidigungsministeriums für den Bundestag, die der FTD vorliegen.

Nach Angaben des Ministeriums ist die neue Einheit für Computernetzwerkoperationen, die beim Kommando Strategische Aufklärung in Gelsdorf bei Bonn angesiedelt ist, seit Ende 2011 einsatzfähig. Die Bundeswehr müsse im Rahmen ihres verfassungsrechtlichen Auftrags auch im Cyberraum operieren können, sagte ein Ministeriumssprecher. Ziel sei es, diese Fähigkeit ständig weiterzuentwickeln.

Angriff aus dem Cyberspace (Symbolbild)

Mit der Hackertruppe verkürzt Deutschland den Rückstand auf andere westliche Staaten. Länder wie die USA und Israel investieren Milliarden, um elektronische Attacken abwehren zu können und auch die Möglichkeit von Offensivschlägen zu entwickeln. Für Militärstrategen gilt der virtuelle Raum bereits als "fünfte Dimension" der Kriegsführung - neben Boden, Luft, Wasser und Weltraum. Dahinter steckt die Annahme, dass Computerangriffe auf Stromnetze oder Wasserwerke weitaus gefährlichere Folgen haben können als konventionelle Schläge. Gleichzeitig sind sie ohne großes Risiko für den Angreifer.

Erst vergangene Woche war bekannt geworden, dass US-Präsident Barack Obama persönlich den Einsatz des Computerwurms Stuxnet angeordnet haben soll. Diese aggressive Software hatte 2010 die iranischen Atomanlagen beschädigt. Zudem entdeckten Computerexperten ein neues Spionageprogramm namens Flame, das sich vor allem auf Rechnern im Nahen Osten ausgebreitet hat. Auch dahinter werden staatliche Stellen vermutet. Nach einer Schätzung des früheren Anti-Terror-Beraters Richard Clarke haben 20 bis 30 Staaten Kapazitäten für Cyberkriegsführung aufgebaut - darunter Nordkorea, China und Russland.

Die israelische Armee erklärte am Sonntag erstmals offiziell, dass sie den Cyberspace als Schlachtfeld betrachtet. Die Armee nutze Computernetzwerke, um Informationen zu sammeln und ihre eigene Infrastruktur zu schützen. "Wenn erforderlich" würden auch Angriffe geführt, heißt es in einem Dokument, das die Armee auf ihrer Internetseite veröffentlichte.

Bislang hatte die Bundesregierung bei der Cybersicherheit vor allem die Bedeutung der Abwehr gegnerischer Angriffe betont. Dennoch läuft der Aufbau einer Hackereinheit bei der Bundeswehr bereits seit 2006. Ursprünglich war geplant gewesen, dass die Truppe 2010 funktionsfähig sein soll. Zu einem großen Teil besteht die Einheit aus Informatikexperten der Bundeswehruniversitäten. Bislang seien die Spezialisten noch nicht eingesetzt worden, sagte der Sprecher des Verteidigungsministeriums.

Die deutschen Militärstrategen gehen davon aus, dass die Bundeswehr einen Angriff mit digitalen Waffen nicht isoliert führt, sondern eingebettet in "abgestimmte Maßnahmen" - also flankierend zum Gebrauch konventioneller Waffen. Noch ungeklärt ist allerdings die rechtliche Grundlage. So ist offen, wie sich Einsätze mit deutschem Recht oder internationalen Abkommen gegen Computerkriminalität vereinbaren lassen. "Sollten Computernetzwerkoperationen im Ausland durch die Bundeswehr konkret geplant werden, so würden die für den Einzelfall erforderlichen rechtlichen Voraussetzungen und Grundlagen geprüft werden", heißt es im Ministerium.

Strittig ist etwa die Frage, ob für Angriffe auf gegnerische Netze der Parlamentsvorbehalt gilt. "Wenn es sich um militärische Anwendungen handelt, brauchen wir die gleiche Legitimation wie für den Einsatz von Soldaten", sagte der SPD-Verteidigungspolitiker Hans-Peter Bartels.

Mehr zum Thema

Irans Kehrtwende im Atomstreit "Wir brauchen die 20 Prozent nicht mehr" (http://www.ftd.de/politik/international/:irans-kehrtwende-im-atomstreit-wir-brauchen-die-20-prozent-nicht-mehr/70043791.html)

Computervirus Cyber-Rüstungswahn (http://www.ftd.de/it-medien/it-telekommunikation/:computervirus-cyber-ruestungswahn/70043613.html)

Krieg gegen Terror Cyberopfer Dschihad
(http://www.ftd.de/it-medien/it-telekommunikation/:krieg-gegen-terror-cyberopfer-dschihad/70042002.html)

Cyberkrieg Hackerangriff legt Website der israelischen Börse lahm
(http://www.ftd.de/it-medien/medien-internet/:cyberkrieg-hackerangriff-legt-website-der-israelischen-boerse-lahm/60155280.html)

Mehr zu: Bundeswehr, Cyberkrieg, Internet, Verteidigung

Pressespiegel 1, 6. 6. 2012

Süddeutsche Zeitung
08.06.2012, S.5
Sicherheit

Bundeswehr rüstet für den Cyber-Krieg

Spezial-Kommando in der Nähe von Bonn soll Hacker-Angriffen offensiv begegnen

Von Peter Blechschmidt

Berlin – Die Bundeswehr will offenbar auch offensiv gegen Bedrohungen ihrer Computersysteme vorgehen. Das ergibt sich aus einer Unterrichtung des Verteidigungsministeriums für den Verteidigungsausschuss des Bundestags, über die am Dienstag zuerst die *Financial Times Deutschland* berichtete. Unter der Überschrift „Cyber-Warfare", was soviel wie Krieg im virtuellen Raum bedeutet, beschreibt das Ministerium, wie es seit 1992 versucht, die Sicherheit seiner IT-Systeme zu gewährleisten. Der „Cyberspace" wird demnach militärisch „als operative Domäne, vergleichbar dem Luft- oder Seeraum, behandelt".

Der Großteil des sechsseitigen Papiers behandelt die Abwehr von Cyber-Angriffen, mit denen Computersysteme der Bundeswehr ausspioniert werden sollen. In einem fünfzeiligen Absatz verbirgt sich die Mitteilung, dass derzeit beim „Kommando Strategische Aufklärung" eine Abteilung „Computernetzwerkoperationen" aufgebaut werde. „Eine Anfangsbefähigung zum Wirken in gegnerischen Netzen wurde erreicht", heißt es da. Verfahren könnten durch „Simulationen in einer abgeschlossenen Laborumgebung" erprobt werden. In diesem Rahmen könne auch ausgebildet werden.

> Jedes Jahr gibt es bis zu 50 ernsthafte Attacken auf Computer staatlicher Institutionen.

Demnach verfügt die Bundeswehr mittlerweile über Spezialisten, die in fremde Netzwerke eindringen, sie auskundschaften und gegebenenfalls auch zerstören könnten. Beispiele dafür sind das Schadprogramm Stuxnet oder der jüngst bekannt gewordene Computervirus Flame. Wie das Verteidigungsministerium in Berlin am Dienstag auf Anfrage mitteile, wurde die sogenannte Anfangsbefähigung Ende 2011 erreicht. Aktiv für Operationen eingesetzt wurde dieses Mittel jedoch noch nicht.

Das Kommando Strategische Aufklärung sitzt in Gelsdorf bei Bonn. Es ist die zentrale Dienststelle der Bundeswehr für die technische Aufklärung und den elektronischen Kampf.

Die IT-Systeme der Bundeswehr würden kontinuierlich durch gezielte Hackerangriffe und das Einbringen von Schadsoftware bedroht, heißt es in dem Papier des Ministeriums. Wie ein Sprecher am Dienstag ergänzend mitteilte, wurden Cyber-Attacken im Sinne eines gezielten Angriffs staatlicher Institutionen bislang noch nicht bemerkt. Hingegen gebe es pro Jahr 20 bis 50 qualifizierte Hackerangriffe. Darüber hinaus würden täglich im Durchschnitt mehrere hundert sogenannte Netzwerk-Scans registriert. Bei diesen Scans werden die Schutzsysteme der Computer mit speziellen Programmen auf Schlupflöcher abgesucht.

Maßnahmen im Cyber-Space würden sowohl in Kriegen zwischen Staaten als auch in Auseinandersetzungen mit nichtstaatlichen Akteuren zunehmend an Bedeutung gewinnen, heißt es in dem Papier weiter. Deshalb arbeite die Bundeswehr eng mit anderen Behörden im Inland sowie mit anderen Staaten zusammen. Das Papier verweist auch auf das jüngste Strategische Konzept der Nato, das Ende 2010 in Lissabon verabschiedet wurde, und in dem erstmals die Sicherheit im Cyberspace als prominente sicherheitspolitische Herausforderung definiert ist.

Ungeklärt ist bislang, auf welcher rechtlichen Grundlage die Bundeswehr im Cyberspace offensiv werden könnte. Dies hänge vom jeweiligen Einzelfall ab, hieß es am Dienstag aus dem Ministerium. Aber einen solchen Fall habe es ja noch nicht gegeben.

Pressespiegel 1, 6. 6. 2012

Financial Times Deutschland
06.06.2012, S.10
Sicherheit

Hacker in Uniform

Die Bundeswehr rüstet sich für Kriege im virtuellen Raum. Dabei kämpft sie mit sehr realen Problemen

Thomas Steinmann, *Berlin*,
und Joachim Zepelin, *Tallinn*

Es sind zwei Welten, die in Geisdorf bei Bonn aufeinanderprallen. Auf der einen Seite ist die Bundeswehr, eine klassische Armee mit starren Strukturen und vielen Generälen, die vom Kalten Krieg geprägt wurden. Auf der anderen Seite ist die Welt der Hacker – jung und anarchisch, den Kalten Krieg kennen die meisten nur aus Geschichtsbüchern. Beim Kommando Strategische Aufklärung sollen diese Welten zusammengebracht werden. Hier hat die Bundeswehr eine Hackertruppe für den modernen Cyberkrieg aufgebaut, die sich nun einsatzbereit meldet.

Natürlich nennt die Bundeswehr die Digitalkämpfer nicht Hacker, bei ihr heißen sie „CNO-Kräfte" – CNO für Computernetzwerkoperationen. Auch führen die Staatshacker im Ernstfall keine Cyberangriffe aus, sondern es geht um „Wirken in gegnerischen Netzen" – Begriffe, die Militärs aus konventionellen Konflikten vertraut sind, die in der digitalen Welt aber eigenartig klingen. Und auch die Tatsache, dass die Bundeswehr erst nach fünf Jahren eine „Anfangsbefähigung" erreicht hat, während Amerikaner und Israelis digitale Waffen wie den Computerwurm Stuxnet bereits eingesetzt haben, ist ein Indiz dafür, dass sich die Deutschen bei der virtuellen Aufrüstung schwertun.

Seit den ersten Schritten für den Aufbau einer Hackertruppe im Jahr 2006 haben die Fachleute bei der Bundeswehr mit mehreren Problemen zu kämpfen. Diese beginnen damit, überhaupt hinreichend Top-Computerexperten zu finden, die ihr Wissen für das bei der Truppe übliche Gehaltsniveau zur Verfügung stellen – während die Industrie, die ebenfalls auf sichere IT-Infrastruktur angewiesen ist, ein Vielfaches zahlt. Satte Boni auf den Sold, wie es die Amerikaner tun, um Hacker für den Staatsdienst zu gewinnen, kann die Bundeswehr nicht zahlen.

„Wenn die Regierung die neue militärische Fähigkeit wirklich haben will, muss sie die Bezahlung liberalisieren oder sie als Dienstleistung von außen zukaufen", sagt der Cyberexperte Sandro Gaycken von der Freien Universität Berlin. Im virtuellen Raum ist es kriegsentscheidend, die besten Köpfe zu gewinnen. Tatsächlich rekrutiert die streng abgeschottete Hackertruppe ihre Spezialisten zum größten Teil aus der Bundeswehr selbst, etwa aus den Informatik-Fachbereichen der eigenen Universitäten. Von „Bundeswehrschülern mit IT-Kurs" redet Gaycken.

Hinter der Know-how-Frage steckt ein Grundsatzproblem. Zwar hat Cybersicherheit für die Bundesregierung hohe Priorität, seit auch Regierungsnetze hierzulande von ausländischen Geheimdiensten attackiert werden. Der Fokus liegt aber klar auf der Abwehr gegnerischer Angriffe. Die Entwicklung eigener Fähigkeiten, fremde Netze und Server zu attackieren, wird dagegen eher halbherzig betrieben – aus Scheu vor den dafür notwendigen Investitionen, aber auch weil auf der Generalsebene viele Männer sitzen, die bei Krieg nicht an virtuelle Schlachten denken. Und dann ist da noch der Auslandsgeheimdienst BND, der auch in Sachen Cyber aktiv ist.

Hinzu kommt eine bestenfalls diffuse Rechtslage. Cyberkonflikte sind ein noch junges Phänomen, es gibt keinen Verhaltenskodex wie das Kriegsvölkerrecht. Auch im nationalen Rahmen sind viele Fragen noch offen. Und anders als Amerikaner, Chinesen oder Russen legen die Deutschen immer Wert darauf, dass der Einsatz von Gewalt legitimiert ist.

Völkerrechtler zweifeln zwar nicht daran, dass die Bundeswehr im Prinzip jede Art von Cyberwaffe für einen Krieg vorbereiten darf. Wolff Heintschel von Heinegg von der Viadrina-Universität in Frankfurt (Oder), Autor eines Handbuchs zum Cyberrecht, hält auch den Einsatz von Cyberwaffen als zusätzliches militärisches Mittel in konventionellen bewaffneten Konflikten für rechtlich unproblematisch. „Es macht keinen Unterschied, ob man eine Bombe wirft oder über ein Computersystem angreift", sagt er. Die Bundeswehr müsse ihr Arsenal erweitern, um ihren Auftrag der Landesverteidigung zu erfüllen.

In Deutschland gibt es aber noch den Parlamentsvorbehalt für den Einsatz militärischer Gewalt. Die Zustimmung des Bundestags ist nach Ansicht Heintschel von Heineggs auch dann erforderlich, wenn nur Cyberwaffen eingesetzt werden – etwa wie im Fall Stuxnet. Für die Praktiker ist das ein Problem. Sollte ein Angriff auf fremde Computersysteme vorher im Bundestag beraten werden, wären Gegner gewarnt. Um für den Cyberkrieg gerüstet zu sein, braucht womöglich auch das deutsche Recht ein Update.

Flame – gut getarnter Schädling

Missbraucht Täglich werden neue Informationen über den neuen Computerschädling veröffentlicht. Jetzt wurde bekannt, dass sich Flame mit Microsoft-Zertifikaten getarnt hat. So wurde er von Sicherheitssoftware nur als normales Programm wahrgenommen. Microsoft hat das Problem mit einem Update gelöst und die gekaperten Zertifikate unschädlich gemacht.

Gefälscht Laut dem Softwarehersteller Kaspersky Lab haben die Urheber von Flame Server, von denen der Trojaner gesteuert wurde, unter falschen Anschriften angemeldet. Besonders häufig seien Adressen in Deutschland oder Österreich verwendet worden.

Anlage 3

Spatschke, Norman

Von: Schallbruch, Martin
Gesendet: Dienstag, 29. Mai 2012 17:58
An: StRogall-Grothe_
Cc: Spatschke, Norman; IT3_; Batt, Peter
Betreff: Eilt sehr!!! MinUnterrichtung Schadsoftware "Flame"

IT 3 – 606 000-2/72#16

Herrn Minister

über
Frau Staatssekretärin Rogall-Grothe
Herrn IT-Direktor [Sb 29.5.]
Herrn SV IT-Direktor [i.V. Sb 29.5.]
Herrn RL IT 3 gez. Dü/Ma 29/5

Abdruck: StF, AL ÖS, Presse

Wegen Eilbedürftigkeit als E-Mailvorlage

Neue Schadsoftware „Flame"

1. Votum
Kenntnisnahme.

2. Sachverhalt
Aktuelle Medienveröffentlichungen berichten über die Entdeckung eines neuen Schadsoftwareprogramms „Flame", dessen Komplexität und Qualität „Stuxnet" und „Duqu" entsprechen und bereits seit mehreren Jahren im Einsatz sein soll. Haupteinsatzgebiet seien der Mittlere Osten und Osteuropa; die meisten infizierten Rechner wurden nach Informationen von Symantec im Iran, Palästina, Ungarn und im Libanon festgestellt.
Das iranische nationale CERT „Maher" ließ verlauten, „Flame" sei zum Zeitpunkt seiner Entdeckung von keinem der getesteten 43 Antivirenprogramme erkannt worden. Zwischenzeitlich hat das iranische CERT ein Werkzeug zur Erkennung von „Flame" (Detektionstool) entwickelt und ausgewählten Unternehmen/Organisationen bereits Anfang Mai zur Verfügung gestellt. Mittlerweile soll auch ein Werkzeug zur Bereinigung entwickelt worden sein.

Nach Informationen des BSI übertrifft „Flame" (Bezeichnung stammt von einem der Hauptmodule des Programms) die Komplexität von „Stuxnet" und „Duqu" deutlich und ist daher nur sehr aufwändig zu analysieren. Auch ist der Code des Schadprogramms - entgegen einiger Medienberichte - komplett verschieden zu den beiden anderen Programmen. Angreifbar sind die Betriebssysteme **Windows XP, Windows Vista und Windows** 7 unter Ausnutzung von Schwachstellen im Windows-Betriebssystem. Derzeit unklar ist, ob „Flame" bei der Infektion auch bislang unbekannte Schwachstellen (sog. Zero-Day-Exploits) nutzt.
Der Einsatzzweck von **„Flame"** scheint das **Ausspähen von Informationen** und Daten zu sein. Das Schadprogramm ist hoch flexibel und konfigurierbar und verfügt über ca. 20 Schadfunktionen, beispielsweise:

- Wurm-Funktionalität zur Verbreitung über Wechseldatenträger und lokale Netzwerke
- Unterwanderung bzw. Deaktivierung einer Vielzahl von Anti-Virus-Produkten und anderer Sicherheitssoftware
- Mitschneiden von Netzwerkverkehr, Erkennung von Netzwerkressourcen und Sammlung von Passwörtern
- Durchsuchen der Festplatte infizierter Systeme nach Dateien mit bestimmten Inhalten
- Anfertigung von Serien von Screenshots des Desktops, wenn bestimmte Prozesse (z.B. Chatprogramme) oder Fenster aktiv sind

- Anfertigung von Audio-Aufnahmen über an das infizierte System angeschlossene Mikrofone (Gespräche in Räumen oder auch Voice-over-IP-Telefonate)
- Nutzung von Bluetooth zur Sammlung von Informationen über andere Geräte in Reichweite des infizierten Systems
- Übermittlung der ausgespähten Daten an Kontrollserver der Angreifer über verschlüsselte Verbindungen (SSH- oder HTTPS).

Über diese Schadfunktionen hinaus wurden eine Reihe von Schutzmaßnahmen implementiert (z.B. Programmierzeitpunktverschleierung, Analyseresistenz, Programmmodul zum spurenfreien Löschen), um die Entdeckung und Analyse des Schadprogramms „Flame" zu erschweren.

Die im Nationalen Cyber-Abwehrzentrum (Cyber-AZ) vertretenen Behörden wurden durch das BSI im Rahmen der heutigen Morgenlage über die vorliegenden Erkenntnisse informiert. Herr VP-BSI kontaktiert das BfV hinsichtlich des vermuteten nachrichtendienstlichen Hintergrunds.

3. Stellungnahme

Nach Auffassung des BSI ist eine **Betroffenheit Deutschlands und deutscher Unternehmen derzeit nicht erkennbar.** Die Qualität und Funktionalität von „Flame" sind sehr hoch und somit durchaus vergleichbar mit „Stuxnet" und „Duqu" (Manipulation von Siemens-Steuerungsanlagen für Produktionsprozesse und Infizieren von Unternehmensnetzen der Hersteller solcher Steuerungssoftware).
Für diese Art neuartiger Bedrohungen hat sich die Bezeichnung Advanced Persistent Threats (APT) etabliert. Die Angriffsvektoren sind sehr gezielt aufgebaut und für den Attackierten kaum nachvollziehbar und sehr gut getarnt. "Persistent" sind sie, weil sie sich sehr passiv verhalten, dadurch kaum auffindbar sind und über einen langen Zeitraum wirken können.

Der aktuelle Vorfall unterstreicht die Bedeutung der durch das BMI seit geraumer Zeit initiierten Maßnahmen. Ausgehend von der nationalen Cyber-Sicherheitsstrategie der Bundesregierung mit den Kernelementen Nationaler Cyber-Sicherheitsrat (Cyber-SR) und Cyber-AZ und einem verstärkten IT-Schutz Kritischer Infrastrukturen. Auch die aktuell durch Herrn Minister geführten Branchengespräche mit den Vertretern Kritischer Infrastrukturen belegen, dass das BMI die veränderte Gefährdungslage registriert und angemessen auf sie reagiert.

Referat IT 3 wird unaufgefordert über aktuelle Entwicklungen berichten.

Gez. Spatschke

Anlage 4 369

Gitter, Rotraud, Dr.

Von: Pilgermann, Michael, Dr.
Gesendet: Montag, 11. Juni 2012 16:19
An: Andris, Ekkehard; Dimroth, Johannes, Dr.; Dürig, Markus, Dr.; Gitter, Rotraud, Dr.; Kurth, Wolfgang; Mantz, Rainer, Dr.; Nimke, Anja; Otte, Kathrin; Pilgermann, Michael, Dr.; Spatschke, Norman; Treib, Heinz Jürgen
Betreff: WG: EILT: Erwartetes Medienecho auf Meldung: Kaspersky findet Verbindung zwischen Stuxnet und Flame

Ref.-Post allen z.K.

Beste Grüße
Michael Pilgermann
-1527

-----Ursprüngliche Nachricht-----
Von: BSI IT-Lagezentrum [mailto:lagezentrum@bsi.bund.de]
Gesendet: Montag, 11. Juni 2012 16:14
An: IT3_; BMIPoststelle, Posteingang.AM1
Cc: IT5_; GPPraesident; GPVizepraesident; GPLeitungsstab; presse@bsi.bund.de; GPAbteilung C; GPFachbereich C 1; GPFachbereich C 2; vlreferatsleiterc@bsi.bund.de; GPReferat B 24; GPAbteilung B
Betreff: EILT: Erwartetes Medienecho auf Meldung: Kaspersky findet Verbindung zwischen Stuxnet und Flame

Sehr geehrte Damen und Herren,

Sachverhalt:
CERT-Bund wurde heute von Kaspersky über eine bei Analysen der Schadsoftware gefundenen Verbindung zwischen Stuxnet und Flame informiert.
Der Sachverhalt wurde soeben von Kaspersky zeitgleich in einem Blogposting veröffentlicht.
URL:
<http://www.securelist.com/en/blog/208193568/Back to Stuxnet the missing link>

Technischer Hintergrund:
In einer frühen Version von Stuxnet wurde ein Flame-Modul für die Infektion über USB-Autorun gefunden. Dieses Modul wurde ab ca. 2010 in späteren Stuxnetversionen durch den LNK-Exploit ersetzt.

Bewertung:
Es ist nicht auszuschließen, dass der von Kaspersky gefundene Sachverhalt wahr ist. Nach der Veröffentlichung von Kaspersky ist mit einem großen Medienecho und einer weiteren Spekulation über den Urheber zu rechnen.
Sollten die von Kaspersky gefundenen Informationen stimmen, ist vermutlich davon auszugehen, dass beide Schadprogramme den selben Urheber haben. Ab einem bestimmten Stand wurden die beiden Schadprogramme aber vermutlich von verschiedenen Entwicklerteams programmiert.
Wenn das Flame Modul in Stuxnet genutzt und im Jahr 2010 durch anderen Code ersetzt wurde, wäre Flame älter als Stuxnet, d.h. vermutlich von 2008 oder älter.
Durch die Verbindung der beiden Schadprogramme, wird die Spekulation des nachrichtendienstlichen Hintergrundes, namentlich USA oder Israel, wieder hochkochen.
Grundsätzlich bleibt die Trennung von Stuxnet als Sabotage und Flame als Spionagewerkzeug erhalten.

Votum:
Kenntnisnahme

Mit freundlichen grüßen
i.A.
--
Michael Dwucet

Lagezentrum und CERT-Bund - Referat C 21
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 185 -189
53175 Bonn
Telefon: +49 (0)228 9582 5110
Telefax: +49 (0)228 9582 7025
E-Mail: lagezentrum@bsi.bund.de
Internet: https://www.bsi.bund.de/CERT-Bund
https://www.buerger-cert.de
https://www.cert-bund.de

Anlage 5

Bundesministerium
der Verteidigung

- 1780001-V633 -

Bundesministerium der Verteidigung, 11055 Berlin

Frau
Dr. h.c. Susanne Kastner, MdB
Vorsitzende
des Verteidigungsausschusses
des Deutschen Bundestages
Platz der Republik 1
11011 Berlin

Thomas Kossendey
Parlamentarischer Staatssekretär
Mitglied des Deutschen Bundestages

HAUSANSCHRIFT Stauffenbergstraße 18, 10785 Berlin
POSTANSCHRIFT 11055 Berlin

TEL +49 (0)30 18-24-8060
FAX +49 (0)30 18-24-8088
E-MAIL BMVgBueroParlStsKossendey@bmvg.bund.de

Berlin, 13. April 2012

Sehr geehrte Frau Vorsitzende,

mit Schreiben Ihres Sekretariats vom 8. März 2012 bitten Sie um Vorlage eines schriftlichen Berichtes zum Themenkomplex „Cyber Warfare".

Den erbetenen Bericht füge ich als Anlage bei.

Mit freundlichem Gruß

Thomas Kossendey

Thomas Kossendey

Anlage zu Parl Sts beim Bundesminister der Verteidigung Kossendey
1780001-V633 vom 13. April 2012

Bericht

zum

Themenkomplex „Cyber-Warfare“

Gefährdungslage

Fehlerbehaftete oder kompromittierte IT-Produkte und Komponenten, der Ausfall von Informationsinfrastrukturen oder schwerwiegende Angriffe im Cyber-Raum können zu erheblichen Beeinträchtigungen der technischen, wirtschaftlichen und administrativen Leistungsfähigkeit und damit der gesellschaftlichen Lebensgrundlagen Deutschlands führen.

Dabei werden die IT-Systeme und -Komponenten aufgrund hoher Komplexität immer verwundbarer. Insbesondere die Wandlungsfähigkeit von Schadsoftware und die Verfügbarkeit von immer ausgereifteren Werkzeugen für das Design und Redesign von Schadsoftware stellen eine zunehmende Bedrohung dar. Potenzielle Angreifer können somit im Internet preiswert angebotene Schadsoftware nebst Werkzeugen zu deren Konfiguration und Anpassung mieten und für missbräuchliche Zwecke nutzen.

Der Vorfall „Stuxnet" (Juli 2010) hat gezeigt, dass Cyber-Angriffe nicht ausschließlich online, sondern z.B. auch über bewegliche Datenträger erfolgen können. Damit sind selbst bislang vom offenen Internet als sicher abgetrennt vermutete IT-Systeme, wie Industrieproduktionsstätten oder Kritische Infrastrukturen, verwundbar. Hieraus muss auch die zunehmende Bedeutung von notwendigen Maßnahmen der IT-Abschirmung abgeleitet werden.

Im Rahmen des Risikomanagements analysiert und bewertet die Bundeswehr kontinuierlich die Bedrohungs- und Gefährdungslage des IT-Systems der Bundeswehr. Das Computer Emergency Response Team der Bundeswehr (CERTBw) führt dazu auf Basis einer Vereinbarung zum Informationsaustausch mit anderen nationalen und internationalen CERT-Organisationen und mit Hilfe seiner technischen Sensorik ein aktuelles Lagebild zur IT-Sicherheit. Das Betriebszentrum IT-System der Bundeswehr führt darüber hinaus ein aktuelles Gesamtlagebild des IT-Systems Bundeswehr, bei dem auch Gefährdungen betrachtet werden, die nicht informationstechnischer Natur sind (z.B. Naturkatastrophen, Feuer). Bei einer möglichen kritischen Lage wird ein Risiko Management Board einberufen, in dem die von der Gefährdung betroffenen Bereiche und die für den Schutz bzw. die Wiederherstellung der Sicherheit zuständigen Funktionsträger die weitere Koordinierung der Maßnahmen übernehmen.

Die extern zugänglichen Schnittstellen des IT-Systems der Bundeswehr werden kontinuierlich durch gerichtete und ungerichtete Angriffe von Hackern bzw. durch das Einbringen von Schadsoftware bedroht.

Zum Begriff des „Cyber-War"

„Cyber-War" beschreibt dem Wortsinn nach gezielte Angriffe staatlicher Institutionen auf Computersysteme und IT-Netzwerke eines oder mehrerer anderer Staaten, die substanzielle Auswirkungen auf die Handlungsfähigkeit dieser Staaten haben. Die nationale Sicherheitsstrategie „Cyber-Sicherheitsstrategie für Deutschland" definiert lediglich den Begriff „Cyber-Angriff" und verwendet den Begriff „Cyber-War" oder „Cyber-Krieg" nicht. Der Begriff „Cyber-Angriff" umfasst je nach Urheber zusätzlich die Aktionen „Cyber-Ausspähung" und „Cyber-Spionage".

Aus Sicht der Bundesregierung beschreibt der Begriff „Cyber-War" oder „Cyber-Krieg" die tatsächlichen sicherheitspolitischen Herausforderungen nur unzureichend und suggeriert ein falsches Bild sowohl betreffend der Bedrohungslage im Cyberspace als auch der möglichen Gegenmaßnahmen.

Das IT-System der Bundeswehr ist, genau wie alle IT des Bundes, zu jeder Zeit einer Vielzahl von unterschiedlich motivierten und technisch versierten Angriffen eines breiten Spektrums von Akteuren ausgesetzt, ohne dass hierfür der Begriff Krieg angemessen wäre.

In der Bewertung der Bedrohungslage durch die Bundesregierung werden Maßnahmen im und durch den Cyberspace zunehmend operative Bedeutung bei kriegerischen Auseinandersetzungen sowohl zwischen Staaten als auch bei Auseinandersetzungen nicht-staatlicher Akteure haben. Militärisch wird der Cyberspace daher, entsprechend der Bedeutung des Faktors Information für die Erfüllung der politisch vorgegebenen Aufgaben, als operative Domäne, vergleichbar dem Luft- oder Seeraum, behandelt.

Cyber-Sicherheit in der Bundeswehr

Die Bundeswehr hat sich sehr frühzeitig auf die Bedrohungen aus dem Cyberspace eingestellt und bereits 1992 begonnen, zur präventiven Cyberabwehr eine IT-Sicherheitsorganisation mit speziell ausgebildeten IT-Sicherheitsbeauftragten in allen Dienststellen der Bundeswehr, aufzubauen. Im Jahr 2002 wurde das CERTBw eingerichtet, das dem Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr (IT-AmtBw) unterstellt ist.

Da zielgerichtete Cyber-Angriffe hoher Qualität durch präventive Maßnahmen nicht vollständig verhindert werden können, kommt dem Krisenmanagement und der Fähigkeit zur Angriffserkennung, Schadensbegrenzung und Wiederherstellung der IT-Systeme eine wachsende Bedeutung zu. Hierzu haben das für die IT-Sicherheitsorganisation zuständige IT-AmtBw und die für den Betrieb des IT-Systems verantwortliche Führungsunterstützungsorganisation der Bundeswehr, geführt durch das Streitkräfteunterstützungskommando, das eingangs erwähnte gemeinsame Risiko Management-Board eingerichtet.

Ende 2010 erreichte die zentrale Betriebsführungseinrichtung für das gesamte IT-System der Bundeswehr seine Grundbefähigung. Dort können Betriebsanomalien, die u.a. durch Cyber-Angriffe hervorgerufen werden können, erkannt werden. Vor allem jedoch erfolgen dort verzugslos alle betrieblichen Steuerungsmaßnahmen für das IT-System der Bundeswehr auf Basis umfassender, aktueller Lageerkenntnisse zu allen wesentlichen IT-Systemen nach aktuellen operationellen Schwerpunkten.

Das IT-System der Bundeswehr nutzt die verfügbaren technischen Sicherheitsmaßnahmen (u.a Virenschutz, Firewalls, Intrusion Detection Sensoren, Verschlüsselung, Schnittstellenkontrollmaßnahmen) und orientiert sich dabei an den grundsätzlichen Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Insgesamt ist zu betonen, dass die Gewährleistung von Sicherheit im Cyber-Raum eine Aufgabe ist, die nicht ausschließlich durch die IT-Sicherheitsorganisation oder die IT-Abschirmung geleistet werden kann. Vielmehr müssen auch die Betreiber der Netze (militärische und nicht-militärische Betriebsführung und IT-Administratoren, aber auch Vertragspartner, sog. Provider) als auch die Nutzer selbst ihren Beitrag zur Sicherheit leisten. Die Bundeswehr trägt dieser Notwendigkeit durch entsprechende Ausbildung ihres IT-Betriebspersonals genauso Rechnung wie durch Sicherheitsauflagen für zivile Provider, ständige Unterrichtungen und Belehrungen der Nutzer.

Die Fähigkeiten der Bundeswehr zur Wirkung in gegnerischen Netzwerken (Computer Netzwerk Operationen (CNO)) ist grundsätzlich getrennt von Maßnahmen der Cyber Defence, also der Abwehr von Cyber-Angriffen, zu sehen. CNO sind ein weiteres Wirkmittel der Streitkräfte.

Die Bundeswehr stellt derzeit beim Kommando Strategische Aufklärung die Abteilung Computernetzwerkoperationen auf. Eine Anfangsbefähigung zum Wirken in gegnerischen Netzen wurde erreicht. Für die Ausbildung bzw. zur Erprobung von Verfahren besteht die Möglichkeit zur Durchführung von Simulationen in einer abgeschlossenen Laborumgebung.

Zusammenarbeit in der Cyber-Sicherheit

Nationale Ebene

IT-AmtBw und CERTBw arbeiten auf Grundlage des BSI-Gesetzes eng mit dem BSI und dem dort angesiedelten IT-Lage- und Analysezentrum zusammen. Ziel der Zusammenarbeit ist es, Gefahrenquellen so früh wie möglich zu erkennen, zu beurteilen und so schnell wie möglich konzertierte Gegenmaßnahmen zu ergreifen. Dabei ist immer auch eine enge Zusammenarbeit mit nationalen und internationalen Herstellern von IT-Sicherheitsprodukten von Bedeutung. Gemäß der „Allgemeinen Verwaltungsverordnung zu § 4 des BSI-Gesetzes" meldet die Bundeswehr kritische IT-Sicherheitsvorkommnisse an das IT-Lage- und Analysezentrum beim BSI. Die Bewertung nimmt der IT-Sicherheitsbeauftragte der Bundeswehr vor. Bei einer vom BSI festgestellten übergreifenden oder nationalen IT-Krise wächst das IT-Lage- und Analysezentrum beim BSI zu einem IT-Krisenreaktionszentrum auf.

Grundsätzliche Fragen der IT-Steuerung und IT-Sicherheit der IT des Bundes werden zudem im ressortübergreifenden Rat der IT-Beauftragten (auch IT-Rat genannt) behandelt. Hier wird die Bundeswehr durch den IT-Direktor vertreten.

Mit der Cyber-Sicherheitsstrategie für Deutschland wurden die bestehenden Maßnahmen der Bundesregierung zur Gewährleistung der Cyber-Sicherheit in Deutschland weiterentwickelt.

Das Bundesministerium der Verteidigung (BMVg) ist ständiges Mitglied des Cyber-Sicherheitsrats, vertreten durch einen beamteten Staatssekretär. Darüber hinaus beteiligt sich die Bundeswehr am Nationalen Cyber-Abwehrzentrum unter Wahrung ihrer verfassungsrechtlichen sowie gesetzlichen Aufgaben und Befugnisse. Im Cyber-Abwehrzentrum tauschen die beteiligten Behörden Erkenntnisse zu neuen Bedrohungen, Sicherheitslücken oder Schadprogrammen aus. Hierzu wurden

Verbindungspersonen der IT-Sicherheitsorganisation der Bundeswehr, der zentralen Betriebsführung und des Militärischen Abschirmdienstes in das Nationale Cyber-Abwehrzentrum entsandt.

Internationale Ebene

Aufgrund des globalen Charakters des Cyberspace kann den sicherheitspolitischen Herausforderungen nur in einem kooperativen und internationalen Ansatz begegnet werden.

Von besonderer Bedeutung ist dabei der zügige Informationsaustausch der Experten auf europäischer und internationaler Ebene zu neuen Sicherheitslücken, Schadprogrammen oder anderen Cyber-Bedrohungen. Das BSI betreibt hierzu für die Bundesverwaltung das CERT-Bund, das mit ähnlichen Einrichtungen innerhalb der EU sowie weltweit in regelmäßigem Kontakt steht, um frühzeitig neue Gefahren zu erkennen und Handlungsempfehlungen zu geben.

Großes Potential zur Verbesserung der Cyber-Sicherheit misst die Bundesregierung Maßnahmen kooperativer Sicherheit im Cyberspace zu. In enger Abstimmung insbesondere mit USA, GBR und FRA setzt sich die Bundesregierung für die Entwicklung von Normen für staatliches Verhalten im Cyberspace und Vertrauens- und Sicherheitsbildende Maßnahmen ein. Anlässlich der Cyber-Sicherheits-Konferenz der OSZE im Mai 2011 hat DEU erste Vorschläge für mögliche Elemente eines solchen, von möglichst vielen Staaten zu zeichnenden Verhaltenskodex vorgestellt, u.a.:

- Die Bestätigung der grundsätzlichen Prinzipien von Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität von Daten und Netzwerken sowie des Schutzes geistigen Eigentums;
- die Verantwortung zum Schutz kritischer Infrastrukturen;
- die Intensivierung internationaler Kooperation mit dem Ziel, Vertrauen, Transparenz und Stabilität zu fördern und Risiken zu reduzieren;
- die Etablierung oder Aufwertung von Krisenkommunikationsverbindungen und Frühwarnmechanismen unter Einbeziehung von Cyber-Angriffen.

NATO

Das 2010 beschlossene Strategische Konzept der NATO identifiziert Cyber-Sicherheit als prominente sicherheitspolitische Herausforderung. Die Staats- und Regierungschefs der Allianz haben anlässlich des Gipfeltreffens in Lissabon die Erarbeitung einer neuen NATO Cyber Defence Policy beauftragt.

Der Kern dieser beim Treffen der NATO-Verteidigungsminister am 8. Juni 2011 beschlossenen Cyber Defence Policy ist die Schaffung klarer Zuständigkeiten für Cyber Defence innerhalb der Organisation, damit diese besser in der Lage ist, einheitliche Grundsätze und Standards für die Netzwerklandschaft der NATO durchzusetzen und auf diese Weise einen wirksamen Schutz der NATO vor Angriffen aus dem Cyber-Raum zu gewährleisten.

Ebenso wichtig ist die Berücksichtigung von Fragen der Cyber-Sicherheit im gesamten Aufgabenspektrum der NATO, d.h. sowohl in der Bewusstseinsförderung von Risiken und Bedrohungen im Umgang mit IT bis hin zur Einbeziehung in den militärischen Planungsprozess, um eine Auftragserfüllung auch bei einer Beeinträchtigung der IT-Netze sicherstellen zu können. Alle Schritte zur Umsetzung der NATO Cyber Defence Policy sind in einem detaillierten Arbeitsplan festgehalten, der durch die jeweiligen Gremien und Agenturen innerhalb der NATO abgearbeitet wird. Die Erfüllung der Maßnahmen wird engmaschig durch das Defence Policy and Planning Committee (DPPC) und das Consultation, Command and Control Board (C3B), in dem auch die Bundesregierung vertreten ist, überwacht.

Wichtigstes Gremium im Falle einer Cyberkrise ist das Cyber Defence Management Board (CDMB), das die notwendigen Maßnahmen zur Krisenbewältigung ergreift und über ein Cyber Defence Coordination and Support Center (CD CSC) u.a. auch das NATO Computer Incident Response Capability (NCIRC) steuert. Auf Arbeitsebene kooperiert das CERTBw eng mit dem CERT der NATO (NCIRC).

Die Bundeswehr beteiligt sich darüber hinaus seit dessen Aufstellung am „Cooperative Cyber Defence Centre of Excellence" (CCD CoE) in Tallinn, das durch die NATO Ende 2008 als Kompetenzzentrum akkreditiert worden ist. Derzeit stellt die Bundeswehr dort den Chef des Stabes, eine Rechtsberaterin und einen Offizier in der Forschungs- und Entwicklungsabteilung. Das BMVg ist stimmberechtigtes Mitglied in der Steuerungsgruppe des CCD CoE.

Bilaterale Beziehungen

Fragen der Cyber-Sicherheit sind grundsätzlich Gegenstand der militärpolitischen Abstimmungen mit DEU Verbündeten und Partnern.

Eine besondere Bedeutung kommt dabei insbesondere den USA, FRA und GBR sowie CHE zu. Mit dem USA Verteidigungsministerium wurde im Mai 2008 ein entsprechendes Kooperationsabkommen der IT-Sicherheitsorganisationen geschlossen, auf militärpolitischer Ebene wurde der Dialog mit den USA im November 2010 aufgenommen. Analog wurde auch mit CHE sowohl auf Arbeitsebene als auch zwischen den beteiligten Regierungsressorts ein Erfahrungsaustausch begonnen.

Anlage 6

Referat V I 2

V I 2 - 110 010/103

RefL: MR'n Bickenbach
Ref: ORR Dr. Seedorf
RRef Dr. Mehlhorn

Berlin, den 5. Oktober 2011

Hausruf: 45547

Fax: 545547

bearb. von: Dr. Seedorf/Dr. Mehlhorn

E-Mail: lutz.mehlhorn@bmi.bund.de

L:\Themen\Wehrverfassungsrecht\IT-Infrastruktur + Netzverteidigung\Ressortgespräche Netzverteidigung\20111005_Vermerk_ Ressortgespräch Cyberabwehr mit BMVg.doc

Betreff: Gespräch zu Rechtsfragen der Verteidigung gegen IT-Angriffe und „Cyber-Abwehr" vom 24. 8. 2011, 14:15 bis 17:00 Uhr

hier: Ergebnisprotokoll und Fragen zur weiteren Vertiefung

Anlagen: - 3 - (Teilnehmerliste, Non-Paper, Protokoll Besprechung 2009)

1) Vermerk:

An der von Frau UAL'n V I geleiteten Besprechung nahmen seitens BMI Herr IT-D sowie Vertreter der Referate V I 2, V I 4 und IT 3 teil; seitens BMVg Herr ALR sowie die Referate FüS III 2, R II 2 und R II 3 (siehe Anlage 1).

Die Teilnehmer haben vereinbart, zentrale Aussagen des Gespräches in einem Non-Paper (siehe Anlage 2) festzuhalten, das zwischenzeitlich zwischen BMI (V I 2; V I 4, IT 3) und BMVg abgestimmt wurde. Auf dieser Grundlage identifizierte Rechtsfragen können dann in einem noch nicht bestimmten Folgetermin weiter erörtert werden.

I. Die Besprechung erbrachte folgende Ergebnisse:

Anfang 2011 hat die Bundesregierung die nationale Cyber-Sicherheitsstrategie für Deutschland beschlossen. In diesem Zusammenhang ist zu prüfen, ob zur Abwehr von Angriffen im Cyber-Raum die gesetzlichen Grundlagen ausreichen und ob evtl. bestehende Rechtslücken zu schließen sind.

Nach operativ/technischem Verständnis ist bei Maßnahmen zur Verhinderung schädlicher Einwirkungen auf IT-Systeme zu unterscheiden:

- „Netzverteidigung" oder Cyber-Abwehr (Cyber Network Defense, CND) bezeichnet nur „passive" Maßnahmen ohne Zugriffe auf fremde Systeme.
- Aktive Maßnahmen unter Zugriff auf fremde Systeme werden unter dem Oberbegriff Cyber Network Operations (CNO) zusammengefasst und beinhalten Cyber Network Exploitations (CNE, wörtl. „Ausnutzungen") und Cyber Network Attacks (CNA).

Eine Zwitterstellung nimmt das Eindringen in fremde Systeme zu Aufklärungszwecken ein: „Staatliche Computerspionage" unterfällt als aktive Maßnahme CNE, sie kann jedoch auch Bestandteil passiver Netzverteidigung sein, wenn sie lediglich dem Zweck dient, Informationen über einen konkreten Angriff zu ermitteln.
Maßgeblich für die Unterscheidung Inland / Ausland ist allein der Standort des Servers, von dem die schädigende Wirkung unmittelbar ausgeht; nicht die Nationalität der Täter, die sich häufig nicht ermitteln lassen.

Auf der Grundlage der bisherigen Praxis lassen sich die folgenden Kategorien der Abwehr schädlicher Einwirkungen auf IT-Systeme bilden:

1. Präventionsmaßnahmen (z.B. Redundanzen vorhalten, bessere Firewalls, Aufklärung über sicherheitsbewusstes Verhalten im Cyber-Raum)
2. Defensive Maßnahmen (z.B. Entfernung von Schadsoftware auf dem eigenen angegriffenen System)
3. Aktive Maßnahmen zur Gefahrenabwehr
   a. Im Inland (z.B. Ordnungsverfügung gegen einen inländischen Serverbetreiber)
   b. Im Ausland (z.B. Rechtshilfeersuchen für Maßnahmen gegen einen ausländischen Serverbetreiber, Hackback)
4. Militärische Maßnahmen im Rahmen mandatierter Auslandseinsätze (z.B. Störung eines Funktelefonnetzes zur Verhinderung von IED-Anschlägen im Mandatsgebiet). Nur für solche Begleitmaßnahmen baut die BW zurzeit Fähigkeiten auf.

Nur die ersten beiden Kategorien beinhalten „Netzverteidigung" im engeren Sinne. Insoweit dürften keine gravierenden völker- oder verfassungsrechtlichen Probleme bestehen. Entsprechende Maßnahmen stellen typischerweise keinen Eingriff in fremde Rechtsgüter dar (anders ggfls. bei Ausspähungen) und liegen im Zuständigkeitsbereich jeder Behörde, die IT-Systeme betreibt.

Für aktive Gefahrenabwehrmaßnahmen im Inland kommt grundsätzlich das bestehende polizei- und strafrechtliche Instrumentarium in Betracht. Inwieweit dieses aus grundrechtlicher Sicht allen Szenarien gerecht wird, müsste vertieft betrachtet werden. Die Bundeswehr sieht gegenwärtig keine Rechtsgrundlage für die aktive Abwehr von IT-Angriffen gegen ihre Einrichtungen durch sie selbst. Aktive militärische Maßnahmen im Cyberraum im Rahmen von mandatierten Auslandseinsätzen werden über Art. 24 Abs. 2 GG mit umfasst und unterliegen insoweit dem Parlamentsvorbehalt.

In Bezug auf aktive Gefahrenabwehrmaßnahmen im Ausland wurden erste rechtliche Rahmenbedingungen identifiziert, die weiterer Erörterung bedürfen.

- Für Maßnahmen mit Wirkung im Ausland dürfte (auch) der Bund zuständig sein.
- Eine besondere verfassungsrechtliche Ermächtigung für Maßnahmen ziviler Bundesbehörden dürfte nicht erforderlich sein. Handlungsbedarf könnte jedoch einfachrechtlich sowohl bei Zuständigkeiten als auch Befugnissen bestehen. Insoweit müsste wohl je nach Maßnahmentyp unterschieden werden, da z.B. Informationsgewinnung von den Befugnissen von MAD, BND und ggfls. BKA gedeckt sein dürfte, Manipulationen an fremden IT-Systemen dagegen eher nicht.
- Für die Nutzung von Bundeswehrfähigkeiten (Personal und Sachmittel) ist eine ausdrückliche verfassungsrechtliche Ermächtigung erforderlich. Zukünftig sind Szenarien denkbar, in denen die Bundeswehr ihre Fähigkeiten den zivilen Behörden zur Verfügung stellt, so dass Art. 35 GG als Verfassungsgrundlage in Betracht kommt.
- Ein Einsatz der Bundeswehr auf Grundlage von Art. 87a Abs. 2 GG (Verteidigung) ist BMVg zufolge sehr unwahrscheinlich (anders noch die Einschätzung des BMVg im Jahre 2009; vgl. das Protokoll Besprechung 2009 – Anlage 3).
- Völkerrechtlich ist insbesondere unklar, inwieweit Staaten Duldungspflichten gegenüber aktiven Gefahrenabwehrmaßnahmen haben, die sich auf ihrem Territorium auswirken können. Teilweise könnten Vereinbarungen für Rechtssicherheit sorgen, die die Zulässigkeit solcher Maßnahmen etwa vergleichbar dem Institut der Nacheile regeln, wobei es schwer fallen dürfte, insoweit eine hinreichend breite Partizipation zu erzielen. Ein denkbarer weiterer Ansatzpunkt könnte darin liegen, in relativ geringfügigen „network operations" gar keinen relevanten Eingriff in fremde Souveränitätsrechte zu sehen.

II. Bewertung und weiteres Vorgehen

Die Besprechung hat insbesondere bei den Begrifflichkeiten und den Einsatzsituationen von IT-Maßnahmen wichtige Vorfragen klären können. Es hat sich gezeigt, dass rechtliche Fragestellungen insbesondere für das Szenario hoheitlicher aktiver IT-Maßnahmen mit Wirkung im Ausland bestehen. Für BMVg scheint zwar eine zeitnahe Fortsetzung der Gespräche keine Priorität zu haben. Sobald ein weiteres Gespräch jedoch zustande kommt, könnten dabei die folgenden Rechtsfragen weiter bzw. wieder unter dem speziellen Aspekt Cybersicherheit erörtert werden:

1. Kompetenz/Zuständigkeit
   - Hat der Bund gegenwärtig die Zuständigkeit für aktive Gefahrenabwehrmaßnahmen gegen IT-Angriffe (ausschließlich/konkurrierend neben den Ländern)?

- Bestehen verfassungsrechtliche Vorgaben bezüglich der Zuständigkeitszuweisung für aktive IT-Maßnahmen an eine bestimmte zivile Bundesbehörde (BKA, BSI)?

2. *Befugnisregelung*
   - Sind hoheitliche IT-Maßnahmen mit Wirkung im Ausland in jedem Fall an den Grundrechten zu messen?
   - Sind Maßnahmen denkbar, die keine grundrechtliche Eingriffsschwelle erreichen?
   - Welchen grundrechtlichen Vorgaben müsste eine Eingriffsbefugnis für IT-Maßnahmen mit Wirkung im Ausland genügen?
   - Welchen Bestimmtheitsanforderungen müsste eine Eingriffsbefugnis genügen; müssten alle denkbaren Maßnahmen hinsichtlich ihrer Wirkung im fremden IT-System explizit genannt werden?
   - Welche Auswirkungen hat es, wenn zu Beginn der Maßnahme nicht bekannt ist, ob/dass ihre Wirkung im Ausland eintritt?
3. Einbeziehung Bundeswehr
   - Können Unterstützungsleistungen der Bundeswehr mit Sachmitteln, Personal und Know-how für zivile Bundesbehörden bei aktiven IT-Maßnahmen technisch-logistische Amtshilfe im Sinne des Art. 35 Abs. 1 GG sein?
   - Wo ist die Grenze der technisch-logistischen Amtshilfe? Erst bei einem „Einsatz bewaffneter Streitkräfte" im Sinne des Art. 87a Abs. 2 GG?
   - Kann die Bundeswehr Eingriffsunterstützungsleistungen auf Basis von Art. 35 Abs. 3 Satz 1 GG zugunsten anderer Bundesbehörden leisten oder ist sie auf Unterstützungsleistungen für Länderbehörden beschränkt?
   - Kann es sich bei den für aktive CNA-Maßnahmen erforderlichen Fähigkeiten um „spezifische militärische Mittel" im Sinne des Art. 35 GG handeln?
   - Sind Art. 35 Abs. 2 Satz 2 und Abs. 3 GG überhaupt bei Unterstützungsleistungen der Bundeswehr einschlägig, wenn die Wirkung der Maßnahmen im Ausland erfolgen soll oder gelten diese Vorschriften nur für Inlandseinsätze?
   - Falls eine IT-Maßnahme der Bundeswehr (ausnahmsweise) auf Art. 87a Abs. 2 GG gestützt werden sollte, welche rechtlichen Voraussetzungen wären zu erfüllen?
   - Welche Auswirkungen hat die vordringende und inzwischen auch von der BReg vertretene Sicht im Völkerrecht, Cyberangriffe bei hoher Intensität als „bewaffnete Angriffe" im Sinne des Art. 51 UN-Charta zu bewerten, auf die innerstaatliche Bewertung der Ermächtigungsgrundlage des Art. 87a Abs. 2 GG?
   - Unter welchen Umständen könnten IT-Maßnahmen dem Parlamentsvorbehalt unterfallen?
   - Müssten mandatsbezogene CNO im Hinblick auf ParlBG ausdrücklich im Antrag der BReg ausgeführt werden?

4. Völkerrecht
   - Wie will sich die BReg – insb. vor dem Hintergrund der möglichen Selbstbetroffenheit als „Host State" eines Cyber Angriffes – in der weiteren Entwicklung des Völkergewohnheitsrechts zu der Frage positionieren, inwieweit Staaten Duldungspflichten gegenüber aktiven Gefahrenabwehrmaßnahmen haben, die sich auf ihrem Territorium auswirken?
   - Können relativ geringfügige „network operations" möglicherweise schon deswegen zu dulden sein, weil sie gar keinen relevanten Eingriff in Souveränitätsrechte darstellen, und wenn ja, wo liegt die entscheidende Erheblichkeitsschwelle?

2) Frau St'n Rogall-Grothe
über
Herrn AL V
Frau UAL'n V I
Frau RefL'n V I 2
m.d.B.u.K.

3) Abdruck Vermerk an V I 4

4) Frau Bickenbach n.R. z.K.

5) z.Vg.

Bundesministerium des Innern

Besprechung

Gesch.Z.: V I 2 - 110 010 / 103

Thema: Gespräch zu Rechtsfragen der Verteidigung gegen IT-Angriffe und "Cyber-Abwehr"		
Datum: 24.8.2011	Uhrzeit: 14.00 - 17.00 Uhr	Ort: Berlin, Fehrbelliner Platz 3, Raum 1.336

Teilnehmerliste

Nr.	Vertretene Stelle (Behörde, Referat)	Name (bitte in Druckschrift)	Dienststellung	Telefon (bitte mit Vorwahl)	E-Mail-Adresse	Unterschrift
01	BMVg Fü S III 2	Brewes, Oberst	RL	2004 8740	carstenbrewer@bmvg.bund.de	
02	"	Radatz, Kpt	Ref	8743	sacharadatz@bmvg.bund.de	
03	BMVg Abt R	Weingärtner	MinDir	0228 12 8176	dietrichweingaertner@bmvg.bund.de	
04	BMVg, R II 2	Spies	MinR'in	" -29350	SylviaSpies@bmvg.bund.de	
05	BMVg, R II 3	CONRADI	MinR	030 1824 29968	andreasconradi@bmvg.bund.de	
06	BMVg, R II 3	Burzer	RDir/R	" 29363	WolfgangBurzer@bmvg.bund.de	
07	BMI, V I 4	Hornung	RDir	030-18681-45548	ulrike.hornung@bmi.bund.de	
08	BMI, V I 4	Plate	ORR	" " -45564	tobias.plate@bmi.bund.de	
09	BMI, V I 4	Merz	ORR	" " -45505	juergenmerz@bmi.bund.de	

Anlage 1
5.1-2

Bundesministerium des Innern

Nr.	Vertretene Stelle (Behörde, Referat)	Name (bitte in Druckschrift)	Dienststellung	Telefon (bitte mit Vorwahl)	E-Mail-Adresse	Unterschrift
10	BMI, IT3	[illegible]	RR'in	1584	costaud. gilles@bmi.bund.de	
11	"	Dr. Dürig	RL	1374	Markus.Duerig@bmi.bund.de	
12	BMI	Schallbruch	ITD	2701	martin. schallbruch@...	
13	BMI	Dr. Mehlhorn	Referendar			
14	BMI, VI2	Seedorf	ORR	-45550	Sebastian.seedorf@bmi.bund.de	
15	BMI - VI2	Bickenbach	Refl'in	-45529	VI2@bmi.bund.de	
16						
17						
18						
19						
20						
21						
22						
23						
24						

Anlage 2 385

Non-Paper: 1. Gespräch zu Rechtsfragen der Abwehr von IT-Angriffen

Anfang 2011 hat die Bundesregierung die nationale Cyber-Sicherheitsstrategie für Deutschland beschlossen. In diesem Zusammenhang ist zu prüfen, ob zur Abwehr von Angriffen im Cyber-Raum die gesetzlichen Grundlagen ausreichen und ob evtl. bestehende Rechtslücken zu schließen sind. Für die Ebene des Bundes ergab eine erste Bestandsaufnahme folgende Ergebnisse:

Maßnahmen von Bundesbehörden zur Verhinderung schädlicher Einwirkungen auf IT-Systeme lassen sich in folgende Kategorien einordnen:

1. Präventionsmaßnahmen (z.B. Redundanzen vorhalten, bessere Firewalls, Aufklärung über sicherheitsbewusstes Verhalten im Cyber-Raum)
2. Defensive Maßnahmen (z.B. Entfernung von Schadsoftware auf dem eigenen angegriffenen System)
3. Aktive Maßnahmen zur Gefahrenabwehr
   a. Im Inland (z.B. Ordnungsverfügung gegen einen inländischen Serverbetreiber)
   b. Im Ausland (z.B. Rechtshilfeersuchen für Maßnahmen gegen einen ausländischen Serverbetreiber, Hackback)
4. Militärische Maßnahmen im Rahmen mandatierter Auslandseinsätze (z.B. Störung eines Funktelefonnetzes zur Verhinderung von IED-Anschlägen im Mandatsgebiet)

In Bezug auf die ersten beiden Kategorien bestehen keine gravierenden rechtlichen Probleme. Für aktive Gefahrenabwehrmaßnahmen im Inland kommt grundsätzlich das polizeirechtliche Instrumentarium in Betracht. Inwieweit dieses aus grundrechtlicher Sicht allen Szenarien gerecht wird, müsste vertieft betrachtet werden. Aktive militärische Maßnahmen im Cyberraum im Rahmen von mandatierten Auslandseinsätzen werden über Art. 24 Abs. 2 GG mit umfasst und unterliegen insoweit dem Parlamentsvorbehalt.

Rechtliche Fragestellungen ergeben sich insbesondere bei aktiven Gefahrenabwehrmaßnahmen im Ausland, die jedoch noch nicht abschließend geklärt worden sind:

- Für Maßnahmen mit Wirkung im Ausland dürfte (auch) der Bund zuständig sein.
- Eine besondere verfassungsrechtliche Ermächtigung für Maßnahmen ziviler Bundesbehörden dürfte nicht erforderlich sein. Handlungsbedarf könnte jedoch einfachrechtlich sowohl bei Zuständigkeiten als auch Befugnissen bestehe. Insoweit müsste gegebenenfalls je nach Maßnahmentyp unterschieden werden (z.B. nur Informationsgewinnung oder auch Manipulation).

- Für die Nutzung von Bundeswehrfähigkeiten (Personal und Sachmittel) ist eine ausdrückliche verfassungsrechtliche Ermächtigung erforderlich. In tatsächlicher Hinsicht wahrscheinlich sind Szenarien, in denen die Bundeswehr ihre Fähigkeiten den zivilen Behörden zur Verfügung stellt, so dass Art. 35 GG als Verfassungsgrundlage in Betracht kommt. Dagegen erscheint ein Szenario des Art. 87a Abs. 2 GG sehr unwahrscheinlich.
- Völkerrechtlich ist insbesondere unklar, inwieweit Staaten Duldungspflichten gegenüber aktiven Gefahrenabwehrmaßnahmen haben, die sich auf ihrem Territorium auswirken können. Teilweise könnten Vereinbarungen für Rechtssicherheit sorgen, die die Zulässigkeit solcher Maßnahmen etwa vergleichbar dem Institut der Nacheile regeln, wobei es schwer fallen dürfte, insoweit eine hinreichend breite Partizipation zu erzielen.

Anlage 3 387

Bundesministerium des Innern

VS – Nur für den Dienstgebrauch

Referat

Az.: IT3-606 000-9/7#1

Ergebnisprotokoll

Thema:	**Handlungsfähigkeit der BReg zur aktiven Abwehr von IT-Angriffen ("hack back") – Schwerpunkt: Aufgabenverteilung BMVg/BMI**

Ort:	**Datum:**	**Beginn:**	**Ende:**
BMI, AM, Raum 9.018	27.5.2009	10.30 h	13 h

Verfasser:	**Seite:**
ORR Dr. Ramsauer (Ltg.)	1 von 3

Teilnehmer:	
LRD'n Spies	BMVg R II 2
OLT i.G. Muermans	BMVg EFS
BDir Zimmerschied	BMVg M II IT 3
OLT i.G. Bertram	BMVg Fü S II 2
RR Hufschmidt	BSI
ORR'n Dr. Kruse	BMI V I 4
RR Dr. Schamberg	BMI V I 4
OAR Franke	BMI V I 1
ORR Dr. Behmenburg	BMI V I 2
ORR Dr. Ramsauer	BMI IT 3

Besprechungsergebnisse:

1. Klärung der Ausgangssituation

- Gegenstand der Erörterung ist die Abwehr eines Angriffs auf IT-Systeme in D durch gezielte Einflussnahme auf das angreifende IT-System mit aktiven Maßnahmen un-

ter Anwendung von Hackermethoden.

- Unterschieden werden können dabei die Unterfälle der Ausschaltung des angreifenden Systems auf der einen und dessen Kompromittierung mit dem Ziel der weiteren Informationsgewinnung über den Hintergrund des Angriffs ("Backtracing") auf der anderen Seite.

- Für die Zwecke der Besprechung wird zusammenfassend von Maßnahmen ausgegangen, die zumindest einen Tatbestand der §§ 202a ff bzw. 303a ff StGB erfüllten.

- Im Diskussionsverlauf Präzisierung der vertieft zu betrachtenden Konstellationen auf Angriffe durch *im Ausland* befindliche IT-Systeme mit jeweils differenziertem Angriffshintergrund (z.B. Einfache Hacker, Terroristen, feindlich gesinnte Staaten – eine Feststellung erscheint nicht möglich). Die aktive Abwehr von Angriffen aus dem Inland wurde vorerst – als in der Praxis weniger relevant – ausser Betracht gelassen.

2. Sachstand der CNO-Kapazitäten in Rheinbach (update zum Protokoll v. 24.11.08)

- Weiter in Aufbau befindlich; 2-jähriges Aufbauprogramm der Experten läuft. Zielgröße 59 MA.

- 2010/2011 Einsatzbereitschaft der ortsfesten Komponente sowie teilweise Einsatzbereitschaft der MA angestrebt. Vollständige Einsatzbereitschaft vorauss. 2015.

- Derzeit Einsatzgrundsätze und Verfahren für Aktivierung der Einheit in der ressortinternen Abstimmung. Für die Aktivierung ist ein Genehmigungsverfahren avisiert; die Genehmigung setzt eine Grundlage – ggf. inzidenter - im jew. Mandat voraus.

3. Abgrenzung der künftigen Aufgabenverteilung zw. BMVg und BMI

- Verf. Grundlage für den vorgesehenen Einsatz der BW-Einheiten können Art. 87a, 24 GG sein. Amtshilfe durch Bw im Sinne des Art. 35 GG unterliegt den einschlägigen Einschränkungen.

- Art. 87a GG: Entscheidend ist das Vorliegen des völkerrechtl. determinierten Tatbestandsmerkmals "bewaffneter Angriff". Ziel der Erörterungen sollte sein, eine einheitliche "Leitlinie"/"Kriterienkatalog"/"Anwendungsgrundsätze" der BReg zu entwerfen, in welchen Fällen ein Angriff auf IT-Systeme einen bewaffneten Angriff darstellt, der nach Art. 87a Abs. 2 GG einen Einsatz der Streitkräfte zur Verteidigung zulässt. Prima vista zentrale Fragen sind:

⇒ Wann erreicht ein Angriff auf ein IT-System das Ausmaß, dass er einem

„bewaffneten Angriff" gleichzusetzen ist?

⇒ Wann steht ein solcher Angriff unmittelbar bevor? (Problematik der Prävention)

⇒ Inwieweit sind Attacken seitens nicht-staatlicher Akteure als "bewaffneter Angriff" i.S.d. Völkerrechts qualifizierbar?

⇒ Inwieweit kann das Unterlassen/Verzögern von Gegenmaßnahmen durch den Staat, in dem das attackierende System steht, zur Zurechenbarkeit führen?

⇒ Welche Anforderungen sind bei der Anwendung der Norm an die Sachverhaltseinschätzung ex ante zu stellen?

- Art. 24 GG: Kann im Rahmen von EU-, NATO- oder UN-Mandaten relevant werden Nach derzeitiger Einschätzung allerdings nicht ersichtlich.

- Art. 35 GG: Parallele zur Konstellation der "Renegade"-Fälle, in denen die Anwendbarkeit des Art. 35 GG kontrovers diskutiert wird. Allerdings kommen bei „Renegade"-Fällen typischerweise spezifisch militärische Mittel zum Einsatz, um die es sich bei „hack back"-Maßnahmen eher nicht handeln dürfte. Eine Erörterung der Anwendbarkeit im vorl. Zusammenhang wird vorerst zurückgestellt.

- Sofern eine Zuständigkeit der Bw nach den o.a. Normen nicht besteht, ist der Bereich der inneren Sicherheit eröffnet. In diesem Fall ist eine Klärung der Zuständigkeitsverteilung zwischen Bund und Ländern herbeizuführen.. Darüber hinaus bedarf es der Definition der erforderlichen Fähigkeiten.

4. Weiteres Vorgehen

- Eine Grundlage für die Erarbeitung von Anwendungsgrundsätzen ist die Präzisierung des relevanten Sachverhalts durch BSI unter Einbeziehung der Fachexpertise der Bundeswehr (Zeithorizont 6-8 Wochen) mit insb. folgendem Ziel:

⇒ Grobe tabellarische Strukturierung mit abstrakter Beschreibung von möglichen Angriffsszenaren auf der Grundlage aktueller Erkenntnisse. Dabei im Schwerpunkt berücksichtigen:

i. Von wo aus wird der Angriff durchgeführt (physikalische Lokalitäten),

Bundesministerium des Innern

VS-NUR FÜR DEN DIENSTGEBRAUCH

ii. von wo aus wird der Angriff gesteuert (tatsächliche(r) Ort(e) der Angriffssteuerung),

iii. wer ist der – ggf. vermutete- Angreifer bzw. was ist die –ggf. vermutete- Motivation des Angriffs.

iv. Differenzierung der Angriffe hinsichtlich des möglichen Schadenspotentials.

⇒ Welche Gegenmaßnahmen (Organisatorische, Technische) sind möglich ?

⇒ Tabellarische Erfassung sämtlicher technischer Maßnahmen. Diese

i. sind grob zu strukturieren nach passiver und aktiver Verteidigung sowie nach IT-Angriff. Versuch von Definitionen und Abgrenzungen dieser Begriffe.

ii. sind aufzuführen (z.B.„Backtracing" und Backhacking"), grob zu erläutern und in die o.g. Strukturierung einzuordnen und

⇒ nach ihrer Wirkungsweise (Auswirkung auf das Zielsystem, Kollateralschäden etc.) zu bewerten.

- Erörterung des BSI-Berichts Ende Juli (Ort wird noch bestimmt).

- Aufbauend darauf gemeinsame Entwicklung der Anwendungsgrundsätze mit Blick auf die künftige Aufgabenverteilung zw. BMVg und BMI (Zeithorizont bis Anfang September).

- BMI IT 3 strebt an, die Schaffung der tatsächlichen und rechtlichen Voraussetzung für die aktive Netzverteidigung in der Koalitionsvereinbarung auf geeignete Weise zu verankern.

- Ein Austausch auf Leitungsebene wird vorerst nicht für erforderlich gehalten.

gez.

Dr. Ramsauer

Dieses Blatt ersetzt die Seiten 391 - 418

Die Entnahme erfolgte mangels Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss

Dieses Blatt ersetzt die Seiten 419 - 429

Die Entnahme erfolgte mangels Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss

Dieses Blatt ersetzt die Seite 430

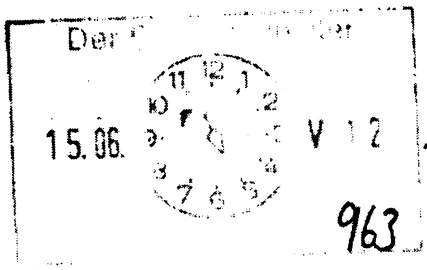
Die Entnahme erfolgte mangels Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss

4/48/12
431

Referat IT 3
IT 3 – 606 000-2/72#16

Berlin, den 14. Juni 2012
Hausruf: 2308/2045

Refl: MinR Dr. Mantz/MinR Dr. Dürig
Sb: AR Spatschke

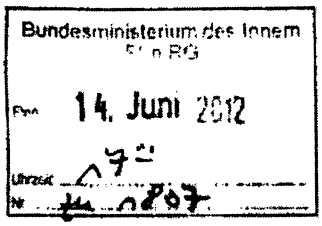


Herrn Minister

über

Abdruck:
St F, LLS, AL ÖS, Presse, IT 5

Frau Staatssekretärin Rogall-Grothe
Herrn IT-Direktor
Herrn SV IT-Direktor



Betr.: Aktuelle Erkenntnisse zur Schadsoftware "Flame"
Anlage: - 1 -

1. Votum
Kenntnisnahme

2. Sachverhalt
Mit Vorlage vom 29.5. (vgl. Anlage) wurden Sie über das Schadsoftwareprogramm „Flame" unterrichtet. Zwischenzeitlich gewonnene neue Erkenntnisse des BSI und der AV-Hersteller K[redacted] und S[redacted], die zusammen mit dem BKA auf Expertenebene eng und konstruktiv kooperieren, lassen sich wie folgt zusammenfassen:
Das BSI wurde am 11.6. durch K[redacted] (Entdecker von FLAME) darüber unterrichtet, dass bei der Analyse des Schadprogramms „Flame" eine Verbindung zu „Stuxnet" festgestellt worden sei. Dabei handelt es sich um ein Modul von

„Flame", welches in sehr ähnlicher Form auch in einer früheren „Stuxnet"-Version zum Einsatz kam und der Verbreitung über Wechseldatenträger dient. Diese Verbindung beider Programme und damit einhergehende Spekulationen über die gemeinsame Urheberschaft wird derzeit verstärkt durch die Medien aufgegriffen.

„Flame" wird mittlerweile durch alle gängigen Antivirenprogramme erkannt. Weltweit ist bislang nur eine relativ geringe Anzahl von Fällen (ca. 500 bestätigte Infektionen) zu verzeichnen, was als Indiz für einen gezielten Angriff gelten könnte. Hauptbetroffen sind nach derzeitigen Erkenntnissen der Iran (185 Infektionen), Israel/Palästina (95) und der Sudan (35). In den USA wurden 10 Infektionen festgestellt.
Das Schadsoftwareprogramm befand sich mindestens zwei Jahre unentdeckt im Einsatz, wobei auch über einen deutlich früheren Einsatzbeginn spekuliert wird.

Die Verteilung von „Flame" erfolgt ausschließlich über das Betriebssystem Microsoft Windows. Auf den betroffenen Systemen sucht „Flame" hauptsächlich nach Informationen und Daten.

Die Verbreitung von „Flame" erfolgte über die Update-Funktion von Windows. Aufgrund eines bislang unbekannten Angriffs auf die Zertifizierungsinfrastruktur von Microsoft konnte ein gefälschtes Zertifikat erstellt werden, mit dem Programmteile von „Flame" signiert werden. Daher betrachteten die betroffenen Windows-Systeme „Flame" als vertrauenswürdiges Update und installierten die Schadsoftware.

Die Analyse des BSI zeichnet ein recht ambivalentes Bild von „Flame" und seinen Schöpfern:
Es wurden fünf verschiedene „Verschlüsselungsalgorithmen" gefunden, die sämtlich nicht dem aktuellen Stand der Technik entsprechen. Andererseits wurde beim Angriff auf die MS-Zertifizierungsinfrastruktur eine neuartige Variante des sog. „Hash-Kollisions-Verfahrens" genutzt, was für sehr gute kryptografische Kenntnisse spricht.

Weiterhin dienen verschiedene Mechanismen von „Flame" der Erschwerung einer Analyse. Andererseits weist der Programmcode verschiedene Informationen auf, die eine Nachkonstruktion sehr erleichtern.

Nach wie vor ist eine Betroffenheit in Deutschland nicht zu erkennen. Auch **aus den Regierungsnetzen** sind anhand der Logdateien im nachvollziehbaren Zeitraum **keine Zugriffe auf bekannte Rückmeldeadressen** feststellbar.

Nur **intern** zu verwendende ergänzende Hintergrundinformation:
Das BSI weist darüber hinaus auf einen möglichen Zusammenhang zwischen „Flame" und „Duqu" hin, der in der Öffentlichkeit und durch Analysten noch nicht hergestellt worden sei. „Duqu" wurde als Spionagesoftware beim Angriff auf die Zertifizierungsstellen im Jahre 2011 verwendet und gemeinhin als „kleiner Bruder" von „Stuxnet" bezeichnet.
Wegen bestimmter Gemeinsamkeiten zwischen „Stuxnet" und „Duqu" einerseits sowie „Duqu" und „Flame" andererseits stammen alle drei „Produkte" unter Umständen aus derselben Quelle.

3. Stellungnahme

Die Verbindung zwischen „Flame" und einer früheren Version von „Stuxnet" könnte darauf hindeuten, dass es eine Zusammenarbeit der Entwickler gegeben haben mag. Ab einem bestimmten Zeitpunkt wurden beide Schadprogramme aber vermutlich von unterschiedlichen Entwicklerteams programmiert, da verschiedene Programmiersprachen und Plattformen verwendet worden sind. Das „Flame"-Modul wurde in einer früheren „Stuxnet"-Version verwendet und im Jahre 2010 durch einen anderen Code ersetzt. Dies könnte darauf hindeuten, dass „Flame" älter als „Stuxnet" ist und vermutlich aus dem Jahre 2008 oder eher stammt.

Hinsichtlich der aktuellen Erkenntnisse und der modifizierten Einschätzung des BSI zur Vergleichbarkeit der genannten Schadprogramme ließen sich folgende „Sprachregelungselemente" für Medienanfragen etc. treffen:

- Das BSI bewertet „Flame" als eine mit einer Vielzahl unterschiedlicher Funktionen ausgestattete modulare Spionagesoftware. Viele dieser Funktionen sind aus dem Bereich anderer Spionageprogramme bekannt und wurden für „Flame" neu zusammengesetzt.
- „Flame" nutzt einen Verbreitungsmechanismus, der sich deutlich von der Masse bisher bekannter trojanischer Pferde abhebt, indem gefälschte Microsoft-Zertifikate genutzt werden.
- Zudem wurden in einem Modul Gemeinsamkeiten von „Flame" und einer früheren Version von „Stuxnet" festgestellt, die sich auf den Verbreitungsmechanismus beziehen. In beiden Programmen wurde ein ähnliches Modul verwendet, das für die Verbreitung der Schadsoftware über Wechseldatenträger sorgte.
- Nach aktuellem Kenntnisstand kann **„Flame"** - in Bezug auf den Verbreitungsmechanismus – als **fortschrittliche „Spionagesoftware"** bezeichnet werden, die **mit hohem Aufwand und neuen Methoden entwickelt** worden ist und sich von bislang bekannten trojanischen Pferden abhebt.
- In der Wirkungsweise der beiden Programme bestehen jedoch Unterschiede: **im Gegensatz zu „Flame" ist „Stuxnet"** als **Sabotagesoftware** zu klassifizieren.

elek. gez. Dr. Mantz

elek. gez. Spatschke

E. K. and CCS

Kroll, Simone

Von:	Schallbruch, Martin
Gesendet:	Dienstag, 29. Mai 2012 17:58
An:	StRogall-Grothe_
Cc:	Spatschke, Norman; IT3_; Batt, Peter
Betreff:	Eilt sehr!!! MinUnterrichtung Schadsoftware "Flame"

IT 3 – 606 000-2/72#16

Herrn Minister

über
Frau Staatssekretärin Rogall-Grothe
Herrn IT-Direktor (Sb 29.5.)
Herrn SV IT-Direktor (i.V. Sb 29.5.)
Herrn RL IT 3 gez. Dü/Ma 29/5

Abdruck: StF, AL ÖS, Presse

Wegen Eilbedürftigkeit als E-Mailvorlage

Neue Schadsoftware „Flame"

AR Spatschke e.u.v.

1. Votum
Kenntnisnahme.

2. Sachverhalt
Aktuelle Medienveröffentlichungen berichten über die Entdeckung eines neuen Schadsoftwareprogramms „Flame", dessen Komplexität und Qualität „Stuxnet" und „Duqu" entsprechen und bereits seit mehreren Jahren im Einsatz sein soll. Haupteinsatzgebiet seien der Mittlere Osten und Osteuropa; die meisten infizierten Rechner wurden nach Informationen von Symantec im Iran, Palästina, Ungarn und im Libanon festgestellt.
Das iranische nationale CERT „Maher" ließ verlauten, „Flame" sei zum Zeitpunkt seiner Entdeckung von keinem der getesteten 43 Antivirenprogramme erkannt worden. Zwischenzeitlich hat das iranische CERT ein Werkzeug zur Erkennung von „Flame" (Detektionstool) entwickelt und ausgewählten Unternehmen/Organisationen bereits Anfang Mai zur Verfügung gestellt. Mittlerweile soll auch ein Werkzeug zur Bereinigung entwickelt worden sein.

Nach Informationen des BSI übertrifft „Flame" (Bezeichnung stammt von einem der Hauptmodule des Programms) die Komplexität von „Stuxnet" und „Duqu" deutlich und ist daher nur sehr aufwändig zu analysieren. Auch ist der Code des Schadprogramms - entgegen einiger Medienberichte - komplett verschieden zu den beiden anderen Programmen. Angreifbar sind die Betriebssysteme **Windows XP, Windows Vista und Windows** 7 unter Ausnutzung von Schwachstellen im Windows-Betriebssystem. Derzeit unklar ist, ob „Flame" bei der Infektion auch bislang unbekannte Schwachstellen (sog. Zero-Day-Exploits) nutzt.
Der Einsatzzweck von **„Flame"** scheint das **Ausspähen von Informationen** und Daten zu sein. Das Schadprogramm ist hoch flexibel und konfigurierbar und verfügt über ca. 20 Schadfunktionen, beispielsweise:

- Wurm-Funktionalität zur Verbreitung über Wechseldatenträger und lokale Netzwerke
- Unterwanderung bzw. Deaktivierung einer Vielzahl von Anti-Virus-Produkten und anderer Sicherheitssoftware
- Mitschneiden von Netzwerkverkehr, Erkennung von Netzwerkressourcen und Sammlung von Passwörtern
- Durchsuchen der Festplatte infizierter Systeme nach Dateien mit bestimmten Inhalten
- Anfertigung von Serien von Screenshots des Desktops, wenn bestimmte Prozesse (z.B. Chatprogramme) oder Fenster aktiv sind

- Anfertigung von Audio-Aufnahmen über an das infizierte System angeschlossene Mikrofone (Gespräche in Räumen oder auch Voice-over-IP-Telefonate)
- Nutzung von Bluetooth zur Sammlung von Informationen über andere Geräte in Reichweite des infizierten Systems
- Übermittlung der ausgespähten Daten an Kontrollserver der Angreifer über verschlüsselte Verbindungen (SSH- oder HTTPS).

Über diese Schadfunktionen hinaus wurden eine Reihe von Schutzmaßnahmen implementiert (z.B. Programmierzeitpunktverschleierung, Analyseresistenz, Programmmodul zum spurenfreien Löschen), um die Entdeckung und Analyse des Schadprogramms „Flame" zu erschweren.

Die im Nationalen Cyber-Abwehrzentrum (Cyber-AZ) vertretenen Behörden wurden durch das BSI im Rahmen der heutigen Morgenlage über die vorliegenden Erkenntnisse informiert. Herr VP-BSI kontaktiert das BfV hinsichtlich des vermuteten nachrichtendienstlichen Hintergrunds.

3. Stellungnahme

Nach Auffassung des BSI ist eine **Betroffenheit Deutschlands und deutscher Unternehmen derzeit nicht erkennbar.** Die Qualität und Funktionalität von „Flame" sind sehr hoch und somit durchaus vergleichbar mit „Stuxnet" und „Duqu" (Manipulation von Siemens-Steuerungsanlagen für Produktionsprozesse und Infizieren von Unternehmensnetzen der Hersteller solcher Steuerungssoftware).
Für diese Art neuartiger Bedrohungen hat sich die Bezeichnung Advanced Persistent Threats (APT) etabliert. Die Angriffsvektoren sind sehr gezielt aufgebaut und für den Attackierten kaum nachvollziehbar und sehr gut getarnt. "Persistent" sind sie, weil sie sich sehr passiv verhalten, dadurch kaum auffindbar sind und über einen langen Zeitraum wirken können.

Der aktuelle Vorfall unterstreicht die Bedeutung der durch das BMI seit geraumer Zeit initiierten Maßnahmen. Ausgehend von der nationalen Cyber-Sicherheitsstrategie der Bundesregierung mit den Kernelementen Nationaler Cyber-Sicherheitsrat (Cyber-SR) und Cyber-AZ und einem verstärkten IT-Schutz Kritischer Infrastrukturen. Auch die aktuell durch Herrn Minister geführten Branchengespräche mit den Vertretern Kritischer Infrastrukturen belegen, dass das BMI die veränderte Gefährdungslage registriert und angemessen auf sie reagiert.

Referat IT 3 wird unaufgefordert über aktuelle Entwicklungen berichten.

Gez. Spatschke

Dieses Blatt ersetzt die Seiten 437 - 441

Die Entnahme erfolgte mangels Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss

446/12
442

Referat IT 3
IT3-606 000-9/31#1

Berlin, den 21. Juni 2012
Hausruf: 1374/2045

Refl: MR Dr. Dürig/MR Dr. Mantz
Sb: AR Spatschke

Herrn Minister

über

Abdruck:
StF, ALÖS, IT5,ÖSII1

Frau Staatssekretärin Rogall-Grothe
Herrn IT-Direktor } (i.V.)
Herrn SV IT-Direktor

LLS ref. f. 27. IT3
1. Dr. Mantz z.K.
2. H. Spatschke m.d.B.
3. z.d.A.

IT3

Betr.: Information US-Cert an BSI bzgl. SCADA-Aktivitäten von Islamisten

Anlage: - 1 -

1. Votum

Kenntnisnahme einer Warnung des US-CERTs an das BSI hinsichtlich einschlägiger Aktivitäten von Islamisten in Bezug auf SCADA-Systeme.

2. Sachverhalt

Sogenannte Prozesssteuerungssysteme (auch Supervisory Control and Data Acquisition) durchdringen mittlerweile fast alle Produktionsprozesse, wie z.B. Stromerzeugung, Gas- und Wasserversorgung, Verkehrsleittechnik und auch Produktionssysteme. Ihre Vorteile liegen in potentieller Kosteneinsparung und zentralisiertem Management.

Prozesssteuerungssysteme basieren zunehmend auf Standardinformationstechnik (z.B. Standard-Hardware mit Windows-Betriebssystemen) und

werden mit gängiger Netzwerktechnik und Kommunikationsprotokollen (Ethernet, TCP/IP) miteinander vernetzt.

Durch zunehmende Verwendung von Standardkomponenten und Anbindung ans Internet werden klassische Angriffsszenarien nun auch für diese Systeme relevant. Standardinformationstechnik ist fehlerbehaftet. Jährlich werden tausende sicherheitstechnisch relevante Schwachstellen bekannt gemacht – mit steigender Tendenz. Ein breites Spektrum von potenziellen Angreifern ist sehr bewandert mit dieser Technologie und entsprechenden Angriffsmethoden.
Klassische Sicherheitsmechanismen (regelmäßige, zeitnahe Patches oder Anti-Virus-Lösungen) sind zur Absicherung der Prozesssteuerungssysteme aufgrund ihrer Besonderheiten (Rund um die Uhr an 365 Tagen, in der der Regel mehrere Jahrzehnte im Einsatz) nicht einfach anwendbar.

Der **Fall Stuxnet** hat in 2010 gezeigt, dass die beschriebenen Bedrohungen aus der Theorie längst in der Praxis angekommen sind.
Die o.g. Infrastrukturen haben bei Schädigung oder gar Komplettausfall eine erhebliche Schadenwirkung für die Gesellschaft – sie sind damit ein Teilbereich des "IT-Schutzes Kritischer Infrastrukturen". SCADA-Systeme sind aufgrund des Einsatzes in sicherheitskritischen Bereichen für verschiedene Angreifer von Interesse.

Das US-CERT (ComputerEmergencyResponseTeam) hat den RegierungsCERTs (u.a. auch BSI) eine Studie übermittelt, die Bestrebungen internationaler Islamisten analysiert, Fähigkeiten zum Angriff auf SCADA-Systeme zu erlangen. Motivation für entsprechende Bemühungen sei demnach die Stuxnet-Berichterstattung gewesen, die auf neue Angriffsmöglichkeiten aufmerksam gemacht habe. Aktuell sei der Fähigkeitsaufbau noch nicht weit vorangeschritten und liege unter dem sog. „Script-Kiddys"

3. Stellungnahme

Es handelt sich bei dieser Warnung generell um den ersten Fall, indem eine derartig aufwändige Analyse mit den RegierungsCERTs anderer Länder geteilt wird. Eine daraus abgeleitete konkrete Bedrohung wird nicht gesehen, es handelt sich um eine sehr frühe Warnung.
Das Bedrohungsszenario für Prozesssteuerungssysteme beschränkt sich nicht „nur" auf intelligente, skalpellartige Angriffe wie Stuxnet. Denkbar sind auch technisch relativ plumpe Angriffe zwecks Sabotage und Distributed-Denial- of-Service (DDoS) von kritischen Prozessen.
Grundsätzlich **unterstreicht dieser Fall die aktuellen Bemühungen des BMI im Bereich des IT-Schutzes Kritischer Infrastrukturen**.

Das BSI (bzw. CERT-Bund) hat diese Information an GTAZ, GIZ und Cyber-AZ weitergeleitet. Die US-Analyse unterstreicht die Bedeutung enger kooperativer Zusammenarbeit bzgl. verschiedener Cyber-Sicherheitsaspekte aller Sicherheitsbehörden im Cyber-AZ.

Dr. Dürig/Dr. Mantz

Spätschke

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Historical Analysis of Online Jihadi Extremist Data Indicates Early Stage Planning Against ICS

June 14, 2012

Executive Summary

Key Points:

- An extensive analysis of online jihadi extremist sources demonstrated that since early to mid 2011, these actors' intent to target the critical infrastructure of the US and its allies via deployed industrial control systems (ICS) has risen significantly.
- It is very likely that Stuxnet played a major role in inspiring jihadi actors to target industrial control systems.
- No specific targeting of ICS via cyber operations has been observed, but ICS assets and vendors have been listed as elements of larger targeting lists for ostensibly kinetic terrorist attacks.

An analysis based on highly reliable liaison source reporting indicates that online jihadi extremist actors have a generally rudimentary understanding of industrial control systems (ICS), but have acknowledged the value of targeting deployed ICS. The vast majority of observed online activity indicating interest in ICS came from a single Arabic-language forum affiliated with al-Qaeda, referred to as "HIVE."

Two distinct periods emerged in the analysis. In the years before 2011, these actors' understanding of the value of cyberspace for offensive purposes was very limited. Since 2011, when HIVE began to understand and internalize the effects of Stuxnet, there has been a significant and notable shift toward accepting and promoting "electronic jihad." Before 2011, the observed online actors seemed more focused on the political and economic influence of ICS vendors, rather than the technologies they create. Starting in June 2011, discussions about electronic jihad became much more frequent and strong indications emerged showing that these actors are at least in the early planning stages of an operation or operations targeting ICS assets. The targeting of ICS is likely very attractive to these actors because it is relatively low risk, the costs are very low (in terms of money and lives) and perhaps because al-Qaeda finds it increasingly difficult to carry out kinetic attacks against Western targets as the group's numbers diminish.

This report focuses on the possibility of cyber attacks against ICS by jihadi extremist online actors. As such, analyses of terrorist group (especially al-Qaeda) leadership dynamics, doctrine, operational tendencies, resource acquisition pathways or in-depth actor profiles would be valuable complementary perspectives.

Jihadi Extremists Historically Focused on ICS Vendors' Perceived Political Influence

An extensive archival search of hundreds of online jihadi extremist resources performed in early June 2012 by a highly reliable liaison source indicated that jihadi extremist actors' understanding of industrial

control systems (ICS) and cyber targets more generally is still rudimentary (i.e., even lower than "script kiddies" in most cases). The search for more than 100 terms related to ICS revealed a historical preoccupation with the perceived political and economic influence of ICS vendors. Observed actors were antagonistic toward Siemens, General Electric, Schneider Electric and ABB for reasons consistent with jihadi extremists' general worldview; they are targets because they are large Western companies conducting business in the Middle East or, more generally, because they are large players in the global economy, which is perceived to be rigged in favor of Western countries. In August 2008, one actor accused Swiss-Swedish company ABB of seeking to promote Christianity, to the detriment of Islam, through the crosses in its logo (below). In the same post, the actor accused Siemens and nuclear energy giant Areva (France) of adding crosses, or plus signs ("+"), to the ends of their product names as a further means of promoting the cross. The discussion did not include any mention of these companies' day-to-day business as major manufacturers of ICS technologies. This post, like a vast majority of known posts referring to ICS, occurred in an Arabic-language forum, referred to as HIVE, where al-Qaeda videos and statements are regularly circulated.

Logo for Swiss-Swedish ICS manufacturer ABB (ABB)

In most of the observed activity, ICS manufacturers were simply elements of larger conceptual groupings, which were typically comprised of companies and organizations perceived to be central players in global political and economic affairs. In 2006 in an English-language forum associated with Hamas, an actor reproduced an article from a UK newspaper detailing firms profiting from the war in Iraq, which included Schneider Electric UK. In two separate 2008 threads on the HIVE forum, General Electric was first listed as a company involved with the "Illuminati and New Masonry" and later listed as a company working in the Israeli information technology industry.

In a post on HIVE from December 2010, deployed GE, Hitachi and Siemens assets, among many others, were listed as potential terror targets after WikiLeaks distributed a diplomatic cable reportedly written by U.S. Secretary of State Hillary Clinton in 2009. As predicted by the Departments of State and Defense in the wake of the leak, the diplomatic cable was indeed used by these actors—classified as terrorists or terrorist supporters—to create a list of potential targets, though any operational targeting or planning against these assets is currently unknown. Although the U.S. Government, which wrote the cable, and the HIVE forum members likely considered these assets as potential targets of traditional kinetic terror attacks, cyberspace could likely be used to aid or potentially execute attacks against some of these targets. The list of potential targets included dams, nuclear facilities, transmission lines, railways and chemical plants, all of which likely use some form of ICS technology.

Interest in ICS Moves Away from ICS Vendors' Political Matters, Moves Toward Practical Exploitation

While the observed activity indicates that jihadi extremists' understanding of ICS is still quite rudimentary overall, a small number of posts starting in 2011 indicate that some of these actors are in the aspirational stages of targeting ICS, with some indications that they are in the early planning stages.

Al-Qaeda and its online supporters were slow to embrace cyberspace as much more than a communication medium; the year 2011 was likely a turning point in the legitimization of online jihad. Some early movement toward embracing cyberspace occurred in 2006. That year, online jihadi magazine *The Technological Mujahid* was launched, though any references to hacking focused primarily on defending against hacking rather than performing it. In 2007, an individual built a simple website, "Emirate of Supporters of Jihad for Hacking," though the site was amateurish and lost support from its creator soon after its launch.

Stuxnet Likely a Turning Point

2011 saw a significant shift toward jihadi acceptance of "electronic jihad," which was likely influenced in large part by these actors' belated understanding of Stuxnet and al-Qaeda's official recognition of the legitimacy and value of "electronic jihad." Despite first making international news in summer 2010, Stuxnet did not appear to be a topic of significant discussion among online jihadi extremist actors until early 2011. While the vast majority of posts focused on trying to understand the effect of Stuxnet on nuclear reactors from a defensive or purely technical perspective, other actors turned the discussion to potential offensive applications of Stuxnet. Some examples of discussions about Stuxnet follow.

- On Jan. 21, 2011, an actor in an Indonesian forum proposed attacking "Malayshit" (most likely a reference to Malaysia) and referred to Stuxnet as a potential weapon to use in such an attack.
- On March 7, 2011, on a forum supportive of Chechen mujahideen, a user posted an article on the threat of Israel using Stuxnet or an analogue on Gaza.
- On March 17, 2011, a HIVE user named "Mujahid Teqani" posted a "brainstorming" post with the subject line "Electronic War Project: Wage Jihad While at Home." The user hoped to unleash an attack on US nuclear reactors just like that which targeted Iranian reactors (i.e., Stuxnet). Mujahid Teqani reproduced a report on Stuxnet from an unknown source. The user added, "I will try to get [a copy of] the code of the stuxnet virus." The actor then linked to the partial decompilations of Stuxnet code from an actor very likely identified as Laurelai Bailey, an Iowa-based actor frequently linked to infighting of Anonymous and Anonymous-affiliated groups. Bailey is not known to be aware of this connection. As with other decompilation efforts, this code would not likely be useful to these actors (for more information, see iSIGHT Partners. "Recently Identified Proliferating Stuxnet 'Source Code' Very Unlikely to be Modified for Other Targets," Intel-427197. July 8, 2011). The actor added, "first we need to study the virus and how it works; second we need to know the program that operate the nuclear reactors in America for example and study them; third, we develop a virus to attack these programs; fourth, we focus on the economic joints and we disable them..."
- On April 19, 2011, a HIVE user claimed that Stuxnet failed in its mission and the actor worried that Iran would subsequently use Stuxnet against Arab states.
- On July 5, 2011, a user of the same Indonesian hacker forum as above reproduced a SecurityNewsDaily article on threats to monitor for 2011, which included Stuxnet.

- On Sept. 21, 2011, a HIVE user warned fellow HIVE users about the then recent discovery of multiple ICS vulnerabilities, cautioning them to update their ICS software "before the disaster." The actor called on other users to update Beckhoff TwinCAT 2.11.0.2004, Rockwell RSLogix 19, Measuresoft ScadaPro 4.0.0, Cogent DataHub 7.1.1.1.63, Azeotech DAQFactory 5.85, Progea Movicon 11.2.1085 and Carel PlantVisor 2.4.4.
- On Oct. 4, 2011, on the same Indonesian forum as above, a poster advertised anti-virus software that could supposedly protect against Stuxnet.

By June 2012, Stuxnet, the potentially related malware "Duqu" and "Flame" and cyber jihad in general became frequently discussed topics on HIVE. While the inherently interesting nature of the malware strains themselves was likely a key reason for the rise in stature of cyber jihad, the notion was likely given a boost by al-Qaeda's recognition of the legitimacy of cyber jihad in June 2011. A video featuring senior al-Qaeda operative Adam Gadahn released June 3, 2011 officially recognized "the importance of inciting its support base to wage electronic attacks." Gadahn noted the availability of free tools and software that would enable supporters to launch attacks on critical electronic infrastructure of governments, corporations and western media outlets.

The group and its supporters almost certainly consider the highly asymmetrical relationship of attacks against ICS and other cyber assets to be an extremely attractive aspect of online operations. Such an attack would likely not require the sacrifice of group members (as with suicide bombings) and very few materials would be necessary, leaving a very small or nonexistent paper trail for intelligence agencies to follow prior to an attack.

Though jihadi extremist hackers' technical capabilities have been assessed as poor overall, they are actively trying to improve. For example, on May 8, 2012, a user on an English-language jihadist forum called on fellow jihadi hackers to attend Hackers Conference 2012 in New Delhi, India, to improve their skills. The conference will feature a number of hacking topics, including supervisory control and data acquisition (SCADA). The user noted, "place will be full of Hindu [intelligence agents], if any brothers do attend try be as inconspicuous as possible and never give your personnel info, name, address etc. to anyone, you are their enemy, remember that, never let down your guard."

ICS Hacking Aspirations and Capabilities Begin to Come into Focus

The March 17, 2011 discussion profiled above and two additional threads from June 11, 2011 indicate that these actors have clearly accepted the value of targeting ICS and may be, at this point, in the early planning stages of operations targeting deployed ICS. Two HIVE threads came on June 11, 2011, eight days after al-Qaeda's official recognition of the legitimacy and value of cyber jihad.

In the first thread, a prominent HIVE forum user solicited fellow forum members for "SCADA qualifications." On June 19, 2011, another Arabic-language user with the handle "Kasser as-Saleeb" responded:

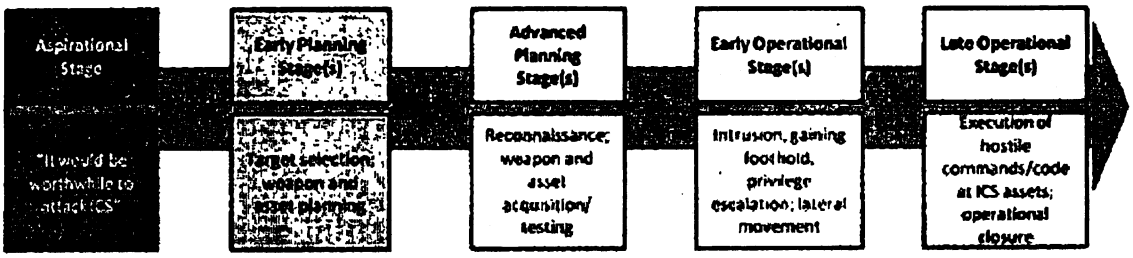
> *"I testify that I meet all the general conditions...and the following classification applies to me: full performance on programming in general (C+ and C++), and highly professional in programming language Object Oriented, and I'm fond of SCADA...[and] I'm expert in industrial control PLCs and control systems."*

In the second thread, a HIVE user with the alias "x101" created a post, "Launch SCADA Missiles 2," in which the actor outlined an organizational structure for cyber operations:

> *"It is very beneficial that a number of computer programmers, a handful, are able to defeat America's military on the ground from their place on the computer... those few will be the tip of the spear in that war, as they will develop programming that suits their targets based on available hacking software... but they will intentionally organize their capabilities and programming and ranks... The brothers will organize themselves in a pyramidal way, meaning there will be leadership for the efficient and fatal electronic attack against America and her allies, and the list of targets to be announced, which will [be comprised of] the few aforementioned individuals with their programmers and they will have a number of assistants, and then there will be a second class that adopts the same work frame... and publicize it among the youths of the ummah, and the third class will be the general participants from the ummah's youth..."*

In response to x101's post, user "Saqr Al-Andalus" posted an excerpt on SCADA likely from training materials from the Etisalat Academy, a legitimate UAE-based company. The excerpt noted "the dangers of network infiltration of automated control systems in the manufacturing of oil and gas" and "the branch systems of SCADA, to include: Human-Machine Interface, Supervisory System, Remote Terminal Units (RTU), programmable logic controller (PLC), Communications vis-à-vis Supervisory, VDN/LAN connections."

The responses to the first thread are indicative of asset planning, as many users, including Kasser as-Saleeb, called out their technical capabilities in hopes of having them used in an operation (see graphic below). Saqr Al-Andalus' response to the second thread is indicative of early target selection, both in terms of potential industry (oil and gas) and technology type (Human-Machine Interface, etc.). It is unknown if the actors in any of the above cases went on to develop specific targets, weaponized code or otherwise moved beyond preliminary planning stages.



Observed online jihadi extremists have shown signs of being in the early planning stages for an operation or operations targeting ICS assets
(ISIGHT Partners)

Characterization of Source Access and Data

The source for this report is a liaison contributor with access to hundreds of Internet-based sources supportive—officially and unofficially—of jihadi extremist causes. The data was collected over two decades, with more data coming more recently. The increase of data over time coincides with the general increase in data worldwide and, more specifically, jihadis' increasing use of cyberspace. For this analysis, a search of forums, chat rooms, blogs, social media feeds and other websites was performed.

The sources are based in many languages, including but not limited to English, Arabic, Urdu, Pashto, Somali, Farsi, Russian, Bahasa and Uzbek. It should be noted that the search terms for this analysis, which consisted of more than 100 ICS-related terms, are very frequently written in English by the observed actors.

Outlook and Implications

The likelihood of a cyber attack targeting US critical infrastructure via deployed ICS has very likely been increasing over time and likely took a significant jump in 2011, when it became clear that al-Qaeda and its supporters have aspirations and may have the capability to carry out such attacks. No specific targeting has been observed, but it is likely that if there are operations currently underway, the actors involved in it have moved to deeper, more obscured channels of communication.

The ease with which critical infrastructure entities (i.e., utilities, manufacturers, etc.) can be accessed via the Internet and the ease with which ICS technologies specifically can be hacked, likely make it easy for a single skilled actor or small group of skilled actors to have an outsized effect on a target. Thus, although the observed online jihadi extremist actors have poor technical skills as a whole, a highly effective cyber operation targeting deployed ICS would likely only require a small number of skilled actors. While such an operation would almost certainly have fewer resources than an operation organized by a state, a jihadi cyber operation would not require nearly the same level of sophistication for it to be considered a success. State actors would assumedly be concerned with retaliation, because states have critical infrastructure and defense assets that could be targeted in kind. Further, because state actors are concerned about retaliation, they would assumedly dedicate resources to obfuscating their identities to prevent attribution (except in the case where a state wants its identity to be known). Assuming that jihadi actors make similar calculations online as they do in the real world, they would likely not be concerned with obfuscating their identities once the attack phase of an operation is underway. However, it is possible that the type of actor inclined to carry out a cyber attack is more concerned with being identified (and in turn imprisoned or killed) than the type of actor inclined to carry out a kinetic attack. As such, the calculations of any suspected actors should be considered on a case by case basis.

Discussions occurring before 2011 indicated that there was a desire among al-Qaeda members to target ICS vendors with kinetic attacks, though—keeping in mind the relatively limited cyber security focus of this analysis—such an attack currently appears less likely. The companies and associated individuals targeted by these actors were part of much larger target lists. Further, al-Qaeda's apparently diminished ability to carry out kinetic attacks and the more "cost effective" strategy of electronic jihad would appear to make a kinetic attack explicitly targeting an ICS vendor relatively less attractive. Still, kinetic attacks targeting critical infrastructure are an on-going concern; in such an event, ICS vendors could be affected, but would not necessarily be explicitly targeted. If a kinetic attack explicitly targeting an ICS vendor were to occur, it is most likely that the target would be a vendor or vendors with a very large global footprint in a number of industries.

Document Control

This document can be shared with personnel who have a valid "need to know" within your federal, state, or local civilian government agency or network, typically defined as a person or group that has a direct role in securing federal, state, or local civilian networks. Recipients of this document cannot add, edit, change, or modify it in any way. This document contains the proprietary information and

Spatschke, Norman

Von: 040-4 Radke, Sven [040-4@auswaertiges-amt.de]
Gesendet: Donnerstag, 24. Mai 2012 15:22
An: Zentraler Posteingang BMI (ZNV)
Cc: BKA SO; IK11; BKA IK13 AAA; 040-40 Maurer, Hubert
Betreff: KRZ001/12 - 120524 - für BMI, SO, IK - BRUEEU*2579: Herausforderung Cyberraum - Was macht die EU?

erl.: -1

1. BMI mit der Bitte um Steuerung
2. BKA / SO vorab zur Kenntnis
3. BKA / IK 11 vorab zur Kenntnis

Beiliegender DB der StV bei der EU in Brüssel zur aktuellen Aktivitäten der EU zum Thema Internet, insbesondere auch Internetsicherheit, wird zur Kenntnis übersandt.

Bei Bedarf der Verwendung der übermittelten Informationen für Gerichtsverfahren wird um Kontaktaufnahme mit IK 13 zur Fertigung eines sachaktenfähigen Vermerks gebeten.

Mit freundlichen Grüßen

Sven Radke
Verbindungsbeamter des Bundeskriminalamtes im AA
Tel.: 030-1817-1735
Email: 040-4@diplo.de

V S - N u r f u e r d e n D i e n s t g e b r a u c h

---

aus: BRUESSEL EURO
nr 2579 vom 23.05.2012, 1741 oz

Fernschreiben (verschluesselt) an KS-CA

Verfasser: R. Schäfer/M. Koeller
Gz.: Gz: 812.02 231741
Betr.: Herausforderung Cyberraum - Was macht die EU?
hier: Eine Bestandsaufnahme
Bezug: Mailweisung von KS-CA vom 14,5,2012

--Zur Unterrichtung--

I. Zusammenfassung

Das Internet ist eine der größten Chancen für Wachstum, Beschäftigung und Wettbewerbsfähigkeit in der EU. Gleichzeitig fordert es die EU heraus, weil sie neue Regelungen für den Marktzugang, die Sicherheit, den Datenschutz oder den Schutz von Verbrauchern und Nutzern festlegen muss.

Im Mai 2010 hat die EU die Digitale Agenda verabschiedet, die diese Zusammenhänge und Handlungsoptionen aufzeigt. Der Europäische Rat hat die Entwicklung des digitalen Binnenmarkts mehrmals als wichtiges Element einer Wachstumsagenda hervorgehoben.

Die EU-Kommissarinnen Kroes und Malmstroem haben für Ende Mai 2012 ein Treffen mit der Hohen Vertreterin für Außen- und Sicherheitspolitik vereinbart, um das weitere Vorgehen in diesem Bereich abzustimmen. Die Koordinierung der verschiedenen Aktivitäten ist wichtig, um die Agenda weiterzuentwickeln und umzusetzen.

II. Im Einzelnen

1. Die EU-Kommission

Kommissarin Kroes - für die Informationsgesellschaft zuständig - hat die Digitale Agenda zusammengestellt. Kroes hat sieben Hürden für die Verwirklichung eines digitalen Binnenmarkts in Europa identifiziert und entsprechende Handlungsvorschläge entwickelt. Unter anderem soll die Interoperabilität verbessert und mehr für Forschung und Entwicklung ausgegeben werden. Ganz prominent fordert Kroes die Erhöhung von Vertrauen und Sicherheit im Internet - also Datenschutz, Bekämpfung von Kriminalität und Schutz von Kindern, aber auch Schutz vor Viren, Anschlägen und Spionage. Insgesamt hat Kroes rund 100 Einzelmaßnahmen vorgeschlagen, darunter 31 Gesetzgebungsvorschläge.

Ausarbeiten müssen diese Gesetzgebungsvorschläge die Generaldirektionen der Kommission, die für die unterschiedlichen Themen zuständig sind. So erarbeitet die GD Markt (Kommissar Barnier) den Vorschlag einer Rahmenrichtlinie über die kollektive Rechtewahrnehmung und europaweite Lizenzierung für die Verwaltung von (Online-) Rechten; die GD Justiz überprüft den EU Rechtsrahmen für den Datenschutz, um das Vertrauen der Bürger und ihre Rechte zu stärken.

Drei besonders stark betroffene Mitglieder der EU-Kommission wollen sich Ende Mai auf ein gemeinsames Vorgehen einigen. Neben Kroes sind dies Innenkommissarin Malmstroem sowie Cathy Ashton, die Hohe Vertreterin für Außen- und Sicherheitspolitik. Kroes hatte bereits eine europäische Strategie zur Internetsicherheit für den Herbst 2012 angekündigt. Möglicherweise wird diese nun in einer veränderten Form vorgelegt und ggf. von der Kommission und der Hohen Vertreterin gemeinsam verantwortet werden.

2. Die Mitgliedstaaten

Die Mitgliedstaaten, die im Rat die Digitale Agenda als Ganzes gebilligt haben, beraten in zahlreichen, jeweils fachlich zuständigen Ratsarbeitsgruppen über die einzelnen Gesetzgebungsvorschläge der Kommission, die dort angekündigt wurden. So beschäftigen sich mit der Frage der Cyber-Sicherheit die Fachleute der Mitgliedstaaten für Telekommunikation und Informationsgesellschaft, aber auch diejenigen für materielles Strafrecht und Strafverfolgung sowie mehrere mit Außenaspekten befasste Gruppen.
Die rotierende Ratspräsidentschaft hat grundsätzlich die Aufgabe, die Arbeit der unterschiedlichen Formationen aufeinander abzustimmen.

Im Ratssekretariat wird auf Arbeitsebene derzeit überlegt, ob eine horizontale Arbeitsgruppe für "Cyberfragen" eingerichtet werden sollte. Die Mitgliedstaaten könnten dort Querschnittsfragen, die nicht allein in einer der Fachgruppen gelöst werden können, beraten. Sie könnten dort bereits auf Arbeitsebene die Kohärenz der unterschiedlichen Vorschläge besser überwachen. Am aussichtsreichsten erscheint es, eine Gruppe "Freunde der Präsidentschaft" einzurichten. Zu diesem Mittel greift man in Brüssel häufiger, wenn man die Zuständigkeit bestehender Fachgruppen grundsätzlich nicht antasten will.

Ob es eine solche Gruppe geben wird, ist noch nicht abzusehen. Die dänische Präsidentschaft hat sich dazu noch nicht positioniert. Die Notwendigkeit einer Koordinierung liegt aber auf der Hand, sodass die Idee auch unter zyprischer Präsidentschaft Fahrt aufnehmen könnte.

3. Das Europäische Parlament

Der Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres, der Industrie-, Forschungs- und Energieausschuss sowie der Unterausschuss Sicherheit und Verteidigung des Auswärtigen Ausschusses haben zu Cyberfragen beraten. Die MdEPs Hohlmeier, Alvaro, Albrecht und Ehler fordern besonders beharrlich eine Koordinierung verschiedener Akteure im Bereich der Cybersicherheit. Sie organisieren auch entsprechende Kontakte (zuletzt im April ein Seminar in der Ständigen Vertretung).

4. Außenaspekte

Die Digitale Agenda hebt die Bedeutung der internationalen Aspekte hervor, macht aber nur relativ allgemeine Vorschläge. Sie beziehen sich auf die Verwaltung des Internet, Handelsfragen und das intellektuelle Eigentum sowie die Anpassung internationaler Vereinbarungen. Sicherheitsfragen werden nicht explizit erwähnt. Hier besteht noch erheblicher Konkretisierungsbedarf, auch zu organisatorischen Fragen.

Das PSK hat sich am 22.10.2011 mit einem Grundsatzpapier zu Chancen und Risiken des Internet beschäftigt, das EAD, GD InfSo und GD Innen vorgelegt hatten. Über Folgemaßnahmen wird der EAD noch entscheiden. Darüber hinaus arbeitet die EU seit 2010 im Rahmen einer EU-US-Arbeitsgruppe zu Cyber-Sicherheit und Cyber-Kriminalität mit den USA zusammen. An dieser Gruppe sind Kommission, EAD, Ratssekretariat, die Europäische Agentur für Netz-und Informationssicherheit ENISA sowie einige MS (aus DEU überwiegend BSI) beteiligt. Eine EU-CHN Cyber Task-Force wird gerade gegründet. Der EAD stellt auch die Schnittstelle der EU zur NATO und deren Arbeiten über sicherheits- und verteidigungspolitische Aspekte im Cyberraum.

Ein baldiger Antrittsbesuch des Leiters des Koordinierungsstabs Cyber-Außenpolitik in Brüssel wäre zu begrüßen. Dabei könnten insbesondere Koordinierungsfragen mit den verschiedenen Akteuren vertieft werden.

Im Auftrag
Schäfer

Anlage:

Zuständigkeiten in der Kommission (Anhaltspunkte):

Die Generaldirektion Informationsgesellschaft und Medien (GD InfSo/ zukünftig DG Connect) ist federführend für Cybersecurity (Computer- und Netzsicherheit). Dazu gehört auch das Mandat der Europäischen Agentur für Netz-und Informationssicherheit (ENISA) und ein Initiativenpaket zu kritischen Infrastrukturen, das noch 2012 vorgelegt werden soll.

Die Generaldirektion Innen (GD Innen) ist federführend für Cyberkriminalität. Die Richtlinie zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie ist bereits im Amtsblatt der EU verkündet worden. Zu der Richtlinie über Angriffe auf Informationssysteme befindet sich der Rat derzeit in Trilog-Verhandlungen mit dem EP. Die GD plant auch das Europäische Zentrum für Cyber-Kriminalität, das bei Europol angesiedelt und zur Zentralstelle für die Bekämpfung der Cyberkriminalität in der EU werden soll.

Der Europäische Auswärtige Dienst (EAD) ist zuständig, sofern außereuropäischen Beziehungen betroffen sind. Seit 2010 arbeitet die EU im Rahmen einer EU-US-Arbeitsgruppe zu Cyber-Sicherheit und Cyber-Kriminalität mit den USA zusammen. Eine EU-CHN Cyber Task-Force befindet sich in der Gründung. Vor allem informelle Kontakte bestehen mit der NATO.

Ende der Anlage

Dieses Blatt ersetzt die Seiten 455 - 457

Die Entnahme erfolgte mangels Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss

Dieses Blatt ersetzt die Seiten 458 - 467

Die Entnahme erfolgte mangels Bezug zum Untersuchungsauftrag bzw. zum Beweisbeschluss

468

BMI

IT3-606 000-9/31#1

Refl: Dr. Dürig/Dr. Mantz
SB: Nimke

Berlin, den 25. Juni 2012
Hausruf: 1374/1642

Leitung/IT3/2012/Juni/06/120625-Einladung RKM.doc

Reg IT3: z.dA

Frau Stn Rogall-Grothe

Bundesministerium des Innern
St'n RG
Eing. 27. Juni 2012
Anlage
Nr. 2160

über

Abdruck:
Referat Z 9

Herrn IT-D (i.V.)
Herrn SV IT-D

Frau Nimke IT3
1. bitte StnRG-Schreiben kopieren + versenden, kopie Zdk-vorlegen
2. bitte Min-Schreiben Zdk-vorlegen

Betr.: IT-Schutz kritischer Infrastrukturen; Ministergespräche mit Wirtschaftsvertretern

3. Dr. P.f.g. z.K., Fr. Olle z.K.

Bezug: Vorlage vom 13. April 2012; Az. IT3-606 000-9/31#1

Anlage: - 3 -

1. Votum

Billigung der Einladung des Herrn Staatsministers Neumann zu dem Ministergespräch mit dem Sektor Medien und Kultur, sowie Zeichnung des anliegenden Einladungsschreibens.

2. Sachverhalt/Stellungnahme

Wie von Herrn Minister gebilligt (Ministervorlage vom 30. Januar 2011; Az. IT3-606 000-9/31#1) sind sechs Gespräche mit jeweils 10 bis 15 Wirtschaftsvertretern zum Thema IT-Schutz kritischer Infrastrukturen für Mai bis August geplant. Die zuständigen Staatssekretäre der Ressorts bzw. den Beauftragten der Bundesregierung für Kultur und Medien hatten Sie

bereits über die Gespräche informiert (Schreiben vom 27. März) und zu den ersten fünf Terminen eingeladen (zuletzt Schreiben vom 21. Mai).

Das Ministerbüro versendet mit Datum vom 25. Juni 2012 das Schreiben für den Termin mit dem Sektor Medien und Kultur am 28. August 2012. Zu diesem Termin sollte der Beauftragte der Bundesregierung für Kultur und Medien aufgrund der Zuständigkeit für diesen Sektor eingeladen werden.

Dr. Mantz

Nimke

Anlage 1

Briefkopf Stn Rogall-Grothe

Berlin, den 25. Juni 2012

Herrn Staatsminister Bernd Neumann
Der Beauftragte der Bundesregierung für Kultur und Medien
Postfach 170286
53028 Bonn

Sehr geehrter Herr Staatsminister ~~Neumann~~,

mit Schreiben vom 27. März 2012 hatte ich Sie darüber informiert, dass Herr Bundesminister Dr. Hans-Peter Friedrich in Gesprächen mit der Wirtschaft die IT-Sicherheit kritischer Infrastrukturen adressieren und voranbringen möchte.

Das Gespräch mit den Vorständen aus dem Sektor Medien und Kultur wird am 28. August 2012 von 14:00 bis 16:00 Uhr im Bundesministerium des Innern stattfinden. In der Anlage übermittle ich Ihnen das Einladungsschreiben von Herrn Dr. Friedrich Minister und den Verteiler.

Zu diesem Gespräch möchte ich Sie herzlich einladen. Wir würden uns freuen, wenn Sie den Prozess aktiv unterstützen und im Anschluss an die Begrüßung durch Herrn Bundesminister Dr. Friedrich einleitende Worte aus Ihrer Sicht an die Teilnehmer richten würden.

Mit freundlichen Grüßen

z.U.
N.d.Fr. Stn RG

Bundesministerium
des Innern

Bundesministerium des Innern, 11014 Berlin

Herrn
Staatsminister Bernd Neumann, MdB
Beauftragter der Bundesregierung
für Kultur und Medien
Bundeskanzleramt
Willy-Brandt-Str. 1
10557 Berlin

Cornelia Rogall-Grothe
Staatssekretärin
Beauftragte der Bundesregierung
für Informationstechnik

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
TEL +49 (0)30 18 681-1109
FAX +49 (0)30 18 681-1135
E-MAIL StRG@bmi.bund.de

DATUM 29. Juni 2012
AKTENZEICHEN IT 3 – 606 00-9/31#1

Sehr geehrter Herr Staatsminister,

mit Schreiben vom 27. März 2012 hatte ich Sie darüber informiert, dass Herr Bundesminister Dr. Hans-Peter Friedrich in Gesprächen mit der Wirtschaft die IT-Sicherheit kritischer Infrastrukturen adressieren und voranbringen möchte.

Das Gespräch mit den Vorständen aus dem Sektor Medien und Kultur wird am 28. August 2012 von 14:00 bis 16:00 Uhr im Bundesministerium des Innern stattfinden. In der Anlage übermittle ich Ihnen das Einladungsschreiben von Herrn Minister Dr. Friedrich und den Verteiler.

Zu diesem Gespräch möchte ich Sie herzlich einladen. Wir würden uns freuen, wenn Sie den Prozess aktiv unterstützen und im Anschluss an die Begrüßung durch Herrn Bundesminister Dr. Friedrich einleitende Worte aus Ihrer Sicht an die Teilnehmer richten würden.

Mit freundlichen Grüßen

Rogall-Grothe

Bundesministerium
des Innern

Dr. Hans-Peter Friedrich
Bundesminister
Mitglied des Deutschen Bundestages

Versand
gemäß anliegendem Verteiler

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
POSTANSCHRIFT 11014 Berlin

TEL +49 (0)30 18 681-1000
FAX +49 (0)30 18 681-1014
E-MAIL Minister@bmi.bund.de
INTERNET www.bmi.bund.de

DATUM Berlin, den 25. Juni 2012

Sehr geehrte Damen und Herren,

die Bundesregierung hat im Februar 2011 die nationale Cybersicherheitsstrategie verabschiedet. Damit wurde der erste Schritt zur Adressierung der jüngsten Entwicklungen bezüglich der Abhängigkeiten vom und der Bedrohungslage im Cyberspace getan.

Als Betreiber Kritischer Infrastrukturen bzw. diese vertretende Verbände kommt Ihnen eine besonders verantwortungsvolle Aufgabe bei der Mitwirkung in der Cybersicherheit zu. Die von Ihrer Organisation bereitgestellten Dienste sind für das gesellschaftliche, wirtschaftliche und auch staatliche Handeln unverzichtbar. Die Durchdringung von Informations- und auch Kommunikationstechnologien ist in den letzten Jahren kontinuierlich vorangeschritten und hat alle Branchen der Kritischen Infrastrukturen erreicht.

Seit 2007 arbeitet die Bundesregierung im Umsetzungsplan KRITIS mit Betreibern Kritischer Infrastrukturen zusammen, um die notwendige Vorsorge zu erfüllen – den beteiligten Organisationen danke ich für Ihr Engagement.

Auch mit der Ende November 2011 durchgeführten LÜKEX als erste nationale IT-Übung konnte gezeigt werden, dass die gemeinsamen Anstrengungen zur Verbesserung des IT-Schutzes Kritischer Infrastrukturen weiter optimiert werden sollten.

Als Bundesminister des Innern habe ich eine Pflicht zur Sicherheitsvorsorge in Deutschland. Die Aufrechterhaltung der von Ihnen betriebenen Kritischen Infrastrukturen ist dabei ein integraler Bestandteil. Die Entwicklungen machen es unverzichtbar, dass sich alle Branchen explizit und umfassend mit dem IT-Schutz bei Kritischen Infrastrukturen auseinandersetzen, um ein umfassendes Mindestniveau in Deutschland zu erreichen.

Als Anlage übersende ich Ihnen ein Arbeitspapier mit Anforderungen an den IT-Schutz Kritischer Infrastrukturen, welche zu diesem Zweck von jeder Branche erfüllt sein sollten. Ich wäre Ihnen dankbar, wenn Sie einen Umsetzungsstand innerhalb der Branche eruieren und bei Bedarf Nachbesserungen initiieren würden.

Für den 28. August 2012 möchte ich Sie in das Bundesministerium des Innern einladen, um die Ausrichtung des Papiers und die Resultate aus den branchenspezifischen Aufarbeitungen in der Zeit von 14:00 bis 16:00 Uhr zu diskutieren. Für eine kurze Bestätigung Ihrer Teilnahme, spätestens bis Montag, den 13. August 2012, danke ich Ihnen. Für Rückfragen steht Ihnen in der Zwischenzeit auch das zuständige Referat im Bundesministerium des Innern (it3@bmi.bund.de, Tel.: 030 / 18 681 - 1642) zur Verfügung.

Mit freundlichen Grüßen

[redacted]
Geschäftsführerin
M[redacted]GmbH

[redacted]
Verwaltungsdirektor
Z[redacted]

[redacted]
Vorsitzende der A[redacted]

[redacted]
Geschäftsführer
r[redacted]

Herrn
[redacted]
Verwaltungsdirektor
B[redacted]

[redacted]
Vorstandsvorsitzender
A[redacted]

Herrn
[redacted]
Geschäftsführer
S[redacted]

[redacted]
Sprecher der Geschäftsführung
F[redacted]

Referat IT 3

IT 3 - 606 000-2/28#1

Refl: MR Dr. Dürig/MR Dr. Mantz
Sb: AR Spatschke

Berlin, den 27. Juni 2012
Hausruf: 1374/2045

Frau Stn Rogall-Grothe

über

Herrn IT-Direktor
Herrn SV IT-Direktor

Abdruck:
LLS

Bundesministerium des Innern
St'n RG
Eing.: 29. Juni 2012

Betr.: Finales Protokoll der 3. Sitzung des Cyber-SR am 31.5.2012

Anlage: - 3 -

1. Votum

Kenntnisnahme und Billigung des vorgelegten Protokollentwurfs der Sitzung des Cyber-SR am 31. Mai 2012 sowie Kenntnisnahme und Billigung des vorgelegten Entwurfs eines Schreibens an die Mitglieder des Cyber-SR zur Übersendung des Protokolls (Anlage 1, Versand durch IT 3).

2. Sachverhalt

Der Entwurf des Protokolls (Anlage 2) wurde auf Arbeitsebene vorabgestimmt. Geringfügige Änderungswünsche seitens AA, BMVg, BMBF und HE wurden übernommen. Ihr Einverständnis erklärten BMF, BMWi, BK und BMJ; die übrigen Mitglieder des Cyber-SR äußerten sich nicht.

3. Stellungnahme

Im Zusammenhang mit der 4. Sitzung des Cyber-SR im Oktober sind folgende Punkte klärungsbedürftig bzw. zu entscheiden:

1.) Zweiteilung

2.) Arbeitsauftrag „Intelligente Netze"

3.) Termin nächste Sitzung

4.) TN AL 6 BK

5.) Umgang mit Bericht des BSI für Cyber-SR (Anlage 3)

Zu 1. Zweiteilung:

Sie hatten am Rande der 3. Sitzung des Cyber-SR angedeutet, die Frage der Zweiteilung angesichts des guten Verlaufs der Sitzung künftig in Abhängigkeit der Tagesordnung in einem Jour-Fixe mit Herrn ITD zu entscheiden.

→ Referat IT 3 hält dies für einen gangbaren Weg, eine mögliche Schwächung des Gremiums Cyber-SR und „Motivationsverluste" der assoziierten Wirtschaftsvertreter zu vermeiden.

Zu 2. Arbeitsauftrag „Intelligente Netze"

P-BSI und BMWi hatten sich in der Sitzung dafür ausgesprochen, das Thema „Intelligente Netze" auf die Tagesordnung der nächsten Sitzung zu setzen, und damit einen über „Smart Grid" / „Smart Meter" hinausgehenden Ansatz zu verfolgen (Hintergrund: bestehendes etabliertes Verfahren für Smart Meter im BMWi),

→ IT 3 schlägt vor, in Ihrem Schreiben zur Übersendung des Protokolls einen entsprechenden Hinweis aufzunehmen, wonach BSI und BMWi zu diesem Punkt in der nächsten Sitzung entsprechend vortragen sollen.

3.) Termin nächste Sitzung

Die 4. Sitzung des Cyber-SR soll in KW 42 oder 43 (ab 15.10.) und damit rechtzeitig vor dem nächsten IT-Gipfel am 13.11. stattfinden.

→ Es wird vorgeschlagen, dass eine entsprechende Terminfestlegung in Ihrem Übersendungsschreiben erfolgt, um allen Beteiligten frühzeitige

Planungssicherheit zu geben (ggf. vorherige Abstimmung mit den jeweiligen St-Büros).

4.) TN AL 6 BK

Sie hatten um einen erinnernden Hinweis gebeten, wegen der zusätzlichen Beteiligung des AL 6 im BK mit Herrn Wettengel zu sprechen.

5.) Umgang mit Statusbericht des BSI für Cyber-SR

In der Rücksprache mit IT 3 am 25.5. hatten Sie sich dafür ausgesprochen, den – inhaltlich nicht sehr ergiebigen – Statusbericht des BSI den Mitgliedern des Cyber-SR (**nur Ressorts**) zur Verfügung zu stellen.
→ IT 3 empfiehlt, den Bericht im Zuge der Protokollversendung zu verteilen, da dies ohnehin in Ziffer 4 der Cybersicherheitsstrategie so vorgesehen ist und man so zudem den vermehrt auftretenden Nachfragen aus dem parlamentarischen Raum aktiv begegnen könnte.

Nach erfolgter Billigung des Protokolls wird Herr Minister über die Ergebnisse der 3. Sitzung des Cyber-SR informiert werden.

Dr. Mantz

Spatschke

Anlage 1

Briefkopf Frau StnRG

Verteiler Cyber-SR
- per E-Mail –

Sehr geehrte ~~Mitglieder des Cyber-SR~~ Damen und Herren,

als Anlage übersende ich das auf Arbeitsebene vorabgestimmte Protokoll der 3. Sitzung des Nationalen Cyber-Sicherheitsrates (Cyber-SR) am 31. Mai 2012 nebst Anlagen.

In unserer Sitzung waren wir uns darüber einig, für die nächste Sitzung erneut die Erörterung eines Technologiethemas vorzusehen. Das BMWi und das BSI haben das Thema „Intelligente Netze" vorgeschlagen, was durch die Mitglieder des Cyber-SR begrüßt wurde.

Die nächste Sitzung des Cyber-SR soll am...[Büro StRG, bitte entsprechend ergänzen] ...stattfinden. Hierfür wird Ihnen eine gesonderte Einladung rechtzeitig zugehen.

Mit freundlichen Grüßen

N.d.Fr.StnRG

Bundesministerium
des Innern

Cornelia Rogall-Grothe
Staatssekretärin
Beauftragte der Bundesregierung
für Informationstechnik

Bundesministerium des Innern, 11014 Berlin

HAUSANSCHRIFT Alt-Moabit 101 D, 10559 Berlin
TEL +49 (0)30 18 681-1109
FAX +49 (0)30 18 681-1135
E-MAIL StRG@bmi.bund.de

DATUM 3. Juli 2012
AKTENZEICHEN IT 3 – 606 000-2/28#1

Verteiler Cyber-SR
- per E-Mail –

Sehr geehrte Damen und Herren,

als Anlage übersende ich das auf Arbeitsebene vorabgestimmte Protokoll der 3. Sitzung des Nationalen Cyber-Sicherheitsrates (Cyber-SR) am 31. Mai 2012 nebst Anlagen.

In unserer Sitzung waren wir uns darüber einig, für die nächste Sitzung erneut die Erörterung eines Technologiethemas vorzusehen. Das BMWi und das BSI haben das Thema „Intelligente Netze" vorgeschlagen, was durch die Mitglieder des Cyber-SR begrüßt wurde.

Die nächste Sitzung des Cyber-SR soll am 23. Oktober 2012, 11 Uhr stattfinden. Hierfür wird Ihnen eine gesonderte Einladung rechtzeitig zugehen.

Mit freundlichen Grüßen

Rogall-Grothe

VS – NUR FÜR DEN DIENSTGEBRAUCH

Anlage 2

Referat IT 3
Bearbeiter: AR Spatschke

7. Juni 2012
Hausruf: 2045

3. Sitzung des Cyber-SR am 31. Mai 2012 – Protokoll

TOP 1 Begrüßung

Fr. Staatssekretärin Rogall-Grothe (BMI) begrüßt die Mitglieder des Cyber-SR zur dritten Sitzung dieses Gremiums. Sie gibt einen kurzen bedauernden Hinweis auf die zweimal aus terminlichen Gründen (des BMI und des BMWi) verschobene Sitzung und betont, der ursprüngliche Tagungsrhythmus solle erhalten bleiben.
Die Teilnehmerliste liegt in Anlage 1 bei.

TOP 2 Cyber-Außenpolitik

Fr. Staatssekretärin Dr. Haber (AA) stellt das unter Federführung des AA und unter Mitwirkung der beteiligten Ressorts entwickelte Strategiepapier *"Internationale Zusammenarbeit zur Cyber-Sicherheit"* vor. Sie dankt für die Beiträge der Länder und betont, dass das Papier ausgehe von allgemeinen Prinzipien und den Vorschlägen zu Normen staatlichen Verhaltens und zu vertrauensbildenden Maßnahmen. Diese Prinzipien würden im zweiten Teil des Papiers auf die verschiedenen Organisationen und Unterorganisationen, in denen Cybersicherheit und Netzpolitik behandelt werden, konkret angewendet.

Fr. Staatssekretärin Dr. Haber führt aus, dass dieses Papier der erste Baustein einer umfassenden Strategie deutscher Cyber-Außenpolitik sei. Dabei stelle Sicherheit die erste Säule einer solchen Cyber-Außenpolitik dar. Die zweite Säule seien Grund- und Persönlichkeitsrechte im Netz, die im Übrigen im Rahmen der 2. Berliner Cyber-Konferenz im AA im September behandelt werden sollten. Die dritte Säule stelle die außenwirtschaftliche, besonders die entwicklungspolitische Dimension des Cyberraums dar.

Im Folgenden stellt sie die aktuellen Entwicklungen in der Cyber-Außenpolitik dar:

- Die Gruppe der Regierungsexperten bei den Vereinten Nationen (VN) wurde durch die Generalversammlung der VN eingesetzt und soll bis zum nächsten Sommer einen Bericht und Vorschläge für konkrete Maßnahmen vorlegen. Seit kurzem sei ein Experte aus dem AA als Mitglied dieses Gremiums berufen worden.
- In der OSZE sei durch Beschluss des Ständigen Rats eine Arbeitsgruppe mandatiert worden, die vertrauensbildende Maßnahmen ausarbeite. Somit würden die Bemühungen für vertrauensbildende Maßnahmen weiterhin parallel auf regionaler Ebene (OSZE) und auf globaler Ebene (VN) verfolgt.
- Im Rahmen des NATO-Gipfels in Chicago sei die in Lissabon eingegangene Verpflichtung zum Schutz der IT-Struktur der Allianz vor Angriffen aus dem Cyber-Raum bekräftigt worden.
- Der Europarat habe im März 2012 eine Vierjahres-Strategie zum Schutz von Menschenrechten, Rechtsstaatlichkeit und Demokratie im Internet verabschiedet. Zudem werde die Konvention zum Schutz personenbezogener Daten aus dem Jahre 1985 modernisiert, indem sie an die sich durch das Internet ergebenden neuen Herausforderungen angepasst werde. Auch solle die Rolle der Budapester Konvention zu Computerkriminalität als internationaler Referenzrahmen gestärkt werden.
- Die Internationale Telekommunikationsunion (ITU) organisiere die „Intergouvernementale Weltkonferenz für Internationale Kommunikation" (Weltfunkkonferenz) Ende des Jahres in Dubai; dabei solle mit der „International Telecommunications Regulations" (ITR) ein völkerrechtlicher Vertrag aus dem Jahr 1988 überarbeitet werden.

Fr. Staatssekretärin Dr. Haber unterstreicht weiterhin die Bedeutung bilateraler Abstimmungen zur Vertrauensbildung, insbesondere auch mit solchen Staaten, die Freiheit und Sicherheit des Cyberraums anders definieren würden.
Sie erwähnt in diesem Zusammenhang die Ende April stattgefundenen Cyber-Konsultationen mit Russland und die Anfang Juni stattfindenden Cyber-Konsultationen mit China.
Weiterhin informiert Fr. Staatssekretärin Dr. Haber über entsprechende Bemühungen auf EU-Ebene, eine umfassende EU-Cyber-Strategie zu entwerfen, bei der neben Sicherheit z.B. auch wirtschaftliche und außenpolitische Gesichtspunkte einfließen sollen. Hierfür habe es am 30. Mai ein Spitzentreffen von Lady Ashton und den

Vizepräsidentinnen Kroes und Malmström gegeben. Sie schlägt daher vor, in der nächsten Sitzung des Cyber-SR das Thema EU vertieft zu erörtern.
Abschließend informiert Fr. Staatssekretärin Dr. Haber über die am 13./14. September 2012 stattfindende 2. Berliner Cyber-Konferenz, bei der der Schwerpunkt auf Menschenrechte im Internet liege. Es sei geplant, dass BM Dr. Westerwelle die Konferenz mit einer Grundsatzrede über den Schutz von Menschen- und Persönlichkeitsschutzrechten im Netz eröffne; die Ressorts - angesichts des Themas insbesondere BMJ - seien eingeladen, sich in diese Konferenz einzubringen.

In der sich anschließenden Diskussion dankt Fr. Staatssekretärin Rogall-Grothe für den vorgelegten Bericht. Sie sieht das Erfordernis, diesen fortzuschreiben, da es sich um einen dynamischen Prozess handele. Sie unterstreicht die Bedeutung bilateraler Kontakte und sieht insbesondere Bedarf zur Intensivierung dieser Kontakte mit Afrika und Südamerika. Afrika sei der weltweit am stärksten digital entwicklungsfähige Kontinent, an internationale Foren jedoch so gut wie nicht angegliedert. Für eine intensivere Zusammenarbeit böte sich beispielsweise Südafrika an.
In Südamerika sei z.B. Brasilien ein wichtiger „BRICS-Staat", der sehr großes Potential habe und auch Partnerland der diesjährigen CeBIT gewesen sei.
Darüber hinaus hält sie bei der Thematik Cyber-Außenpolitik die Behandlung außenwirtschaftlicher Fragen für bedeutsam. So sei beispielsweise vorstellbar, dass sich der Cyber-SR der Thematik Chinese Compulsory Certification (CCC) und der damit verbunden Offenlegung von Quellcodes in China annehmen könne. Sie appelliert an die assoziierten Wirtschaftsvertreter, sich dieser die Wirtschaft betreffenden Fragen verstärkt anzunehmen. AA bestätigt, dass man bei den bevorstehenden Cyber-Konsultationen in Peking diese Dinge gemäß Absprache im Ressortkreis aktiv ansprechen werde.
Hr. Staatssekretär Dr. Schütte (BMBF) betonte die Bedeutung der europäischen und internationalen Kooperation in den Bereichen Forschung und Entwicklung für die Schaffung von mehr Vertrauen und Cybersicherheit. So habe BMBF aktuell ein EUREKA Forschungsprojekt SASER (Safe and Secure European Routing) mit Frankreich und fünf weiteren Partnerländern zur Entwicklung neuer Routingtechnologien initiiert. Ein Ziel ist es, die Abhängigkeit von außereuropäischen Anbietern in diesem Kernbereich des Internets zu verringern.
Hr. Dr. Achatz (BDI) schätzt die mit CCC verbundene Offenlegung geistigen Eigentums als kritisch ein. Er gibt jedoch zu bedenken, dass eine generelle und gegenseitige

Offenlegung des Quellcodes von Kommunikationstechnik (im Gegensatz zu Anwendungen) durchaus Vertrauen schaffen könnte.

Fr. Staatssekretärin Rogall-Grothe begrüßt abschließend den Vorschlag des AA zur vertieften Erörterung der EU-Thematik in der nächsten Sitzung des Cyber-SR. Die Thematik wird auf die TO gesetzt, das AA soll unter Mitwirkung der Ressorts ein entsprechendes Non-Paper vorbereiten.

TOP 3 Vortrag P - BSI

Der Präsident des BSI, Hr. Hange, erläutert anhand des in der Anlage 2 beigefügten Vortrags die aktuelle Bedrohungslage und eine Bilanz der Tätigkeit des Nationalen Cyber-Abwehrzentrums (Cyber-AZ) nach einem Jahr seines Bestehens.
Hr. Hange informiert zudem über das durch die aktuelle Berichterstattung im Fokus stehende Schadsoftwareprogramm „Flame". Angreifbar seien die Betriebssysteme Windows XP, Windows Vista und Windows 7 unter Ausnutzung von Schwachstellen im Windows-Betriebssystem.
Hr. Hange informiert zudem knapp über die von BSI und BITKOM kürzlich initiierte „Allianz für Cybersicherheit" und appelliert an BDI und DIHK, sich dieser Initiative anzuschließen.
Fr. Staatssekretärin Rogall-Grothe betont abschließend die Bedeutung des Cyber-AZ und eine angemessene Kooperation mit der Wirtschaft.

TOP 4 IT-Schutz Kritischer Infrastrukturen

Fr. Staatssekretärin Rogall-Grothe führt in die Thematik ein und informiert kurz über die Entwicklungen seit der letzten Sitzung des Cyber-SR vom 18.November 2011.
Es habe sich herausgestellt, dass branchenübergreifende IT-Sicherheitsstandards allgemein bekannt seien, so z.B. der IT-Grundschutz und die ISO-Normen 27000. Als Mindeststandard sei etwas Vergleichbares in Deutschland jedoch nicht gesetzlich festgeschrieben. Die Verfügbarkeit/Umsetzung branchenspezifischer Mindestsicherheitsanforderungen sowie gesetzl. Verankerung in Aufsichtsnormen sei durch das BMI gemeinsam mit den Ressorts aufgearbeitet worden. Im Ergebnis wurden durchaus unterschiedliche Niveaus der Branchen festgestellt. Im Übrigen werde die Sektoren-/Branchenübersicht mit Zuordnung entsprechender Bundesaufsichtsbehörden und zuständiger Ressorts im Rahmen der Ressortabstimmungen kontinuierlich weiterentwickelt.

Aktuell habe Minister Dr. Friedrich entschieden, selbst Gespräche mit Betreibern Kritischer Infrastrukturen und deren Verbänden unter Einbeziehung der jeweils fachlich zuständigen Ressorts zu führen. Insgesamt seien 6 Gespräche mit 7 Sektoren anberaumt. Grundlage der Gespräche sei ein Diskussionspapier „IT-Schutz Kritischer Infrastrukturen in Deutschland", welches den Teilnehmern als Tischvorlage vorliege. Fr. Staatssekretärin Rogall-Grothe erbittet ausdrücklich Kommentare und Anregungen zum Papier.

Aktuell seien die Gespräche mit dem IKT- und dem Finanzsektor bereits absolviert. Die Frage von [redacted] (A[redacted]), ob es ein Feedback zum am 13. Juni stattfindenden Gespräch mit dem Energiesektor gebe, bejaht sie.

Fr. Staatssekretärin Rogall-Grothe erläutert die Intention der Ministergespräche dahingehend, dass das BMI als für das Gemeinwesen zuständiges Ressorts sich mit Fragen der Absicherung der IT-Steuerung der kritischen Infrastrukturen gemeinsam mit den jeweils fachlich zuständigen Ressorts beschäftigen müsse; auch in anderen Staaten würden diese Frage diskutiert, in den USA würden gerade unterschiedliche Gesetzentwürfe verhandelt. Auch die Cyber-Sicherheitsstrategie gebe den Auftrag, rechtlichen Regelungsbedarf, beispielsweise die Vorgabe von Meldeverpflichtungen, zu prüfen. Ohne den Gesprächsergebnissen vorgreifen zu wollen habe sie den Eindruck, dass die jeweiligen Branchen recht unterschiedlich aufgestellt seien. Es gebe weitreichende Abhängigkeiten zwischen den Kritischen Infrastrukturen, so z.B. immense Abhängigkeit von Energie- und IKT-Versorgung. Die Folge dieser Komplexität sei es, dass sich niemand mehr für die Sicherheit des Gesamtsystems verantwortlich fühle.

Fr. Staatssekretärin Rogall-Grothe stellt abschließend fest, dass dem Thema IT-Schutz Kritischer Infrastrukturen eine hohe Priorität in der Cybersicherheitsstrategie zukomme und daher regelmäßig über den Sachstand im Cyber-SR berichtet werden solle.

TOP 5 Trusted Computing

Frau Staatssekretärin Rogall-Grothe führt in die Thematik Trusted Computing (TC) ein. Die Trusted Computing Group (TCG) wolle mit der Entwicklung und Produktion des Trusted Platform Moduls (TPM) einen Beitrag zur Sicherheit von Informationssystemen leisten. Auf dem TPM-Chip können sicherheitsrelevante Informationen wie Verschlüsselung oder Zertifikate sicher gespeichert werden.

Sie habe das Thema auf die Agenda des Cyber-SR gesetzt, da es unter Punkt 3 des Arbeitsschwerpunktepapiers des Cyber-SR (*Begleitung technologischer Innovationen*) als strategisches Zukunftsthema zu erörtern sei.

Die TCG sei 2003 mit der Zielsetzung der Entwicklung und Förderung offener, herstellerunabhängiger Industriestandard-Spezifikationen gegründet worden. Aktuell seien ca. 200 Unternehmen und staatliche Organisationen in die TCG involviert, darunter auch das BSI, deutsche Hersteller und Wissenschaftsinstitute.
BMI und BMWi hätten bereits 2007 ein Eckpunktepapier veröffentlicht, welches jetzt überarbeitet werden müsse, da die TCG eine neue Version der TC-Spezifikation entwickelt habe und beabsichtige, diese im Laufe des Jahres 2013 als ISO-Standard zu veröffentlichen. Die in der TCG zusammengeschlossen Unternehmen hätten bekundet, TPMs nach diesem neuen Standard herzustellen und in die Geräte einzubauen.

Fr. Staatssekretärin Rogall-Grothe führt weiterhin aus, dass der potentielle Sicherheitsgewinn der neuen TPM-Version einhergehe mit Kontrollverlusten für Nutzer. Hersteller seien mit Unterstützung des TC-Moduls in der Lage, Rechner so einzurichten, dass das Ausführen anderweitiger, z.B. herstellerfremder Programme unterbunden würde. Problematisch hierbei sei es, dass die Eigentümer der Geräte dann nicht mehr die volle Oberhoheit über ihre Informationstechnik besäßen und nicht bestimmen könnten, mit welcher Software auf die Daten zugegriffen wird. In der Folge verlören Eigentümer auch die Oberhoheit über die auf ihren Systemen verarbeiteten und gespeicherten Daten.
Für die Bundesverwaltung und auch die kritischen Infrastrukturen sei das Thema TC von großer Relevanz: Die Bundesverwaltung und die KRITIS-Betreiber müssten weiterhin allein darüber entscheiden können, was mit ihren Daten geschehe.
Das Eckpunktepapier aus 2007 sei aus diesen Gründen überarbeitet worden. Es müsse nunmehr unterschieden werden zwischen einem Privatanwender/ KMU und der öffentlichen Verwaltung/den Betreibern von Kritischen Infrastrukturen.

In der anschließenden Diskussion begrüßt [redacted] (B[redacted]) die Überlegungen der Bundesregierung und bietet die Unterstützung des [redacted] an.
Hr. Hange (BSI) sieht in der Kontrollfähigkeit den entscheidenden Faktor, der eine Diskussion im politischen Raum nach sich ziehen könnte, wenn die Spezifikationen erst einer breiteren Öffentlichkeit bekannt werden würden.

Hr. Staatssekretär Beemelmans (BMVg), und Fr. Staatssekretärin Grundmann (BMJ) schlossen sich dem an und plädierten dafür, die fehlende Wahlmöglichkeit (opt-in/opt-out) gegenüber der TCG stärker als nicht akzeptabel darzustellen; der Transparenzaspekt allein sei zu wenig. Dies würde politisch negativ auf die Bundesregierung zurückfallen.

[redacted] weist darauf hin, dass die TC-Spezifikationen ursprünglich zur Erhöhung der Sicherheit in Unternehmen dienten. Für Privatanwender seien diese Ansätze nicht ohne Weiteres zu akzeptieren. Er regt daher ein konzertiertes Vorgehen von Wirtschaft und Politik gegenüber der EU-Kommission (KOM) an.

Hr. Hange unterstützt diesen Ansatz und informiert, dass das Eckpunktepapier 2007 auch an die KOM übersandt worden sei.

Im Folgenden (Stn Dr. Grundmann, [redacted] Hr. Dr. Schuseil (BMWi)) herrscht breiter Konsens, dass ein Mehr an Transparenz das Problem nicht löse, wenn es keine Wahlmöglichkeit gebe.

Fr. Staatssekretärin Rogall-Grothe stellt abschließend fest, dass weitere Überlegungen, auch unter Einbeziehung der Wirtschaft und der Länder nötig seien. Die Ressortabstimmung solle im Lichte der heutigen Diskussion wiederholt werden.

TOP 6 Sonstiges

Fr. Staatssekretärin Rogall-Grothe schlägt vor, in der nächsten Sitzung des Cyber-SR die vertiefte Erörterung eines Technologiethemas (Punkt 3 des Arbeitsschwerpunkteprogramms) vorzusehen. Aus ihrer Sicht böten sich hierfür die Themen „*Cloud Computing*" oder „*Intelligente Netze*" an, die u.a. auch Sicherheitsfragen aufwerfen würden. Die Themen KRITIS und Cyber-Außenpolitik sollten erneut auf die Tagesordnung gesetzt werden.

[redacted] (D[redacted] hält es für erforderlich, dass sich der Cyber-SR mit Smart Grids/Smart Meter beschäftigen solle. Hier stelle sich u.a. die Kostenfrage (Vergemeinschaftung von Kosten). Hr. Hange und Hr. Schuseil weisen diesbezüglich darauf hin, dass zur Kommentierung der Smart Meter (TR/PP) ein offenes und transparentes Verfahren im BMWi etabliert sei. Hingegen würde sich das Thema „*Intelligente Netze*" mit einem breiteren, über Smart Grids reichenden Ansatz durchaus für eine Erörterung im Cyber-SR eignen.

Fr. Staatssekretärin Rogall-Grothe stellt abschließend fest, in der kommenden Sitzung des Cyber-SR die Erörterung des Themas „*Intelligente Netze*" vorzusehen. „*Cloud Computing*" solle dann in der übernächsten Sitzung diskutiert werden.

Unter dem Top „Sonstiges" informiert Hr. Dr. Zinell (BW) über den Aufbau von CERT-Strukturen in den Ländern. Eine Arbeitsgruppe des IT-Planungsrats arbeite derzeit eine „Leitlinie Informationssicherheit des IT-Planungsrats" aus. Ziel sei die Förderung des Aufbaus von VerwaltungsCERTs, wobei ein einheitliches Vorgehen und die Einbeziehung der Kommunen im Vordergrund stehe.
Hr. Jurk (HE) informiert über die parallelen Bemühungen der durch die IMK einberufenen Länder-Arbeitsgruppe „Cybersicherheit", in der aktuell 15 Länder auf Staatssekretärs- und Arbeitsebene mitarbeiten würden.
Es sei einerseits geplant, bis zur 4. Sitzung des Cyber-SR im Oktober eine synopsenartige Übersicht der Aktivitäten der Länder zum CERT-Aufbau vorzulegen. Darüber hinaus beabsichtige man, für kleinere und mittlere Kommunen eine Art „Blaupause" für den Aufbau von CERT-Strukturen zu erstellen. Dies sei als Angebot zur Unterstützung der Kommunen zu verstehen. Auch dieses Papier solle dem Cyber-SR im Oktober vorgelegt werden.
Fr. Staatssekretärin Rogall-Grothe dankt den beiden Ländervertretern für ihre Ausführungen. Wichtig sei die Einbeziehung der Sicherheit der IT der Länder- und Kommunalverwaltungen in die Arbeit des CyberAbwehrzentrums; dabei sei wichtig, dass keine Doppelarbeit geleistet werde. Das Thema *Aufbau von CERT-Strukturen in den Ländern* soll in der nächsten Sitzung des Cyber-SR erneut behandelt werden.

Die vierte Sitzung des Cyber-SR soll in der 42. oder 43. KW im Oktober 2012 stattfinden.

VS-NUR FÜR DEN DIENSTGEBRAUCH

3. Sitzung des Cyber-SR am 31. Mai 2012

- Teilnehmerliste -

BMI:	Stn Rogall-Grothe, Hr. Dr. Dürig, Hr. Spatschke
BK:	Hr. Dr. Wettengel, Fr. Dr. Klee, Dr. Nierhoff
AA:	Stn Dr. Haber, Hr. Fleischer
BMVg:	St Beemelmans, Hr. Dr. Theis, Hr. Sohm
BMWi:	Hr. Dr. Schuseil, Fr. Husch
BMJ:	Stn Dr. Grundmann, Fr. Schmierer
BMF:	Fr. Dr. Stahl-Hoepner, Hr. Schulz
BMBF:	St Dr. Schütte, Hr. Lange
HE:	Hr. Jurk
BW:	Hr. Dr. Zinell, Hr. Dr. Hermann
BSI:	Hr. Hange

Assoziierte Wirtschaftsvertreter:

D[redacted]

A[redacted]:

B[redacted]:

B[redacted]

Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
Cyber-Abwehrzentrum

Cyber-Abwehrzentrum

Michael Hange
Präsident des Bundesamtes für Sicherheit in der
Informationstechnik

3. Sitzung des Cyber-Sicherheitsrates
31. Mai 2012

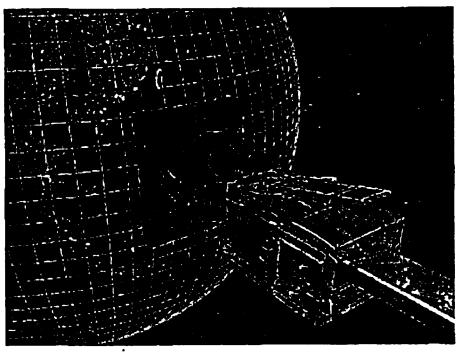
Bundesamt
für Sicherheit in der
Informationstechnik

Evaluierung

Nationales
Cyber-Abwehrzentrum

- **Botnetze:**
  Miner-Botnetz

Datendiebstahl:
Sony



Bloßstellung:
PATRAS

- **Sicherheitsinfrastrukturen:**
  DigiNotar, Duqu

Im Cyber-AZ bearbeitete Fälle:	483
Ausführlich analysiert:	9
Höher VS-NfD:	2

Bundesamt für Sicherheit in der Informationstechnik

Folgerungen für mehr Cyber-Sicherheit

Nationales Cyber-Abwehrzentrum

- Diskrepanz zwischen bekannten Cyber-Angriffen und festgestelltem Angriffspotential.
- Sicherheitsmaßnahmen:
  - Standard für 80 Prozent der Cyber-Angriffe.
  - Individuelle für 20 Prozent der Cyber-Angriffe.
- Bisher konnte aus den Cyber-Angriffen nur ein unklares Täterbild (Aussagen zu Fähigkeiten, Ressourcen, Zielen) abgeleitet werden.

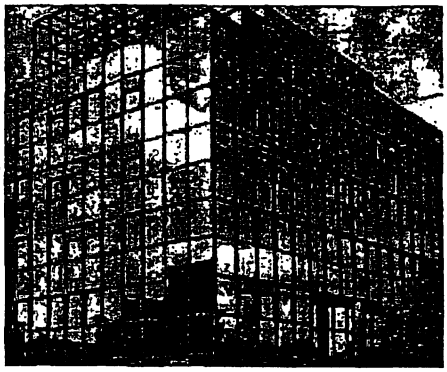
→ Maßnahmen gegen Standardangriffe: CERT-System, Lage- und Krisenreaktionszentren

→ Maßnahmen gegen (individuelle) Angriffe: Austausch zu Vorfällen

Bundesamt
für Sicherheit in der
Informationstechnik

Kontakt

Nationales
Cyber-Abwehrzentrum



Bundesamt für Sicherheit in der Informationstechnik (BSI)

Michael Hange
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)228 99-9582-5200
Fax: +49 (0)228 99-109582-500

Michael.Hange@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de

Anlage 3

Nationales Cyber-Abwehrzentrum

Statusbericht Nationales Cyber-Abwehrzentrum

zur Unterrichtung des Cyber-Sicherheitsrates

Nationales Cyber-Abwehrzentrum
Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6000
E-Mail: cyber-az@bsi.bund.de

Inhaltsverzeichnis

1 Überblick

Am 1. April 2011 hat das Nationale Cyber-Abwehrzentrum mit 10 Mitarbeitern aus den Behörden BBK, BfV und BSI seine Arbeit aufgenommen. Ab 16. Juni 2011 wurde es um Mitarbeiter der assoziierten Behörden BKA, BND, Bundespolizei, Bundeswehr, MAD und ZKA erweitert. Aufgabe des Nationalen Cyber-Abwehrzentrums ist, im Sinne einer Informationsdrehscheibe Cyberangriffe behördenübergreifend zu analysieren und zu bewerten sowie Handlungsempfehlungen zur Verbesserung der Cybersicherheit vorzuschlagen.

Das Nationale Cyber-Abwehrzentrum hat im Zeitraum April 2011 bis März 2012 rund 500 nationale und internationale IT-Sicherheitsvorfälle registriert. Im Ergebnis kann festgehalten werden, dass der Großteil der Vorfälle kriminell motiviert war und eine Gewinnerzielungsabsicht zum Hintergrund hatte. Hauptopfer waren dabei Privatanwender.

An zweiter Stelle findet sich mit dem „Hacktivismus" ein recht junges Phänomen wieder. Mit nicht klar einzuordnenden, oft divergierenden Zielsetzungen wurden Unternehmen und staatliche Stellen durch Angriffe auf ihre Datenbestände und anschließende Veröffentlichung der Daten bloßgestellt. Oftmals wurden dabei unbeteiligte Dritte zum Opfer, deren Daten im Nachgang von Kriminellen missbraucht wurden.

Angriffe auf die Kommunikationsnetze und Internetauftritte deutscher Bundes- und Landesbehörden gehören mittlerweile zum Alltag in der Angriffsbeobachtung des BSI, blieben im Betrachtungszeitraum jedoch ohne nennenswerte Erfolge. Auf internationaler Ebene konnten im Jahr 2011 jedoch einige Angriffe beobachtet werden, die erfolgreich waren, aufgrund ihrer Beschaffenheit weltweit einsetzbar sind und daher Anlass zur Besorgnis geben. Dies gilt insbesondere deshalb, da sie nach Einschätzung der am Cyber-Abwehrzentrum beteiligten Dienste staatlich gelenkt waren.

Insgesamt hat sich die Gefährdungslage verschärft, was angesichts einer immer stärker werdenden Vernetzung und der zunehmenden Nutzung des Internets durch mittlerweile alle Bevölkerungsgruppen zu erwarten war. Zu beobachten war zum einen eine weitere Professionalisierung der Angreifer, die sich einer arbeitsteilig organisierten Underground Economy bedienen können. Auffällig waren zudem eine kleine Anzahl äußerst versiert ausgeführter mehrstufiger Angriffe, bei denen das Eindringen in ein IT-System nur erfolgte, um Informationen für einen Angriff auf das eigentliche Zielsystem (eines völlig anderen Unternehmens) zu erbeuten. Die Masse der Angriffe war erfolgreich, weil seitens der Nutzer elementare Sicherheitsvorkehrungen nicht beachtet wurden. So konnten beispielsweise aufgrund nachlässigen Patch-Managements bereits lange vom Hersteller geschlossene Schwachstellen ausgenutzt werden.

Ernstzunehmende Angriffe mit Schadenswirkung auf das Funktionieren des Staates sowie kritischer Infrastrukturen waren im vergangenen Jahr, anders als in anderen Staaten, nicht zu verzeichnen. Durch die immer weiter steigende Abhängigkeit einer modernen Gesellschaft von der Informationstechnik werden die mit solchen Angriffen verbundenen Risiken allerdings ansteigen. Die im November 2011 durchgeführte LÜKEX-Übung hat dies eindrucksvoll bestätigt.

Zusammenfassend lassen sich zwei Ergebnisse festhalten:

- Die Beobachtung von Sicherheitsvorfällen und die daraus abgeleitete Gefährdungslage wird immer mehr unverzichtbare Voraussetzung der IT-Sicherheitsgestaltung. Eine enge Zusammenarbeit der Sicherheitsbehörden ist hierbei zwingend. Ein frühzeitiger Informationsaustausch zwischen den Akteuren ist grundlegende Voraussetzung für ein konsequentes und – unter Nutzung der jeweiligen Kompetenzen in präventiven und repressiven Bereichen – wirksames Vorgehen im Schadensfall.
- Durch mit vertretbarem Aufwand erreichbare Mindestsicherheitsstandards lassen sich bereits 80 Prozent der beobachteten Angriffe abwehren (Pareto-Prinzip).

2 Besondere Cyber-Angriffe

2.1 S[redacted]

Das Eindringen in die Systeme von S[redacted] und die Veröffentlichung mehrerer Millionen Kundendatensätze zeigt, dass selbst Global Player im IT-Markt betroffen sein können. Nachdem S[redacted] zwei Hacker verklagt hatte, da diese den Kopierschutz der S[redacted] umgangen hatten, wurden als Gegenreaktion durch die Hacktivismusgruppe „Anonymous" eine Reihe von S[redacted]-Websites durch DDoS-Angriffe lahmgelegt. Darüber hinaus gelang es Hackern, in das S[redacted] und das S[redacted] Netzwerk sowie in den Musikdienst Qriocity einzudringen und rund 100 Millionen Kundendaten zu stehlen. Hiervon waren etwa 5 Millionen deutsche Nutzer betroffen, zum Teil sogar mit Kontodaten. S[redacted] war dem Angriff auf seine Datenbanken zunächst hilflos ausgeliefert und musste zeitweise seine Nutzerangebote abschalten. Verantwortlich machte S[redacted] auch für diese Angriffe die Gruppe „Anonymous", die dies allerdings bestritt. Leidtragende waren später jedoch die Kunden von S[redacted], die dem Risiko ausgesetzt waren, dass ihre Daten von Kriminellen missbraucht werden.

Das Image von S[redacted] hat durch einen unzureichenden Schutz seiner Dienste mit diesem Vorfall nachhaltigen Schaden genommen.

2.2 Duqu

Das Bekanntwerden der Schadsoftware „Duqu" zeigt, dass Stuxnet kein Einzelfall war. Nach den Erkenntnissen des Nationalen Cyber-Abwehrzentrums handelt es sich bei Duqu um ein Schadprogramm, das große Teile des Stuxnet-Codes enthält. Betroffen waren bisher nicht näher bezeichnete Unternehmen im Sudan, Iran, Frankreich, Niederlande, Ungarn, Schweiz und Indonesien. Die Auswahl der Branchen, die angegriffen wurden, lässt darauf schließen, dass Duqu zur Angriffsvorbereitung bzw. Aufklärung eingesetzt wurde.

Von Duqu ist auch der KRITIS-Bereich potenziell gefährdet. Da Duqu vermehrt bei Herstellern von SCADA[1]-Systemen aufgetreten ist, kann vermutet werden, dass der Angreifer gezielt Informationen zu solchen Systemen erhalten wollte. Grundsätzlich könnten die abgeflossenen Informationen zu SCADA dazu genutzt werden, die Systeme anzugreifen, die auch in KRITIS Unternehmen im Einsatz sein könnten. Sofern die kritischen Prozesse der KRITIS Unternehmen von den betroffenen SCADA-Systemen (stark) abhängig sind bzw. durch diese erbracht werden, könnte es im Falle eines Angriffes zu einer relevanten Beeinträchtigung oder dem Ausfall der Versorgung mit dem Service der jeweiligen KRITIS führen. Dies wäre verbunden mit entsprechenden Auswirkungen auf die Bevölkerung, auf staatliche Stellen und auf die Wirtschaft.

2.3 DigiNotar

Der Angriff auf DigiNotar erfolgte, um im Nachgang Dritte anzugreifen. Mit dem Einbruch bei DigiNotar und der Erzeugung von SSL-Zertifikaten war es möglich, die vertrauliche, verschlüsselte Kommunikation von Internetnutzern auszuspähen. Außerdem verursachte der Vorfall enorme Kosten für die niederländische Regierung, da diese die Zertifikate für die Absicherung von Regierungswebseiten und -diensten komplett austauschen musste. Zeitweise mussten sogar einige Online-Regierungsdienste abgeschaltet werden, zum Beispiel die elektronische Abgabe der Lohnsteuererklärung. Betroffen waren aber weit mehr Fachverfahren der niederländischen Regierung.

Da es sich bei SSL um einen internationalen Standard handelt, werden auch im deutschen Behördennetz SSL-Zertifikate an vielen verschiedenen Stellen zur Absicherung der Kommunikation eingesetzt. Das deutsche Netz ist daher für einen Angriff wie den oben beschriebenen prinzipiell genauso anfällig wie das niederländische. Der Vorfall bei DigiNotar steht dabei sogar nur für einen von mehreren erfolgreichen Angriffen auf Zertifizierungsstellen in allen Teilen der Welt im Jahr 2011. Das BSI hat daher eine Projektgruppe eingesetzt, um eine technische Lösung für dieses Problem zu erarbeiten.

---

[1] Supervisory Control and Data Acquisition (SCADA)-Systeme dienen zum Überwachen und Steuern technischer Prozesse.

Unternehmen und Einrichtungen aus dem KRITIS-Bereich können in derselben Weise wie nicht-KRITIS Unternehmen und Einrichtungen betroffen sein - sowohl als Nutzer/Anwender als auch als Diensteanbieter. Dies wäre im KRITIS-Kontext insbesondere dann relevant, wenn z.B. kritische Prozesse von der Verfügbarkeit einer vertrauenswürdigen, TLS/SSL-gesicherten Kommunikationsinfrastruktur abhängig sind. Der Angriff auf DigiNotar oder ähnlich gelagerte IT-Sicherheitsvorfälle könnten im KRITIS-Bereich zu Beeinträchtigungen und Störungen führen. So wäre es beispielsweise möglich, dass manipulierte Softwareprodukte, die mit validen Zertifikaten signiert wurden, in der Folge eingesetzt werden, um an Informationen und Unternehmensdaten zu gelangen bzw. durch Sabotage Betriebsabläufe zu stören. In Bezug auf diesen konkreten Fall gibt es keine Hinweise darauf, dass KRITIS in Deutschland betroffen war. Vorrangig waren verschiedenen Anwendungen der Niederländischen Regierung sowie iranische Nutzer betroffen.

2.4 PATRAS

Der „Einbruch" in das GPS-basierte Zielverfolgungssystem „PATRAS" blieb nicht ohne Auswirkungen auf die Ermittlungsarbeit deutscher Sicherheitsbehörden. Die mit Hilfe dieses Systems durchgeführten Lokalisierungsdienste mussten für einen kurzen Zeitraum unterbrochen werden. Grundsätzlich ist auch nicht auszuschließen, dass Kriminelle (vornehmlich aus dem Bereich des Menschen- und Drogenhandels) durch Veröffentlichung der ermittelten Bewegungsprofile davon Kenntnis erlangten, Ziel einer staatlichen Überwachungsmaßnahme gewesen zu sein.

Verursacht wurde der Zwischenfall durch eine Kette von Fehlern auf verschiedenen Ebenen, die allesamt sehr leicht vermeidbar gewesen wären und die schließlich durch einen Unberechtigten ausgenutzt wurden.

Der PATRAS-Fall war die erste Bewährungsprobe für das Nationale Cyber-Abwehrzentrum. Der Vorfall ereignete sich nicht nur kurz nach dessen offizieller Eröffnung, es waren darüber hinaus auch zwei der beteiligten Behörden unmittelbar betroffen. Im Rahmen mehrerer anlassbezogener Treffen und Vollversammlungen des Cyber-Abwehrzentrums konnte der Vorfall analysiert werden. In der Folge hat die Bundespolizei ihre IT-Prozesse optimiert.

2.5 RSA/Lockheed Martin

Der Vorfall bei dem Unternehmen RSA zeigt anschaulich, dass die Angriffsszenarien komplexer geworden und Angriffe immer häufiger mehrstufig aufgebaut sind. In diesem Fall wurde zunächst durch einen Einbruch im März 2011 in die IT-Systeme der Firma RSA technologisches Wissen erbeutet, das dazu verwendet werden konnte, das von RSA vertriebene SecurID-Einmalpasswort-System zu schwächen.

Einige Monate später wurde mit den beim RSA-Angriff gewonnenen Informationen das Rüstungsunternehmen Lockheed-Martin angegriffen.

Die Kommunikationspolitik der Firma RSA trug dabei zur Aufklärung des Falles wenig bei. Nachdem anfangs von Unternehmensseite noch die Ansicht vertreten wurde, die Sicherheit des SecurID-Systems sei nicht beeinträchtigt, gab man nach und nach zu, dass man sich seiner Sache doch nicht ganz sicher sei. Angesichts der Tatsache, dass weltweit etwa 40 Millionen SecurID-Hardware-Tokens verkauft wurden und dazu noch einmal schätzungsweise 250 Millionen Software-ID-Generatoren kommen, ist diese Zurückhaltung aus wirtschaftlichen Erwägungen zwar verständlich, aus Kundensicht jedoch nicht. Knapp 300 Millionen Nutzer darüber im Unklaren zu lassen, dass ihre Zugangsdaten vermutlich kompromittiert wurden, ist unter Sicherheitsaspekten nicht zu verantworten. Erst knapp drei Monate nach dem Vorfall begann das Unternehmen RSA damit, einen Teil der Hardware-Tokens auszutauschen. Und erst im Dezember 2011 berichtete RSA der Bundesverwaltung detailliert über den genauen Ablauf des Angriffs.

Auch Unternehmen und Einrichtungen aus dem KRITIS-Bereich, die die SecureID Lösung von RSA einsetzen, könnten betroffen sein. Zum einen ist eine direkte Folge für Unternehmen, die die möglicherweise kompromittierte Lösung einsetzen, in erster Linie in der ggf. notwendigen Evaluierung bzw. dem Ersatz/Austausch des 2-Faktor Authentifizierungsverfahrens zu sehen. Zum anderen könnte der vorliegende IT-Sicherheitsvorfall im KRITIS-Bereich zu Beeinträchtigungen und Störungen führen, wenn sich die Täter durch das kompromittierte SecureID System mit geringerem Aufwand Zugang zu relevanten Systemen der KRITIS verschaffen können. In diesem Fall sind nach aktuellen Kenntnissen Unternehmen und Einrichtungen aus dem KRITIS-Bereich in Deutschland nicht betroffen. Unternehmen und Einrichtungen aus dem KRITIS-Bereich könnten aber sowohl durch das Angriffsmuster des primären Vorfalls (RSA, Eindringen in Systeme zur Informationsbeschaffung) als auch durch das Angriffsmuster des sekundären Vorfalls (Lockheed, Angriff unter Verwendung zuvor gewonnener Informationen) betroffen sein.

2.6 Miner Bot-Net

Mit Hilfe von Bot-Netzen versuchten Angreifer im vergangenen Jahr, Geld von verschiedenen Website-Betreibern zu erpressen und drohten diesen damit, ihre Website mittels eines DDoS-Angriffes lahmzulegen. Es handelt sich also um die digitale Entsprechung der herkömmlichen Schutzgelderpressung. Ein Spezialfall war das „Miner-Bot-Net", welches sich durch die verwendete Kommunikationsstruktur sehr resistent gegenüber Gegenmaßnahmen zeigte. Es nutzte keine zentralen Steuerungssysteme, sondern verteilte seine Angriffsbefehle über Peer-to-Peer-Kommunikation[2]. Im Visier der Angreifer standen zunächst Pizzabringdienste, später kamen

[2] Viele Bot-Netze verwenden eine Kommunikationsstruktur, bei der die einzelnen Bots Befehle von übergeordneten „Command-and-Control"-Servern erhalten. Gelingt es, die Hoheit über die „Command-and-Control"-Server zu erhalten oder diese abzuschalten, kann ein davon abhängiges Bot-Netz in der Regel unschädlich gemacht werden. In einem „Peer-to-Peer-Netz" sind alle Computer gleichberechtigt und können sowohl Dienste in Anspruch nehmen,

größere Unternehmen der Immobilienbranche und weitere Sektoren (vereinzelt auch Behörden) als Angriffsziele hinzu. Die strafrechtliche Verfolgung ist inzwischen von den Polizeien übernommen worden.

2.7 Sicherheitsvorfälle in internationalen Organisationen

Bei einem umfangreichen Angriff auf den Internationalen Währungsfonds (IWF) wurde – vermutlich staatlich gelenkt – versucht, sich interne Informationen des IWF zu verschaffen. Die Bemühungen, von Seiten des IWF Informationen über die näheren Hintergründe bzw. einen etwaigen Schaden zu erhalten, verliefen jedoch erfolglos.

Auch in Bezug auf die EU wurde im Jahr 2011 ein gezielter Angriff öffentlich. Über einen längeren Zeitraum hatten die Angreifer Zugriff auf das interne (offene/nicht VS-) Netzwerk der EU-Kommission.

3 Grundsätzliche Schlussfolgerungen

Die geforderte und anzustrebende Cyber-Sicherheit ist kein statischer Zustand, sondern ein kontinuierlicher Prozess, der die Risiken des Cyber-Raums und die erforderlichen und angemessenen Gegenmaßnahmen in ein effektives und tragbares Verhältnis zueinander stellt.

Da der Cyber-Raum essentielle Bedeutung für alle Akteure erlangt hat, müssen sich Staat, Wirtschaft, Wissenschaft und Bevölkerung weiterhin stark engagieren.

- Aktives Beobachten und Analysieren der Bedrohungslage ist unverzichtbare Voraussetzung für die Cybersicherheitsgestaltung.
- Es besteht eine Diskrepanz zwischen öffentlich gewordenen Cyber-Angriffen und sich im Internet darstellenden Angriffspotenzial.
- 80:20-Regel: Durch konsequentes Umsetzen von Standardsicherheitsmaßen ist die Masse der Cyber-Angriffe beherrschbar.
- Für die 20 Prozent hochwertiger Angriffe werden verbesserte Sicherheitskonzepte und Lösungen benötigt (dies gilt insbesondere für den Bereich KRITIS).

als auch zur Verfügung stellen. Es existieren keine „Command-and-Control"-Server. Das Netz organisiert sich selbst. Die Bekämpfung ist daher wesentlich aufwändiger.

- Die Ermittlung von Tätern (Attributierung) auf Basis eines erfolgten Cyber-Angriffs ist schwierig.

461/12
503

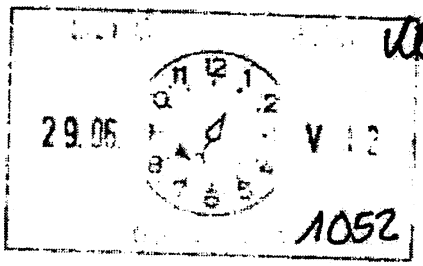
BMI

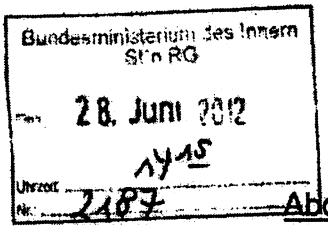
IT3-606 000-9/31#1

Refl: Dr. Dürig/Dr. Mantz
Ref: Dr. Pilgermann/RRn Otte

Berlin, den 28. Juni 2012

Hausruf: 1374/1527/2808





Herrn Minister

über

Frau Stn Rogall-Grothe

Herrn IT-D

Herrn SV IT-D

Abdrucke:

Herrn PSt Dr. Bergner;
Herrn St Fritsche;
Herren LLS, AL ÖS und AL KM;
Referate Presse, Z 9 und B 3.

Betr.: IT-Schutz kritischer Infrastrukturen; Vorbereitung Ministergespräch mit Vertretern des Sektors Transport und Verkehr

Bezug: Ministervorlage vom 17. April 2012; Az. IT3-606 000-9/31#1

Anlage: Vorbereitungsmappe

Zur Vorbereitung Ihres Gesprächs mit Vertretern des Transport- und Verkehrswesens am **5. Juli 2012 von 13.00 bis 15.00 Uhr** erhalten Sie anliegende **Vorbereitungsmappe**.

Bereits geführt wurden Gespräche

- am 9. Mai mit Vertretern des Finanz- und Versicherungswesens,
- am 23. Mai mit Vertretern des IKT-Sektors und
- am 13. Juni 2012 mit Vertretern des Energie-Sektors.

Während die an den bisherigen Gesprächen beteiligten Unternehmen gut aufgestellt und zur Erfüllung von IT-Sicherheitsanforderungen größtenteils

gesetzlich verpflichtet waren, bestehen solche Regelungen für das weitestgehend liberalisierte Transport- und Verkehrswesen nicht. Um auf Unterschiede und Lücken hinzuweisen, wurde der Mappe ein neues Vorblatt hinzugefügt, das wesentliche Punkte hervorhebt.

Teilnehmer: Bisher haben 11 Teilnehmer aus der Wirtschaft zugesagt. Teilnehmen wird zudem Herr Staatssekretär Prof. Scheurle, BMVBS (s. Teilnehmerliste, **Fach 1**).

Hinweis Ministerbüro: Eine aktualisierte Teilnehmerliste wird rechtzeitig zum Termin vorgelegt.

Dr. Mantz

gez.
Dr. Pilgermann / Otte

Ministergespräch IT-Schutz kritischer Infrastrukturen

Transport und Verkehr

BMI, Raum 1.071, 5. Juli 2012, 13-15 Uhr

➢ Übersicht zu wesentlichen Punkten für das Gespräch	**Fach 1**
➢ Agenda und Teilnehmerliste	**Fach 2**
➢ Gesprächsführungsvorschlag Begrüßung	**Fach 3**
➢ Gesprächsleitfaden Cybersicherheit aus fachspezifischer Sicht	**Fach 4**
➢ Gesprächsleitfaden und Unterlagen Cybersicherheitslage	**Fach 5**
➢ Gesprächsleitfaden und Diskussionspapier Anforderungen an IT-Schutz aus Sicht BMI	**Fach 6**
➢ Gesprächsleitfaden Diskussion der Anforderungen	**Fach 7**
➢ Gesprächsleitfaden Zusammenfassung / Ausblick	**Fach 8**
➢ Potentielle Fragen der Wirtschaft (und Antworten)	**Fach 9**
➢ Hintergrundinformationen KRITIS Allgemein	**Fach 10**
➢ Hintergrundinformationen KRITIS Transport und Verkehr	**Fach 11**
➢ Cybersicherheitsstrategie	**Fach 12**

Ministergespräch IT-Schutz kritischer Infrastrukturen Transport und Verkehr

Übersicht

- **Sektor mit sechs Branchen (Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr und Logistik); weitgehend liberalisiert.**

  Hinweis für Gespräch: Branchen sind bis auf Seeschifffahrt (Zentralverband der deutschen Seehafenbetriebe hat kurzfristig abgesagt) und Straßenverkehr (Länderzuständigkeit) über Unternehmen und/oder Verbände vertreten; Teilnehmer sehr heterogen und aus unterschiedlichen Bereichen.

- **Während im Finanz-, IKT- und Energiesektor zentrale Aufsichtsstrukturen (BaFin, Bundesnetzagentur) auf Bundesebene vorhanden sind, bestehen Aufsichten und Einwirkungsmöglichkeiten des Bundes im Sektor Transport und Verkehr nur für Teilbereiche; Länderzuständigkeit bei Straßenverkehr (Auftragsverwaltung), Binnenhäfen und Teile der Luftfahrt.**

- **Keine dem Kreditwesengesetz (MA RISK), Telekommunikationsgesetz oder Energiewirtschaftsgesetz vergleichbaren gesetzlichen Regelungen mit Anforderungen an den IT-Schutz; keine branchenspezifischen Mindeststandards.** Allerdings positive Initiativen zu branchenspezifischen Standards.

  Hinweis für Gespräch: Bestehende Lücken sollten angesprochen werden; Frage nach IT-Sicherheit kritischer Prozesse in den Unternehmen und Adressierung der Frage durch die Verbände.

- **Zusammenarbeit im UP KRITIS nicht umfassend. Von den Anwesenden nur D[redacted], D[redacted], F[redacted], D[redacted] Mitglieder; Verbände sind nicht vertreten.** Airlines scheuen beispielsweise Einordnung als „kritische Infrastruktur".

  Hinweis für Gespräch: Aufforderung zur Mitarbeit im UP KRITIS.

- **BMVBS agiert als Unterstützer des offenen Marktes und sieht Auflagen zur Sicherstellung der Versorgung auch aufgrund bestehender Redundanzen (Umsteigen auf Straße oder Wasser bei Ausfall von Schiene etc.) nicht als Priorität. Kenntnisse hinsichtlich der IT-Sicherheitssituation liegen kaum vor.**

Stand: 3. Juli 2012

Ministergespräch IT-Schutz kritischer Infrastrukturen

Teilnehmerliste Transport und Verkehr

Teilnehmer Wirtschaft

Schienenverkehr

1. [redacted], Vorstand, D[redacted] AG

Logistik

2. [redacted] Executive Vice President, D[redacted] AG

Luftverkehr

3. [redacted], CIO, F[redacted] AG
4. [redacted] Vorstandsvorsitzender, A[redacted] KG
5. [redacted] Leiter Konzernsicherheit, D[redacted] AG
6. [redacted] Vorsitzender der Geschäftsführung, D[redacted] GmbH

Verbände

7. [redacted], stellvertretender Hauptgeschäftsführer, D[redacted] e. V.
8. [redacted] Geschäftsführer, B[redacted] e. V.
9. [redacted] Präsident, B[redacted] e. V.
10. [redacted] Fachbereichsleiter Normung, V[redacted] e. V.
11. [redacted], Präsident, B[redacted] e. V.

Staatliche Teilnehmer

12. **Herr Prof. Klaus-Dieter SCHEURLE**, Staatssekretär
    Bundesministerium für Verkehr, Bau und Stadtentwicklung
13. **Herr Andreas KRÜGER**, Unterabteilungsleiter,
    Bundesministerium für Verkehr, Bau und Stadtentwicklung

Stand: 3. Juli 2012

BMI

14. **Frau Cornelia ROGALL-GROTHE**, Staatssekretärin
15. **Herr Peter BATT**, ständiger Vertreter des IT-Direktors
16. **Herr Arne SCHLATMANN**, Leiter Leitungsstab
17. **Frau Barbara KLUGE**, Leiterin Ministerbüro
18. **Herr Norbert SEITZ**, Abteilungsleiter KM
19. **Herr Thomas FRANKE**, Referat ÖS II 1
20. **Herr Dr. Markus DÜRIG**, Leiter IT 3
21. **Frau Kathrin OTTE**, Referat IT 3

Geschäftsbereich

22. **Herr Michael HANGE**, Präsident, BSI
23. **Herr Christoph UNGER**, Präsident, BBK
24. **Herr Peter HENZLER**, Abteilungsleiter, BKA
25. **Herr Dr. Burkhard EVEN**, Abteilungsleiter, BfV

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 27.06.2012
Hausruf: 1527

3. Cybersicherheit im Verkehrs-Sektor aus fachspezifischer Sicht

Herr St. Prof. Scheurle (BMVBS) wurde mit Einladungsschreiben von Stn. Rogall-Grothe um Vorbereitung eines kurzen Beitrags gebeten.

I. Sprechempfehlung

- Darstellung der gemeinsamen Vorgehensweise zw. **Innenminister als KRITIS-Koordinierer** und Fachressorts mit sektorspezifischer Kompetenz
- Hinweis auf die **hohe Komplexität des Sektors mit allein sechs Branchen**, was auch im Vergleich zu den anderen Sektoren **hohe Anforderungen an das Fachressort** stellt
- Verweis auf Herrn St. Prof. Scheurle für einen Beitrag „Cybersicherheit im Verkehrs- und Transport-Sektor aus fachspezifischer Sicht"

II. Aktueller Sachstand

- BMVBS hat begrenzt Möglichkeiten, auf die Unternehmen Einfluss zu nehmen – der **Markt** ist in Vergangenheit mit Nachdruck **dereguliert** worden.
- Vor diesem Hintergrund scheut sich BMVBS auch in der Zusammenarbeit, das Thema Cybersicherheit/IT-Schutz aktiv und prioritär anzugehen.

Bundesamt
für Sicherheit in der
Informationstechnik

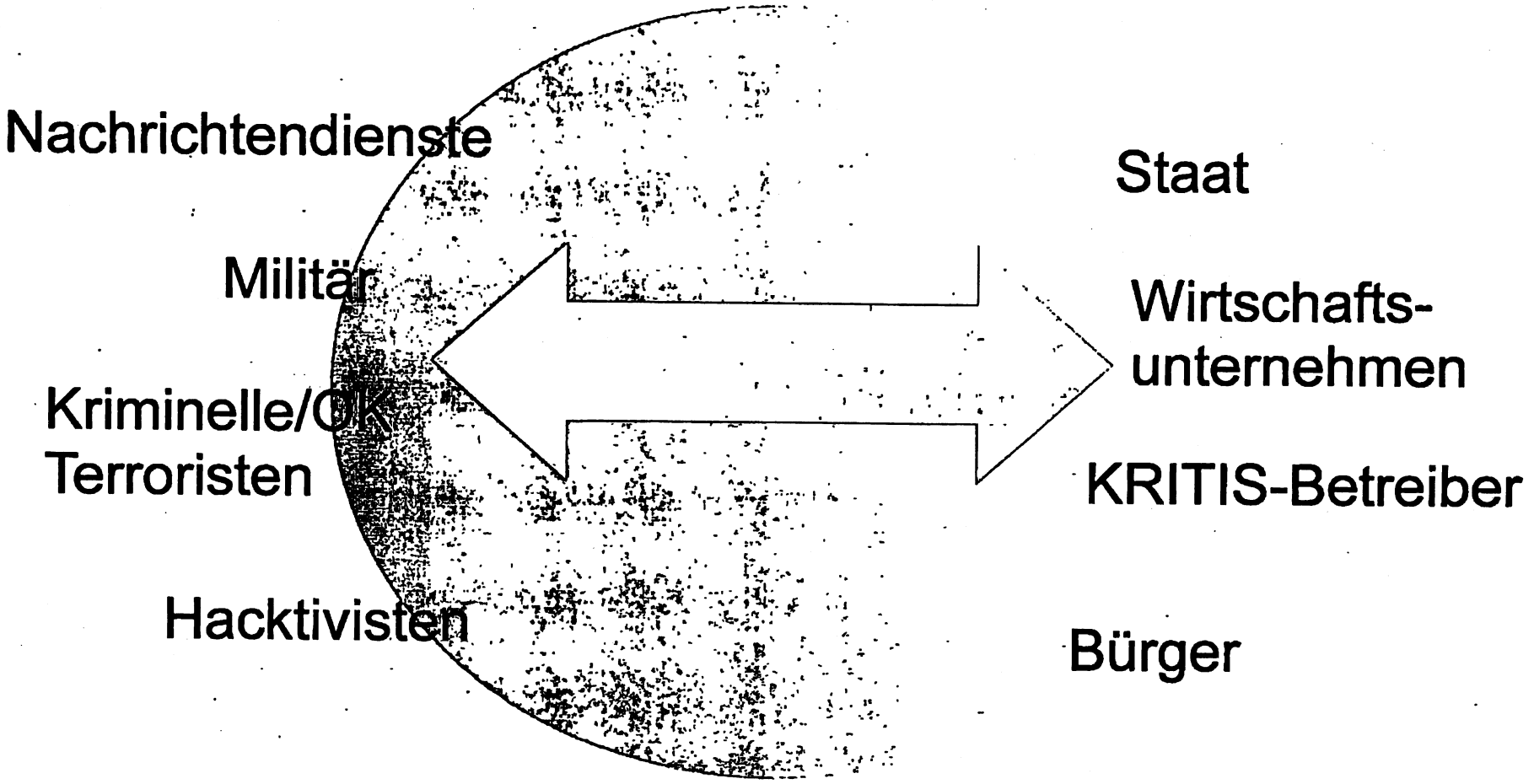
Gefährdungslage

Michael Hange

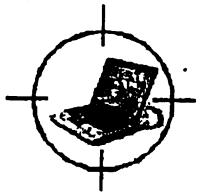
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

5. Juli 2012

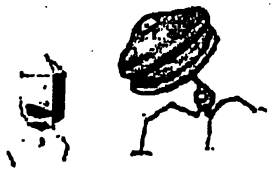
Cyberangriffe und Cyber-Abwehr ein permanenter Wettlauf



Gefährdungen



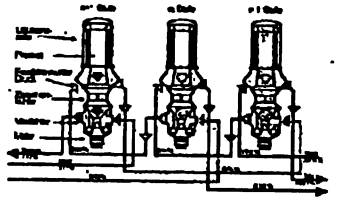
Skalpellartige Angriffe



Gezielte Angriffe

Ungezielte Angriffe

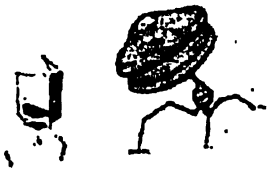
- Manipulation und Sabotage mit großem Schadensausmaß
- Komplexe, langwierige Vorbereitung
- **Stuxnet**



- Spionage, Sabotage, Identitätsdiebstahl
- Spezielle Zielgruppen
- **DigiNotar**
- **Duqu**

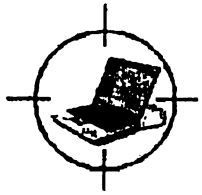
- Verfügbarkeit, Sabotage, Betrug
- Unspezifische Zielgruppen
- **Conficker**

Gefährdungen



Ungezielte Angriffe

- Spanien 08: Virus Mitursache bei Flugzeug-Absturz
- USA 11: Hacker übernehmen Steuerung von Bahnstrecken- Signalen



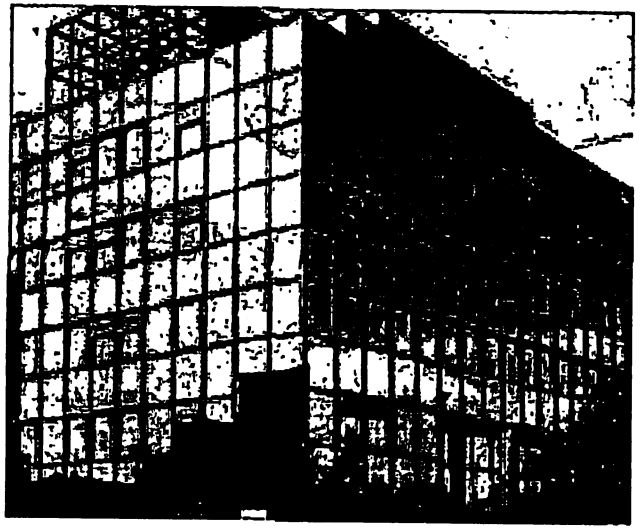
Gezielte Angriffe

- Aktuell: Phishing-Attacken auf DHL-Packstationen
- DHS 02/2012: Starker Anstieg der Anzahl der Angriffe auf KRITIS-Systeme innerhalb eines Jahres (von 11 auf 86)

Skalpellartige Angriffe

- **APT-Angriffe**
- **(Advanced Persistent Threat)**

Kontakt



Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Michael Hange
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-0
Fax: +49 (0)22899-10-9582-0

Michael.Hange@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de

Ministergespräch KRITIS
05. Juli 2012
Kernbotschaften P BSI – Information für BMI

Kurze Einleitung (ohne Folie) und Folie 2

Kernbotschaft 1 (Überleitung von Minister):

Das Thema Cyber-Sicherheit gehört zum gesellschaftlichen und politischen Diskurs. Sicherheit ist dabei ein menschliches Grundbedürfnis, das jedoch oftmals erst begriffen wird, wenn es fehlt bzw. Vorfälle dies offensichtlich machen.

Kernbotschaft 2:

IT-Gefährdungslage hat sich in den letzten zehn Jahren dramatisch entwickelt.

- 90er Jahre Breitenangriffe durch Viren, die im Loveletter-Virus gipfelten. Erste große Denial-of-Service-Angriffe fanden statt. Hacken zur Darstellung des technischen Könnens/Know-hows.
- 2004: große Spam-Welle, von der auch die Bundesverwaltung betroffen war. Neben Hackern wachsen Aktivitäten Krimineller und auch ND-Aktivitäten.
- 2007: Zunahme der gezielten Angriffe (China-Angriff auf Deutschland).
- 2010: Stuxnet.

Folie 3: Gefährdungen

Kernbotschaft 3:

Bei Angriffen unterscheiden wir drei Arten von unterschiedlichem Niveau:

1. Ungezielte Angriffe:

Allgemeines Beispiel: Conficker,

Beispiel für den Sektor: Manipulation Bahnstrecken-Signale (USA 2011).
Botschaft: Zahlreiche Steuersysteme sind über das Internet erreichbar und weisen verheerende Sicherheitslücken auf. Um die Kontrolle über ein solches System zu übernehmen, genügt frei verfügbare Software wie das Angriffsframework Metasploit.

2. Gezielte Angriffe:

Allgemeines Beispiel: DigiNotar,

Beispiel für den Sektor: Phising-Attacke auf DHL-Packstation (aktuell).

Botschaft: Die Angriffe werden immer gezielter und ausgefeilter. Dabei kommen auch vermehrt Methoden des Social Engineering, wie Phishing zum Einsatz. Die Attacken beschränken sich dabei aber keineswegs auf die Kunden von KRITIS, sondern auch Mitar-

beiter der KRITIS selbst werden vermehrt gezielt attackiert.

3. **Skalpellartige Angriffe:**

Allgemeines Beispiel: Stuxnet.

Botschaft: Selbst Luftschnittstellen und proprietäre Systeme sind kein verlässlicher Schutz. Und unsere Erkenntnisse als Folge des Austausches mit Siemens sind, dass SCADA-Systeme in der Regel nicht sicher (im Sinne IT-Sicherheit) betrieben werden (der entsprechende Schalter wird nicht umgelegt). Es besteht Handlungsbedarf!

Kernbotschaft 4:

Wir befinden uns in einem permanenten Wettlauf zwischen Cyber-Angriffen und Cyber-Abwehr. Die durchschnittliche Zeit, bis Reparaturprogramme bzw. Patches für eine Schwachstelle verfügbar sind, beträgt ca. einen Monat. Hinzu kommt die Verzögerung im unternehmensinternen Patchmanagement (prüfen und freigeben). Die Folge: Es sind immer Schwachstellen für Angriffe vorhanden.

Eine effiziente und effektive Cyber-Abwehr ist nur möglich, wenn die Gefährdungslage bekannt ist.

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 27.06.2012
Hausruf: 1527

5. Anforderungen an den IT-Schutz KRITIS aus Sicht BMI

Herr SV ITD Batt hat einen Vortrag zur Vorstellung des Diskussionspapiers vorbereitet

I. Sprechempfehlung

- mit verschärfter Bedrohungslage Notwendigkeit zum sektorübergreifenden, koordinierten Vorgehen
- alle Betreiber in allen Sektoren müssen ein gewisses Mindestmaß an KRITIS-Schutz gewährleisten
- BMI hat dies in 7 Kernforderungen in einem Diskussionspapier zusammengefasst und mit der Einladung übersandt
- Verweis an SV ITD Herr Batt zur Vorstellung der konkreten Forderungen aus Sicht BMI

II. Aktueller Sachstand

- BMI hat Diskussionspapier „IT-Schutz Kritischer Infrastrukturen in Deutschland" mit 7 grundlegenden Forderungen zum IT-Schutz KRITIS erarbeitet
- An Wirtschaftsvertreter übersandt im Rahmen der Einladungsschreiben von Herr Minister

Bundesamt
für Sicherheit in der
Informationstechnik

Gefährdungslage

Michael Hange
Bundesamt für Sicherheit in der
Informationstechnik

5. Juli 2012

Entwicklung Gefährdungslage

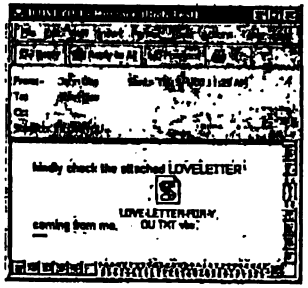
2000 — 2004 — 2007 — 2010

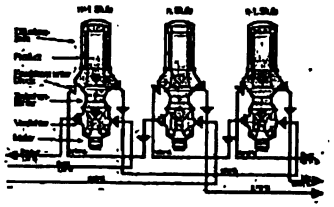
Loveletter-Virus

Spam-Welle

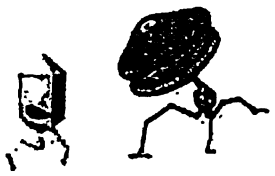
Zunahme gezielte Angriffe

Stuxnet





Gefährdungen



Ungezielte Angriffe

- Verfügbarkeit, Sabotage, Betrug
- Unspezifische Zielgruppen

- **Conficker**
- **USA 2011: Manipulation Bahnstrecken-Signale**

Gezielte Angriffe

- Spionage, Sabotage, Identitätsdiebstahl
- Spezielle Zielgruppen

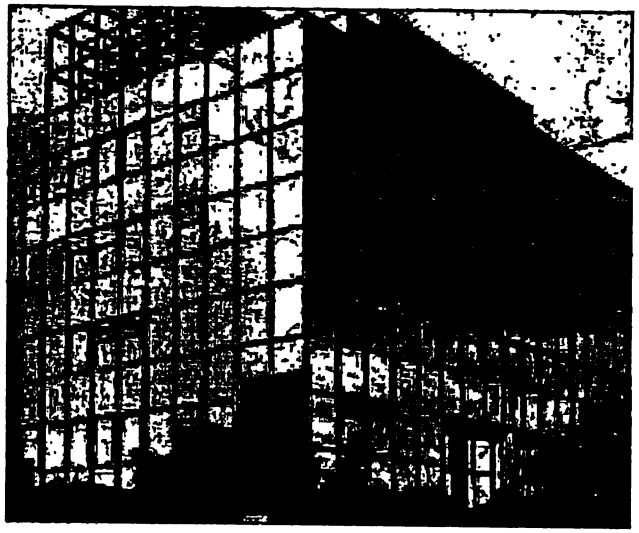
- **DigiNotar**
- **Aktuell: Phishing-Attacken auf DHL-Packstationen**

Skalpellartige Angriffe

- Manipulation und Sabotage mit großem Schadensausmaß
- Komplexe, langwierige Vorbereitung

- **Stuxnet**
- **Advanced Persistent Threat**

Kontakt



Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Michael Hange
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-0
Fax: +49 (0)22899-10-9582-0

Michael.Hange@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de

Bundesministerium des Innern

Agenda

IT-Schutz kritischer Infrastrukturen Transport und Verkehr

5. Juli 2012, 13-15 Uhr, Raum 1.071

Bundesministerium des Innern, Alt-Moabit 101D, 10559 Berlin

13:00 – 13:07 Begrüßung und Einführung
Dr. Hans-Peter Friedrich, Bundesminister des Innern

13:07 – 13:10 Cybersicherheit/IT-Sicherheit im Sektor Transport und Verkehr aus fachspezifischer Sicht
Prof. Klaus-Dieter Scheurle, Staatssekretär im Bundesministerium für Verkehr, Bau und Stadtentwicklung

13:10 – 13:20 Cybersicherheitslage in Deutschland
Michael Hange, Präsident des BSI
Möglichkeit zu Rückfragen zur Gefährdungslage

13:20 – 13:25 Anforderungen an den IT-Schutz kritischer Infrastrukturen aus Sicht des BMI
Peter Batt, Ständiger Vertreter des IT-Direktors im Bundesministerium des Innern

13:25 – 14:50 Diskussion der Anforderungen an den IT-Schutz kritischer Infrastrukturen und der getroffenen Maßnahmen
Diskussionsleitung: Dr. Hans-Peter Friedrich, Bundesminister des Innern

14:50 – 15:00 Zusammenfassung und Ausblick
Dr. Hans-Peter Friedrich, Bundesminister des Innern

Referat IT 3

Konkrete Fragen

- Wie sind die Unternehmen konkret zum Schutz der IT gestützten Prozesse aufgestellt?
- Wie werden die wirklich kritischen Prozesse in den einzelnen Unternehmen/Sektoren festgelegt?
- Existieren Kenntnisse über gegenseitige Abhängigkeiten von
  - unternehmensinternen Prozessen
  - brancheninternen Prozessen
  - branchenübergreifenden Prozessen?
- Wie wird das jeweilige Schutzniveau festgelegt?
- Existieren brancheninterne Arbeitskreise zu Cyber-Sicherheit
- Existieren branchenspezifische IT-Mindeststandards?
  Hinweis: Iniative innerhalb der Luftverkehrswirtschaft loben, solchen Standard zu entwickeln und abzustimmen – Sachstand könnte erfragt werden

Konkrete Aufforderungen:

- Zur Mitarbeit im UP K aufgefordert werden!°
- Zum Aufbau von Single Point of Contacts aufgefordert werden, über die Sicherheitsvorfälle an das BSI übermittelt und Handlungsempfehlungen vom BSI an die Unternehmen übermittelt werden könnten.
-

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 27.06.2012
Hausruf: 1527

6. Diskussion der Anforderungen an den IT-Schutz

Diskussionspapier aus 5) war Wirtschaftsvertretern in Vorbereitung zur Verfügung gestellt worden

Moderation: Minister (entlang Diskussionspapier)

(Vorgeschlagener Fragesteller (Min/StnRG/ITD) jeweils in Klammern; **prioritäre Fragen fett)**

I. Sprechempfehlung

(Min) **Allgemeine Fragen** (insbesondere nach **Rahmenbedingungen und Lücken; HINWEIS nach hiesiger Kenntniss keine rechtlichen Anforderungen, keine Initiativen der Verbände und keine Teilnahme dieser am UPK**; insgesamt aber wenig bekannt):

- **Einschätzung zum Sachstand des IT-Schutzes** der Kritischen Infrastrukturen in den Bereichen Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr und Logistik und im Sektor insgesamt
- **Welche Auflagen und Rahmenbedingungen bestehen? Sind diese kompatibel mit Auflagen und Rahmenbedingungen in anderen Ländern?**
- **Welche Maßnahmen haben Sie in Ihren Unternehmen getroffen?**
- **Ist IT-Sicherheit ein Thema der Verbände?**
- Erfahrungen aus der Zusammenarbeit im UPK seit 2007?

Fragen zu den Punkten aus dem Diskussionspapier:

1) *Mehr Transparenz schaffen*

(Die kritischen Geschäftsprozesse müssen identifiziert; die Abhängigkeit dieser Prozesse von IKT bekannt sein.)

- *StnRG:* **Wie werden Risiken für die Gesellschaft im Risikomanagement prominent abgebildet?**
- *SV ITD:* Wie lange können Unternehmen bei Ausfall des Internet überleben?

2) *Robuste Grundlagen*

(Mindeststandards müssen definiert sein. Regelmäßige Überprüfungen (Audits) verifizieren deren Umsetzung.)

Mindeststandards

- *StnRG:* **In einigen Branchen – wie z.B. der Luftfahrtbranche – werden unserer Kenntnis nach Standards entwickelt und auch in die internationale Standardisierung geleitet. Wie verbindlich sind diese Standards in der Anwendung – wie wird das überprüft? Gibt es Standards auch in anderen Bereichen (Straßenverkehr, Logistik, Schifffahrt, bei der Bahn)?**

Audits

- *SV ITD:* Wie groß ist inzwischen der Anteil von IT-Anforderungen in den regelmäßigen Audits (intern oder auch durch Externe)?
- *SV ITD:* Wie könnte in diesem Bereich eine Zusammenarbeit mit dem BSI aussehen?

3) *Kritische Prozesse autonom gestalten*

(Kritische Prozesse dürfen weder mit dem Internet verbunden sein noch von dessen Funktionstüchtigkeit abhängen.)

- *StnRG:* **Können zentrale IT-Systeme (zur Aufrechterhaltung der eigenen, zentralen Prozesse) unabhängig vom öffentlichen Internet fortbetrieben werden?**

4) *Produkt- und Dienstleistungssicherheit*

(Für besonders sensible Bereiche kommen zertifizierte Produkte zum Einsatz; IT-Sicherheit fließt von Anfang an mit in Planung von IKT-Diensten ein.)

- *Min:* **In BReg besondere Zulassungsverfahren für IT in sensiblen Bereichen. Gibt es vergleichbare Vorkehrungen zum Einsatz ausschließlich zertifizierter Systeme in den kritischen Bereichen?**

5) *Lagefortschreibung und Frühwarnung*

(Alle Unternehmen sind über die Warn- und Alarmierungsmechanismen des UPK an das BSI angeschlossen.)

- Min: **Was fehlt den Organisationen, um umfassend Meldekontakte einzurichten und in einem zweiten Schritt die Kommunikation mittels Einrichtung branchenspezifischer SPOCs zu bündeln?**

- *StnRG:* Vergleichsweise **geringes Meldeaufkommen über UPK-Strukturen** im Vergleich zur Lage in der Bundesverwaltung. Wie ist großer Unterschied zu erklären?

6) *Regelmäßige Übungen*

(Mit regelmäßigen Übungen werden aufgebaute Strukturen überprüft.)

- *SV ITD:* LÜKEX als erste nationale IT-Übung (Bund, Länder, KRITIS) Ende 2011 ein Erfolg – welche Formate des gemeinsamen Übens werden gebraucht?
- *SV ITD:* Wie ergänzen die Branchen die übergreifenden regelmäßigen Übungen aus dem UPK sektorspezifisch?

7) *Institutionalisierte Kooperation*

(Alle Branchen müssen im UPK vertreten sein. Darüber hinaus muss das Thema Cybersicherheit auch in allen Branchen intern in einer institutionalisierten Zusammenarbeit aufgearbeitet werden.)

- Min: Wie können alle Branchen Strukturen aufbauen und unter Anbindung an den Umsetzungsplan KRITIS institutionalisieren?

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 27.06.2012
Hausruf: 1527

4. Cybersicherheitslage in Deutschland

Herr P BSI Hange hat (in Abstimmung mit BKA / BfV) einen kurzen Vortrag zur Cyber-Bedrohungslage vorbereitet – Übergabe an diesen

I. Sprechempfehlung

- Einführung zu Stuxnet als Schadprogramm, welches Ende 2010 mit seinen potentiellen Auswirkungen auf Atomkraftwerke das Thema Cybersicherheit endgültig auf die Tagesordnung aller Entscheider gesetzt hat
- Erinnerung an letzte LÜKEX-Übung von Nov. 2011, bei welcher im Bereich Kritischer Infrastrukturen breitflächige Ausfälle ein Bestandteil waren.
- Verweis an P BSI Herr Hange m.d.B. um einen Einblick in die Bedrohungslage im Cyberspace

II. Aktueller Sachstand

- Angespannte IT-Sicherheitslage, weil Abhängigkeit der Gesellschaft von Kritischen Infrastrukturen erheblich gestiegen ist und Angreifer sich professionalisiert haben

Referat: IT3
Verfasser: Dr. Pilgermann

Datum: 28.06.2012
Hausruf: 1527

IT-Schutz KRITIS im Verkehrs- und Transportsektor

I. Hintergrundinformationen

Der KRITIS-Sektor „Transport und Verkehr" ist in folgende Branchen aufgeteilt:

- Luftfahrt,
- Seeschifffahrt,
- Binnenschifffahrt,
- Schienenverkehr,
- Straßenverkehr, und
- Logistik.

Marktsituation und Branchenorganisation

Grundsätzlich stellen die fünf Branchen Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr und Straßenverkehr Infrastrukturen zur Verfügung – die Anbieter aus der Branche Logistik nutzen jene Basisinfrastrukturen, um Transport, Lagerung, Bereitstellung, Beschaffung und Verteilung von Gütern zu steuern und zu optimieren.
Der gesamte nationale Güterverkehr verteilt sich überschlagsartig folgendermaßen auf die Verkehrsträger:

- 70 % Straße
- 15 % Bahn
- 10 % Binnenschifffahrt

Innerhalb der 6 Branchen existieren jeweils weitere Unterteilungen (z.B. Flughäfen / Airlines bei Luftfahrt oder Häfen, Hafendienstleister und Wasserstraßen (mit Schleusen etc.) bei Seeschifffahrt.
Insb. im Bereich Logistik agieren wenige große Anbieter als echte Steuerer ([redacted], L[redacted], [redacted], [redacted] etc.); das tatsächliche Transportgeschäft ist dann mittelständisch geprägt (ca. 60.000 Unternehmen).

Die Komplexität des Sektors spiegelt sich auch in der Verbandssituation wider; allerdings scheinen sich auch alle Branchen in Verbänden organisiert zu haben. Für die Logistik ist insb. relevant der DSLV[1].

Aufsichtssituation

Der Markt im Sektor Verkehr und Transport wurde in den letzten Jahren mit Nachdruck dereguliert.

Deutsche Aufsichtsgesetzgebung ist eher die Ausnahme im Sektor – so z.B. zu finden für die Branche Schienenverkehr mit Aufsichtsfunktionen des Eisenbahnbundesamt.

Auflagen oder Richtlinien ergeben sich zu weiten Teilen aus europ. Gesetzgebung. Primär sind diese jedoch als Standards ausgestaltet. Internationale Standardisierungsgremien (allgemein wie ISO, aber auch branchenspezifisch wie ICAO[2] oder IMO[3]) spielen eine große Rolle.

IKT-Abhängigkeit

In Deutschland werden in den Branchen des Sektors sehr unterschiedliche Infrastrukturen mit hohen Kritikalitäten für das gesellschaftliche Leben über das Gebiet der Bundesrepublik hinaus betrieben (Luftverkehrsdrehkreuze in DE wie Frankfurt oder große Seehäfen wie Hamburg als Träger des Welthandels).

Der Sektor stützt sich sehr stark auf Dienstleistungen aus anderen KRITIS-Sektoren (insb. Energie und IKT) ab. Im Gegenzug stellt der Transport-Sektor kritische Dienstleistungen an andere KRITIS-Sektoren zur Verfügung (bspw. für Minieralöl-Transport oder auch die Lebensmittelversorgung).

Obgleich die IT-Abhängigkeit nicht so naheliegend wie in anderen Sektoren ist, stützt sich doch jede Branche an kritischen Punkten zunehmend auf IKT (Steuerungstechnik) ab (Verkehrsleittechnik bei Straßen oder Schienenverkehr, Schleusen in der Schifffahrt) – für die Infrastrukturbranchen ist jedoch grdsl. von einer geeigneten Entkopplung zu öffentlichen Netzen auszugehen.

[1] Deutscher Speditions- und Logistikverband e. V.
[2] International Civil Aviation Organization (eine UN-Organisation)
[3] International Maritime Organisation

Die Branche Logistik ist sehr IKT-durchdrungen; eine Unabhängigkeit von öffentlichen Netzen / dem Internet erscheint nicht zuletzt wegen der komplexen Lieferketten und der hohen Dezentralität als unwahrscheinlich.

Schutzniveau und Lücken

In den Branchen gibt es lange Traditionen (und auch Vorgaben / Standards) für die Betriebssicherheit (Safety). Innerhalb der Branchen existieren eine Vielzahl von Redundanzen; zudem besteht grdsl. immer die Möglichkeit, einen ausfallenden Verkehrsträger durch andere zu ersetzen.

Lücken bezüglich der Versorgungssicherheit:

- Insgesamt existiert sehr wenig Regulierung, welche als Ansatzpunkt für IT-Sicherheitsspezifische Anforderungen/Maßnahmen dienen könnte.
- Das zuständige Fachressort (BMVBS) agiert als Unterstützer des offenen Marktes und versteht Auflagen zur Sicherstellung der Versorgung nicht als Priorität. Folglich existiert bei BMVBS auch keine tiefgreifende Transparenz bzgl. der Branchenstrukturen; und schon gar nicht bzgl. der IT-Sicherheitssituation.
- Seitens der Bundesregierung existieren keine branchenspezifischen Einwirkungsmöglichkeiten, da weitestgehend keine Aufsicht verankert ist.
- Für die Branche Logistik ist von einer hohen Abstützung auf das Internet auszugehen.

Organisationsgrad

Einzelne Mitglieder des Sektors sind aktiv im Umsetzungsplan KRITIS (UPK). Von einer repräsentativen Abdeckung aller Branchen ist man jedoch weit entfernt – ganz explizit die Airline-Betreiber scheuen bspw. eine freiwillige Teilnahme, weil sie eine Stigmatisierung als „Kritisch" und damit einhergehende Auflagen fürchten.

Entsprechend wäre die umfassende Etablierung von branchen- / sektorspezifischen Arbeitskreisen zum IT-Schutz mit Verzahnung zu den branchenübergreifenden UPK-Strukturen zu fordern.

Aktuelle Entwicklungen

- EU KOM (DG HOME) evaluiert in Zusammenarbeit mit den MS aktuell die EKI-Richtlinie (Europ. Kritische Infrastrukturen) von 2008, die Teil des Europ. Programms zum Schutz Kritischer Infrastrukturen (EPSKI) ist. In der Richtlinie wurden nur Regelungen für Energie und Transport/Verkehr getroffen. Die Evaluierung, die bis Ende 2012 angelegt ist, ist ergebnisoffen. Eine denkbare Zukunftsoption ist die Ausweitung auf andere Sektoren; im Vordergrund steht dabei die IKT. DE hält die bestehende Richtlinie für verfehlt und lehnt eine Ausweitung ab.
- Branche Luftfahrt: ein von der Wirtschaft entwickelter Standard auf Basis eines einschlägigen internationalen Standards zu IT-Sicherheit (sog. ISO27001) befindet sich aktuell in offizieller Anerkennung.
- Das Verkehrsleistungsgesetz befindet sich in Novellierung; das Seeaufgabengesetz soll bis Ende 2012 überarbeitet sein.

Stand: 31.05.2012

KRITIS-Sektor „Transport und Verkehr"

Teilnehmende Unternehmen

Name	Aktien-Index	Umsatz in Mrd. (2011)	Mitarbeiter (2011)	Hauptsitz	Mitglied UPK (Bezug Nr. 5)	Übungs-beteiligung (Bezug Nr.6)	Kurzbeschreibung
D[redacted]AG	-	38	285319	[redacted]	Ja	Ja	Das bundeseigene Unternehmen das größte Eisenbahnverkehrs- und Eisenbahninfrastruktur-unternehmen in Mitteleuropa. Mit zum Konzern gehören verschiedene Tochterunternehmen, die ebenfalls in verschiedenen Branchen des Sektors vertreten sind, z.B. [redacted]
D[redacted]AG	DAX	53	423348	[redacted]	Ja	Ja	Die D[redacted]AG ist das größte Logistik- und Postunternehmen weltweit. [redacted] (abgekürzt [redacted]) ist der Name, unter dem der Konzern seit 11. März 2009 in der Öffentlichkeit auftritt.
[redacted]	-	0,16	61500	[redacted]	*Nein*	*Nein*	[redacted] ist ein international tätiges Logistik- und Gütertransportunternehmen mit Hauptsitz in der [redacted]
D[redacted]	-	3,8	19250	[redacted]	*Nein*	*Nein*	[redacted] ist in den Geschäftsfeldern Europa-Logistik, der Luft- & Seefracht sowie der Lebensmittellogistik vertreten. Im Bereich der Kontraktlogistik werden neben Transport auch Lagerung und Mehrwertdienst-leistungen angeboten. Im Segment Systemlogistik gehört [redacted] zu den Weltmarktführern.
[redacted]	MDAX	2,1	19425	[redacted]	*Nein*	Ja	Die F[redacted]AG ist die börsennotierte Betreibergesellschaft des [redacted] F[redacted]ist an weiteren deutschen und ausländischen Flughäfen beteiligt.

Stand: 31.05.2012

Name	Aktien-Index	Umsatz in Mrd. (2011)	Mitarbeiter (2011)	Hauptsitz	Mitglied UPK (Bezug Nr. 5)	Übungs-beteiligung (Bezug Nr.6)	Kurzbeschreibung
D[redacted]AG	DAX	27	11019	[redacted]	*Nein*	*Nein*	Das Hauptgeschäftsfeld des weit gefächerten Luftfahrtkonzerns D[redacted]AG ist neben dem Frachtverkehr der Linienflugverkehr.
A[redacted]	-	3,7	9200	[redacted]	*Nein*	*Nein*	A[redacted] ist die zweitgrößte deutsche und sechstgrößte europäische Fluggesellschaft und verfügt mit Stand Mai 2012 über eine Flotte von 137 Flugzeugen.
D[redacted]	-	0,9	>5600	[redacted]	Ja	Ja	Die [redacted] ist als beliehenes Unternehmen Teil der Luftverkehrsverwaltung des Bundes und befindet sich im Eigentum der Bundesrepublik Deutschland, die durch das BMVBS vertreten wird. Die [redacted] ist vom BMVBS mit der Wahrnehmung hoheitlicher Aufgaben zur Flugsicherung beliehen.
H[redacted]	MDAX	1,2	4797	[redacted]	Ja	*Nein*	Die H[redacted] ist der börsennotierte Hafenbetreiber Hamburgs. Der [redacted]Konzern untergliedert seine Geschäftstätigkeit in die vier Segmente Container, Intermodal, Logistik und Immobilien.

Stand: 31.05.2012

Teilnehmende Verbände

Name	Angeschlossene Institutionen	Beschäftigte der angeschlossenen Institutionen	Hauptsitz	Mitglied UPK (Bezug Nr. 5)	Übungs-beteiligung (Bezug Nr. 6)	Kurzbeschreibung
D [redacted] e.V.	4000	-	[redacted]	*Nein*	*Nein*	Der [redacted] ist die Dachorganisation der Spediteure in Deutschland. Die angeschlossenen Speditionen erwirtschaften etwa 90 Prozent des bei circa 55 Milliarden Euro liegenden Branchenumsatzes (Stand 2009).
B [redacted]	10000	-	[redacted]	*Nein*	*Nein*	Der [redacted] ist der Spitzenverband des Transportlogistikgewerbes in Deutschland. Die Mitgliedsunternehmen betätigen sich schwerpunktmäßig in den Bereichen Straßengütertransport, Logistik, Spedition, Lagerung und Entsorgung.
Z [redacted] e.V.	-	-	[redacted]	*Nein*	*Nein*	Die wesentlichen Aufgaben des [redacted] sind die Vertretung der deutschen Seehäfen zur Verbesserung der Wettbewerbsfähigkeit, der Sicherung der Standortbedingungen mit Einbeziehung der Wasserwege, Straßen und Schienenanbindung und der Abschluss von Tarifverträgen für die Hafenarbeiter
Bu [redacted]	100	-	[redacted]	*Nein*	*Nein*	Der [redacted] vertritt derzeit ca. 90 Betreiber von Binnenhäfen in Deutschland. Als „Sprachrohr der deutschen Binnenhäfen" beteiligt sich der [redacted] am politischen Meinungsbildungsprozess.

Stand: 31.05.2012

Name	Angeschlossene Institutionen	Beschäftigte der angeschlossenen Institutionen	Hauptsitz	Mitglied UPK (Bezug Nr. 5)	Übungs-beteiligung (Bezug Nr. 6)	Kurzbeschreibung
B[redacted] e.V.	-	-	[redacted]	*Nein*	*Nein*	Der Verband vertritt zahlreiche Unternehmen der Luftfahrt-Branche. Darunter sind sowohl Flughäfen (Fraport, KölnBonn, …) als auch Fluggesellschaften (Lufthansa, AirBerlin, …) sowie Verbände (ADV - Arbeitsgemeinschaft Deutscher Verkehrsflughäfen) und die Deutsche Flugsicherung.
V[redacted]r e.V.	600	-	[redacted]	*Nein*	*Nein*	Im [redacted] sind die Unternehmen des öffentlichen Personennahverkehrs und des Güterverkehrs mit Schwerpunkt Eisenbahngüterverkehr in Deutschland organisiert.