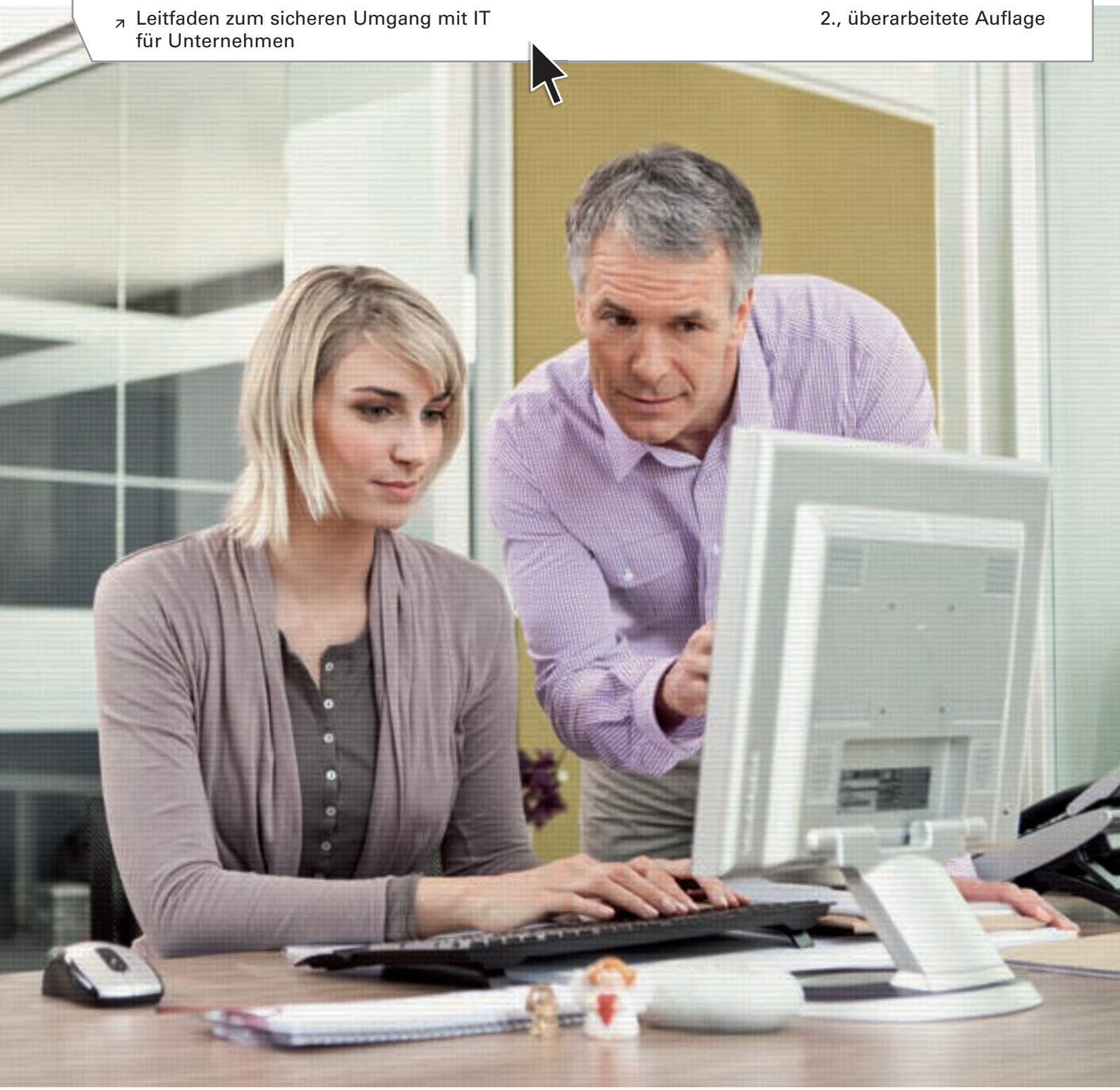
DATEV

Sicher im Netz

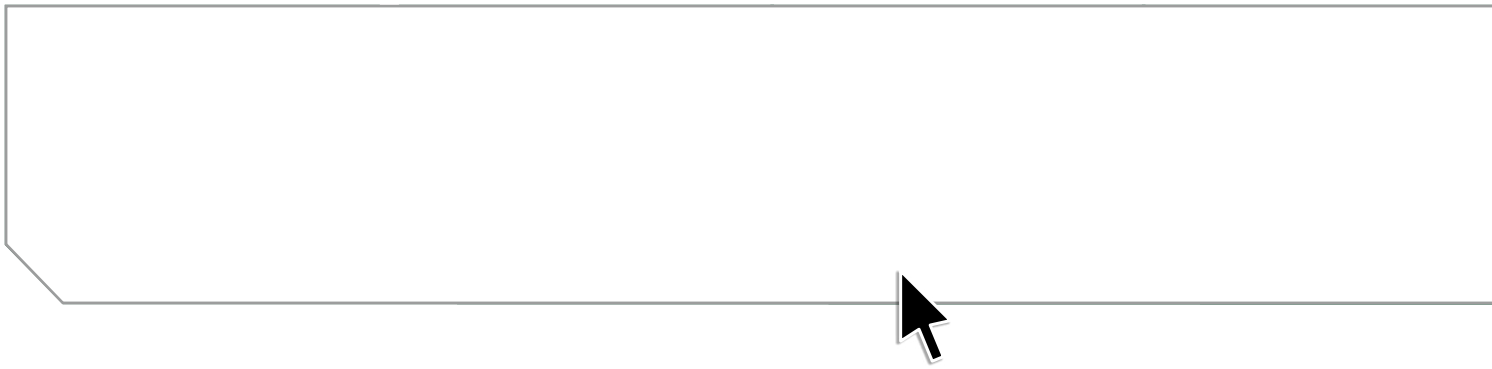
↗ Leitfaden zum sicheren Umgang mit IT für Unternehmen

2., überarbeitete Auflage



↗ Eine Informationsbroschüre von DATEV und Deutschland sicher im Netz e. V.

DsiN.de



Vorwort

Arbeiten über das Internet gewinnt zunehmend an Bedeutung. Für den elektronischen Geschäftsverkehr wird damit der Sicherheitsaspekt zu einem entscheidenden Punkt: Die firmenübergreifende Nutzung von IT und damit das Aufbrechen der Firmengrenzen erfordern einen flexiblen, aber dennoch sicheren Zugriff auf verteilte Daten und Dienste. Was folgt aus dieser Entwicklung? Das sichere Management der elektronischen Identitäten von Personen wird zu einer entscheidenden Aufgabe. Nur so kann Missbrauch verhindert und Rechtssicherheit erhalten bzw. gewonnen werden. Im betrieblichen und privaten Umfeld ist der sichere Umgang mit der digitalen Identität die wichtigste Herausforderung bei der IT-Sicherheit. Aktuelle Anwendungen, bei denen die digitale Identität eine Rolle spielt, kommen aus dem E-Government, E-Business, E-Justice und Social Networking.

Ohne Frage, der Nutzen digitaler Geschäftsprozesse liegt auf der Hand. Sie sind schnell, komfortabel, unabhängig und kostensparend. Der Trend ist unaufhaltsam – von Seiten des Staates und von Seiten des Marktes. Die Zahl der digitalen Identitäten wird stetig steigen und damit unsere Übersicht und Kontrolle erschweren. Internet-Dienste sind deswegen nicht in Frage zu stellen, man darf ihnen aber auch nicht blind vertrauen. Vielmehr gilt es, sich im Internet mit Vorsicht zu verhalten und die eigene Infrastruktur (PC, Netzwerk) sicherheitstechnisch zu optimieren. Das ist leider noch zu selten der Fall.

Hier wird auch staatliche Einflussnahme nur unterstützen können – selbst wenn zwei Projekte des Bundesministeriums des Innern zu einer erhöhten Sicherheit beitragen können: der elektronische Personalausweis und die sogenannte De-Mail. Der einzelne Nutzer und die Unternehmen müssen sich ihrer Verantwortung bewusst sein. Sachgerechte Informationen über Schutzmechanismen und neue Technologien sollen helfen, diese Bewusstseinsbildung aktiv zu fördern. Mit dieser Broschüre, die in Kooperation mit dem Verein „Deutschland sicher im Netz“ entstanden ist, wollen wir für die IT-Sicherheit sensibilisieren und die Kompetenz und Eigenverantwortung der Nutzer weiter stärken, indem nicht nur das Gefahrenpotenzial beschrieben wird. Konkrete Handlungsempfehlungen zeigen Wege auf, wie man sich sicherer im Netz bewegt.

Prof. Dieter Kempf

Sicher im Netz

Leitfaden zum sicheren Umgang mit IT für Unternehmen*

Teil 1 | Informationsgesellschaft und Medien – eine Gesellschaft im Wandel

01 | Marktplatz der Zukunft 8

- 1 Im Netz der Möglichkeiten 10
- 2 Die Plattform für Interaktion 12
- 3 Internet als Marktplatz 14

02 | Kriminalität im Internet 20

- 1 Internetkriminalität boomt 22
- 2 Wirtschaftsspionage 29
- 3 Angriff erfordert Gegenwehr 32
- 4 Ausblick in eine sichere Zukunft 32

Teil 2 | IT-Management im Unternehmen

01 | Sicherheitsvorkehrungen 36

- 1 Vom Papier zur Datei 38
- 2 Elementarschutz IT-Organisation 39
- 3 Internet 54
- 4 E-Mail-Verkehr 66
- 5 Mobile Endgeräte 72
- 6 Notfallkonzept 76
- 7 Rechtliches zum Datenschutz 79

Teil 3 | Digitale Korrespondenz

01 | Kommunikation online 86

- 1 Das Finanzwesen online 88
- 2 Der Staat online – E-Government 90
- 3 Privat online 101
- 4 Geschäftspartner online 103
- 5 Social Media 106

* Die Broschüre besteht aus vier unabhängigen Teilen.

Teil 4 | Technische Entwicklungen und deren Auswirkungen – Geschäftsprozesse im Wandel

01 | Mobile Computing in der Cloud 116

- 1 Neue Anforderungen 118
- 2 Cloud Computing 119

02 | Servicemodelle des Cloud Computings 128

- 1 Klassifizierung der Services 130
- 2 Virtualisierung 131
- 3 (Out-)Sourcing 132
- 4 Application Service Providing (ASP) 134
- 5 Managed Security Services 134
- 6 Hosting und Housing 134
- 7 Software on Demand 135
- 8 Software as a Service 136

03 | Mobilität – ein Muss 138

- 1 Voraussetzungen 140
- 2 Mobilität als Standard 141
- 3 Wandel auf drei Ebenen 142
- 4 Gefährdungen 143
- 5 Folgen bei Infektion 152
- 6 Tipps und Lösungsansätze 154

04 | Informationen im Netz 156

- 1 DATEV Sicherheitscheck 158
- 2 Deutschland sicher im Netz e. V. 158
- 3 Leitfäden des BITKOM 159
- 4 BSI für Bürger 160
- 5 Das Bürger-CERT 161

Informationsgesellschaft und Medien – eine Gesellschaft im Wandel

Teil 1

In den vergangenen zwanzig Jahren hat die Entwicklung der Informations- und Kommunikationstechnik die Art und Weise, wie wir leben und arbeiten, dramatisch verändert. Der Mikrocomputer, heute besser bekannt als „PC“, trat seinen Siegeszug an. Später begann sich das Internet langsam zu entwickeln. Heute ist der Einsatz dieser Technik selbstverständlich geworden und aus dem Alltag praktisch nicht mehr wegzudenken. Der klassische Telefonanschluss und Brief auf Papier werden dadurch ebenso abgelöst wie Musik- und Videoangebote auf den bisher üblichen Datenträgern. Die großen Trends Cloud Computing und Mobile Computing verändern nachhaltig und unumkehrbar die internationaler werdenden Geschäftsprozesse.

Dabei ist die absolute Blütezeit des Internets noch nicht erreicht: Tourismusbranche, Versandhandel, Handwerkerportale, Medien, Polizei, Ämter, Versicherungen und beispielsweise Banken haben gerade erst begonnen, sich richtig auf den Geschäftsbetrieb im Internet einzustellen.

Wie bei allen bahnbrechenden Entwicklungen kann sich niemand mehr, vor allem aus wirtschaftlichen Gründen, dem Einsatz des Internets als Plattform für den elektronischen Geschäftsverkehr entziehen. Um das vorhandene Potenzial auszuschöpfen, müssen Unternehmen, öffentliche Institutionen und Bürger ihre Kompetenzen noch weiter ausbauen.

1 Im Netz der Möglichkeiten
2 Die Plattform für Interaktion
3 Internet als Marktplatz

01 | Marktplatz der Zukunft

Der Marktplatz: seit jeher Zentrum gesellschaftlichen und geschäftlichen Lebens. Ob im Handel oder für den Staat – das Internet gewinnt an Bedeutung. Über kurz oder lang werden wesentliche Teile des geschäftlichen Lebens nur noch im Internet stattfinden. Der Nutzen digitaler Geschäftsprozesse liegt auf der Hand: schnell, komfortabel und kostensenkend. Ideal also in Zeiten globaler Wirtschaft – ginge damit nicht mit gleicher Intensität die professionelle Kriminalisierung des Webs einher. Dem gilt es zu begegnen: mit der ständigen Weiterentwicklung der Online-Sicherheit.

1 Im Netz der Möglichkeiten

Von der Privatperson über den Unternehmer bis hin zum Staat profitieren alle von den vielen Chancen, die das Netz eröffnet, können sich allerdings aber auch nicht den negativen Entwicklungen entziehen. Der Staat setzt zunehmend auf das Internet als Medium, unterstützt durch die Breitbandverkabelung: EHUG (elektronisches Handels- und Genossenschaftsregister), ELSTER (elektronische Steuererklärung), „De-Mail", elektronisches Mahnverfahren, EGVP (elektronisches Gerichts- und Verwaltungspostfach) sind da nur einige aktuelle Beispiele.

Für einen Unternehmer kann das konkret bedeuten:
Wer künftig im Wettbewerb bestehen möchte, sollte sich zeitig mit den neuen Verfahren und der zugrunde liegenden technischen Entwicklung auseinandersetzen. Auch, um drohendes Gefahrenpotenzial zu umgehen: Im fremden Namen eingereichte UStVA (Umsatzsteuer-Voranmeldung), der Bank falsch übermittelte Finanzdaten, eine Homepage, die Viren verbreitet, üble Nachrede im Internet, fehlende Werbung auf dem elektronischen Marktplatz oder entgangene Ausschreibungen.

Schöne neue Welt: das Unternehmen im Netz

Umdenken ist gefragt, für Unternehmer und Mitarbeiter. Vor allem müssen sie für den Umgang mit neuen Prozessabläufen verstärkt sensibilisiert werden.

In dieser neuen, digitalen Welt gilt es, sich den neuen Gegebenheiten anzupassen. Und das heißt: Umdenken ist gefragt, für Unternehmen und Mitarbeiter.
Einerseits erfordern die neuen Bedingungen eine völlig neue Vermarktung der Leistung, andererseits bergen neue Verfahren, Methoden und Technik auch neue Risiken. Hier stehen Unternehmer und ihre Mitarbeiter gleichermaßen im Fokus: Neue Technik muss richtig eingesetzt werden. Unbedarfte sind mit der Einrichtung und Bedienung verzahnter und moderner Software schnell überfordert. Gerade durch den sorglosen Umgang mit dem Internet geraten sie verstärkt in das Fadenkreuz der „Bad Boys" im Netz: Ein falscher Klick führt schnell in die Kostenfalle. Vor allem die Mitarbeiter müssen also in puncto „typische Fallen und Angriffsmuster" sensibilisiert werden.

Neue Sicherheitsvorkehrungen für neue Anforderungen

Trotz zahlreicher Datenschutzskandale: Der Nutzen digitaler Geschäftsprozesse liegt auf der Hand. Sie sind schnell, komfortabel, unabhängig und kostensparend. Der Trend ist unaufhaltsam – von Seiten des Staates und von Seiten des Marktes. Denn auch immer mehr Firmen bieten die Geschäftsabwicklung via Internet an. Traditionelle, eher räumlich orientierte Schutzmaßnahmen sind nicht mehr ausreichend. Für elektronisch gespeicherte Kunden- und Lieferantendaten oder die E-Mail-Kommunikation müssen die Schutzmechanismen angepasst werden.

Weil traditionelle Schutzmaßnahmen nicht mehr greifen, müssen neue etabliert werden.

Vorsicht im Internet

Im Web lauern viele Gefahren, zum Beispiel durch:

- Viren, Würmer und andere Schadsoftware
- Phishing
- Datenspionage
- Hackerangriffe
- Spam-Mails
- Botnetze und Cyberkriminalität

Bereits einfache Maßnahmen helfen, um grundlegend geschützt zu sein. Eine Übersicht der wichtigsten Elemente finden Sie im Teil 2, Kapitel 2 „Elementarschutz IT-Organisation“ (S. 39).

2 Die Plattform für Interaktion

Eine Welt ohne Internet? Kaum mehr vorstellbar. Im weltweiten Netz spielt sich ein immer größerer Teil unseres Lebens ab – geschäftlich wie privat. Diese Umstellung in der Kommunikation führt auch in kriminellen Kreisen fast zwangsläufig zu einer entsprechenden Umstellung im Handeln. Eine Veränderung, die angepasster Sicherheitsvorkehrungen bedarf. Daher liegt die Herausforderung der Zukunft in der Absicherung der vernetzten Systeme.

Webciety – die vernetzte Gesellschaft

Webciety steht für eine Gesellschaft, die sich unter dem Einfluss der Vernetzung vollkommen neu organisiert.

Im Internet gelten andere Regeln als in der realen Welt. Das erlernte Gespür für den Umgang miteinander, gesellschaftliche Gepflogenheiten und Kultur oder staatliche Rahmenbedingungen verlieren in der virtuellen Welt an Bedeutung. Hier treffen verschiedene Kulturen und Staaten aufeinander, unterschiedliche Rechtssysteme und Gepflogenheiten unterschiedlichster Länder und Gruppierungen. Was bisher erlernt wurde und als Orientierungshilfe diente, wie Aussehen, Kleidung, Geschlecht, örtliche Gegebenheiten, liegt nicht mehr vor. Der Marktplatz und der Eindruck seines Umfeldes sind nicht mehr transparent.

Web 2.0 – das „Mitmach-Medium" für geschäftliche Beziehungen

Web 2.0 steht für den Übergang vom Informationsmedium zur interaktiven Plattform.

Auch das Internet entwickelt sich weiter. So kennzeichnet das Schlagwort „Web 2.0" den Übergang vom Recherche- und Informationsmedium hin zu einer interaktiven Plattform, auf der mehr als nur Wissen ausgetauscht wird. Es ist das Medium für die digitale Wirtschaft: das E-Business.

Ein wesentlicher Aspekt dafür ist die Verwendung „Aktiver Inhalte", die die Interaktion erst ermöglichen. Die Internet-Seiten werden damit nicht mehr allein zur Darstellung von fest vorgegebenen Inhalten verwendet, sondern auch zum Austausch multimedialer Informationen und Diskussionen etc.

Kritisch für Unternehmen kann sich dabei die zunehmende Bedeutung von Foren und Blogs entwickeln. In diesen virtuellen Treffpunkten werden Kommentare zu Produkten und Dienstleistungen abgegeben und Meinungen ausgetauscht. Hier ist es für ein Unternehmen entscheidend, die Diskussion nie aus den Augen zu verlieren. Denn negative Kommentare schlagen sich oft auf die Verkaufszahlen nieder. Besonders perfide, wenn ein Wettbewerber die oft anonym eingestellten Beiträge nutzt, um einen unliebsamen Konkurrenten in Misskredit zu bringen.

Wer im Internet unterwegs ist, macht sich angreifbar. Doch genau darin unterscheidet es sich in keiner Weise von den traditionellen Risiken. Gefahren lauern nicht nur durch schädliche Software, sondern auch durch ganz „normale" Kriminelle: Ein Online-Geschäftspartner verschwindet plötzlich oder Verträge werden einfach nicht erfüllt.

Sicherheit im Web 2.0 – „Aktive Inhalte“[1]

„Aktive Inhalte“ sind eigenständige Programme, die beim Aufruf einer Internetseite ausgeführt werden. Was so harmlos klingt, ist oft die Eintrittskarte für Viren oder Spionageprogramme. Besonders ärgerlich ist jedoch, dass insbesondere die Angebote im Web 2.0 darauf aufbauen. Grundsätzlich können diese per Einstellung im Internet-Browser gesteuert werden. So können aktive Inhalte auf vertrauenswürdigen Seiten explizit erlaubt und für alle übrigen Seiten deaktiviert werden. Wichtig dabei: Nicht alle populären Seiten sind automatisch vertrauenswürdig.

Foren, Blogs, aktive Inhalte etc. – willkommene Ansatzpunkte für die „Bad Boys“ im Netz.

[1] www.bsi-fuer-buerger.de/ContentBSIFB/SicherheitImNetz/WegInsInternet/DerBrowser/AktiveInhalte/aktiveinhalte.html

3 Internet als Marktplatz

Das Internet ist aus dem Wirtschaftskreislauf nicht mehr wegzudenken. Längst geht es nicht mehr nur darum, dass Bücher, CDs oder andere Waren über das Netz bestellt werden. Auch die Unternehmen arbeiten mit ihren Partnern und Zulieferbetrieben eng über das Netz zusammen. Die Gefahr, dass hier sensible Daten eingesehen werden können oder gar gestohlen werden, ist deutlich angestiegen.

Online-Shopping und E-Commerce

E-Commerce steht für elektronischen Handel im Rahmen der Internetwirtschaft.

Der elektronische Marktplatz bietet Chancen, auch künftig im Wettbewerb zu bestehen. Doch durch die Globalisierung gibt es hier auch Risiken: Im realen Leben ist das Vortäuschen falscher Tatsachen oder einer fremden Identität wesentlich schwieriger als im Internet. Ein bestehender Geschäftspartner ist bei wiederholten Kontakten an seinem Gesicht, seiner Stimme oder seiner Unterschrift zu erkennen. Im Internet ist dies etwas schwieriger, aber ebenfalls möglich! Der Trend ist jedoch eindeutig: Der elektronische Einkauf verzeichnet hohe Zuwächse. Die Vorteile des Online-Shoppings liegen auf der Hand: Ausgiebiges Stöbern vom eigenen Wohnzimmer aus, unkompliziertes Bestellen per Mausklick – und die Lieferung erfolgt praktisch aus allen Teilen der Welt.

Wo Licht ist, ist auch Schatten

Mit der zunehmenden Beliebtheit des Online-Shoppings wird auch das Online-Bezahlen und damit das Online-Banking immer populärer. Im gleichen Maße gewinnt das Thema Sicherheit an Bedeutung: Fast drei Viertel der Fälle mit Internet als Tatmittel entfallen derzeit auf Betrugsdelikte. Aber nicht jeder trifft Vorsichtsmaßnahmen. Bereitwillig werden persönliche Angaben preisgegeben und AGBs oder Datenschutzeinstellungen ignoriert. Dabei scheint den Betroffenen nicht klar zu sein, dass die Eingaben nicht automatisch der deutschen Rechtsprechung und den deutschen Datenschutzregelungen unterliegen. Auch ist nicht sichergestellt, wo die Daten gespeichert und verarbeitet werden – und damit ist man vor Missbrauch nicht gefeit.

Wer nur auf den Preis achtet, den kann dies schnell teuer zu stehen kommen.

Problematisch im E-Commerce sind mitunter mangelhafte Sicherheitsvorkehrungen auf Seiten der Anbieter, auch resultierend aus neu entstandenen IT-Möglichkeiten. In Verbindung mit der Professionalität der Internetkriminellen stellt dies im Geschäftsverkehr für beide Seiten ein erhöhtes Risiko dar.

Wer Angebote im Internet nutzt, muss damit rechnen, dass der Geschäftspartner

- seine Pflichten als Vertragspartner nicht erfüllt, z. B. gekaufte Waren nicht liefert
- persönliche Daten oder Zahlungsinformationen (z. B. Kreditkartenangaben) missbraucht.

Risiko minimieren, Sicherheit maximieren

Doch gibt es einfache Maßnahmen, das mögliche Risiko zu reduzieren. Prüfen Sie im Vorfeld Ihren Geschäftspartner durch Referenzen, Empfehlungen oder Online-Gütesiegel[2] – bei vertrauenswürdigen und renommierten Anbietern eine Selbstverständlichkeit.

Ist eine Eingabe von Kontendaten erforderlich, sollte die Adresszeile im Browser geprüft werden: Bei Internetseiten, die mit „https://" beginnen, wird die Übertragung der Informationen verschlüsselt. Die eingegebenen Daten können somit nicht mitgelesen werden. Darüber hinaus wird beim Aufruf der Seite auch deren Echtheit geprüft.[3]

Einige Verhaltensweisen verbessern die Sicherheit im Online-Handel[4]

Bei seriösen Seiten sind beispielsweise folgende Angaben enthalten:
- Klare Identifizierung des Unternehmens durch Kontaktangaben.
- Vertragsbedingungen, Leistungen und ggf. Garantiebedingungen sind leicht zugänglich und verständlich.
- Der tatsächliche Endpreis wird genannt, ggf. mit aufgeschlüsselten Kosten.
- Es wird eine sichere Zahlungsmethode angeboten.
- Bestellungen werden per E-Mail bestätigt.
- Auf das Widerrufsrecht wird deutlich hingewiesen.
- Die Lieferzeit wird angegeben.

Homepage – Werbung in eigener Sache

Das Internet hat sich in kürzester Zeit zu einem Massenmedium entwickelt. Das Informationsverhalten verändert sich, weg von Prospekten und Papier, hin zum Stöbern auf Angebotsseiten, in Testberichten und Foren. Um das vermeintlich günstigste Produkt zu finden, werden Preis-Suchmaschinen eingesetzt. In diesen Zeiten ist eine eigene Unternehmens-Homepage bereits „Stand der Technik". Die Marktmacht von beispielsweise Google ist nicht zuletzt auf seinen frühzeitigen Markteinstieg und seine Orientierung am neuen Suchverhalten der Internetgemeinde zurückzuführen. Mit einer eigenen Homepage oder zumindest auf einem Angebotsportal im Internet vertreten zu sein, wird zunehmend wichtiger. Umso erstaunlicher ist es, dass im Zeitalter des Internets viele kleine und mittelständische Firmen immer noch keine eigene Seite besitzen, obwohl diese nachweislich einen positiven Einfluss auf Umsatzentwicklung und Kundenkommunikation hat.

[2] www.internet-guetesiegel.de

[3] www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/WegInsInternet/DerBrowser/SSL/ssl_node.html

[4] www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/e-commerce/tipps.html

Die Homepage als Marketing-Instrument

Die eigene Homepage wird zum wichtigen Marketing-Instrument.

Eine eigene Homepage kann im Vergleich zu anderen Marketing-Instrumenten sogar wirtschaftlicher sein. Der Grund hierfür ist, dass eine Internetseite weltweit und rund um die Uhr verfügbar ist und dass ihre Reichweite verhältnismäßig hoch im Vergleich zum relativ geringen Kostenaufwand ist. Daher eignet sich dieses Online-Marketing-Instrument gerade für kleine und mittelständische Unternehmen mit begrenztem Budget besonders gut.

Die eigene Homepage muss dabei keine ausgefeilte Multimedia-Show sein. Im Gegenteil: Die wichtigsten Informationen sollten Sie kurz und prägnant in einer einfachen und eingängigen Struktur darstellen. Wer bereits auf seiner Seite mit dem potenziellen Kunden in Kontakt treten möchte, hat natürlich mit etwas mehr Aufwand zu rechnen. Dabei sollte jedoch grundsätzlich auf den Sicherheitsbedarf der Kunden Rücksicht genommen werden: Ist die Kontaktaufnahme per E-Mail gewünscht, genügt oft die Angabe einer E-Mail-Adresse. Sollen hier jedoch bereits konkrete Informationen über Spezifikationen, Auftragskonditionen oder persönliche Angaben gemacht werden, müssen zusätzliche Sicherheitsvorkehrungen getroffen werden. Eine gewöhnliche E-Mail, also ohne Signatur (= Zertifikat), kann technisch ohne große Probleme auf ihrem Weg vom Absender zum Empfänger so modifiziert werden, dass weder Inhalt noch Absender etc. korrekt übermittelt werden. Sie ist für den Geschäftsbetrieb mehr oder weniger wertlos. Gute Fälschungen sind rein technisch nicht festzustellen. Der Einsatz einer digitalen Signatur, vorzugsweise mittels SmartCard, beseitigt dieses Manko.

Zertifikate sorgen für mehr Seriosität von Angebot und Nachfrage.

Die Kontaktaufnahme ist jedoch auch direkt auf der Homepage möglich und sollte grundsätzlich mit verschlüsselten Seiten – beginnend mit https:// – angeboten werden.[5] Das Zertifikat zur Echtheitsprüfung der Seite wird automatisch im Browser angezeigt.

Beim Gang ins Internet ist einiges zu beachten

Die verstärkten Abmahnwellen bei zu unbedarfter Nutzung des Internets in den letzten Jahren sind ein deutliches Zeichen für fehlendes Know-how im Umgang mit dem neuen Medium – und mussten von den Anbietern bzw. Besitzern von Homepages vielfach teuer bezahlt werden. Auch die Kunden im Internet wurden oft für Betrug seitens der Anbieter zur Kasse gebeten. Doch auch hier wurden Fortschritte erzielt: Heute können die Anbieter im Internet beispielsweise durch Impressum und Hinweis auf den Datenschutz etc. auf ihre Seriosität überprüft werden.

Suchmaschinen finden angreifbare Lücken.

Doch nicht nur Rechtsvorschriften für die Pflichtangaben sind zu beachten. Immer wieder werden beliebte Internet-Auftritte von Kriminellen manipuliert. Die Absicherung gegen Manipulation der Inhalte ist daher von großer Bedeutung: Verwundbare Seiten lassen sich beispielsweise via Google leicht aufspüren und können dann verändert oder mit Viren versehen werden.

Grundsätzlich sollte bei der Auswahl der Software, der Agentur und des Providers für den Internet-Auftritt die gleiche Sorgfalt gelten wie für andere eingekaufte Produkte des Geschäftsbetriebes.

[5] vgl. Kapitel 3 „Internet als Marktplatz“, S. 14 ff.

Die digitale Identität

Wer als Kunde am Online-Banking teilnimmt, bei Online-Shops einkauft, Internet-Marktplätze oder auch die Kommunikation via Handy oder E-Mail nutzt, besitzt eine digitale Identität. Im Internet steht sie stellvertretend für die Präsenz einer natürlichen oder juristischen Person.
Oft ist die Identität lediglich durch ein Passwort abgesichert. Wer dieses kennt, kann im Namen eines anderen auftreten – mit all den Konsequenzen, die damit verbunden sind: Der eigene Ruf bzw. die Bonität stehen auf dem Spiel!

Der Schutz der eigenen digitalen Identität ist im Internet überlebenswichtig!

Identität absichern

Wird die digitale Identität allzu leichtfertig an falscher Stelle eingegeben, kann sie „gestohlen" werden: Es werden regelmäßig Internetseiten von Online-Shops, Banken etc. gefälscht (Phishing, Pharming), um den unbedarften Surfer zur Eingabe seiner Daten zu bewegen.

Beim Versenden einer E-Mail kann die Identität des Absenders in Form einer elektronischen Signatur hinzugefügt werden. Diese entspricht der digitalen Unterschrift des Absenders. So kann das E-Mail-Programm des Empfängers prüfen, wer tatsächlich der Absender der E-Mail ist, und ob die E-Mail unverfälscht übermittelt wurde.

Sicher durch SmartCard

Wesentlich mehr Sicherheit bietet eine „SmartCard", die auch als Signatur-Karte bezeichnet wird. Bei dieser wird nicht nur ein Passwort (hier: PIN) zur Nutzung benötigt, sondern die Karte muss auch physisch verfügbar sein. Hier wirken die Aspekte „Besitz und Wissen" als Sicherheitsplus zusammen. Im Gegensatz zu den „Magnetkarten", die für Abhebungen oder Bezahlung an Kassensystemen verwendet werden, kann die auf den SmartCards enthaltene Information nicht ohne Weiteres kopiert werden. Damit entspricht sie in etwa der Rolle des elektronischen Personalausweises.

Eine SmartCard bietet mehr Sicherheit zum Schutz der „Digitalen Identität".

Durch das vorgeschriebene Ausgabeverfahren wird eine Identifikation des Inhabers durchgeführt. Die so erhaltene digitale Identität unterstützt die Seriosität im Umgang mit Geschäftspartnern: Die im Internet nicht sichtbaren Personen können sich so durch Vorlage dieses digitalen Ausweises authentifizieren.

Grundsätzlich gibt es zwei Arten der digitalen Identität, die sich im Hinblick auf ihre Sicherheit(-smöglichkeiten) unterscheiden:

- Passwortschutz:
  Eine reine Wissenskomponente, die abhanden kommen kann. Eine Feststellung der tatsächlichen, analogen Identität mit der digitalen wird nicht zwingend durchgeführt.
- SmartCard:
  Eine Wissens- und Besitzkomponente, bei der eine Identifikation mittels Post-Ident-Verfahren durchgeführt wird. Ein Abgleich zwischen analoger und digitaler Identität wird durchgeführt.

Perspektiven für die Wirtschaft

Mit der Einführung der EDV wurden bis dato manuelle Prozessabläufe stark beschleunigt und damit die anzusetzenden Kosten für Leistungen stark reduziert. Ein echter Wettbewerbsvorteil. Das Internet seinerseits kann die vorhandenen Arbeitsabläufe aber noch weiter beschleunigen und ist deshalb zu einem unverzichtbaren Instrument in der modernen Wirtschaft geworden.

In erster Linie betrifft dies die elektronische Kommunikation: Für einen Brief wird derzeit eine Laufzeit von ca. 3 Tagen angesetzt. Die Übermittlung einer E-Mail findet dagegen in der Regel im Sekundenbereich statt.

Im Zeitalter des Web 2.0 verändern sich auch die Formen der Kooperationen durch die Internet-Zusammenarbeit. Bestellt und bezahlt wird „online". Die Präsentation des eigenen Unternehmens, die Recherche von Leistungen, Geschäftspartnern oder Konkurrenten und die Abwicklung von Rechtsgeschäften im Internet werden zunehmend wichtiger. Diese veränderte Arbeitsweise und ebenso das veränderte Informationsverhalten haben auch Auswirkung auf die Werbung: Die Ausgaben für Print-Werbung können so deutlich reduziert werden.

Im Gegensatz zum Personalausweis besitzt die digitale Identität kein Gesicht und ebensowenig eine körperliche Präsenz.

Je mehr der persönliche Kontakt durch elektronische Medien ersetzt wird, desto wichtiger ist der Schutz der digitalen Identität. Grundsätzlich sollte sehr sparsam mit Angaben über die eigene Person umgegangen werden: Je mehr Informationen zu einer Person vorliegen, desto leichter kann von Kriminellen eine falsche Identität vorgespiegelt werden.

Digitale Zukunftschancen für viele Anwendungen

Ein Zertifikat ermöglicht die rechtsverbindliche Authentifikation.

Die Anwender können immer mehr Prozesse digital abwickeln. Die Authentifikation mittels SmartCard ebnet Unternehmen auch den Zugang zu Online-Angeboten von Behörden, aber auch die digitale Kommunikation mit Ämtern und Gerichten. Stichwort ELSTER: Im Rahmen solcher E-Government-Anwendungen können bzw. müssen Unternehmen beispielsweise die elektronische Steuererklärung oder ihre Umsatzsteuer-Voranmeldung einreichen. Die Lohnsteuer-Anmeldung ist ebenfalls möglich.

Insbesondere der elektronischen Übermittlung von Rechnungen, dem E-Billing, bescheinigen Experten eine große Zukunft. Rechnungen werden digital erstellt, übermittelt und weiterverarbeitet. Papier wird nicht mehr benötigt. Die Echtheit der Herkunft und die Unversehrtheit des Inhaltes müssen gewährleistet sein (durch jegliche innerbetriebliche Kontrollverfahren, die einen verlässlichen Prüfpfad zwischen Rechnung und Leistung schaffen können; UStG §14 Abs. 1). Unbeschadet dieser zulässigen Verfahren kann dies auch mittels qualifizierter elektronischer Signatur oder elektronischem Datenaustausch erfolgen (UStG §14 Abs. 3).

Wachsendes Sicherheitsbewusstsein

Die positive Nachricht: Das Sicherheitsbewusstsein der Anwender wächst. Virenscanner und Firewall als Grundausstattung haben sich etabliert. Auch die Notwendigkeit regelmäßiger Updates sehen immer mehr Anwender. Doch um Art und Umfang von Sicherheitsmaßnahmen einschätzen zu können, sind Hintergrundinformationen zum Vorgehen und den Trends der Schattenwirtschaft notwendig.

Diese Broschüre versucht, relevante Entwicklungen besonders im Umfeld der kleinen und mittleren Unternehmen (KMU) aufzuzeigen und die wichtigsten Maßnahmen zu skizzieren. Häufig wird vergessen, dass das eigene Unternehmen mit Kunden und Lieferanten – mehr oder weniger – per EDV verknüpft ist. Der Schutz des eigenen Unternehmens und der eigenen Infrastruktur dient auch dem Schutz der Kundenbeziehung und umgekehrt. Besonders bedeutsam ist dabei, dass die wichtigsten Maßnahmen sich gerade dadurch auszeichnen, dass sie mit wenig Aufwand durchgeführt werden können. Die sich regelmäßig verbreitenden Viren sind leider ein Beispiel dafür, dass offensichtlich viele Nutzer selbst die bereits veröffentlichten Sicherheitslücken nicht oder nicht zeitnah mit den vorhandenen Sicherheitsupdates schließen.

Fazit

Grundsätzlich spricht nichts dagegen, das Internet geschäftlich oder privat als virtuellen Marktplatz zu nutzen. Wer mit dem Internet arbeitet, muss nur die Sicherheitsvorkehrungen an die Eigenarten des Mediums anpassen. Beispielsweise beim Besuch von unbekannten Internetseiten sollten diese zunächst auf ihre Seriosität überprüft werden.

Beim Gestalten der eigenen Homepage sollte darauf Wert gelegt werden, dass diese vor Manipulation sicher ist und gegebenenfalls eine abgesicherte Kontaktaufnahme unterstützt. Die Pflichtangaben schützen vor einer möglichen Abmahnung. Die digitale Identität sollte in besonderer Weise, am besten durch die Verwendung einer SmartCard, geschützt werden.

Grundsätzlich müssen bei allen digitalen Prozessen die sicherheitsrelevanten Ziele Verfügbarkeit, Vertraulichkeit und Integrität gewahrt sein. Eine Übersicht der wichtigsten Elemente finden Sie im Teil 2, Kapitel 2 „Elementarschutz IT-Organisation“ (S. 39).

1 Internetkriminalität boomt
2 Wirtschaftsspionage
3 Angriff erfordert Gegenwehr
4 Ausblick in eine sichere Zukunft

02 | Kriminalität im Internet

Die Computerkriminalität ist längst zum Alltag geworden. Sie reicht von der Software-Piraterie über das Ausspähen von Daten bis hin zur Fernsteuerung gekaperter PCs. Das Auftreten in fremdem Namen und auf fremde Rechnung kann für den Betroffenen existenzbedrohend werden. Der Schaden für die Wirtschaft ist dabei immens – ganz zu schweigen vom Verlust der Vertraulichkeit sensibler Daten. Dabei werden die Tricks der Computerkriminellen immer einfallsreicher. Gut, wenn man darauf vorbereitet ist.

1 Internetkriminalität boomt

Wirtschaftskriminalität ist keine Erfindung aus dem Internetzeitalter. Doch leider gewinnen die internetbasierten Angriffe zunehmend an Bedeutung. Dies liegt nicht zuletzt an den Vorteilen und der größeren Verbreitung des Mediums. Räumliche Abstände schrumpfen; mit einen Klick ist man an jedem Winkel der Welt. Ein Eldorado für alle, die diese Technik besser beherrschen als der gelegentliche Nutzer. Denn das Internet macht keinen Unterschied zwischen Gut und Böse. Ebenso wie beispielsweise Banken, Touristik oder staatliche Stellen durch den Einsatz der neuen Technik Kosten sparen, wird es auch für die Schattenwirtschaft einfacher und lukrativer, Umsätze zu erwirtschaften.

Angriffe nehmen zu

Angesichts der verschärften Konkurrenzsituation auf dem Weltmarkt gewinnen sowohl die Wirtschaftsspionage als auch ihre erfolgreiche Abwehr an Bedeutung.[6]

Der Schutz, durch die Masse als Einzelner unterzugehen, geht über in das Risiko, als einer von vielen im Netz der Bad Boys im Internet hängen zu bleiben. Schadprogramme wie Trojaner, Würmer oder Viren stehlen Daten, löschen Dokumente und spähen Konto- und Kreditkartennummern aus, ohne dabei Standesunterschiede zu machen. Es wird mitgenommen, was sich gerade bietet. Natürlich gibt es auch – wie in der „analogen Welt" – die großen Fische. Diese warten nicht erst, bis sich eine Gelegenheit ergibt. Sie schaffen Gelegenheiten: gezielte Angriffe auf lohnende Ziele.

Schaden in Milliardenhöhe

Und das Potenzial ist riesig: Verbrauchern und Unternehmen entsteht allein durch Malware[7] geschätzt weltweit ein Schaden von ca. 7 Mrd. Euro pro Jahr; der Schaden durch Wirtschaftsspionage ist deutlich höher. Die Dunkelziffer dürfte weit höher liegen, denn ein Schaden muss überhaupt erst einmal entdeckt und zudem gemeldet werden. Hinzu kommt noch, dass Betroffene ungern durch einen Sicherheitsvorfall von sich reden machen wollen.

Sicherheitssoftware und -updates sind grundlegende Maßnahmen gegen Angriffe.

Die Angreifer entwickeln dabei immer raffiniertere Methoden, um an die Daten zu kommen. In den meisten Fällen profitieren sie aber von Nachlässigkeiten und Sicherheitslücken auf Seiten der angegriffenen Firmen: Bei Untersuchungen konnte immer wieder festgestellt werden, dass Schäden durch kompetente Pflege der Sicherheitssoftware und die Installation von Sicherheitsupdates hätten vermieden werden können.

Gut bezahlte Jobs im Cybercrime

Dieser Wirtschaftszweig blüht auch in Krisenzeiten: Das Schreiben von Hacker-Programmen ist zum einträglichen Geschäft geworden. Dabei werden die Cyberkriminellen immer professioneller. Mittlerweile werden ganz unverhohlen hoch qualifizierte Studienabgänger und IT-Freaks von der Schattenwirtschaft mit Stellenausschreibungen im Internet angeworben.

Die Verlockung ist groß: Als Hacker-Programmierer lässt sich schnell viel Geld verdienen. Durch Auftragsarbeiten ist zudem das Risiko, entdeckt zu werden, vergleichsweise gering. Dazu kommt die Lage auf dem Arbeitsmarkt. Wer keinen oder einen nur schlecht bezahlten Job hat, ist für solche Angebote anfälliger.

[6] www.verfassungsschutz.de: Verfassungsschutzbericht, Abschnitt „Spionage und sonstige nachrichtendienstliche Aktivitäten", Kap. VII, „Wirtschaftsschutz"

[7] vgl. „Schutz vor Malware", S. 44

Bereits zur Tagesordnung der Cyberkriminellen gehört der Handel mit Sicherheitslücken, Kredit- und Online-Banking-Daten sowie Passwörtern. In der Schadenshöhe stehen Konkurrenzausspähungen sowie echte Wirtschaftsspionage durch ausländische Geheimdienste an erster Stelle – auch wenn hier lohnende Ziele begrenzt sind.

Sensibler Umgang mit sensiblen Daten

Moderne Kommunikationsmittel erlauben es, unbemerkt sensible Daten aus Unternehmen zu schleusen. Firewall und Antivirensoftware bieten keinen wirkungsvollen Schutz dagegen. Denn dies ist auch nicht ihre Aufgabe. Schutz gewährleisten beispielsweise Zugriffsberechtigungen und organisatorische Maßnahmen[8]. Aber auch schlichtweg nachlässiger oder schlecht geschulter Umgang der Mitarbeiter mit den zur Verfügung gestellten IT-Systemen und -Anwendungen birgt eine große Gefahr für die Vertraulichkeit und Integrität von Daten. Vielfach werden IT-Sicherheitsmaßnahmen aus einem mangelnden Sicherheitsbewusstsein heraus nicht beachtet. Umfangreich getätigte, kostspielige Sicherheitslösungen werden somit unterlaufen. Die im Vordergrund stehenden technischen Vorkehrungen zum Schutz gegen Hacker müssen daher durch die Sensibilisierung der Mitarbeiter, aber auch durch strikte Vorgaben zum sensiblen Umgang mit Daten ergänzt werden.[9]

Wer nicht feststellen kann, ob er angegriffen wird, kann sich auch nicht vor Angriffen schützen! Dies gilt selbst beim Einsatz von Virenscanner und Firewall.

Trügerische IT-Sicherheit

Die größten Fehler bei Sicherheitsvorkehrungen sind der Glaube an die Möglichkeiten und die Unfehlbarkeit der eingesetzten Sicherheitssoftware sowie das Vertrauen in die richtige Installation bzw. Konfiguration. Denn egal wie gut eine Software ist: Wird sie falsch konfiguriert bzw. bedient, ist de facto keine Sicherheit gegeben. Zum Beispiel, wenn Sicherheitssoftware modifiziert oder gar abgeschaltet werden kann.

Eine „Einmalinvestition“ in Sicherheitssoftware ist zwar ein guter Anfang, jedoch bei Weitem nicht ausreichend.

Wird beispielsweise ein Virenscanner oder eine Firewall nach bestem Wissen bei der Installation eingerichtet, muss dennoch regelmäßig nach Updates und Funktion geprüft werden: Wurde eventuell nachträglich die Konfiguration verändert? Entspricht die Konfiguration noch den aktuellen Erfordernissen? Wurden die Sicherheitsupdates auch für Sicherheitssoftware eingespielt? Werden Vorschriften aus mangelndem Sicherheitsbewusstsein nicht beachtet, können softwarebasierte Lösungen auch unterlaufen werden. Der „Faktor Mensch“ darf also nicht vernachlässigt werden.

Eine Gefährdung geht nicht zwangsläufig nur von Schadsoftware aus. Fehlfunktionen von Hardware und Fehlbedienung von Software können ebenfalls einen nicht unbeträchtlichen Schaden verursachen. Wird ein fehlerhaftes Programm ausgeführt, kann dies zum Absturz des kompletten PCs und zu Datenverlust führen. Zudem treten immer wieder Unverträglichkeiten zwischen einzelnen Programmen auf, die zu Fehlfunktionen führen können.

[8] www.bsi.bund.de/ContentBSI/Publikationen/Lageberichte/bsi-lageberichte.html

[9] vgl. Teil 2, Kapitel 2 „Elementarschutz IT-Organisation“, S. 39

Schädlinge breiten sich aus

Die nachhaltige Verbreitung von bereits bekannten Schädlingen ist ein Zeichen dafür, dass die getroffenen Maßnahmen entweder isoliert, ohne Konzept, schlecht gewartet oder nicht umfangreich genug stattfinden und keinen ausreichenden Schutz darstellen.

Um tatsächlich Sicherheit zu gewährleisten, müssen

- Arbeitsprozesse, Soft- und Hardware zusammenpassen bzw. zusammenspielen,
- die Komponenten eingerichtet und
- aufeinander abgestimmt werden.

Nachlässigkeit der Verantwortlichen

Angriffe haben oft Erfolg, weil selbst bekannte Sicherheitslücken nicht geschlossen werden.

Alle paar Jahre erreicht Malware in den Medien traurige Berühmtheit. Ein extremes Beispiel für unzulängliche Sicherheit auch bei kritischen nationalen Strukturen ist der Superwurm „Conficker". Er knackte die Rechner der finnischen Regierung und der Landesregierung in Kärnten. Er nistete sich in Computern der Bundeswehr, der französischen Luftwaffe und der Marine ein. Er infizierte Millionen Computer und offenbarte die Sicherheitslücken vieler IT-Abteilungen. Dabei ist die Sicherheitslücke, die der Schädling über ein halbes Jahr hinaus ausnutzte, nicht nur in den IT-Medien ein guter Bekannter. Doch viele IT-Abteilungen scheinen davon nichts mitbekommen zu haben. Anders ist es kaum zu erklären, dass Sicherheitsupdates nicht zeitnah installiert wurden. Denn schon einen Monat vor der ersten Attacke hatte Microsoft zur Schließung dieser Sicherheitslücke ein Software-Update bereitgestellt.

Conficker: Hacker proben Großangriff.

Im Netz der Computerkriminellen

Botnetz – der ferngesteuerte PC.

Der Betrieb von Botnetzen ist neben der Herstellung von Malware und dem Phishing die gefährlichste Erscheinungsform des Cybercrime.

Am meisten Schaden verursachen die sogenannten Botnetze. Die einzelnen Bots sind dabei normale PCs, die durch spezielle Programme zur Fernadministration gesteuert werden. Eine einzige kriminelle Person kann so alle angeschlossenen Bots zentral in ihrem Netzwerk fernsteuern. Meist werden diese Programme per E-Mail versendet oder auf präparierten Internetseiten abgelegt. Einmal infiziert, bilden die Bots eine mächtige Infrastruktur und umfassen oft mehrere hunderttausend heimlich aus der Ferne gesteuerte Computer. Mit deren Hilfe können Spam-E-Mails versendet, Passwörter geknackt, Zugangsdaten ausgespäht oder Finanztransaktionen durchgeführt werden. Das Schlimmste daran: Der befallene PC tritt als Akteur von kriminellen Handlungen auf. Im Fall der Entdeckung durch Polizei, BKA oder Verfassungsschutz ist der Besitzer eventuell sogar in der Beweispflicht, nicht der Urheber der Aktivitäten zu sein. Wer in diesem Fall keine Sicherheitsvorkehrungen aufweisen kann, muss sich den Vorwurf der Fahrlässigkeit gefallen lassen.

Der Geschäftspartner als Schwachstelle

Der Partner als unfreiwilliger Informant.

Wer auf diese Weise angegriffen wird, ist also nicht immer Ziel der Angreifer. Gerne werden auch Geschäftspartner eines Zielobjektes infiltriert, um weitere Kenntnisse über dieses zu erhalten. Ein beliebter Weg führt über das schwächste Glied der informellen bzw. geschäftlichen Kette. Natürlich werden dabei Kontodaten oder Passwörter ausgespäht, wenn diese verfügbar sind. Mitarbeiter von Unternehmen sind unter Umständen willkommene Informanten. Kann ihre digitale Identität übernommen oder vorgetäuscht werden, werden sie indirekt zu Beteiligten.

Drive-by-Downloads

Web 2.0 hat die Gefahr, unwissentlich Schadprogramme herunterzuladen, enorm verschärft.

Der Verbreitungsweg von gefährlichen Schädlingen hat sich im Laufe der Zeit den veränderten Gewohnheiten der Internetnutzer angepasst. Durch den Übergang zum sogenannten Web 2.0 mit seinen aktiven Inhalten und interaktiven Komponenten ist es für die Cyberkriminellen wesentlich leichter geworden, ihre Schadprogramme bei unbedarften Nutzern zu verbreiten: Blogs, Foren, Social Networks oder „MediaCenter" mit Bild, Ton und Video verführen zum Aktivieren von sogenannten „Aktiven Inhalten" in Form von Plug-ins, Add-ins oder Skripten. Eine Infektion kann jedoch ebenso durch andere Mechanismen erfolgen: zum einen durch das Öffnen von Office-Dokumenten oder PDF-Dateien, zum anderen aber auch durch Online-Buchungen von Hotels, Online-Bezahlen beim E-Shopping sowie durch die Teilnahme an Online-Auktionen.

Vorsicht vor präparierten Webseiten

In dieser schönen neuen Welt tummeln sich auch spezielle Schädlinge, die durch Manipulation der ursprünglichen Internetseite praktisch unbemerkt mit auf den PC geladen werden. Hersteller von Antivirensoftware bezeichnen das unwissentliche Herunterladen von Malware als „Drive-by-Download". Die Schädlinge dringen beim Surfen über den Browser in nicht ausreichend geschützte Systeme ein. Der PC wird allein durch Öffnen der Seite infiziert. Wird dann beim nächsten Gang ins Internet online bestellt und bezahlt, übermittelt der infizierte PC unbemerkt die Zugangsdaten zum Shop, Kreditkartendaten oder PIN und TAN.

Der sichere Weg zum eigenen Shop

Wer nun eine eigene Homepage betreiben möchte, um bei Kunden seine Produkte oder Dienste anzubieten, muss sich dem Thema Web 2.0 stellen, um sich nicht von vornherein als „wenig innovativ" zu präsentieren. Content-Management ist gefragt. Hierbei werden Inhalte und interaktive Komponenten dynamisch zur Verfügung gestellt. Doch der Umgang mit der komplexen Software will gelernt sein, möchte man nicht riskieren, dass der eigene Internetauftritt zur Viren- oder Spam-Schleuder wird. Diese Tatsache soll aber nicht davon abschrecken, einen Online-Shop zu betreiben: Von Seiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gibt es einen „Leitfaden für die Einrichtung einer Internetvertriebsplattform (E-Shop)"[10]. Gütesiegel für Online-Shops[11] sind ebenfalls ein auch von staatlichen Stellen empfohlenes Gütekriterium, mit dem bei Kunden für das sichere Einkaufen im Internet geworben werden kann.

[10] www.ecommerce-verbindungsstelle.de, Broschüre „Shopping Online"

[11] www.internet-guetesiegel.de
www.kaufenmitverstand.de

Gefahren von Social Engineering

Vielfach haben Unternehmen schon die Vorteile erkannt, die Web-Anwendungen bei Geschäftsvorgängen wie Kundensupport, Marktforschung und Werbekampagnen bieten. „Netzwerken" ist notwendig, um Kontakte zu knüpfen und Geschäftsbeziehungen aufzubauen bzw. zu verbessern. Das ist nichts Neues. Neu ist aber, dass dies nun ebenfalls ins Internet verlagert wird. Und: Im Gegensatz zur heutigen Generation wird die nachkommende verstärkt das Internet nutzen.

Mehr als Kontaktbörsen

Die sogenannten Social Networks wie XING, Facebook oder MySpace sind auch bei Cyber-Gangstern beliebte Plattformen. Zum einen, um potenzielle Opfer zu finden, zum anderen, um sich Informationen über das soziale und geschäftliche Umfeld eines potenziellen Ziels zu beschaffen. Ohne viel Aufwand holen sich Kriminelle persönliche Daten der Betroffenen aus Netzwerken, wo sie die Opfer selbst hinterlegt haben. Das Medium und seine Glaubwürdigkeit setzen auf Offenheit und Ehrlichkeit bei der Angabe persönlicher Daten und im Umgang mit anderen. Aber gerade dadurch wird besonders transparent, dass die digitale Identität einen elementaren Nachteil besitzt: Personalausweis, Gesicht, Kleidung oder Umgangsformen können im analogen Leben entschieden schwerer gefälscht werden als eine digitale Identität. Um es den Nutzern einfach zu machen, erfolgt zudem keine echte Identifikation der Person bei ihrer Registrierung im Vorfeld. Auch die Anmeldung selbst verzichtet in der Regel auf ein Sicherheitsmerkmal wie die SmartCard. Bei Geldautomaten kommt es nicht von ungefähr, dass eine Karte Grundvoraussetzung für Abhebungen ist und diese nur mit der zugehörigen PIN funktioniert.

Verlust der digitalen Identität

Viele Social-Networking-Nutzer sind zu naiv.

Im Umfeld dieser Communitys kommt damit der Diebstahl von digitalen Identitäten besonders häufig zum Tragen: Wird durch Spionagesoftware das Kennwort eines Nutzers ausgespäht, können dessen Freunde, Bekannte und Geschäftspartner getäuscht werden. Besonders tragisch ist die Mehrfachnutzung eines Kennwortes – für unterschiedlichste Dienste im Netz. Kriminelle nutzen das gnadenlos aus. Sie geben sich beispielsweise als „alter Bekannter" aus und schicken einen Link zu einer angeblich interessanten Webseite. Auf dieser haben die Angreifer dann Schadsoftware hinterlegt. Selbst wer sich als Mitarbeiter oder Unternehmer „nur im Privaten" auf diesen Plattformen austauscht, gibt Computerkriminellen nützliche Informationen preis, und sei es nur in Form der eigenen E-Mail-Adresse. Diese kann dann verwendet werden, um zum Beispiel einen Geschäftspartner mit einer gefälschten E-Mail anzugreifen.

Der Ruf im Netz

Social Networks bergen aber nicht nur Risiken für deren Teilnehmer. Als Kommunikationsplattform ohne ethische oder journalistische Kontrolle dienen sie auch zu haltlosen Wertungen oder zur Diffamierung ihres sozialen oder geschäftlichen Umfeldes. Es ist ein Leichtes, unter fremden Namen Rufmord an Personen, Produkten oder Unternehmen zu begehen. Und da das Netz nichts vergisst, ist es schwer, das einmal Eingestellte aus der Welt zu schaffen. Wer die neuen Kommunikationsplattformen und -medien nicht kennt, kann sich noch nicht einmal der gegen ihn vorgebrachten Aussagen erwehren.

Sensationelle, kulturelle und soziale Ereignisse

Internetkriminelle nutzen immer wieder Schlagzeilen und besondere Ereignisse zur Verbreitung ihrer Schädlinge. In regelmäßigen Abständen werden Sex-Videos oder intime Fotos von Prominenten angepriesen. Populär sind ebenso Sportereignisse, Naturkatastrophen oder auch kulturelle bzw. religiöse Feste.

Nur bei elektronisch signierten E-Mails kann der Absender identifiziert werden.

Alle Jahre wieder werden gerade in der Weihnachtszeit, zu Ostern, am Muttertag etc. Mails von Freunden, Bekannten und Verwandten versendet, hinter denen sich tatsächlich gefährliche Malware verbirgt. Die Kriminellen schlachten dann einfach den Wirbel für ihre kriminellen Zwecke aus. Erschreckend ist das Ausmaß, in dem dies immer wieder funktioniert. Anscheinend ist den Betroffenen nicht bewusst, wie einfach sich eine gewöhnliche E-Mail fälschen lässt. Ebenso ist anscheinend nicht bekannt, wie leicht man sich dagegen schützen kann bzw. wie einfach sich der Absender einer elektronisch signierten E-Mail identifizieren lässt.

Cybercrime – hier lauern die Gefahren

- Social Networks als Quelle und Ort für potenzielle Angriffe
- Internetsurfen auf mit Schadcode infizierten Seiten
- Finanz- und Bankgeschäfte online bergen Risiken durch Diebstahl von Passwörtern und Kreditkarten-Daten.
- Sicherungen zur Filterung gefährlicher oder unerwünschter Inhalte werden immer wichtiger. Nur so können gerade jugendliche Mitarbeiter geschützt werden.
- Fake- und Crimeware (gefälschte Sicherheits-Software) enthalten verstärkt Technologien zum Schutz vor Entdeckung und dem Löschen durch Antivirus-Software.
- Virenschreiber spüren plattformübergreifend Schwachstellen in Betriebssystemen auf.
- Botnetze sind Netzwerke aus Computern, die mit einem Schadprogramm infiziert sind. Dadurch lassen sich die befallenen Rechner fernsteuern.

Die mobile Gefahr

Ein Megatrend sind Angriffe auf mobile Geräte.

Der aktuelle Trend geht eindeutig in Richtung kleinerer und leistungsstärkerer Hardware. Smartphones – eine Kombination aus Mobiltelefon und Mini-PC – sind stark auf dem Vormarsch. Typisch für technische Neuerungen ist jedoch, dass zunächst nur die Kernfunktionen implementiert werden. Erst wenn die Akzeptanz im Markt gegeben ist, werden Sicherheitsfunktionen nachgerüstet. Eine Tatsache, die auch der Schattenwirtschaft nicht unbekannt ist. Ist das Marktpotenzial groß genug, beginnen auch hier die Angriffe: Fachleute sehen bei mobilen Geräten einen weiteren Trend im Bereich der Cyberkriminalität. So wird prognostiziert, dass die Zahl der Angriffe auf Smartphones rasant zunehmen wird. Generell gilt: Je mehr Applikationen eine Plattform unterstützt und je populärer ein Gerät oder Betriebssystem ist, desto größer die Gefahr.

Vorbeugende Maßnahmen

Schützen Sie Ihre persönlichen Daten:
Seien Sie vorsichtig mit deren Preisgabe auch bei Social-Networking-Angeboten. Dort hinterlegte Daten können missbraucht werden. Einmal veröffentlicht, können sie über Archivseiten sehr lange auffindbar sein – auch wenn Sie die Daten auf der Social-Networking-Seite bereits gelöscht haben.

Sichern Sie Ihren E-Mail-Verkehr ab:
Allen eingehenden E-Mails sollten Sie mit Vorsicht begegnen. Auch wenn Sie den (vermeintlichen) Absender kennen, können Sie nicht sicher sein, dass die E-Mail wirklich von ihm ist. Zweifelsfrei können Sie einen Absender nur identifizieren, wenn die E-Mail digital signiert ist.

Schützen Sie Ihren Internetzugang im Unternehmen:
Kostenfreie Antivirensoftware und Firewalls sind durch deren Einschränkungen bestenfalls für den privaten Einsatz ausreichend. Ein unternehmensweit genutzter Internetzugang muss professionell abgesichert werden.

Schützen Sie Ihren Heimarbeitsplatz:
Sensible Daten müssen genauso vertraulich behandelt werden wie im Büro. Das bedeutet, dass auch der PC zu Hause abgesichert sein muss. Die Art der Nutzung sollte nicht über die im Unternehmen hinausgehen, da die unternehmensweiten Sicherheitsvorkehrungen nur auf diese Art der Nutzung ausgelegt sind. Der PC sollte beispielsweise nicht von Familienmitgliedern zum Spielen oder für Tauschbörsen genutzt werden.

2 Wirtschaftsspionage

Im Zuge der Globalisierung und mit zunehmender Verzahnung der Datenverarbeitung vom Zulieferer bis zum Endkunden hat auch das Risiko des illegalen Know-how-Transfers zugenommen. Dies gilt prinzipiell für jedes Unternehmen, insbesondere aber für Unternehmen, die über hoch technologisches Wissen verfügen. Als Informations-Lieferant kann jeder dienen, der in irgendeiner Weise Teil der Wertschöpfungskette des Zielobjektes ist.

Wissen ist wertvoll – auch für andere

Ein Wirtschaftszweig, der gerade in schwierigen Zeiten erblüht, ist die Spionage. Aufgrund ihrer Intensität und der zur Verfügung stehenden Mittel unterscheidet man zwischen Wirtschaftsspionage und Konkurrenzausspähung.

Wirtschaftsspionage meint vor allem die Aktivitäten staatlicher Nachrichtendienste. Erfolgt die Spionage durch konkurrierende Unternehmen, spricht man von Konkurrenzausspähung.

Kleine Unternehmen brauchen mehr Schutz

Wirtschaftsspionage betrifft nicht nur große, multinationale Konzerne. Insbesondere kleinere, kreative Unternehmen leisten ihren Beitrag zu ungewöhnlichen, neuen Ideen und effizienten Abläufen. Weil jedoch gerade diese Unternehmen häufig organisatorisch, rechtlich und informell nicht genügend abgesichert sind, können ihre Ideen leichter geklaut werden. Diese gelangen unter Umständen außerhalb des eigenen Unternehmens zur Marktreife. Ein immenser Verlust – für die Firma selbst wie auch für die inländische Wirtschaft.

Kleine, innovative Unternehmen sind für die Schattenwirtschaft besonders interessant.

Sparen an der falschen Stelle

Die Innovationsfähigkeit und das Know-how deutscher Unternehmen genießen noch immer weltweit hohes Ansehen. Besonders in Zeiten der Wirtschaftskrise florieren jedoch Wirtschafts- und Industriespionage besonders. Denn die Unternehmen sparen oftmals gerade an den Maßnahmen, die zur Verbesserung der Sicherheitsinfrastruktur beitragen würden, weil daraus kein direkter Beitrag zur Wertschöpfung des Unternehmens zu erkennen ist. Das kann sich als fataler Fehler herausstellen. Vor allem, wenn man berücksichtigt, dass in manchen Branchen 70 % der immateriellen Vermögenswerte aus Informationen bestehen.

Die Schätzungen der jährlichen Schadenshöhe durch Wirtschafts- und Industriespionage pendeln sich bei Werten um 50 Milliarden Euro ein. Eine Tatsache, die vom Mittelstand oftmals unterschätzt wird. Während Konzerne entsprechend in ihre IT-Sicherheitsstruktur investieren, liegt bei kleineren, nicht weniger innovativen Unternehmen oft keine ausreichende Sensibilität über die Auswirkungen fehlender Sicherheitsvorkehrungen und das Know-how für deren Planung und Einführung vor. Auch werden die finanziellen Mittel für die Umsetzung lieber in die Forschung und Entwicklung neuer Produkte gesteckt.

Analoger und digitaler Datenabfluss

Ein Großteil des Informations- und Datendiebstahls erfolgt über die Informationstechnologie, da die physische Anwesenheit einer Person nicht mehr erforderlich ist.

Viele Unternehmen hierzulande sind durch mangelhafte Kenntnis der technischen Möglichkeiten nur unzureichend auf die drohenden Gefahren durch Industriespionage vorbereitet. Sie müssen sich der wachsenden Bedrohung bewusst werden. So gehören Viren und sonstige Malware seit Langem zum typischen Handwerkszeug der Wirtschaftsspione. Zudem ist es im Zeitalter der digitalen Datenhaltung prinzipiell einfacher geworden, große Datenmengen unauffällig in seinen Besitz zu bringen. Allerdings ist auch die „altmodische Art" des Informationsdiebstahls nicht zu unterschätzen – angefangen vom Einbruch mit Hardwarediebstahl über vermeintliches Reinigungspersonal oder Handwerker bis zum Aushorchen von Mitarbeitern bei Messen oder Geschäftsreisen.

Ein ganzheitliches Konzept ist gefragt

Ausreichend Schutz bietet ein ganzheitliches Sicherheitskonzept, das die gegenseitigen Wechselwirkungen von Maßnahmen berücksichtigt. Dies beinhaltet auch eine gelebte Sicherheitskultur, die auch das Sensibilisieren der Mitarbeiter umfasst. In Summe führt dies zu einem höheren Sicherheitsniveau als die isolierte Nutzung selbst der teuersten Produkte: Der beste Virenschutz und die teuerste Firewall verpuffen wirkungslos, wenn Datensicherungs-Medien einfach entwendet werden können oder Zugangspasswörter am Monitor angebracht sind. Kundendaten und strategisch wichtige Information sollten grundsätzlich unzugänglich aufbewahrt werden, sobald diese nicht mehr benötigt werden. Werden Unterlagen nicht mehr benötigt, sind diese zu schreddern; dasselbe gilt für ausgemusterte Datenträger. Kopierer, Scanner und Faxe verfügen mitunter ebenfalls über große Speichereinheiten, die ausgebaut oder deren Daten über das Netzwerk abgezogen werden können. Gerade durch den Trend zu mehr Mobilität sollte dafür Sorge getragen werden, dass versehentlich liegen gelassene Notebooks oder USB-Sticks nicht unberechtigt benutzt werden können.

Besonders beim Einsatz von Funknetzen wie WLAN oder Bluetooth ist Vorsicht geboten. Diese besitzen Schnittstellen, die durch ihre hohe Verbindungsfähigkeit zu beliebigen anderen Geräten ein besonders hohes Gefährdungspotenzial aufweisen. Ungesichert stellen sie ein Einfallstor für Spione jeglicher Art dar, vor allem, wenn mit ihnen regelmäßig Verbindung zum Unternehmensnetzwerk aufgenommen wird.

Wirtschaftsspione lesen E-Mails von Unternehmen

Als Kommunikationsmittel Nummer eins ist die E-Mail für nahezu alle Unternehmen unverzichtbar geworden. Die reibungslose, zeitnahe Kommunikation zum Geschäftspartner ist ein wichtiger Erfolgsfaktor. Sie ermöglicht den Mitarbeitern, jederzeit und ortsunabhängig zu kommunizieren. Die dabei ausgetauschten Informationen wie etwa Geschäftspläne und Kundendaten können jedoch auch für die Konkurrenz eine wichtige Rolle spielen.

Kommunikation via E-Mail absichern

E-Mail-Verschlüsselung schützt vor unerwünschten Mitlesern.

Damit die Kommunikation nicht zum Risikofaktor wird und sensible Daten in falsche Hände geraten können, sollte dieser Kanal angemessen abgesichert werden. Doch die elektronische Post stellt oft den unsicheren Bestandteil von

Die E-Mail-Signatur gibt Aufschluss über den Absender und die Originalität des Inhaltes.

Unternehmensprozessen dar. Üblicherweise wird sie als Klartext über unverschlüsselte Kommunikationswege übertragen. Wer Wert auf Vertraulichkeit legt, sollte in der digitalen Kommunikation Verschlüsselungstechnik einsetzen. Bei einer gewöhnlichen E-Mail ohne zusätzliche Vorkehrung können zudem sowohl Absender als auch Inhalt gefälscht werden, ohne dass der Empfänger dies feststellen kann. Wer sicherstellen möchte, wer tatsächlich Absender der E-Mail ist und ob diese unverfälscht übermittelt wurde, benötigt eine elektronische Signatur. Diese bietet den weiteren Vorteil, dass nachträgliche Manipulationen sichtbar gemacht werden können.

Verfassungsschutz oder Polizei?

Für das Thema Konkurrenzausspähung ist die Polizei zuständig. Dabei ist es unerheblich, ob der Konkurrent im In- oder im Ausland ansässig ist. Mit Fällen von Wirtschaftsspionage befasst sich der Verfassungsschutz. Dieser verfügt auch über weitergehende Befugnisse bzw. Informationsquellen. Einen erheblichen Teil ihrer Informationen gewinnen die Verfassungsschutzbehörden aus allgemein zugänglichen Quellen. Sofern dies nicht möglich oder nicht effektiv ist, dürfen sie sich im Rahmen gesetzlich festgelegter Befugnisse und unter Wahrung des Grundsatzes der Verhältnismäßigkeit auch sogenannter nachrichtendienstlicher Mittel zur Informationsbeschaffung bedienen.[12]

Zahlreiche Informationen und Tipps befinden sich zum Beispiel im Internet auf der Seite **www.verfassungsschutz.de**. Hier stehen weitere Informationen kostenlos zum Download bereit, unter anderem eine Broschüre mit den „10 Goldenen Regeln der Prävention".

Zusätzlich bietet das Bundesamt für Verfassungsschutz auch kostenlose Beratungsgespräche an.

Die 10 Goldenen Regeln der Prävention

1. nicht warten, bis der Spionagefall eingetreten ist
2. aktuelle Informationen bei kompetenten Partnern einholen
3. Informationsschutz als wichtigen Bestandteil der Firmenphilosophie und Firmenstrategie verankern
4. Sicherheitsstandards regelmäßig analysieren
5. ganzheitliches Sicherheitskonzept realisieren und permanent fortschreiben
6. Schutzmaßnahmen auf den Kernbestand zukunftssichernder Informationen konzentrieren
7. Einhaltung und Erfolg der Sicherheitsvorkehrungen kontrollieren, Sicherheitsverstöße sanktionieren
8. „Frühwarnsystem" zur Erkennung von Know-how-Verlusten installieren
9. Auffälligkeiten und konkrete Hinweise konsequent verfolgen, professionelle Hilfe in Anspruch nehmen
10. Informationsschutz als strategischen Erfolgsfaktor nutzen

[12] www.verfassungsschutz.de, Verfassungsschutzbericht 2011 (Vorabfassung), S. 354 ff.; siehe auch „Elektronische Angriffe", 350 ff.

3 Angriff erfordert Gegenwehr

Das Internet hat in den letzten 10 Jahren einen phänomenalen Siegeszug angetreten und ist aus unserem täglichen Leben, weder im privaten noch im geschäftlichen Bereich, kaum mehr wegzudenken. Leider haben sich auch die Computerschädlinge ebenso rasant weiterentwickelt. Doch wenn man ein paar Sicherheitsaspekte beachtet, kann man unbesorgt auf digitale Geschäftsprozesse umstellen. Mit einem überschaubaren Maßnahmenbündel erhält man ein hohes Maß an Betriebs- und Angriffssicherheit.

4 Ausblick in eine sichere Zukunft

Das Sicherheitsbewusstsein der Anwender wächst, vermeldet das Bundesamt für Sicherheit in der Informationstechnik (BSI). Bereits 92% der Anwender in Deutschland nutzen ein Virenschutzprogramm auf ihrem PC. Auch die Notwendigkeit regelmäßiger Updates sehen immer mehr Anwender. Für einen guten Schutz ist es jedoch notwendig, Zusammenhänge zu beachten. Dabei spielt die richtige Konfiguration eine wichtige Rolle.

Im Teil II haben wir für Sie ein Bündel an Maßnahmen zusammengestellt, die in keinem Unternehmen fehlen sollten.

Tipps für mehr Sicherheit im Netz

- **Virenscanner und Firewall**
  Nur wenn sichergestellt ist, dass die Programme ordnungsgemäß funktionieren, ist Sicherheit gewährleistet: Dies erfordert profunde Kenntnisse bei der Konfiguration, die anschließend nicht mehr manipulierbar sein darf.
- **Sicherheitsupdates**
  Bei aktueller Software kann der technische Laie das Zusammenwirken unterschiedlicher Komponenten nicht mehr erfassen. Hierdurch ist das regelmäßige Update **aller** installierten Programme erforderlich.
- **Spam-Filter**
  Ein Teil der Spam-E-Mails ist mit Malware versehen, sodass bereits beim Öffnen einer E-Mail Vorsicht angebracht ist: Eingebettete Software wird bereits durch das Öffnen ausgeführt.
- **Phishing-Filter**
  Phishing-E-Mails enthalten in der Regel keine Malware. Der Anwender soll durch pseudo-persönliche Ansprache dazu bewegt werden, einen manipulierten Link anzuklicken, der auf eine gefälschte und mit Malware versehene Internetseite verweist. Schutz bietet hier eine Firewall, die den Link sperrt.
- **Cookie-Verwaltung (Nutzungs-Historie, Nutzerprofil)**
  Durch Cookies und Historienfunktion des Browsers können Nutzerbewegungen ausgelesen und nachvollzogen werden. Wenn hierzu gleichzeitig die IP-Adresse des PCs mit ausgelesen wird, können so über einen längeren Zeitraum Namen, Kontodaten und Lese- sowie Einkaufsgewohnheiten gesammelt werden.
- **Persönliche Daten nur auf gesicherten Seiten eingeben (z.B. https)**
  Sollen persönliche Daten nicht vom Betreiber, von Dritten oder Suchmaschinen gesammelt werden, dürfen diese nur auf geschützten Seiten eingegeben werden. Wer sicher gehen möchte, sollte auf Gütesiegel achten.
- **Eigennamen**
  sollten in Foren/Social Communities etc. nicht verwendet werden (Nutzerprofil).
- **E-Mail**
  Nur eine elektronische Signatur (Zertifikat) identifiziert den Absender und stellt sicher, dass keine Manipulation des Inhaltes erfolgt ist. Nur Verschlüsselung stellt die Vertraulichkeit des Inhaltes sicher.

IT-Management im Unternehmen

Teil 2

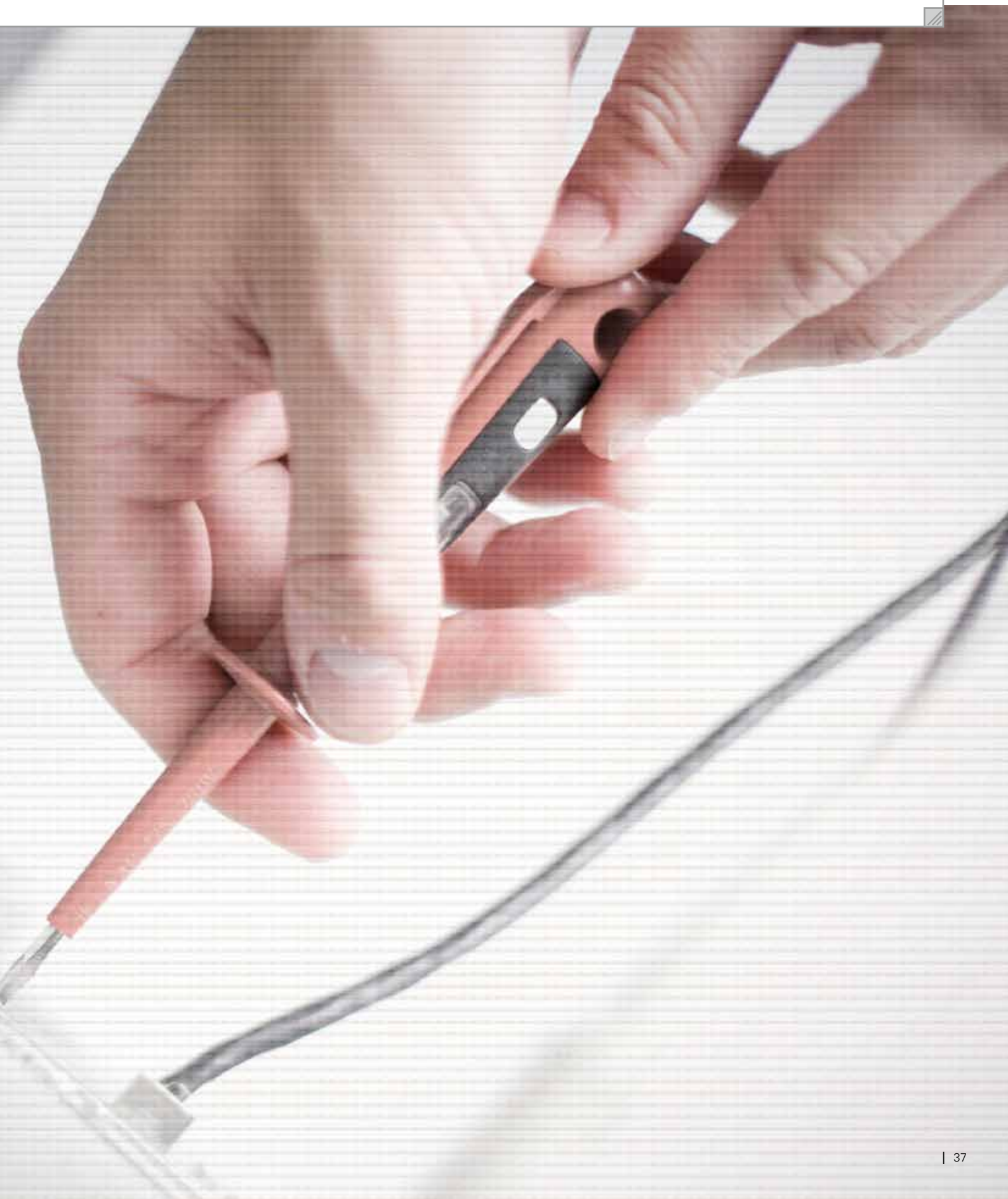
Ob bei Kalkulationen, beim Erstellen von Ausschreibungen oder bei der Warenwirtschaft – die elektronische Datenverarbeitung hat Einzug in die Unternehmen gehalten und erleichtert dort viele Arbeitsprozesse. Gerade deshalb ist es wichtig, dass ein funktionierendes IT-Management zum Einsatz kommt.

Dabei gilt es einiges zu beachten: Die Voraussetzungen für die ordnungsgemäße Nutzung der Software müssen ebenso berücksichtigt werden wie die Sicherung von Daten und Arbeitsergebnissen oder die unverfälschte Übertragung an staatliche Stellen und Institutionen. Außerdem sollten zumindest die grundlegenden Sicherheitsstandards aus rechtlichen Gründen eingehalten werden: beispielsweise gesetzliche Verpflichtungen und Anforderungen aus dem Bundesdatenschutzgesetz (BDSG).

1 Vom Papier zur Datei
2 Elementarschutz IT-Organisation
3 Internet
4 E-Mail-Verkehr
5 Mobile Endgeräte
6 Notfallkonzept
7 Rechtliches zum Datenschutz

01 | Sicherheitsvorkehrungen

Ein Klick zu viel oder zu wenig, ein Absturz der Festplatte oder ein Virus – und schon sind wichtige Daten für immer verloren. Wer seine Arbeitsprozesse digital abwickelt, muss dafür Sorge tragen, dass seine Daten ausreichend gesichert sind: durch entsprechende Maßnahmen der Datensicherung, durch das Schließen von Sicherheitslücken, durch Schutz vor Malware und eine durchdachte Benutzerverwaltung.



1 Vom Papier zur Datei
2 Elementarschutz IT-Organisation
3 Internet
4 E-Mail-Verkehr
5 Mobile Endgeräte
6 Notfallkonzept
7 Rechtliches zum Datenschutz

1 Vom Papier zur Datei

In den traditionellen, etablierten Prozessabläufen von Unternehmen sind grundlegende Sicherheitsvorkehrungen integraler, gewachsener Bestandteil. Durch das Internet werden dagegen die historischen, räumlichen Sicherheitsaspekte außer Kraft gesetzt. Selbst die staatlichen Einrichtungen können im weltumfassenden World Wide Web keinen ausreichenden Schutz mehr garantieren. Die Gesetzgebung endet entweder an den nationalen Grenzen oder den Grenzen der diplomatischen Reichweite.

Dennoch: Die von staatlicher Seite und der EU forcierte Entwicklung geht in Richtung Kommunikation via Internet. Über kurz oder lang wird das Internet das traditionelle Kommunikationsmittel Brief in vielen Bereichen ablösen. GDPdU[1], EHUG[2], ELSTER[3], bzw. De-Mail[4], elektronisches Mahnverfahren, EGVP[5] und damit auch GoBS[6] sind aktuelle Beispiele für eine Entwicklung, die zunehmend an Bedeutung gewinnt. Mit Online-Banking, Online-Shops, Portalen für Anbieter von Dienstleistungen und Produkten oder durch Angebote auf einer eigenen Homepage ist der nächste Schritt zur Digitalisierung von Geschäftsbeziehungen getan.

Digitale Prozesse erfordern Umdenken

Bei allem technischen Fortschritt: Papier verschwindet nicht auf Knopfdruck.

Doch die neuen Verfahren, Techniken und Technik bergen Risiken, die es im wirtschaftlichen Rahmen bisher nicht gegeben hat. Für einen Unternehmer beispielsweise, der sein Unternehmen Anfang der 90er Jahre aufgebaut hat, waren andere Sachverhalte wichtig und die Schwerpunkte im Bereich Medien- und Marketingkompetenz anders gelagert. Die aktuellen Entwicklungen erfordern ein Umdenken zur nachhaltig erfolgreichen Vermarktung seiner Leistungen. Der vielleicht wichtigste Aspekt beim Umstieg ins digitale, papierlose Zeitalter: Anders als bei digitalen Dokumenten verschwindet Papier nicht auf Knopfdruck und Änderungen daran können nur physisch vorgenommen werden.

Vorkehrungen für Ihre Sicherheit

Um für digitale Dokumente und Daten einen adäquaten Schutz vor Verlust oder unberechtigter, nachträglicher Veränderung zu erhalten, müssen Sicherheitsvorkehrungen getroffen werden. Art und Umfang der Maßnahmen können jedoch leicht mit Hilfe eines pragmatischen Vergleichs eingegrenzt werden: Auch Papier kann gefälscht oder vernichtet werden. Augenmaß ist also gefragt.

Grundsätzlich sollten jedoch immer die im folgenden Kapitel ineinandergreifenden Aspekte für Ihren Datenschutz berücksichtigt werden. Der große Vorteil liegt darin, dass die rechtlichen Auflagen dadurch bereits in hohem Maße abgedeckt werden. Soll spezifisches Know-how abgesichert werden oder muss in einem Geschäftsverhältnis – begründet durch die wirtschaftliche Stellung eines Unternehmens – besonders Rücksicht auf mögliche Wirtschaftsspionage genommen werden, sind zusätzliche Maßnahmen auch bei den Geschäftspartnern erforderlich.

[1] Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen

[2] Gesetz über elektronische Handelsregister, Genossenschaftsregister sowie das Unternehmensregister

[3] Elektronische Steuererklärung

[4] Ziel: ein rechtsverbindlicher, sicherer E-Mail-Verkehr

[5] Elektronisches Gerichts- und Verwaltungspostfach

[6] Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme

2 Elementarschutz IT-Organisation

Sicherheit ist zweifellos wichtig, jedoch beschäftigt sich jedes Unternehmen auch mit der Frage: Wie viel Sicherheit ist tatsächlich notwendig? Notwendig sind zunächst vor allem Maßnahmen, welche die Funktionsfähigkeit der EDV sicherstellen. Um haftungsrechtlich auf der sicheren Seite zu sein, sind darüber hinaus auch einige rechtliche Aspekte zu beachten. Dazu gehören beispielsweise Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS, Abgabenordnung (AO), Telemediengesetz (TMG), § 203 StGB oder Bundesdatenschutzgesetz (BDSG). Unabhängig davon, welche konkreten Maßnahmen tatsächlich ergriffen werden, müssen deren Wechselwirkungen berücksichtigt werden. Daher sind für eine Absicherung der EDV auch die Rahmenbedingungen für deren Einsatz zu beachten.

Rahmenbedingungen für die Absicherung der EDV

- Räumliche Maßnahmen und physische IT-Sicherheit/ Technische Absicherung
- Vertragliche und organisatorische Absicherung
- Schulungen für Mitarbeiter zu den Maßnahmen und deren Hintergründen

Räumliche Maßnahmen schaffen den Rahmen für den Arbeitsprozess im Unternehmen. Durch organisatorische, vertragliche und softwaretechnische Vorkehrungen kann das Haftungs- und Betriebsrisiko durch Geschäftspartner, Dienstleister oder ein mögliches Fehlverhalten von Mitarbeitern minimiert werden.

Als sicherheitstechnische Basis werden im Folgenden zunächst die wichtigsten softwaretechnischen Absicherungen beschrieben. Diese Maßnahmen sollten prinzipiell beachtet werden, auch wenn kein Zugang zum Internet existiert. Im Anschluss daran werden die Aspekte zur Absicherung des physischen Zugangs behandelt.

Auch ohne Internet sind Sicherheitsvorkehrungen erforderlich.

Grundlegendes zu den Sicherheitsmaßnahmen

Besonders in Zeiten stagnierender Umsätze werden mögliche Potenziale zur Kostensenkung gesucht. Dies sollte jedoch nicht zu Lasten der Sicherheit gehen.

Auf Business Continuity achten

Der Werterhalt des Unternehmens darf nicht aus den Augen gelassen werden – die sogenannte Business Continuity. Essenziell hierfür sind die Datenbestände. Sie enthalten jahrelang gesammeltes Know-how, Kundendaten oder auch Informationen aus sämtlichen Geschäftsfällen. Sind diese Datenbestände nicht mehr vorhanden oder nicht mehr richtig bzw. vollständig, ist die Leistungserstellung des Unternehmens nicht mehr sichergestellt. Ein Sachverhalt, der den Fortbestand der Unternehmung gefährdet. Die zunächst wichtigste Maßnahme ist damit die Datensicherung. Darüber hinaus sind weitere, prophylaktische Maßnahmen erforderlich, die verhindern sollen, dass auf eine Sicherung zurückgegriffen werden muss. Denn eine Sicherung bedeutet auch, dass die Arbeit von bis zu einem Tag verloren geht und dass es Stunden oder sogar Tage dauert, bis wieder normal gearbeitet werden kann.

Je nach Einschätzung des individuellen Schutzbedarfs sind unterschiedliche Aspekte relevant.

Ein ganzheitliches Konzept ist gefragt

Alle Sicherheitsvorkehrungen müssen ganzheitlich betrachtet werden.

Alle Maßnahmen sollten aufeinander abgestimmt sein. Was auf den ersten Blick trivial erscheint, ist in der betrieblichen Realität oft nicht direkt ersichtlich: Ein Virenscanner ist zwar installiert, kann aber prinzipiell von jedem Mitarbeiter beliebig modifiziert oder gar abgeschaltet werden. Die Verträge mit Geschäftspartnern liegen nur auf einem bestimmten PC im Netzwerk, aber jeder könnte Spionagetools installieren. PDA bzw. Smartphone werden zwar regelmäßig synchronisiert, der verwendete Datenpfad wird bei der Datensicherung aber nicht berücksichtigt. Für das Arbeiten im Internet wurde eine Sicherheits-Suite eingekauft und die Belegschaft speziell geschult, die Datensicherungen liegen jedoch für einen Besucher frei zugänglich auf einem Schreibtisch. Ein Internetanschluss ist im Netzwerk nicht vorhanden, aber ein neu hinzugekommenes Notebook verfügt über WLAN oder UMTS – damit ist auch das Netzwerk ans Internet angebunden, die Sicherheitsvorkehrungen sind jedoch nicht darauf ausgelegt.

Je nach individuellem Schutzbedarf sind unterschiedliche Lösungen möglich.

Dazu gehören:
- räumliche Maßnahmen und physische Sicherheit
- technische und organisatorische Absicherung
- vertragliche Absicherung
- softwaretechnische Absicherung
- technische IT-Sicherheit
- Administration
- Entsorgung

Im Sinne eines skalierbaren Elementarschutzes sind im Folgenden die eigentlich aufeinander aufbauenden Teile in der Reihenfolge ihrer Dringlichkeit angeordnet. Weiterführende Information finden Sie auf den Seiten des BSI[7].

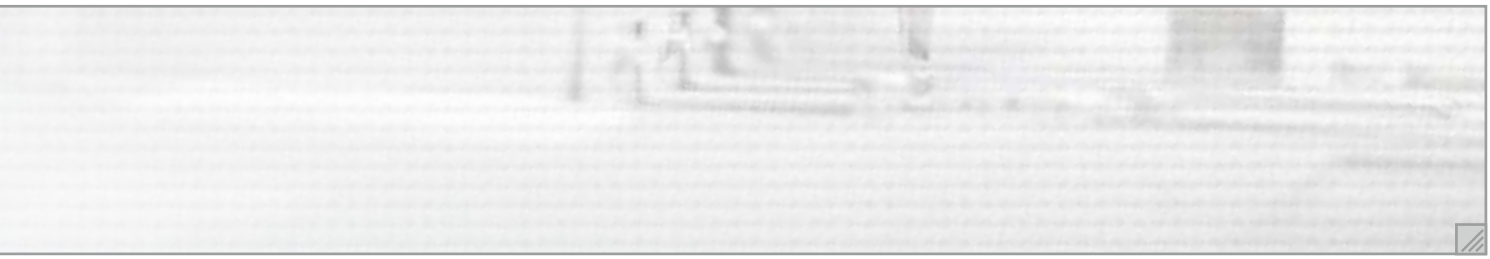
Notfallmaßnahme Datensicherung

Die Datensicherung ist in der EDV der Airbag, wenn die Bremsen versagen: Sie sorgt dafür, dass selbst nach dem Gau in einem Unternehmen weitergearbeitet werden kann.

Ob Fahrlässigkeit, Fehler, Viren oder ein Defekt – die Gründe für Datenverlust sind vielfältig. Dies gilt auch bei der mobilen Arbeit mit PDA und Handy.

Nicht nur Viren gefährden den Datenbestand von Unternehmen. Auch Hardwaredefekte, Hitze, Wasser oder Fehlbedienung können Schäden verursachen. Ein häufiger Weg des Datenverlustes: Die Daten werden unbeabsichtigt gelöscht oder versehentlich überschrieben. Gerne werden bestehende Dokumente als Vorlagen geladen und mit dem ursprünglichen Dateinamen erneut abgespeichert.

[7] Bundesamt für Sicherheit in der Informationstechnik, www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html



Die häufigsten Ursachen von Datenverlust:

- höhere Gewalt (Feuer, Wasser, Blitzschlag etc.)
- organisatorische Mängel
- menschliche Fehlhandlungen
- technisches Versagen
- vorsätzliche Handlungen

Regelmäßige Datensicherungen sind wichtig

Datensicherungen schützen vor endgültigem Verlust.

Wichtige Daten, die für die tägliche Arbeit benötigt werden, können durch regelmäßige Datensicherungen vor Verlust geschützt werden. Bereits das Betriebssystem eines PCs verfügt über einfache Möglichkeiten der Datensicherung. Zum Schutz der Sicherungsmedien sollten diese gemäß den Vorschriften der Hersteller aufbewahrt werden. Hierfür eignet sich beispielsweise ein Tresor, der darüber hinaus auch vor den elementaren Risiken wie Feuer, Wasser etc. schützt.

Wenn Daten und Programme so verändert wurden, dass die ungewollte Veränderung nicht mehr nachvollzogen werden und der Originalzustand nicht mehr mit vertretbarem Aufwand wiederhergestellt werden kann, muss auf die Datensicherung zurückgegriffen werden. Im schlimmsten Fall müssen das Betriebssystem und die verwendeten Programme neu installiert und die Daten von der Sicherung wieder eingespielt werden.

Backup-Lösungen müssen vor allem einfach sein

Bei der Auswahl einer geeigneten Backup-Lösung sollte zunächst geklärt werden, wer die Konfiguration und Sicherung durchführt: Ein Profi-System mag zunächst als die erste Wahl erscheinen – ein Laie wird jedoch damit nicht ohne Weiteres zurechtkommen. Wenn Fehler in der Konfiguration oder beim Handling mit den Medien erst entdeckt werden, wenn die Sicherung benötigt wird, ist es definitiv zu spät und die Daten sind unwiederbringlich verloren.

Was gehört in die Sicherung?

Solange es sich nur um einen einzelnen PC handelt, ist die Sicherung – es genügt z. B. eine externe Festplatte – noch überschaubar. Arbeiten mehrere Personen mit unterschiedlichen Geräten und legen diese gar ihre Daten nach Belieben an unterschiedlichen Orten ab, wird es schnell unübersichtlich. Es sollte daher zunächst organisatorisch geregelt sein, dass alle Daten ausnahmslos in einer vereinbarten Struktur abgelegt werden. Nur so ist sichergestellt, dass alle relevanten Daten auch tatsächlich gesichert werden.

Daten zentral speichern

Die Einrichtung eines abgetrennten Serverraums schützt Hardware und Daten.

Ein wichtiger Schritt zu mehr Sicherheit ist die zentrale Datenhaltung für alle stationären und mobilen Geräte. In einem zweiten Schritt sollten die Server in einem separaten Raum untergebracht werden, zu dem nur autorisierte Personen Zutritt haben: Die physische Trennung erschwert Besuchern, Dienstleistern und Mitarbeitern das Beschädigen oder Entwenden der Hardware und den unbefugten Zugang zu den Daten. Der Standort sollte einbruchsicher sein und zum Schutz vor Elementarschäden nicht in der Nähe von Versorgungsleitungen liegen.

Ist die Integrität der gesicherten Daten gegeben?

Die Daten sind gesichert – aber wertlos.

Die Sicherung ist laut Meldung des Sicherungsprogramms ordnungsgemäß durchgeführt worden. Und doch kann die Sicherung durch Fehler im Festplattenmanagement oder im Datenmanagement der Datenbank wertlos sein. Die heutige Hardware ist zweifellos sehr gut, aber eben nicht unfehlbar. In regelmäßigen Abständen sollten deshalb die Festplatten auf Fehler geprüft werden. Beim Einsatz von Datenbanken sind in der Regel Tools beigegeben, die auf mögliche Fehler prüfen. Unter Umständen muss bereits an dieser Stelle eine ältere Sicherung in Anspruch genommen werden. Eine Rücksicherung der gespeicherten Daten sollte ebenfalls in regelmäßigen Abständen durchgeführt werden. Erst dieser erfolgreich absolvierte letzte Schritt gewährleistet eine funktionsfähige Datensicherung.

Wo wird die Sicherung aufbewahrt?

Sicherer aufbewahrt im Rechenzentrum.

Wird die Sicherung mittels Festplatte, Band, DVD oder ähnlicher Speichermedien im Unternehmen durchgeführt, muss sichergestellt sein, dass die Sicherungsmedien bei einem Schaden nicht mit vernichtet bzw. entwendet werden. Eine Datensicherung, bei der alle relevanten Daten Nacht für Nacht automatisch an ein Rechenzentrum übertragen werden, bietet deshalb diverse Vorteile: Die Sicherung wird vor allem nicht am Ort des Geschehens aufbewahrt, das Sicherungsmedium ist immer verfügbar und die Daten sind lesbar.

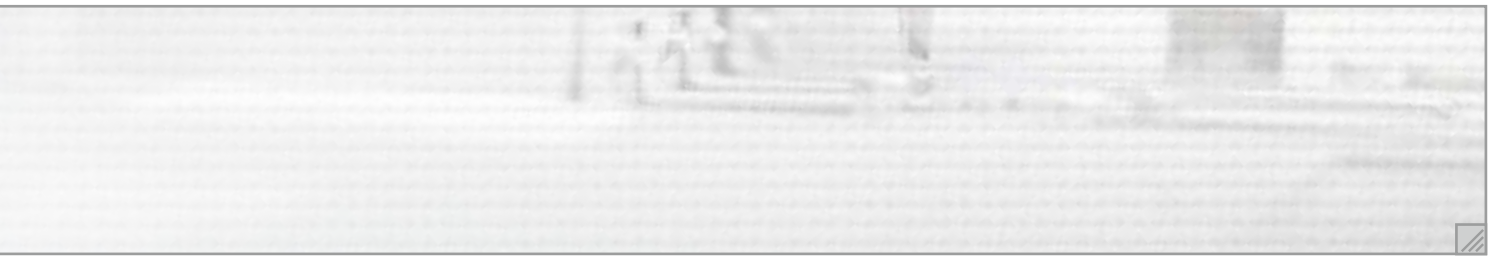
Schneller Wiederanlauf – die Rolle des EDV-Partners

Beim Ausfall der Hardware sollte eine schnelle Wiederinbetriebnahme sichergestellt werden, selbst, wenn es nur um einen einzigen PC bzw. ein einziges Notebook geht. Sind Termine für die Abgabe von Erklärungen, Ausschreibungen etc. einzuhalten, Bestellungen vorzunehmen oder Rechnungen zu begleichen, wird eine Nacherfassung verlorener Daten schnell zu einer sehr zeitintensiven und damit kostspieligen Angelegenheit.

Vereinbarte Reaktionszeiten senken Kosten.

Es zahlt sich in jedem Fall aus, wenn durch Wartungsverträge sichergestellt ist, dass die eingesetzte Hardware schnell wieder ersetzt werden kann und mit dem Partner vorab Reaktionszeiten vereinbart wurden. Nichts ist ärgerlicher, als im Krisenfall lange auf einen verfügbaren Spezialisten warten zu müssen.

Die Datenarchivierung dient der längerfristigen Aufbewahrung von Daten, um den gesetzlichen Anforderungen des Handelsgesetzbuches (§§ 239, 257 HGB), der Abgabenordnung (§§ 146, 147 AO) und den GoBS an die sichere, ordnungsgemäße Aufbewahrung von kaufmännischen Dokumenten sicherzustellen.



Archivierung

Neben der Datensicherung muss der Unternehmer auch dafür Sorge tragen, dass steuerrelevante Daten über Jahre hinweg gemäß den Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) lesbar sind. Gerne wird dabei unterschätzt, dass hierfür oft die Programme erforderlich sind, mit denen die Daten erstellt wurden. Diese wiederum laufen unter Umständen nur auf bestimmten Betriebssystemen. Die Betriebssysteme ihrerseits haben zur Zeit eine Lebensdauer von ca. 5 Jahren, bevor der Hersteller die Supportzusage einstellt. Und selbst wenn Betriebssystem, Programme und Daten verfügbar sind, muss darüber hinaus sichergestellt sein, dass das Betriebssystem sich überhaupt noch auf der vorhandenen Hardware installieren lässt.

Die Lesbarkeit auch alter Daten muss sichergestellt sein.

Allein durch diese Abhängigkeiten ist es sinnvoll, ein Archivierungskonzept über den vorgeschriebenen Zeitraum zu erstellen. Dabei müssen alle Daten regelmäßig in die aktuellen Formate transformiert werden. Dies erledigt dann entweder der IT-Verantwortliche im Unternehmen – oder ein externer Dienstleister.

Sichern oder archivieren?

↗ Zwei Begriffe, die häufig synonym verwendet werden, gleichwohl aber ganz verschiedene Vorgehensweisen beinhalten. Die Implementierung einer neuen Datensicherung in die IT-Landschaft entspricht dem Abschluss einer Versicherung für den Notfall. Alle getroffenen Maßnahmen dienen primär dazu, die wirtschaftliche Unternehmung vor Datenverlusten jeglicher Art zu bewahren. Hierfür gibt es von Seiten des Gesetzgebers keine zeitlichen Vorgaben, jedoch einige Rahmenbedingungen anhand der Anlage § 9 Satz 1 Bundesdatenschutzgesetz. Danach ist zur Gewährleistung einer erfolgreichen Umsetzung eine ganze Reihe technischer als auch organisatorischer Maßnahmen zu treffen. Parallel besteht der existenzielle Anspruch des Unternehmers, die geschäftlich relevanten Daten auf keinen Fall zu verlieren – zumindest bis zur nächsten Datensicherung. Landläufig wird eine tägliche Datensicherung zum Abschluss eines Arbeitstages durchgeführt. Auch definierte Datenstände können festgehalten werden, beispielsweise wenn Inhalte nach ihrem zeitlichen Stand oder ganze Systemplattformen möglichst schnell wieder hergestellt werden sollen. Die Auswahl der zu sichernden Daten ist über die Anforderungen des Gesetzgebers hinaus beliebig erweiterbar und obliegt stets der alleinigen Verantwortlichkeit des Dateneigentümers. Bereits deshalb ist eine Datensicherung niemals mit den völlig anders gearteten Anforderungen für eine revisionssichere Archivierung gleichzusetzen. Die Datenarchivierung dient der längerfristigen Aufbewahrung von Daten, um den gesetzlichen Anforderungen des Handelsgesetzbuches (§§ 239, 257 HGB), der Abgabenordnung (§§ 146, 147 AO) und den GoBS an die sichere, ordnungsgemäße Aufbewahrung von kaufmännischen Dokumenten zu entsprechen.

Schutz vor Malware

Malware steht als Sammelbegriff für Programme, die in irgendeiner Weise dazu geeignet sind, Schaden anzurichten.

Malware ist die Kurzform von „malicious software", dem englischen Sammelbegriff für schädliche Software jeglicher Art. Hierunter fallen Spyware, Trojaner, Keylogger, Würmer etc. und eben die eigentlichen Viren, die umgangssprachlich synonym für schädliche Software verwendet werden.

Viren benötigen kein Internet

Virenschutz ist nicht nur bei der Internet-Nutzung, sondern grundsätzlich beim Austausch von Daten erforderlich.

Auch wer ohne Verbindung zum Internet arbeitet, ist durch Viren gefährdet. Überträger können alle mobilen Endgeräte sein, die mit einem PC im Unternehmensnetzwerk in Verbindung stehen: Handys, USB-Sticks oder PDAs. Aktuelle Geräte sind in ihrem Leistungsumfang vergleichbar mit einem PC. Darüber hinaus besteht durch deren vielfältige Schnittstellen ein besonderes Risiko. Sobald eines dieser Geräte via Schnittstelle Kontakt zum Unternehmensnetzwerk hat, besteht Virengefahr. Daher sollte grundsätzlich jeder PC über einen eigenen Virenscanner verfügen. Gewerbliche Scanner bieten eine zentrale Managementkonsole, um die Administration und Prüfung zu erleichtern. Fehlerhafte bzw. manipulierte Konfigurationen können so leichter festgestellt und behoben werden.

Desktop-Virenscanner bilden im geschäftlichen Bereich den Basisschutz vor schädigender Software und Hacker- bzw. Cracker-Tools.

Besteht auch nur gelegentlich eine Verbindung zum Internet, sind weitere Maßnahmen erforderlich: Ein modernes Smartphone[8] mit eigenem Internetzugang kann beispielsweise per Bluetooth oder WLAN mit dem Unternehmensnetz verbunden werden. Damit erhält das gesamte Netzwerk einen Zugang zum Internet[9]. In diesem Fall ist eine Firewall sinnvoll und sämtliche verfügbaren Sicherheitsupdates sollten installiert sein.

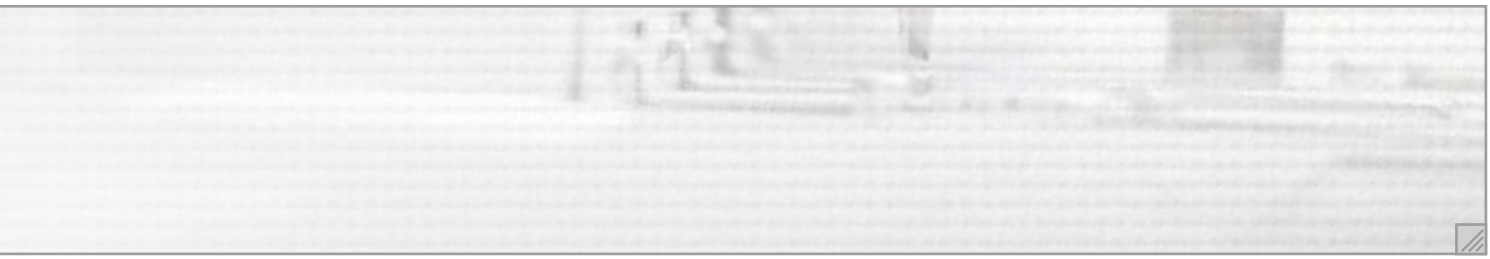
Spionage-Tools – auch ohne Internet

Wissensabfluss in Bild und Ton.

Besteht kein Zugang zum Internet, sind spezielle Spionageprogramme wie Keylogger oder Sniffer und Viren von Bedeutung. In wirtschaftlich schwierigen Zeiten und in Verbindung mit persönlichen Problemen wie Scheidung, Spielsucht oder einer drohenden Entlassung besteht immer die Möglichkeit, dass vertrauliche Informationen über das Unternehmen und seine Geschäftspartner unberechtigt gesammelt und gegen Geld weitergegeben werden. Auch zur Sicherung des eigenen Arbeitsplatzes können Mitarbeiter Informationen sammeln, die als Druckmittel eingesetzt werden. Zudem kommen weitere Personengruppen wie Handwerker, Besucher oder auch die Putzkolonne in Betracht, die gegen Bezahlung Informationen durch Tools abgreifen können. Keylogger protokollieren hierfür alle Tastatureingaben, machen Screenshots vom Bildschirm oder von Filmen in Bild und Ton mit Hilfe einer eingebauten Kamera und deren Mikrofon. Sniffer protokollieren den Datenfluss im Netzwerk. Damit können erstellte Geschäftsbriefe ebenso mitgelesen werden wie Passwörter und Ausdrucke. Viren hingegen befallen Programmdateien und führen in der Regel dazu, dass nicht mehr fehlerfrei gearbeitet werden kann – der Gau im Geschäftsbetrieb. Im schlimmsten Fall kommt es zum kompletten Systemausfall.

[8] vgl. Kapitel 5 „Mobile Endgeräte", S. 72 ff.

[9] vgl. Kapitel 3 „Internet", S. 54 ff.



Die Konfiguration von Sicherheitssoftware – Tücke des Objekts

Produkte und Preis vergleichen, kaufen, installieren, Updates aktivieren und künftig in Ruhe unter dem Schutz des Wächters arbeiten. Es klingt zu schön, um wahr zu sein. Denn tatsächlich: Ist der Virenscanner nicht abgesichert gegen Veränderung seiner Konfiguration oder seiner Deaktivierung, steht der Schutz auf wackeligen Beinen.

Dabei sind zwei wesentliche Aspekte von besonderer Bedeutung: die beabsichtigte individuelle Veränderung der Einstellung durch die jeweiligen Benutzer und die unbeabsichtigte durch Malware.

Es gibt viele Gründe, die Konfiguration von Sicherheitssoftware vorsätzlich zu verändern: Mal funktionieren die Programme zu langsam, mal kann Musik nicht vom USB-Stick gespielt oder können liebgewonnene Tools, Hintergrundbilder oder Bildschirmschoner nicht installiert werden etc. Jedes laufende Programm „erbt" vom angemeldeten Benutzer die Berechtigungen und damit auch die Möglichkeit, Einstellungen an Programmen vorzunehmen. Unbewusst kann so auch Malware für weitergehende Veränderungen an den Einstellungen verantwortlich sein: Kann der Virenscanner vom Benutzer beliebig modifiziert werden, arbeitet er im Grundsatz zwar immer noch zuverlässig, wird den Schädling aber durch die Modifikation eines Nutzers bzw. Angreifers nicht mehr entdecken.

Die Berechtigungen des Nutzers gelten für die Programme, die er ausführt – auch für Viren etc.

Mögliche Schäden lassen sich leicht vermeiden, wenn ausschließlich Sicherheitsprogramme eingesetzt werden, die nur von einem Administrator konfiguriert werden können oder zumindest über einen Passwortschutz für die Konfiguration verfügen.

Die Konfiguration von Sicherheitssoftware sollte nur mit Administrator-Rechten möglich sein.

Um die Einstellungen und die Funktionsfähigkeit sicherzustellen, sind darüber hinaus auch vorhandene Sicherheitsupdates erforderlich. Fehlfunktionen durch Fehler bzw. Lücken lassen sich so vermeiden. Eventuell besteht die Möglichkeit, dass diese Updates automatisiert stattfinden.

Zuverlässig funktioniert Sicherheitssoftware nur mit Sicherheitsupdates.

Benutzerkonten – Administrator oder Benutzer

In jedem Betriebssystem gibt es zwei grundsätzlich verschiedene Typen von Nutzern: den Administrator und den Benutzer. Diese sind jeweils für unterschiedliche Aufgaben vorgesehen:

Ein Administrator konfiguriert und verwaltet die Hard- und Software eines PCs. Er installiert, deinstalliert und konfiguriert Programme so, dass die Nutzung des Rechners möglich ist. Er steuert den Programmzugriff für die Benutzer und die Berechtigungen für den Datenzugriff und sorgt für den ordnungsgemäßen Betrieb der Software.

Ein Benutzer verwendet den PC und die ihm zur Verfügung stehenden Programme. Er erfasst und verarbeitet Daten und speichert die so erstellten Arbeitsergebnisse. Geschäftsbriefe, Kalkulationen, Rechnungen etc. sollten demzufolge vom Benutzer erstellt bzw. Buchungen vorgenommen werden.

Arbeiten Sie immer als „Benutzer".

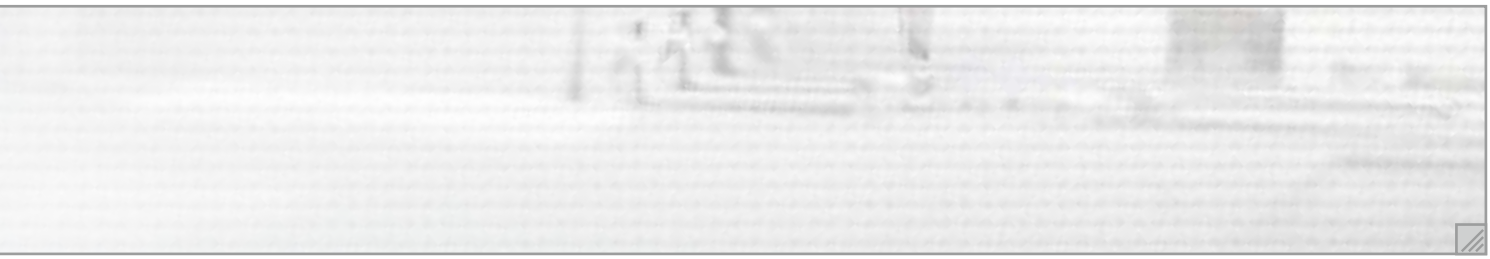
Gibt es diese Rollentrennung nicht und arbeitet der Nutzer als „Administrator", hat dies Konsequenzen für die Sicherheit. Programme, die er bewusst oder unbewusst ausführt, verfügen ebenfalls über administrative Rechte: Geht er als Administrator ins Internet, haben Viren & Co. auf Internetseiten gleichsam die Berechtigung zum Installieren, Kopieren, Verändern oder Löschen. Besonders kritisch wird dies, wenn Malware den lokalen Virenscanner und die Firewall manipuliert. Auch wenn alles normal und funktionsfähig wirkt, kann der PC bereits aus dem Internet ferngesteuert werden. Grundsätzlich sollte daher die normale Nutzung des PCs als „Benutzer" stattfinden. Wichtige Systemeinstellungen können so nicht verändert werden.

Administration von Unternehmensnetzwerken

Grundsätzlich sollte jeder Mitarbeiter nur auf die Programme und Daten zugreifen können, die er für seine Arbeit benötigt.

Durch die Benutzerkonten kann der Zugriff auf die Daten eines Unternehmens gezielt gesteuert werden. Nach Einteilung dieser Daten in Finanzinformationen, Mitarbeiter- und Kundendaten und eventuell unternehmensspezifisches Know-how können diese den jeweiligen Aufgabenschwerpunkten und Bearbeitern zugeordnet werden. Keine dieser Informationen muss für jeden Mitarbeiter in gleicher Weise zugänglich und nutzbar sein. Jeder Zugriff sollte sich auf die Daten beschränken, die für die jeweilige Aufgabe benötigt werden. Am besten noch kombiniert mit einer Definition, wie der Nutzer mit diesen Daten umgehen muss. Um fahrlässige oder vorsätzliche Handlungen zu erschweren, ist die Absicherung für die Nutzung eines PCs mit Hilfe von Benutzerkonten und Passwörtern unerlässlich. Damit werden Zugangs- bzw. Zugriffsberechtigungen vergleichbar zur analogen, realen Welt gesteuert: Nicht jeder Mitarbeiter hat Zugang zu allen Räumen bzw. Aktenschränken. Die Identifikation der Person wird ersetzt durch das Benutzerkonto. Die Absicherung in der analogen Welt mittels Schlüssel wird in der digitalen ersetzt durch Passwörter.

Benutzerkonto und Passwort schränken Missbrauch ein.



Die Installation und Konfiguration neuer Software sollte ausnahmslos dem Administrator vorbehalten sein, da der normale Nutzer deren Auswirkungen auf die gesamte Softwarelandschaft in der Regel nicht einschätzen kann. Um den ordnungsgemäßen Betrieb der eingesetzten Software und speziell von Sicherheitssoftware zu gewährleisten, darf die Konfiguration nicht durch einen Benutzer veränderbar sein. Für die Anschaffung von Sicherheitssoftware sollte ausschlaggebend sein, dass eine Option zur Absicherung der Konfiguration und zum Schutz vor unberechtigtem Beenden der Software vorhanden ist. Auch der Einbau von Bauteilen oder Anschluss von externen Geräten sollte nur vom Administrator oder mit seiner ausdrücklichen Genehmigung vorgenommen werden.

Passwörter – Zugriffe regeln

Datensicherheit erfordert auch Rechtemanagement und Zugriffskontrolle.

Je weniger Personen Zugriff zu einzelnen Datenbeständen haben, desto geringer ist das Risiko eines Datenverlusts durch Fehlbedienung. Wird festgelegt, dass jeder Mitarbeiter nur mit bestimmten Programmen arbeiten und nur auf die Daten seines Aufgabengebietes zugreifen darf, lässt sich die Wahrscheinlichkeit von Fehlern, Störungen oder Wissensabfluss stark reduzieren. Zudem wird dabei gleich ein Aspekt des Datenschutzes erfüllt.

Passwörter sind ein einfaches, aber wirksames Mittel zum Schutz vor unerlaubtem Zugriff.

Passwörter identifizieren den einzelnen Benutzer. Mit dieser Zuordnung wird der Zugriff auf Programme und Daten reglementiert. Dies schützt zum einen vor unerlaubtem Zugriff. Zum anderen kann protokolliert und damit nachvollzogen werden, wer wann was erstellt oder verändert hat. Dies ist natürlich nur möglich, wenn sichergestellt ist, dass Passwörter nicht allgemein zugänglich sind. Gelbe Zettel am Monitor, unter der Tastatur oder in der Schreibtischschublade machen dies wieder hinfällig.

Ein passwortgeschützter Bildschirmschoner verhindert die Nutzung durch Unberechtigte.

Auch wenn der Arbeitsplatz nur kurz verlassen wird, sollte daher immer der Bildschirmschoner „mit Passwortschutz“ aktiviert werden – aufgrund der Zurechenbarkeit von Eingaben auf den angemeldeten Benutzer. Hat der Administrator in der Benutzerverwaltung ein Benutzerkonto entsprechend eingerichtet, genügt die Tastenkombination „Strg + Alt + Entf“, um durch einen Klick auf „Computer sperren“ den PC für andere Benutzer unzugänglich zu machen. Ist sichergestellt, dass Unbefugte nicht in den Besitz der Passworte gekommen sind, kann zum Weiterarbeiten nur der Benutzer oder der Administrator den PC wieder entsperren. So gelangen weder Kollegen noch Besucher des Unternehmens unbefugt an Informationen. Unerwünschte Software kann dadurch ebenfalls nicht installiert werden.

Risikofaktor Mensch

Eine besondere Problemzone ist zweifellos der Mensch. Studien zufolge ist ein hoher Anteil der Sicherheitsvorfälle auf die eigenen Mitarbeiter zurückzuführen. Dabei geht es nicht nur um vorsätzliche, sondern auch um fahrlässige Aktivitäten.

Die folgenden Aktivitäten und Verhaltensmuster bedrohen die Sicherheit der Geschäftsdaten am meisten und sollten daher vermieden werden:

- eigenmächtige Änderungen an den Sicherheitseinstellungen
- ungeschützte Aufbewahrung von Sicherungsmedien
- Installation nicht genehmigter Software
- unerlaubter Zugriff auf ungeschützte Geschäftsdaten
- Preisgabe vertraulicher Firmeninformationen
- Weitergabe firmeneigener IT
- ungeschützte Arbeitsgeräte
- ungeschützte Aufbewahrung von Logins und Passwörtern
- Verlust tragbarer Speichermedien
- Zutritt für Unberechtigte

BIOS-Passwort

Das Betriebssystem darf zur Sicherheit nur von der eingebauten Festplatte geladen werden.

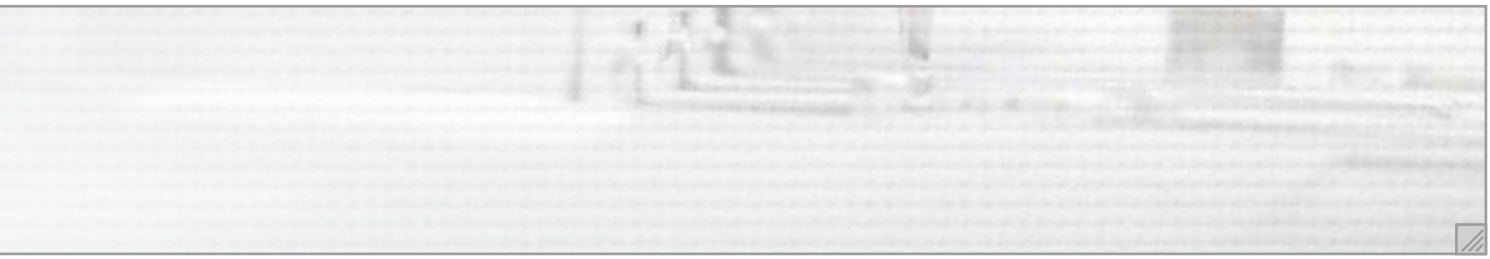
Grundsätzlich besteht bei jedem PC die Möglichkeit, die Einstellungen zur Nutzung der Hardware zu ändern. Dabei kann unter anderem festgelegt werden, von welchem Datenträger das Betriebssystem geladen wird. Stammt dieses beispielsweise von einer DVD, werden sämtliche Software-Schutzmechanismen dieses PCs ersetzt durch die Einstellungen auf der DVD. Mit kleinen Hilfsprogrammen kann die Benutzerverwaltung manipuliert oder können alle Daten des PCs ausgelesen werden. Erhält ein Angreifer so den Zugang zum PC, kann er leicht Spionagetools einrichten.

Die Lösung ist denkbar einfach und bereits an jedem PC vorhanden: Die BIOS-Konfiguration muss lediglich so eingestellt werden, dass nur mit der eingebauten Festplatte gebootet werden kann. Anschließend wird die Konfiguration mit einem Passwort abgesichert. Aus Sicherheitsgründen sollte dies natürlich nur dem Administrator bzw. dem Unternehmer zugänglich sein.

Benutzerkennung und Passwort

Zu den Aufgaben des Administrators gehört das Anlegen von Benutzerkonten.

Der Administrator legt in der Benutzerverwaltung für den Nutzer ein Konto an. Dort werden auch die Bedingungen für ein „gutes“ Kennwort festgelegt. Dies ist besonders wichtig, da beispielsweise umgangssprachliche Begriffe mit 6 Stellen bereits innerhalb einer Stunde bequem geknackt werden können. Die Tools sind im Internet schnell verfügbar und für den Gebrauch „eigener vergessener Passwörter“ legal zu beziehen.



Der Administrator legt auch für den Bildschirmschoner die Einstellungen fest. Es sollte die Option „Kennworteingabe bei Reaktivierung“ aktiviert werden. Damit ist auch in Abwesenheit eines angemeldeten Mitarbeiters sichergestellt, dass niemand in dessen Namen Unfug treiben kann.

Ein gutes Passwort[10] sollte:

- aus mindestens 8 Zeichen bestehen.
- aus Buchstaben mit Groß- und Kleinschreibung, Ziffern und Sonderzeichen bestehen.
- keine aus dem sozialen Umfeld zu erratenden Namen, Begriffe oder Zahlenfolgen enthalten.
- keine Wörter aus einem Wörterbuch enthalten.
- nicht am Monitor angebracht werden oder in anderer Weise griffbereit sein.
- nicht in den Programmen, eigenen Dateien oder auf dem Desktop gespeichert werden.

Bewährt hat sich die Bildung eines Merksatzes, bei dem z. B. nur die Anfangsbuchstaben verwendet werden. So wird beispielsweise aus „**M**ontag **u**m **8** **g**ehe **i**ch **z**ur **A**rbeit**!**“ das sichere Passwort „**Mu8gizA!**“

Installation, Deinstallation und Konfiguration

Dem Administrator obliegt die Aufgabe, das Netzwerk und den PC in Betrieb zu nehmen und anschließend betriebsfähig zu halten. Jede unbedachte Installation kann die Stabilität des PCs gefährden. Dies gilt besonders für beliebte Tools der Mitarbeiter, die ursprünglich für bereits abgekündigte, d. h. nicht mehr gepflegte bzw. veraltete Betriebssysteme geschrieben wurden. Die persönliche Gestaltung durch Bildschirmschoner, audio-visuelle Effekte, Plug-ins, Add-ins etc. ist ebenfalls kritisch, da diese Programme gerne Viren mit sich führen oder unsauber programmiert sind. Letzteres ist besonders beim Zugang zum Internet kritisch, da auch deren Sicherheitslücken missbraucht werden können.

Vorsicht mit Freeware

Bei Scareware bzw. Fakeware handelt es sich um gefälschte Sicherheitssoftware.

Wird die eigene Gefährdung als gering eingeschätzt, ist dennoch Vorsicht angesagt. Gerade dann wird gerne auf sogenannte Freeware zurückgegriffen. So gut diese in vielen Fällen auch tatsächlich ist: Es handelt sich um Einsteigervarianten, die eher für den Heimgebrauch als für den professionellen Einsatz gedacht sind. Für einen Unternehmer ist diese Software nicht zu empfehlen: Zum einen ist meist der Funktionsumfang reduziert, zum anderen sind diese für den gewerblichen Einsatz in der Regel kostenpflichtig. Auch bei der Auswahl der Bezugsquelle ist Vorsicht angebracht. Der Anteil an sogenannter Scareware bzw. Fakeware nimmt deutlich zu. Ziel dieser Art von Software ist es beispielsweise, den Anwender im Schutz eines voll funktionsfähigen Virenscanners zu wiegen und ihm stattdessen Malware unterzujubeln.

[10] Wie Sie ein sicheres Passwort erhalten: www.sicher-im-netz.de

Wer kümmert sich, wer trägt die Verantwortung?

Die Qualifikation entscheidet über die Funktionsfähigkeit und Sicherheit des Netzwerks.

Was in großen Unternehmen üblicherweise ein eigenständiger IT-Administrator übernimmt, wird in kleineren Unternehmen oft einem Mitarbeiter übertragen oder vom Chef selbst erledigt – angesichts der Kosten für einen gut ausgebildeten IT-Fachmann mehr als verständlich. Allerdings verfügt ein Spezialist natürlich auch über entsprechend hohes Know-how. Die Qualifikation ist ein besonders wichtiger Aspekt bei der Beurteilung, wer sich um Konzeption, Installation und Pflege der Sicherheit kümmern sollte. Sie entscheidet, ob die Maßnahmen nicht nur Sicherheit vorgeben, sondern diese auch tatsächlich gewährleisten: Die Zuweisung der Verantwortung allein befähigt in der Regel keinen Mitarbeiter dazu, ein Netzwerk zu administrieren und Sicherheitssoftware auf die Spezifika des Unternehmens anzupassen sowie auf dem aktuellen Stand zu halten. Es muss zudem ausreichend Zeit eingeplant werden, um sich mit der Materie auseinanderzusetzen. Hinzu kommt die wachsende Komplexität der Anforderungen im Bereich Internetsicherheit, Betriebssicherheit und Datensicherung sowie Systemwartung, z. B. in Form von Updates. Ist grundlegendes Wissen vorhanden, muss dieses immer wieder auf den neuesten Stand gebracht werden.

Eigene Expertise

Liegt die Verantwortung für Wartung und Pflege der Sicherheitssoftware beim Unternehmen, müssen bereits bei ihrer Auswahl, aber auch bei Wartung und Pflege einige wichtige Aspekte beachtet werden. Dazu gehören beispielsweise regelmäßiges Kontrollieren der Funktionsweise und der Einstellungen des Virenscanners. Allein die Meldung über gerade stattfindende Updates ist nicht ausreichend, um seine ordnungsgemäße Funktion zu gewährleisten. Kann vom Benutzer die Konfiguration verändert werden, z. B. festgelegt werden, welche Verzeichnisse und welche Dateien gescannt werden, ist unter Umständen auch Malware hierzu in der Lage.

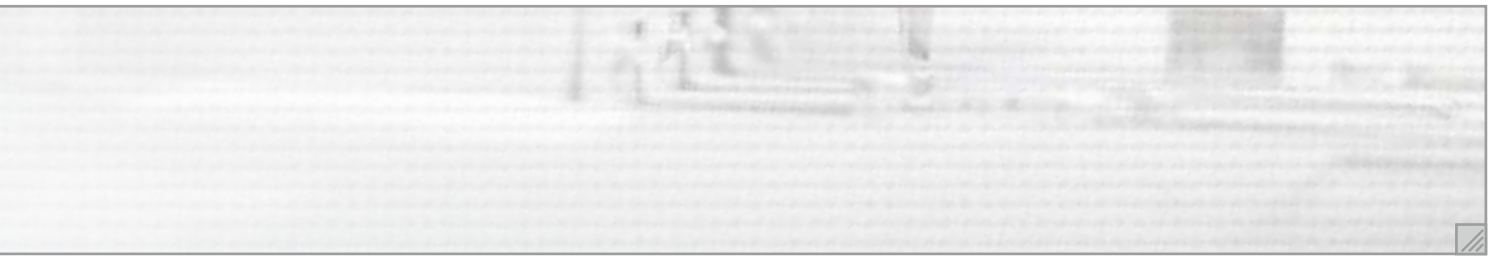
Systempartner, IT-Spezialisten und (Out-)Sourcing

Wer nicht selbst über ausreichende Kenntnisse verfügt, den Sicherheitsbedarf festzustellen, Sicherheitskomponenten zu vergleichen und diese auf den Bedarf hin zu konfigurieren, sollte auf einen externen Experten zurückgreifen. Dies wird in der Regel ein Systemhaus sein, das neben Hard- und Software auch Dienstleistungen anbietet. Ist kein vertrauenswürdiger bzw. kompetenter EDV-Partner verfügbar, können Sicherheitsfunktionen bzw. -komponenten auch ausgelagert werden. Dabei müssen jedoch die Vorschriften des Datenschutzes sichergestellt sein.

Bei „Managed Security Service" übernehmen externe Spezialisten Teilbereiche der IT-Dienste.

Bei „Managed Security Service" als Dienstleistung werden einzelne Funktionen oder thematische Bereiche wie das Sicherheitsmanagement ausgelagert. Spezialisten übernehmen Update-, Wartungs- und Konfigurationsdienste. Sie setzen sich permanent mit den aktuellen Bedrohungen und den daraus notwendigen Maßnahmen auseinander. Damit ist die Sicherheit zeitnah gewährleistet. Beim (Out-)Sourcing/ASP[11] werden darüber hinaus die Server für Programme und Daten an den Dienstleister ausgelagert. Programmaktualisierungen und Hardwareaustausch obliegen dann ebenfalls dem Dienstleister.

[11] weiterführende Information siehe Teil 4, Kapitel 02.3 „(Out-)Sourcing", S. 132 f. und Kapitel 02.4 „Application Service Providing (ASP)", S. 134



Entsorgung

Gerne unterschätzt, aber gerade hinsichtlich Datenschutz, Wettbewerbsfähigkeit oder Know-how-Abfluss besonders wichtig ist die Entsorgung von Akten, Kalkulationen, Businessplänen, Verträgen oder Kontoauszügen etc. Gerade für Letztere ist beispielsweise bei Kontoauszugsdruckern in Banken seit einigen Jahren ein Sicherheitshinweis zu lesen, dass sie nicht unbedacht in den öffentlich zugänglichen Papierkorb entsorgt werden sollten. In Papierform ist die sichere Entsorgung beispielsweise durch einen zentral aufgestellten Schredder relativ einfach zu gewährleisten. Ebenfalls zu berücksichtigen ist die sichere Entsorgung aber auch für jegliche Art von Datenträgern. Um hier nicht den Überblick zu verlieren, sollten die zulässigen Speichermedien per Anweisung abschließend aufgelistet werden. Akten, Datenträger, aber auch USB-Hardware, defekte Festplatten oder in Druckservern eingebaute Speicher sollten so entsorgt werden, dass eine Wiederherstellung der Daten nicht mehr möglich ist. Dies kann durch ein Entsorgungsunternehmen erfolgen. Dabei muss dem Datenschutz Rechnung getragen werden.

Eine sichere Entsorgung gewährleistet, dass eine Wiederherstellung der Daten nicht mehr möglich ist.

Räumliche Maßnahmen

Der Schutz Ihrer Daten beginnt bereits mit dem Schutz der Räumlichkeiten. Denn was nützen gute softwaretechnische Abwehrmechanismen, wenn Ausdrucke, Akten, DVDs oder sogar ganze Computer einfach mitgenommen oder die Räumlichkeiten des Unternehmens geleert oder zerstört werden können. Die räumliche Gestaltung ist zwar zunächst abhängig vom zur Verfügung stehenden Gebäudegrundriss und von den Arbeitsabläufen. Dennoch sollte der Sicherheitsaspekt bereits bei der Planung berücksichtigt werden: Besucher sollten sich beispielsweise nicht unbeaufsichtigt bewegen, Akten und Ausdrucke nicht von Unberechtigten eingesehen werden können. Um nach Feierabend die Putzkolonne oder Handwerker nicht in Versuchung zu bringen, sollten Aktenschränke abschließbar sein und mobile Hardware sicher verstaut werden. Auch Arbeitsverträge gehören allein aus Gründen des Datenschutzes nicht öffentlich zugänglich aufbewahrt.

Physische Sicherheit

Gerade bei älteren Gebäuden ist die physische Sicherheit zu prüfen. Wie stabil ist die Eingangstüre? Verwehrt ein Sicherheitsschloss den Zugang zum Gebäude oder nur zu den Unternehmensräumlichkeiten? Kann das Schloss eventuell von außen durch Abnehmen der Blende herausgeschraubt werden? Auch bei der Benutzung von Kellerräumen sollte Wert auf Sichtschutz gelegt werden. Gerne sind Kellerräume deutlich schwächer abgesichert. Dies beginnt bei einfach abnehmbaren Gitterrosten bis hin zu einfachen Fenstern, die vielleicht sogar nicht immer am Ende der Geschäftszeit geschlossen werden und unter Umständen auch leicht von außen auszuhebeln sind. In Verbindung mit Meldeeinrichtungen für Feuer, Wasser, Einbruch etc. wird im Katastrophenfall die Schadenshöhe erheblich reduziert.

Physische Sicherheit ist die Grundlage für softwaretechnische Maßnahmen.

Je nach Lage des eigenen Unternehmens besteht beispielsweise durch die Nähe zu sozialen Brennpunkten ein erhöhtes Risiko, durch einen Einbruch die gesamte Hardware zu verlieren. Verstärkt wird dieses Risiko durch auffällige Hardware-Anlieferung oder mangelnden Sichtschutz in die Räumlichkeiten hinein. Eine Versicherung ist in diesem Fall eine lohnende Sicherheitsvorkehrung. Da Versicherungen normalerweise aber nur die Hardware abdecken, muss für Programme und Daten eine andere Lösung gefunden werden. Wer besonderen Wert auf seine Daten legt, sollte organisatorisch dafür sorgen, dass diese zentralisiert auf einem Fileserver abgelegt werden. Ist zudem eine WTS-Lösung vorhanden, sind auch die Programme nur an zentraler Stelle installiert. Jeder PC muss sich in diesem Fall nur noch am Server anmelden, um mit Daten und Programmen arbeiten zu können. Unberechtigter Zugriff und Manipulation sind so deutlich erschwert. Ein separater und abschließbarer Serverraum verhindert den Ausbau von Komponenten oder Datenträgern. Als positiver Nebeneffekt wird dabei auch der Einbau von Spionage-Hardware unterbunden.

Um den Einsatz von Programmen nachhaltig sicherzustellen, sollten auch von diesen Sicherungskopien vorhanden sein, die zusammen mit Sicherungskopien der Geschäftsdaten zumindest in einem Tresor untergebracht werden. Liegen diese beispielsweise für jedermann zugänglich in den Räumlichkeiten des Unternehmens, werden teure Sicherheitsvorkehrungen an anderer Stelle zu Fehlinvestitionen. Darüber hinaus ist die Aufbewahrung an einem anderen Ort außerhalb des Unternehmens deutlich sicherer. Selbst im Katastrophenfall können so neue PCs schnell wieder beschafft und mit Programmen und Daten neu bestückt werden.

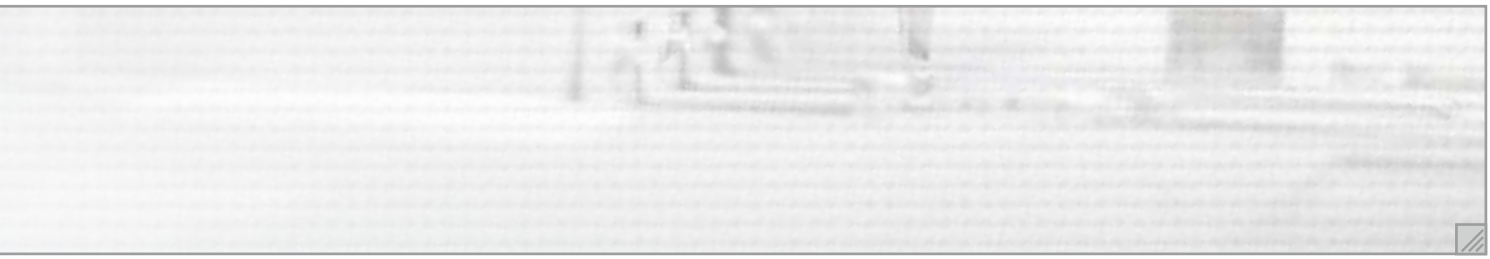
Die physische Sicherheit ist damit eigentlich Grundlage für die darauf aufbauenden softwaretechnischen Maßnahmen. Doch die Einschätzung der Gefährdung und damit die Auswahl von Art und Umfang der konkret zu treffenden Maßnahmen kann nur vom Verantwortlichen und für den Einzelfall getroffen werden.

Im Detail sollten Maßnahmen wie beispielsweise Meldeeinrichtungen für folgende sicherheitsrelevanten Aspekte berücksichtigt werden:

- Einbruch, Vandalismus (Zutritt)
- defekte Versorgungsleitungen, Installation (Strom, Wasser)
- Feuer
- Elementarschäden

Organisatorische Absicherung

Zusätzlich zu den grundlegenden Überlegungen der physischen IT-Sicherheit sollten auch Aspekte berücksichtigt werden, die den Zutritt von Personen und den Zugang zu Daten innerhalb des Unternehmens betreffen. Die zentralen Fragen sind hier: „Wer darf wohin?“ und „Wie wird dort sichergestellt, dass dort nur auf Akten und Daten zugegriffen werden kann, die zum Arbeiten erforderlich sind? Wo



dürfen sich Besucher aufhalten, zu welchen Bereichen haben Handwerker Zutritt? Sind die interne Kostenrechnung und diverse Kalkulationen für jeden Mitarbeiter zugänglich?"

Offensichtlich gefährdet sind vertrauliche Daten, die im Papierkorb statt im Reißwolf entsorgt wurden oder in offenen Aktenschränken liegen. Gleiches gilt für Bilanzen oder interne Abrechnungen auf dem Schreibtisch. Um die Daten vor Einsichtnahme Dritter zu schützen, gehören Papierunterlagen immer in verschlossene Schränke. Ein besonderes Augenmerk sollte dem Zugriff und der Aufbewahrung der Datensicherungen gelten. Die beste technische Sicherheit nützt wenig, wenn mit den unverschlüsselten Datensicherungen sämtliche Daten im Klartext entwendet werden können.

Organisatorische Aspekte:

- **Aufstellung zentrale Drucker**
  Vertrauliche Ausdrucke dürfen nicht unbemerkt entwendet, Druckausgaben nicht umgeleitet werden können.
- **Aktenschränke bzw. Räume abschließbar**
  Sensible Dokumente können nicht kopiert oder entwendet werden.
- **Separater, abgeschlossener Serverraum**
  verhindert den Ausbau von Komponenten oder Datenträgern ebenso wie den Einbau von Hardware oder Installation von Software für Fernzugriff bzw. für das Abgreifen von Daten.
- **Wertschutzschränke und Tresore**
  für vertrauliche Akten bzw. Datenträger mit vertraulichen Daten oder zur Wahrung des Datenschutzes bei personenbezogenen Daten. Verhindert das Mitnehmen von mobiler Hardware, von Programm- bzw. Datenträgern oder auch von Sicherungsbändern.
- **Entsorgung vertraulicher und personenbezogener Daten**
  Akten, Datenträger, aber auch USB-Hardware, defekte Festplatten oder Druckserver sollten so entsorgt werden, dass eine Wiederherstellung ihrer Daten nicht mehr möglich ist.
- **Speichermedien**
  Als Speichermedien bieten sich vor allem CD-ROMs, DVDs, USB-Sticks oder Wechselfestplatten an. Wenn Sie Daten allerdings langfristig aufbewahren wollen, sollten Sie auch auf die Lebensdauer und auf die Angaben der Hersteller zur Aufbewahrung der Medien achten.

Vertragliche Absicherung

Informieren Sie Mitarbeiter über die Richtlinien des gesetzlichen Datenschutzes, um das Haftungsrisiko zu minimieren. Lassen Sie sich die Richtlinien durch Unterschrift bestätigen. Verträge mit externen Unternehmen sollten Verfügbarkeiten, Reaktions- und Behebungszeiten sowie die Verschwiegenheit einzelner Mitarbeiter verbindlich gewährleisten. Insbesondere beim Outsourcing von IT-Systemen sollte sich der Auftraggeber das Recht auf die Auditierung seines Partners einräumen lassen, um den Datenschutz zu gewährleisten.

Mitarbeiter sind über die Richtlinien des gesetzlichen Datenschutzes zu informieren.

3 Internet

Das Internet ist aus dem heutigen Geschäftsleben nicht mehr wegzudenken. Viele Prozesse lassen sich schneller und effizienter abwickeln, Kommunikation kann flexibler gestaltet werden. Und auch der Gesetzgeber stellt strenge Anforderungen an den Datenaustausch via Web. Mit gutem Recht. Denn für die vertrauensvolle Zusammenarbeit mit Geschäftspartnern sind sichere Internet-Lösungen für Unternehmen, Home Office oder den mobilen Einsatz eine notwendige Basis. Via Internet kommunizieren Sie täglich mit Behörden und externen Partnern. Direkt von Ihrem Schreibtisch aus, einfach per E-Mail. Über das World Wide Web haben Sie auch jederzeit Zugriff auf aktuelle Nachrichten und die neuesten Informationen. Das Internet gehört damit zu Ihren wichtigen Arbeitsmitteln – egal ob im Unternehmen oder unterwegs.
Es ist unverzichtbar geworden!

Risiken steigen

„Unbemerkt Missbrauch betreiben" ist die Devise im kriminellen Internetgeschäft.

Wie in den Kapiteln zu Internetkriminalität und Wirtschaftsspionage bereits aufgezeigt wurde, ist in den letzten Jahren die Gefahr, einer Internetattacke zum Opfer zu fallen, wesentlich höher, als beispielsweise Opfer eines Überfalls oder Einbruchs zu werden. Neben der klassischen Gefahr von Viren, die den Arbeitsablauf im Unternehmensnetzwerk erheblich stören, aber dadurch auch verhältnismäßig schnell bemerkt und beseitigt werden können, sind die neueren Risiken wesentlich gefährlicher. Sie lassen den Anwender zunächst in Ruhe weiterarbeiten und richten ihren Schaden im Verborgenen an. Die Rede ist hierbei von Keyloggern, Spyware, Trojanern, RAT[12] usw. Diese schleichen sich durch diverse Hintertüren in die Unternehmensnetzwerke ein.

Kriminelle nutzen hauptsächlich 3 Methoden, um Macht über fremde PCs zu erlangen.

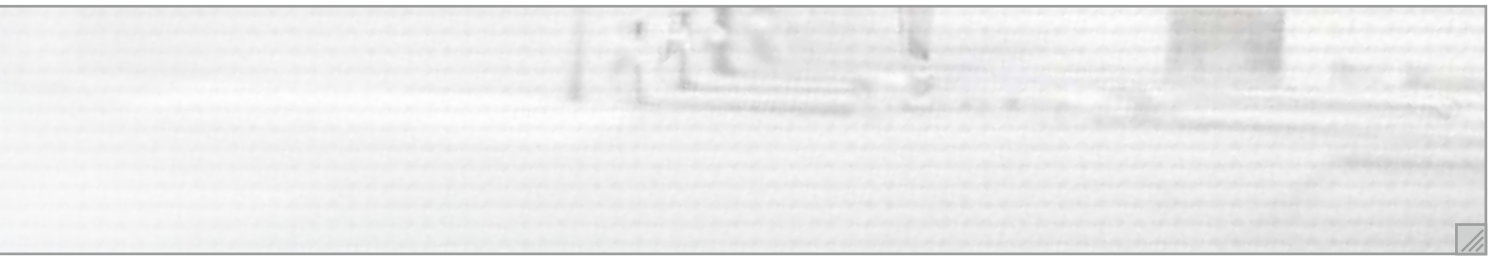
1. Sie kommen durch die Hintertüre, hierfür nutzen sie ungepatchte[13] Sicherheitslücken im Betriebssystem, im Browser oder in einer Anwendung.
2. Sie kommen über Social Engineering[14]: Unbedarfte Anwender wollen z.B. kostenlose Angebote, Programme oder Onlinespiele nutzen oder geben Auskünfte an vermeintlich Berechtigte und eröffnen so Wege ins Unternehmensnetzwerk.
3. Drive-by-Downloads[15]: Hierbei werden harmlose bzw. normale Webseiten von Kriminellen mit tückischen Schädlingen infiltriert.

[12] Remote Access Tool = Tool zur Fernadministration

[13] ungepatcht = ohne Sicherheitsupdate

[14] Social Engineering = ungefähr: Ausnutzen menschlicher Verhaltensweisen im jeweiligen sozialen Umfeld. Hierzu gehören bspw. auch Hierarchien, Zuständigkeiten und Vorschriften im Arbeitsumfeld.

[15] Drive-by = im Vorbeisurfen. Beim Aufruf einer manipulierten Internetseite werden Programme auf den PC automatisch heruntergeladen und installiert. Dies geschieht entweder durch aktive Inhalte (z.B. JavaScript) oder durch Fehler bzw. Lücken im Browser.



Die Anbieter von Sicherheitssoftware haben diese Problematik erkannt und bieten natürlich auch Lösungen an. Doch was im Straßenverkehr gilt, gilt in gleicher Weise auch für den Verkehr im Internet: Es besteht ein grundsätzliches Betriebsrisiko. Doch dieses kann mit geeigneten Maßnahmen reduziert werden. (Software-)Technische Maßnahmen ersetzen dabei nicht einen umsichtigen Umgang mit dem Medium, reduzieren das Risiko aber erheblich.

(Software-)Technische Maßnahmen ersetzen nicht den umsichtigen Umgang mit dem Medium Internet.

Ungepatchte PCs, unzureichend geschützte Datenbanken im Internet oder Sicherheitslücken im Internetauftritt zu finden, ist dabei gar nicht so schwer. Suchmaschinen wie z.B. Google leisten hierbei gute Dienste: Man muss nur wissen, welche Suchphrasen hierzu eingegeben werden müssen. Das Tückische an gekaperten Internetauftritten und infiltrierter EDV ist deren durchschnittliche Lebensdauer: Sie sind meist nur wenige Tage am Netz – ein Horrorszenario für jeden Administrator. Jede derartige Veränderung der Gefahrensituation sollte zusätzlich zum Virenschutz mit Einstellungen in der Firewall beantwortet werden – ist die Gefahr vorüber, müssen die Vorkehrungen ebenso wieder entfernt werden. Ist beispielsweise ein Geschäftspartner infiltriert worden, sollten bis zur Bereinigung seiner EDV keine E-Mails empfangen oder dessen Internetseiten nicht mehr aufgerufen werden. Nach der Säuberung der befallenen EDV des Partners müssen die eigenen Sicherheitsvorkehrungen jedoch wieder zurückgenommen werden, denn sonst wäre die Wiederaufnahme des elektronischen Geschäftsverkehrs nicht mehr möglich.

Absicherung durch Netzwerkadministration

Auch beim Arbeiten im und mit dem Internet ist eine auf Sicherheit ausgelegte Administration des Unternehmensnetzwerks von grundlegender Bedeutung. Erfolgt die Netzwerkadministration anhand eines umfassenden Sicherheitskonzeptes[16], das beispielsweise Benutzerkonten[17] und Zugriffsrechte beinhaltet, werden nicht nur datenschutzrechtliche Anforderungen erfüllt: Nebenbei steigt auch die Sicherheit bei Nutzung von Programmen und Daten oder beim Arbeiten im Internet. Beispielsweise ist nur ein Administrator zur Installation von Programmen berechtigt, während die Gruppe der Benutzer zur Erledigung der täglich anfallenden Aufgaben nur über eingeschränkte Rechte verfügt. Davon sollten Sie Gebrauch machen und die Nutzung in der Rolle des Administrators auf Installationen und administrative Aufgaben beschränken. Die Sicherheitssoftware wie Virenscanner oder Firewall etc. sollte nur als Administrator installiert und konfiguriert werden können. So wird verhindert, dass ein Benutzer oder eines der von ihm gestarteten Programme die Sicherheitssoftware beenden oder modifizieren kann. Wer beispielsweise die Berechtigung hat, ein Virenschutzprogramm zu installieren oder zu konfigurieren, kann es auch so modifizieren, dass das Programm zwar läuft, Spionage-Software aber nicht mehr gefunden werden kann. Dies ist mit Benutzerrechten nicht möglich. Auch machen Benutzerrechte das versehentliche Löschen von Systemdateien und Verzeichnissen unmöglich. Zudem kann dadurch das ungefragte Installieren von Eindringlingen aus dem Internet weitestgehend unterbunden werden.

Durch das Zugriffs- und Rechtemanagement kann verhindert werden, dass ein Virus als Administrator im Unternehmensnetzwerk unterwegs ist.

[16] vgl. Kapitel „Notfallkonzept“, S. 75; Abschnitt „Datenschutz und IT-Sicherheit: Gefragt ist ein ganzheitliches Konzept“, S. 82

[17] vgl. Abschnitt „Benutzerkonten – Administrator oder Benutzer“, S. 46

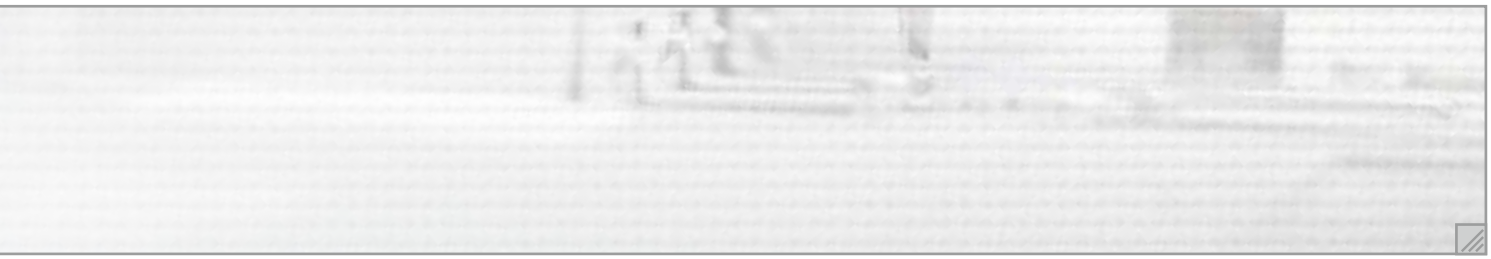
Kann ein isolierter Internet-PC vor Gefahren schützen?

Nicht nur staatliche Stellen forcieren die Datenübermittlung per Internet – beispielsweise bei der elektronischen Steuererklärung. Immer mehr Institutionen nutzen diesen Weg: Krankenkassen, Banken, Berufsgenossenschaften und Sozialversicherungsträger. Im Zuge dessen müssen zunehmend mehr Daten aus dem Unternehmensnetzwerk via Internet versendet werden. Erfolgt geschäftliche Korrespondenz bzw. ein Datenaustausch mit Geschäftspartnern, werden auch Daten empfangen, die im Unternehmensnetzwerk weiterverarbeitet werden müssen.

Was auf den ersten Blick sicher erscheint, stellt bei genauerem Betrachten eine nicht zu unterschätzende Sicherheitslücke dar. Zum einen benötigen Sie für die Datenübertragung zwischen den zwei Systemen einen Datenträger. Dabei können ebenfalls die Schädlinge aus dem Internet ins Netzwerk gelangen. Der Datenträger muss also vor dem Einsatz im Netzwerk geprüft werden. Dazu benötigen Sie ein aktuelles Prüfprogramm. Das können Sie aber nur online aktualisieren – und dazu benötigen Sie einen Internetzugang. Der Virenscanner muss sich daher auf dem Internet-PC befinden und vor Manipulation geschützt werden. Auch hier muss beispielsweise als „Benutzer" gearbeitet werden. Zum anderen müssen die gesendeten und empfangenen Daten nach erfolgter Transaktion wieder gelöscht werden. Wird dies versäumt, kann ein Angreifer auf diese Daten zugreifen, sodass sich kein verbesserter Schutz ergibt. In Summe entsteht damit kein Mehrwert durch die zusätzliche Barriere. Im Gegenteil, die Arbeitsprozesse werden behindert.

Absicherung des Internetzugangs

Wird das Internet ins Unternehmensnetzwerk eingebunden, so müssen weitere Maßnahmen durchgeführt werden, die spezifisch für den Einsatz dieses Mediums erforderlich sind. Aufgrund der dauerhaften Erreichbarkeit aus dem Internet müssen Sicherheitsupdates für alle genutzten Programme so früh wie möglich installiert werden. Die Kriminellen sind gerade über Lücken in Programmen bestens informiert: Durch einfache Analyse der Sicherheitsupdates wird Malware darauf programmiert, diese Lücken auszunutzen. Mit Sicherheitsprogrammen wie Virenscanner und Firewall kann der Internetzugang bereits gut abgesichert werden. Richtig eingerichtet, schützen sie vor Viren und Angriffen von Hackern. Solche Lösungen erkennen häufig auch Viren, die bei der Zustellung einer Mail noch nicht bekannt waren. Ist die neu programmierte Malware erst wenige Stunden alt, ist vor allem das Verhalten des Nutzers und die Konfiguration der im Internet genutzten Programme ausschlaggebend. Der Internet-Browser beispielsweise stellt nicht nur die Inhalte der Internetseiten dar, er ist auch eine Art Betriebssystem für Programme, die in den Internetseiten eingebettet sind. Sie bestehen beispielsweise aus JavaScript VB-Script oder ActiveX etc. und werden gerne als sogenannte „Aktive Inhalte" bezeichnet. Auch Office-Programme



oder PDF-Dateien beinhalten seit einigen Jahren aktive Inhalte, sodass dies ebenfalls bei der Konfiguration berücksichtigt werden muss. Grundsätzlich sollten aktive Inhalte nur sehr restriktiv und nur für vertrauenswürdige Seiten zugelassen werden.

Schutz durch Sicherheitsupdates

Sicherheitslücken sind Hintertürchen in Programmen, die es einem Angreifer ermöglichen, Kontrolle über einen fremden PC zu erlangen. Besonders kritisch sind neu entdeckte Sicherheitslücken, da diese meist bereits am Tag ihres Bekanntwerdens ausgenutzt werden.

Grundsätzlich mussten auch vor dem Einzug des Internets Berechnungen, wie beispielsweise im Rahmen der Buchführung, zuverlässig zum richtigen Ergebnis kommen (GoBS). Durch die wachsende Verbreitung des Internets erhält dieser Aspekt jedoch große Bedeutung. Ist ein PC mit Zugang zum Internet dort permanent angemeldet, kann er online erreicht und angegriffen werden. Auch durch die stärkere Nutzung steigt die Wahrscheinlichkeit, Opfer von Angriffen zu werden. Letztlich genügt jedoch bereits der Aufruf einer präparierten Internetseite, um von Malware infiziert zu werden.

Sicherheitslücken und Konsequenzen daraus

Ein Angriff aus dem Internet hat schon seit einigen Jahren nicht mehr das Ziel, Daten oder Programme zu zerstören. Heute soll mit einem Angriff möglichst viel Geld verdient werden. Dies geschieht beispielsweise, indem ein Computer gekapert wird. Dabei wird Software installiert, die eine Fernsteuerung aus dem Internet heraus ermöglicht.

Besonders beliebte Ansatzpunkte sind Schwachstellen in der Programmierung der gerade genutzten Programme. Das wichtigste und immer aktive Programm ist das Betriebssystem, das damit im Zentrum möglicher Angriffe steht. Um Fehler im E-Mail-System auszunutzen, werden E-Mails versendet, die mit Programmfunktionen versehen sind; um Fehler im Browser auszunutzen, werden Internetseiten mit besonders präparierten Programmen versehen. Aber auch Office-Programme können Dateien im Internet öffnen – ebenso wie andere Programme PDF-Dateien, Animationen, Videos oder Musikdateien. Einige ermöglichen es Schadprogrammen, ihre Funktionen im Hintergrund des Browsers unbemerkt auszuführen.

Durch ihre Funktionsvielfalt sind auch Handy, Organizer, Navigationsgerät etc. betroffen. Selbst wer eine Webseite betreibt, muss sich auch um die Sicherheitslücken der Präsentations- bzw. Content-Management-Systeme kümmern.

Virenscanner oder Firewalls sind auch nur Programme, die letztlich weder perfekt programmiert noch unfehlbar in ihrer Funktion sind.

Auch die Sicherheitsprogramme werden angegriffen. Insbesondere bei diesen sollte darauf geachtet werden, dass Schwachstellen und Sicherheitslücken zeitnah geschlossen werden, da die Kriminellen in der Regel hervorragend informiert sind. Eine Funktion „Automatisches Update" leistet hier gute Dienste.

Sicherheitslücken und wie man sie schließt

Da heutzutage zahlreiche Softwareprodukte eingesetzt werden, wird es immer schwieriger, einen Überblick sowohl über die neuesten Angriffstypen als auch die zur Verfügung stehenden Sicherheitsupdates zu erhalten. Bei manchen Programmen ist eine automatische Update-Funktion enthalten. Oft muss sich jedoch jeder selbst um die notwendigen Updates kümmern.

Tipps, um ein System in Ihr Patchmanagement zu bringen und sich damit vor bösen Überraschungen zu schützen[18]:

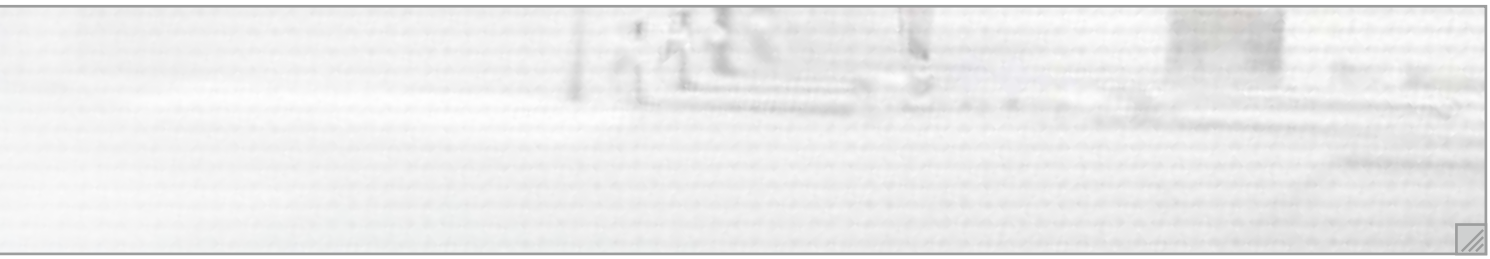
- Verschaffen Sie sich einen Überblick über die wichtigsten von Ihnen eingesetzten Programme!
- Prüfen Sie, ob bzw. zu welchen Produkten Sie automatische Update-Services erhalten!
- Prüfen Sie die Vertrauenswürdigkeit der Downloadquelle!
- Machen Sie es sich zur Regel, Hinweise auf Updates zu beachten und nicht wegzuklicken!
- Erstellen Sie eine Übersicht darüber, für welche Programme Sie eigenständig auf Updates achten müssen!
- Informieren Sie sich regelmäßig über Updates – etwa durch Newsletter oder Branchenplattformen!
- Laden Sie Patches rasch herunter und installieren Sie diese!
- Achten Sie auf Mitteilungen, die das Auslaufen des Supports für Produkte ankündigen!
- Installieren Sie gegebenenfalls Upgrades für neue Programmversionen!

Vorsicht vor „Aktiven Inhalten"

„Aktive Inhalte" sind Programme, die in den Internetseiten eingebettet sind.

Neben Sicherheitslücken vor allem im Browser und Betriebssystem sind „Aktive Inhalte" besonders kritisch. Das Internet hat sich vom Recherche- und Informationsmedium hin zu einer interaktiven Plattform weiterentwickelt. Die bisher verwendete Plattform musste um interaktive Elemente erweitert werden. Diese aktiven Inhalte sind Programme, die in den Internetseiten eingebettet sind. Damit besteht ein moderner Internetauftritt bzw. eine Homepage aus mehr als der text- und bildbasierten eigenen Vorstellung und Darbietung der eigenen Leistung etc. Es werden Gästebücher geführt, Kontaktformulare oder Diskussionsforen angeboten. Innovative Unternehmen

[18] www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/UpdatePatchManagement/updatePatchManagement_node.html



bieten beispielsweise einen Online-Warenkorb, der aus ihren Angeboten zusammengestellt werden kann, sowie eine Kommunikationsschnittstelle mit ihren Zulieferern.

Der Internet-Browser stellt hierbei nicht nur die Inhalte der Internetseiten dar, er ist auch eine Art Betriebssystem für die Programme, die in den Internetseiten eingebettet sind. So vorteilhaft die neue Technik für eine schnelle und kostengünstige Zusammenarbeit ist, die digitale Welt ist genauso angreifbar wie die reale, analoge Welt. Sie ist nicht gefeit gegen Angriffe und Manipulation. Auch hier müssen „Verkehrsregeln" im Umgang mit Geschäftspartnern eingehalten werden. Die Prüfung der Vertrauenswürdigkeit eines potenziellen Partners wird nicht ersetzt durch die Verwendung eines neuen Mediums. Aktive Inhalte sind die Grundlage für interaktive Elemente. Sie sollten nur für denjenigen zugelassen werden, dessen Reputation für eine Zusammenarbeit spricht. Mit Hilfe der Internet-Browser kann hierfür eine Kategorisierung für Internetseiten vorgenommen werden. Dies ist insbesondere sinnvoll, da gerade die Kriminellen über sehr gute Programmierkenntnisse verfügen und auch über Lücken in Programmen bestens informiert sind.

Die Programmteile des Internet-Browsers zur Ausführung der aktiven Inhalte tragen meist die Bezeichnung Plug-in, Add-in oder Add-on. Die Programme selbst bestehen beispielsweise aus JavaScript, VB-Script, Flash oder ActiveX und sind auch in Office-Programmen oder PDF-Dateien enthalten. Ob ActiveX, Java-Skript, Flash-Videos oder PDF-Dateien – man sollte aktive Inhalte möglichst nur für vertrauenswürdige Seiten zulassen. Die Einstellungen hierzu können im Internet-Browser vorgenommen werden. Wichtig auch: das eigene Verhalten im Internet. So verlockend beispielsweise kostenlos angebotene Gruß- oder Glückwunschkarten, Gedichte, Rezepte, Spiele oder Freeware auch sind: Nicht alles ist so harmlos, wie es auf den ersten Blick scheint. Die Vertrauenswürdigkeit des Seitenbetreibers und dessen Sicherheitsvorkehrungen sollten die Grundlage für die Nutzung der Inhalte sein.

Schutz durch Virenscanner

Der bloße Einsatz eines aktiven Virenscanners reicht nicht aus, um sich gegen Viren zu wehren. Aus dem vorhergehenden Abschnitt dieses Kapitels „Absicherung durch Netzwerkadministration" (S. 55) wird ersichtlich, dass der Schutz eines Virenscanners durch seine Konfiguration begrenzt wird. Es ist von entscheidender Bedeutung, wer ihn modifizieren bzw. beenden kann. Grundsätzliches zum Einsatz eines Virenscanners finden Sie im Kapitel „Elementarschutz IT-Organisation", dort speziell in den Abschnitten:

- Schutz vor Malware (S. 44)
- Vorsicht mit Freeware (S. 49)
- Wer kümmert sich, wer trägt die Verantwortung? (S. 50)

Moderne Virenscanner verfügen über eine heuristische Suche bzw. verhaltensbasierte Erkennung.

Wird seitens der Mitarbeiter intensiv mit Internet und E-Mail gearbeitet und werden auch Downloads durchgeführt oder multimediale bzw. aktive Elemente genutzt, sollte der Virenschutz mehrstufig erfolgen. Zum einen zentral, speziell für die Prüfung von E-Mails, zum anderen lokal; dabei sollten Virenscanner unterschiedlicher Hersteller verwendet werden. Beispielsweise für den Einsatz von E-Mail gibt es spezielle Verfahren und Scanner am E-Mail-Server, um die Inhalte auf Spam-E-Mails, Viren und unerwünschte Programme zu prüfen. Dabei werden Dateianhänge, Inhalte und eingebettete Links überprüft. Bei verschlüsselten Internetseiten und E-Mails ist ergänzend ein lokaler Virenscanner zwingend erforderlich, da erst am lokalen PC die Entschlüsselung erfolgt und erst dann eine Prüfung möglich ist. Gerade bei Nutzung des Internets ist ein regelmäßiger, vollständiger Prüflauf besonders wichtig, zusätzlich zu den Prüfungen durch den Zugriffsscanner. Bei Zugriff bedeutet, dass eine Prüfung nur bei einem Schreib- und/oder Lesevorgang erfolgt. Gerne erfolgt die Prüfung „bei Zugriff" nur mit eingeschränktem Funktionsumfang. Grundsätzlich sollte die Option zur Prüfung von Scripten aktiviert sein. Zudem wird von Virenscannern seit einiger Zeit ein Verfahren eingesetzt, welches auch das Verhalten von Programmen analysiert. Damit kann brandneue Malware bereits identifiziert werden, noch bevor sie weitläufig bekannt wird: Grundsätzlich vergehen von der Freisetzung eines Virus über seine Erkennung bis zum Schutz durch Sicherheitssoftware ca. 6 Stunden. Neue Malware kann sich in diesem Zeitraum bereits eingenistet haben. Zum Verständnis: Täglich werden Tausende neuer Varianten von Schädlingen erstellt. Ein regelmäßiger, vollständiger Scan aller Dateien sorgt für zusätzlichen Schutz. Hierbei sollten auch Optionen wie komprimierte bzw. gepackte Dateien oder heuristische Suche aktiviert werden.

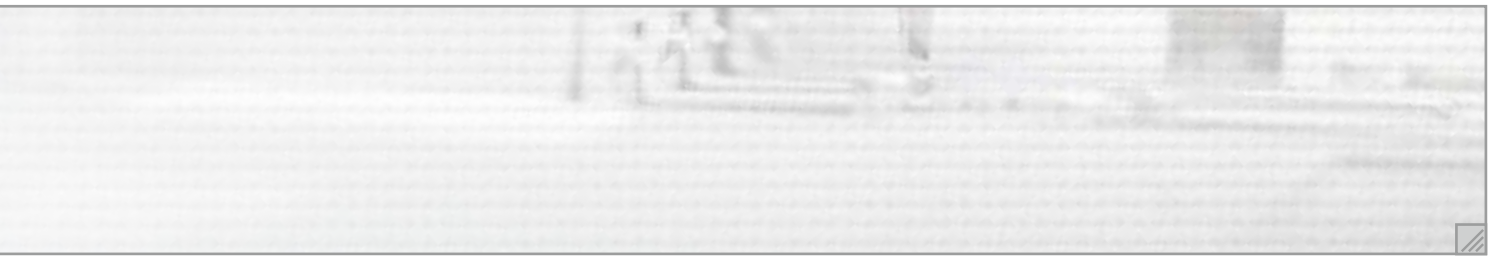
In einem Netzwerk muss gewährleistet sein, dass alle eingesetzten PCs gleich konfiguriert und mit Updates auf dem gleichen Stand sind. Dabei dürfen auch die Server, Notebooks oder Handys etc. nicht vergessen werden, also jegliche Hardware mit Kontakt zum Unternehmensnetzwerk.

Wer einem Virenscanner alleine nicht vertraut, kann sich zusätzlich mit Spezial-Software auf die Suche nach einzelnen Schädlingstypen machen oder seinen PC gegen unberechtigte Änderungen absichern. Empfehlenswert sind Spezialprogramme zum Schutz vor Rootkits und Spyware, soweit diese Funktion nicht bereits im Virenscanner enthalten ist. Dabei muss jedoch besonders darauf geachtet werden, dass sich die unterschiedliche Software nicht gegenseitig in die Quere kommt oder gar den PC zum Absturz bringt.

Personal Firewall

Eine Firewall alleine bietet nicht immer ausreichend Schutz.

Eine gut gepflegte Firewall trägt zu einem Mehr an Sicherheit gerne mit. Firewalls gehören heute ebenso wie Virenscanner zu den etablierten Schutzprogrammen. Daher wiegen sich viele Anwender in Sicherheit. Die klassischen Firewalls schützen vor unbefugtem Zugang zum PC von außen. Aus diesem Grund werden beim ersten kriminellen Angriff vor allem kleine Programme zur Organisation und Steuerung der eigentlichen Schadprogramme installiert. Von dort aus werden dann weitere Programme aus dem Internet nachgeladen. Werden diese vom Computer angefordert, ist dies für klassische Firewalls ein zulässiger Vorgang, der nicht unterbunden wird.



Enthält eine Firewall eine Applikations-Komponente, dürfen nur explizit freigegebene Programme online gehen. Zulässige Programmoperationen können durch eine Feinsteuerung explizit zugelassen oder verboten werden. Damit wird verhindert, dass Spyware sich selbst Zugang zum Internet verschafft. Mit Hilfe einer Blacklist werden bestimmte, als gefährlich eingestufte Adressen im Internet unzugänglich gemacht. Diverse Hersteller von Sicherheitssoftware prüfen Herkunfts- und Zieladressen von bekannter Malware und nehmen diese Server auf den Index, solange Gefahr besteht. Dies hat den Vorteil, dass einmalig befallene Internet-Seiten wie auch Privat-PCs nach ihrer Säuberung wieder im Internet erreichbar sind.

Beim Einsatz einer Firewall sollte diese als zentrale Komponente an einem Server betrieben werden. Gibt es keine zentrale Firewall, liegt die Verantwortung beim Administrator oder bei den einzelnen Mitarbeitern. Die Qualität der Absicherung entspricht dann der Fähigkeit, die vorhandene Personal Firewall zu konfigurieren und deren Funktion und Aktualität zu prüfen. Analog zum Virenscanner gilt: Wird die Firewall nicht ordnungsgemäß gepflegt und werden nicht Regeln angepasst und Sicherheitsupdates aktualisiert, können Hacker auf die Computer eindringen und dort Daten manipulieren, löschen oder auch einfach ausspionieren. Achten Sie deshalb darauf, dass Ihre Personal Firewall durch die Installation von Patches immer auf dem aktuellen Stand und Ihrem individuellen Schutzbedarf entsprechend konfiguriert ist.

Im gewerblichen Bereich sollte nicht auf die Lernfunktion einer Firewall gesetzt werden. Im Zweifel besitzen Mitarbeiter kein ausreichendes Know-how, um die je nach Software sehr technischen Einstellungen zu beurteilen und die Konfiguration vorzunehmen. Ein EDV-Partner ist hier die erste Wahl. Unternehmen, die keine oder nur eine rudimentäre Firmen-Firewall haben, können diese auch als Managed Security Services zu einem Dienstleister auslagern. Dieser installiert die nötige Hard- und/oder Software und übernimmt Update-, Wartungs- und Konfigurationsdienste.

Gefahren ins Bewusstsein bringen

Internetnutzung im Unternehmensnetz ist kein Risiko, wenn Sie eine professionell gepflegte Sicherheitslösung einsetzen.

Auch wenn beim Einsatz von IT ein vollständiger Schutz nicht permanent möglich ist, lässt sich doch das Risiko deutlich verringern. Behörden, Provider und Sicherheitsexperten verschiedener Unternehmen gehen gegen die kriminellen Aktivitäten an – mit mehrstufiger, professioneller Sicherheitssoftware und fundiertem Know-how. Gefährliche Seiten und viele aktuelle Angriffe können durch die aufgebaute Infrastruktur innerhalb weniger Tage aus dem Netz eliminiert werden. Jeder Nutzer sollte aber auch selbst aktiv werden: Das Bewusstsein über Gefährdungen und die ständige Information über die neuesten Methoden ist ein wesentliches Element, nicht auf aktuelle Machenschaften der Kriminellen hereinzufallen.

Verzichten Sie nicht auf die Vorzüge des Internets: Ausgeklügelte Sicherheitssysteme, die rund um die Uhr von Experten gepflegt werden, und hilfreiche Tools ermöglichen einen einfachen und sicheren Gebrauch.

Das Bundesamt für Sicherheit in der Informationstechnik informiert über grundlegende Sicherheitsmaßnahmen.

Wer mit personenbezogenen Daten arbeitet, sein Firmen-Know-how schützen möchte oder Finanztransaktionen im Internet durchführt, ist gut beraten, die Sicherheitsvorkehrungen den aktuellen Anforderungen anzupassen. Dies kann jedoch nur funktionieren, wenn der Verantwortliche über mögliche Gefahren und Bedrohungsszenarien umfassend informiert ist. Viele Maßnahmen können in Eigenregie umgesetzt werden. Einen Überblick über die Möglichkeiten bieten die Grundschutzkataloge des BSI (Bundesamt für Sicherheit in der Informationstechnik, www.bsi.de).

Die Verwendung von Security-Software stellt dabei heute nur mehr den Grundschutz dar. Die einmalige Einrichtung von Sicherheitslösungen ist jedoch nicht ausreichend, um nachhaltig den Schutz der EDV zu gewährleisten. Eine regelmäßige Überprüfung und Anpassung an die aktuellen Erfordernisse ist für das Aufrechterhalten der Sicherheit wichtig. Um mit der Entwicklung der finanziell gut situierten Schattenwirtschaft mithalten zu können, gehen die Sicherheitsanbieter dazu über, Managed Security Services (MSS) anzubieten, die Betreuung der IT-Sicherheit als Dienstleistung.

Die derzeit häufigsten Gefährdungen:
Keylogger

Das kriminelle Werkzeug mancher Angreifer sind sogenannte Keylogger[19], die sowohl in Software als auch in Hardware vorkommen können. Die Software-Keylogger besitzen ausgefeilte Methoden, um sich vor dem Anwender zu verbergen und Anti-Spyware bzw. Virenscanner auszutricksen. Sie können auch „Schnappschüsse" des Monitorbildes oder Tonaufzeichnungen anfertigen. Der Angreifer erhält die Daten per Mail.

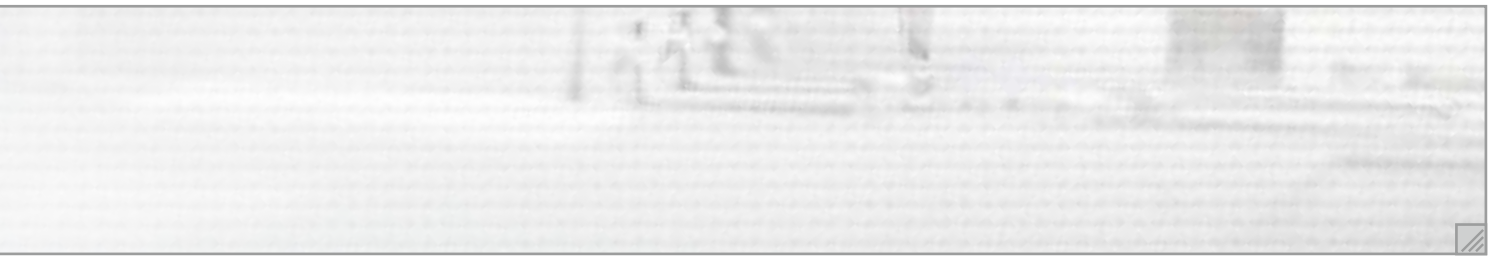
Aber auch sogenannte Innentäter verursachen mit Hardware-Keyloggern auf vergleichbare Weise Schäden. Hardware-Keylogger sind zwar im Funktionsumfang beschränkt, müssen aber aufgrund ihrer fehlenden Wechselwirkung mit dem PC erst einmal gefunden bzw. identifiziert werden: Sie befinden sich beispielsweise in USB-Steckern zwischen Tastatur und PC, was der technische Laie kaum bemerkt. Als Innentäter kommen nicht nur Mitarbeiter, sondern auch Dritte wie Besucher, Geschäftspartner und Dienstleister in Frage. Sie haben unter Umständen ebenfalls Zutritt zu den Aktenschränken, Servern, Rechnern und zu mobiler Hardware. Als potenzieller Angreifer kommt bereits in Frage, wer

- im Unternehmen Software installieren kann bzw.
- in die Nähe der Rechner gelangt.

In der Regel werden Software-Keylogger bei bzw. nach ihrer Installation von einem Virenscanner in aktueller Version und mit aktueller Signatur-Datenbank erkannt. Wer jedoch über die Berechtigung verfügt, Programme zu installieren, kann unter Umständen vorhandene Programme wie einen lokalen Virenscanner auch modifizieren.[20]

[19] Keylogger = Es werden in der Grundfunktion sämtliche Tastatureingaben protokolliert.

[20] vgl. Kapitel 2 „Elementarschutz IT-Organisation" (S. 39 ff.) bzw. Abschnitt „Absicherung durch Netzwerkadministration" (S. 55)



Eine Möglichkeit, die Protokollierung von Passwörtern zu verhindern, sind virtuelle Tastaturen[21]. Nachteil dieser Variante ist allerdings, dass die Eingabe im Einzelfall nicht vertraulich ist. Doch auch der richtige Einsatz der Benutzerverwaltung des Betriebssystems leistet hier gute Dienste.

Botnetz – die unfreiwillige Teilnahme an Betrügereien

Ein Botnetz ist ein Verbund von PCs, auf denen Software zur Fernadministration installiert wurde. Es ist eine Art Trojaner, durch die ein befallener PC über das Internet ferngesteuert werden kann. Besonders perfide dabei: Der PC scheint ganz normal zu arbeiten, während sich gleichzeitig im Hintergrund lauter unerfreuliche Dinge abspielen. Damit wird ein Rechner nicht nur Opfer, sondern gleichzeitig auch Täter. Er erhält seine Befehle aus dem Internet und führt diese ohne Ihre Kontrolle aus. Eine einzige kriminelle Person kann so alle angeschlossenen Bots zentral in ihrem Netzwerk steuern. Die Infektion mit einem Schadprogramm kann auf verschiedene Wege erfolgen. Bots werden, wie andere Schadprogramme auch, oft mittels eines Virus oder Wurms auf den Computer eingeschleust. Von nun an ist man Besitzer eines Zombie-PCs. Der Computer kann von einem Dritten ferngesteuert werden und wird zum Mitglied eines aus vielen Computern bestehenden virtuellen Verbundes: dem Botnetz.

Drive-by-Downloads[22]: Vorsicht beim Surfen

Eine außerordentlich gefährliche Variante von manipulierten Webseiten, bei der keine Aktion des Benutzers erforderlich ist, sind Drive-by-Downloads: Die Infektion vollzieht sich als Download schon allein beim Betrachten einer Seite. Hier werden die Schwachstellen des Browsers ausgenutzt. Auch harmlos erscheinende Seiten können von Crackern ohne Wissen der Webseitenbetreiber verändert und zur Verbreitung von Schadsoftware genutzt werden. Ein solcher Vorgang erfolgt, ohne dass der Anwender davon Kenntnis hat. Daher wird er durch den Besuch einer präparierten Webseite selbst zum Wirt und infiziert andere. Schließlich sollte noch eine letzte Internetgefahr erwähnt werden, die im Web-2.0-Zeitalter verstärkt um sich greift. Hier wird die arglose Mitteilsamkeit und Selbstdarstellung mancher Zeitgenossen im Internet für kriminelle Machenschaften missbraucht.

Social-Networking-Webseiten

Bei Social-Networking-Webseiten handelt sich um Internet-Plattformen, bei denen Einzelpersonen persönliche Profile hinterlegen, aber auch Bekanntschaften zu anderen Personen angeben können.

Durch die Veröffentlichung privater und beruflicher Daten sowie die Bekanntschaft zu anderen Personen sollen soziale Netzwerke aufgebaut werden. Doch mit diesen Daten lässt sich auch Missbrauch betreiben. So kann eine „persönliche" E-Mail formuliert, die beim Netzwerk hinterlegte E-Mail-Adresse eines Freundes gefälscht und ein Trojaner angehängt werden.

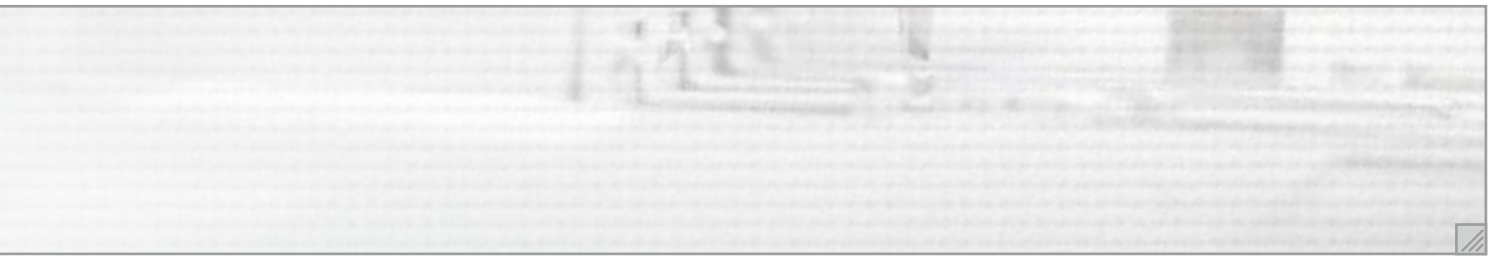
[21] Mit virtuellen Tastaturen ist eine Software gemeint, die eine Tastatur am Bildschirm anzeigt.

[22] Drive-by = im Vorbeisurfen. Beim Aufruf einer manipulierten Internetseite werden Programme auf den PC automatisch heruntergeladen und installiert. Dies geschieht entweder durch aktive Inhalte (z. B. JavaScript) oder durch Fehler bzw. Lücken im Browser.

Schutzmaßnahmen im Überblick

- Installieren Sie ein Viren- und Spyware-Schutzprogramm und halten Sie dieses nicht nur mit Signatur-Updates, sondern auch mit Programm-Upgrades immer auf dem aktuellen Stand.
- Setzen Sie eine Personal Firewall ein – aktualisieren Sie diese regelmäßig und passen Sie die Firewall-Regeln den aktuellen Erfordernissen an. Nutzen Sie darüber hinaus Firewall-Optionen wie Intrusion Prevention bzw. Intrusion Detection.
- Prüfen Sie regelmäßig die Protokolle des Antiviren- und Spyware-Programms sowie der Firewall.
- Prüfen Sie regelmäßig den Zustand der Sicherheitssoftware.
- Achten Sie darauf, ob es Sicherheitsupdates für Ihr Betriebssystem und für jede weitere von Ihnen installierte Software gibt, und führen Sie diese durch.
- Arbeiten Sie nach Möglichkeit nicht als Administrator an Ihrem PC, denn so können Schadprogramme noch mehr Unheil anrichten. Richten Sie für alle Nutzer eines PCs unterschiedliche Benutzerkonten ein.
- Vorsicht bei Downloads aus dem Internet. Vergewissern Sie sich, ob die Quelle vertrauenswürdig ist. Bei Tauschbörsen besteht beispielsweise eine hohe Wahrscheinlichkeit, sich zu infizieren.
- Besuchen Sie keine zwielichtigen Internetseiten.
- Deaktivieren Sie im Browser „Aktive Inhalte“. Über „Aktive Inhalte“ können sich Bots und andere Schadprogramme leichter auf Ihrem Rechner installieren.
- Und für den Fall, dass doch Schaden an Programmen oder Daten entstehen sollte, bewahren Sie regelmäßig eine Datensicherung auch außerhalb von ihrem PC auf.

Achten Sie auf Hinweise der Betreiber von Social-Network-Plattformen im Hinblick auf Sicherheit: Seriöse Anbieter geben beispielsweise ihren Nutzern konkrete Hinweise und Handlungsanweisungen, wie man sich sicher in einem sozialen Netzwerk verhält und welchen Gefahren man begegnen kann.



Gut beraten mit Managed Security Service

Was in großen Unternehmen üblicherweise ein eigenständiger IT-Administrator übernimmt, wird in kleineren Unternehmen oft einem Mitarbeiter übertragen oder vom Chef selbst erledigt. Bei Betrachtung der Kosten für einen gut ausgebildeten IT-Fachmann mehr als verständlich. Allerdings verfügt ein Spezialist natürlich auch über entsprechend hohes Know-how. Liegt die Verantwortung für Wartung und Pflege der Sicherheitssoftware beim Unternehmen, müssen bereits bei Auswahl, aber auch bei Wartung und Pflege einige wichtige Aspekte beachtet werden. Dazu gehört das regelmäßige Kontrollieren der Funktionsweise und der Einstellungen der Sicherheitssoftware. Die Qualifikation ist ein besonders wichtiger Aspekt bei der Beurteilung, wer sich um Konzeption, Installation und Pflege der Sicherheit kümmern sollte. Sie entscheidet, ob auf den Maßnahmen nicht nur Sicherheit draufsteht, sondern auch gewährleistet ist: Die Zuweisung der Verantwortung allein befähigt in der Regel keinen Mitarbeiter dazu, ein Netzwerk zu administrieren, Sicherheitssoftware auf die Spezifika des Unternehmens anzupassen und auf dem aktuellen Stand zu halten. Es muss ausreichend Zeit eingeplant werden, um sich mit der Materie auseinanderzusetzen. Hinzu kommt die wachsende Komplexität der an den Verantwortlichen gestellten Anforderungen im Bereich Internetsicherheit, Betriebssicherheit und Datensicherung sowie Systemwartung, z.B. in Form von Updates. Ist grundlegendes Wissen vorhanden, muss dieses immer wieder auf den neuesten Stand gebracht werden.

Die Verwendung von Security-Software stellt dabei lediglich den Grundschutz dar. Es ist erforderlich, die Arbeitsweise im Unternehmen mit ihren Vorschriften und Maßnahmen in ihrer Wechselwirkung zu berücksichtigen. Die einmalige Einrichtung von Sicherheitslösungen beispielsweise ist nicht ausreichend, um nachhaltig den Schutz der EDV zu gewährleisten. Eine regelmäßige Überprüfung und Anpassung an die aktuellen Erfordernisse ist für das Aufrechterhalten der Sicherheit wichtig.

Die ordnungsgemäße Funktion von Sicherheitssoftware steht und fällt mit der kompetenten Konfiguration der Software – und der Möglichkeit, diese für den normalen Anwender zu sperren. Wer auf jeden Fall sichergehen möchte, lagert diese Funktionen als Managed Security Service an Spezialisten aus. Um mit der Entwicklung der finanziell gut situierten Schattenwirtschaft mithalten zu können, gehen die Sicherheitsanbieter dazu über, Managed Security Services (MSS) anzubieten, die Betreuung der IT-Sicherheit als Dienstleistung. Das speziell hierfür ausgebildete Personal eines Dienstleisters sorgt dann dafür, dass nicht nur Sicherheit installiert, sondern auch vorhanden ist. Doch selbst in diesem Fall ist die Mitwirkung der Mitarbeiter erforderlich: Sie müssen ihren Teil dazu beitragen, dass aus Sicht der Software legale Vorgänge, also Aktionen ohne erkennbaren Hackereinfluss oder Viren, keinen Schaden verursachen.

4 E-Mail-Verkehr

Die Kommunikation per E-Mail ist im geschäftlichen Bereich nicht unumstritten.

Die zunehmende Digitalisierung von Geschäftsprozessen wurde maßgeblich durch den Übergang von analoger auf digitale Kommunikation bestimmt. Vom reinen Informationsaustausch bis hin zur Abwicklung rechtsgültiger Geschäfte – heute wird die elektronische Post immer wichtiger. Doch leider lässt die Sicherheit der E-Mail-Kommunikation häufig noch zu wünschen übrig. Neben Viren, Phishing und Spam sind sowohl die Integrität und Authentizität als auch die Verschlüsselung bei der E-Mail-Sicherheit zu berücksichtigen. Von besonderer Bedeutung ist die Überprüfbarkeit des Absenders und der Integrität der E-Mail bzw. deren Anhänge. Dazu kommt die Archivierungspflicht geschäftskritischer E-Mails aufgrund gesetzlicher Vorschriften.

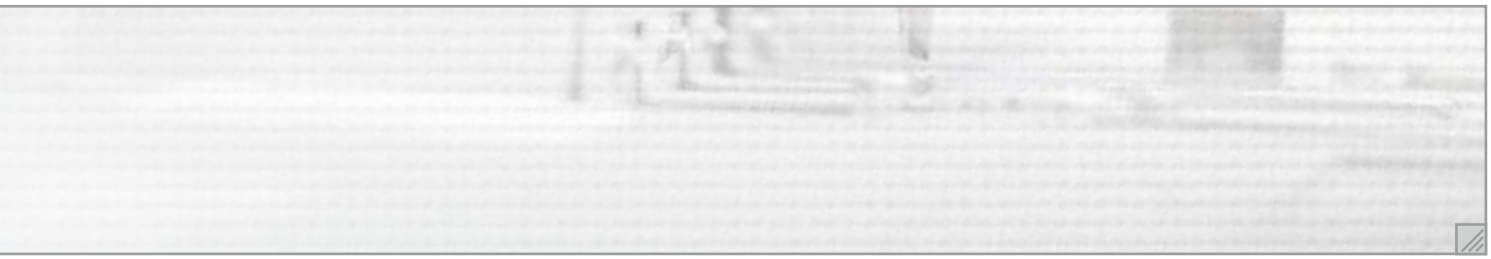
Entscheidend für den E-Mail-Verkehr ist, dass:

- die E-Mail-Systeme rund um die Uhr verfügbar sind und die Nachrichten in angemessener Zeit bearbeitet werden (Verfügbarkeit).
- die Kommunikationspartner eindeutig zu identifizieren sind (Authentizität).
- die Inhalte der Nachrichten auf dem Übertragungsweg nicht verändert werden (Integrität).
- die Inhalte nicht in die Hände unberechtigter Dritter fallen (Vertraulichkeit).

Datenaustausch mit Geschäftspartnern

E-Mail-Verschlüsselung und -Signaturen helfen bei der Sicherstellung von Integrität, Authentizität und Vertraulichkeit der elektronischen Firmenkorrespondenz.

Seit dem Siegeszug der Breitbandverkabelung ist es üblich, neben dem Nachrichtentext der E-Mail auch umfangreiche Dokumente kurzfristig und kostengünstig zu versenden. Verträge, Gesprächsnotizen, interne Unterlagen oder andere vertrauliche und personbezogene Daten werden täglich per E-Mail versandt. Dieser Datenaustausch wird immer häufiger genutzt: Er geht schnell und einfach. Dieses bequeme Verfahren hat jedoch auch einige Schattenseiten. Einfache E-Mails lassen sich mit einigem Aufwand auch abfangen, lesen und manipulieren. Mit einer zusätzlichen Softwarekomponente können diese Mängel jedoch beseitigt werden. Nützlich sind hier Softwarepakete, mit denen E-Mails sowohl signiert als auch verschlüsselt werden können. Der Empfänger kann so sicher sein, dass der Absender wirklich der ist, für den man ihn hält, und dass die Nachricht nicht von unberechtigten Dritten gelesen oder sogar verändert wurde. Bei geschäftlichen E-Mails sollten diese Kriterien unbedingt beachtet werden.



Vertraulichkeit durch Verschlüsselung

Vertraulichkeit durch Verschlüsselung.

Im Internet ist ein Mitlesen der E-Mails durch unberechtigte Dritte nicht ausgeschlossen. Zumindest solange die E-Mail unverschlüsselt auf ihrem Weg ist: Bei der einfachen E-Mail-Kommunikation ist die Vertraulichkeit nicht gegeben, denn der Inhalt der Dokumente ist für jeden einsehbar, genau wie bei einer Postkarte auf dem Postweg. Beim Datenaustausch mit Geschäftspartnern muss aber gewährleistet sein, dass nur der gewünschte Empfänger die Daten einsehen kann. Dabei darf nicht vergessen werden, dass die eingehenden Mails und Dateianhänge nach der Entschlüsselung noch auf Viren geprüft werden müssen.

Vorsicht ist auch geboten bei kostenlosen E-Mail-Anbietern. E-Mails der Nutzer werden z. T. elektronisch ausgewertet. Ein Hinweis darauf ist oft Bestandteil der AGBs.

Sich selbst und den Inhalt ausweisen durch Signatur

Integrität und Authentizität durch Signatur.

Zusätzlich kann die E-Mail signiert werden. Die Signatur ermöglicht es zu erkennen, ob die elektronische Post auf dem Weg durch das Internet verändert wurde. Zum anderen ist der Absender zweifelsfrei identifizierbar.

Elektronische Signatur

Das deutsche Signaturgesetz schafft den Rahmen für die Rechtsverbindlichkeit.

Elektronische Signaturen basieren auf digitalen Zertifikaten. Diese sind mit einem digitalen Personalausweis vergleichbar und dienen der Authentifizierung und Identifizierung im Internet. Das deutsche Signaturgesetz schafft einen rechtlichen Rahmen für elektronische Signaturen mit dem Ziel, ein elektronisches Äquivalent zur handschriftlichen Unterschrift zu haben. Daher führt im Allgemeinen der Einsatz qualifizierter elektronischer Signaturen zur Erfüllung gesetzlicher Schriftformerfordernisse.

Spam-E-Mail

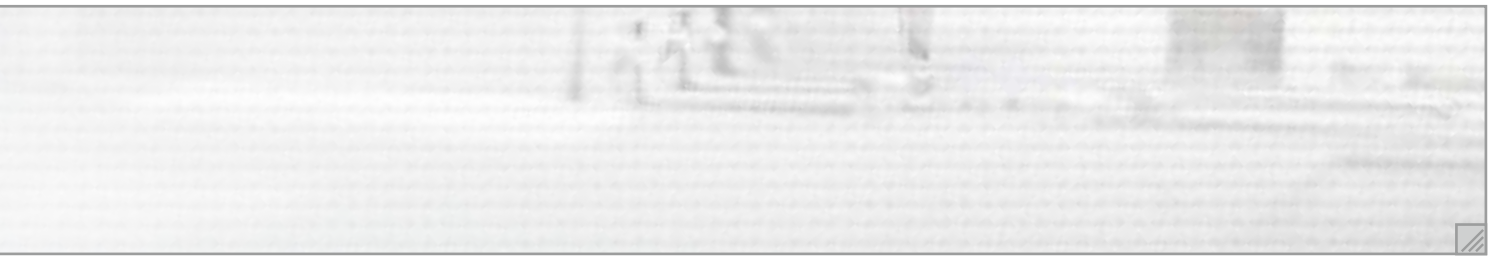
Das automatisierte Ausfiltern unerwünschter E-Mails kann mit einem E-Mail-Filter erfolgen. Ein Spezialfall bei der E-Mail-Kontrolle sind „False Positives", also fälschlicherweise aussortierte E-Mails. Da es kein absolut perfektes System hierfür gibt, muss der Administrator regelmäßig die aussortierten E-Mails durchforsten und kommt so in direkten Kontakt mit E-Mails, die nicht für seine Augen bestimmt sind. Auf der einen Seite ist es daher erforderlich, die Mitarbeiter über dieses notwendige Verfahren in Kenntnis zu setzen. Auf der anderen Seite muss sich der hierfür Verantwortliche seiner Verpflichtung im Klaren sein, solche Einblicke vertraulich zu behandeln. Der Datenschutzbeauftragte spielt hierbei eine wichtige Rolle als Aufklärungs- und Kontrollinstanz.

Elektronisch signierte Rechnungen

Immer häufiger versenden Unternehmen, besonders Telekommunikationsanbieter und Versorgungsunternehmen, ihre Rechnungen elektronisch. Nicht ohne Grund, denn das Verfahren spart Porto, Druck und Papier. Der Versandaufwand ist wesentlich geringer, wodurch sich Arbeitsprozesse optimieren lassen. Um den Vorsteuerabzug geltend zu machen, gilt es aber zu beachten, dass die Echtheit der Herkunft und die Unversehrtheit des Inhaltes gewährleistet ist.
Gemäß dem durch das Steuervereinfachungsgesetz 2011 geänderten §14 UStG kann dies erreicht werden durch jegliche innerbetriebliche Kontrollverfahren, die einen verlässlichen Prüfpfad zwischen Rechnung und Leistung schaffen können (§14 Abs. 1 UStG). Unbeschadet dieser zulässigen Verfahren kann dies auch mittels qualifizierter elektronischer Signatur oder elektronischem Datenaustausch erfolgen (UStG §14 Abs. 3).
Ein innerbetriebliches Kontrollverfahren erfüllt die Anforderungen, wenn es einen verlässlichen Prüfpfad gibt, durch den ein Zusammenhang zwischen der Rechnung und der zugrunde liegenden Leistung hergestellt werden kann. Dies kann im Rahmen eines entsprechend eingerichteten Rechnungswesens erfolgen, aber z. B. auch durch einen manuellen Abgleich der Rechnung mit vorhandenen geschäftlichen Unterlagen (z. B. Kopie der Bestellung, Auftrag, Kaufvertrag, Lieferschein, Überweisungs- oder Zahlungsbeleg). Es werden keine technischen Verfahren vorgegeben, die die Unternehmen verwenden müssen. [23]

Der Empfänger muss, bei Verwendung einer Signatur, neben der elektronischen Rechnung auch die Nachweise über die Echtheit der Herkunft und die Unversehrtheit des Inhaltes aufbewahren, also auch die Signatur und das Ergebnis der Signaturprüfung. Besonders bei elektronischen Eingangsrechnungen sind deshalb klare Vereinbarungen zwischen Unternehmen und Geschäftspartner erforderlich, damit der Vorsteuerabzug nicht nachträglich versagt wird.

[23] vgl. Teil 3, Kapitel 2, Abschnitt „De-Mail", S. 94



Voraussetzungen für die sichere Kommunikation

Beide Seiten müssen dieselbe Technologie verwenden und auch beherrschen. Neben der Installation und Einrichtung müssen vor dem gesicherten Versand einer E-Mail erst erfolgreich die Verschlüsselungsschlüssel (öffentliche Schlüssel) gegenseitig ausgetauscht werden. Während innerhalb einzelner Geschäftsverhältnisse diese Hürden problemlos genommen werden können, ist die Kommunikation mit Institutionen und Behörden meist schwieriger. Öffentliche Einrichtungen stellten bisher wenige Möglichkeiten bereit, vertrauliche Daten per E-Mail gesichert zu übermitteln.[24] Deshalb ist es nicht verwunderlich, wenn im Zweifelsfall dann doch eine unverschlüsselte E-Mail versendet wird. Beispielsweise sind beim Versenden von Änderungen von Personaldaten etc. oder Lohnauswertungen auch personenbezogene Daten der Mitarbeiter betroffen, sodass auch deren Zustimmung vorliegen muss. Es kommt somit entscheidend auf den verschickten Inhalt an. Um im Sinne von Compliance-Regeln beim E-Mail-Versand nach den bestehenden Gesetzen und Rechtsvorschriften zu handeln, ist eine Lösung notwendig, die sich in Ihre Arbeitsabläufe integriert, unternehmensweite Sicherheitsrichtlinien definiert und Sie in deren Umsetzung unterstützt.

Archivierung von E-Mails

Auch für E-Mails können gesetzliche Aufbewahrungspflichten gelten.

Zunehmend werden Angebote, Verträge usw. per E-Mail verschickt. Steuerrelevante Mails gelten als originär elektronische Dokumente und müssen daher elektronisch archiviert werden. Fehlende oder unsachgemäße Archivierung kann beispielsweise zu Problemen bei der digitalen Betriebsprüfung führen. Konventionelle E-Mail-Systeme sind oft nur bedingt für die langfristige Aufbewahrung konzipiert. Geeignet hierfür sind Dokumenten-Management-Systeme (DMS), die als revisionssicher zertifiziert sind.

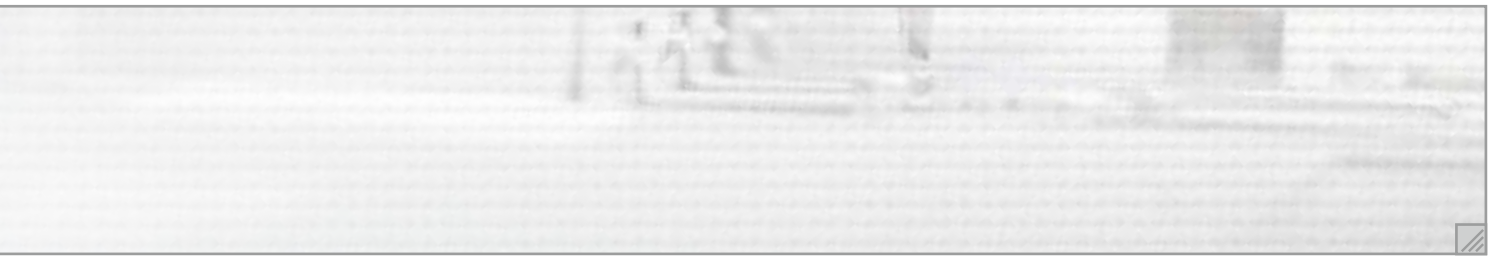
[24] vgl. zu aktuelle Bestrebungen, Teil 3, Kapitel 2 „Der Staat online – eGovernment", S. 90

Anders als bei Datensicherungen, die ausschließlich dazu dienen, einen bestimmten Bearbeitungsstand im Notfall wiederherzustellen, müssen bei einer ordnungsmäßigen Aufbewahrung von Daten und Dokumenten viele Einzelaspekte berücksichtigt werden. Zweck der steuerrechtlichen Aufbewahrungsvorschriften ist die Dokumentation und Beweissicherung gegenüber der Finanzverwaltung. Die gesetzlich festgelegten Aufbewahrungszeiträume erstrecken sich über mehrere Jahre.

Fazit

Um Sicherheit zu gewährleisten, muss der komplette Prozess der E-Mail-Kommunikation auf den Prüfstand. Neben Computerschädlingen sind auch die Verschlüsselung der E-Mails und aufgrund gesetzlicher Vorschriften auch die Archivierung geschäftskritischer E-Mails zu berücksichtigen.[25]

[25] vgl. Broschüre „Sichere E-Mail-Kommunikation“: www.datev.de/sicherheit



Aspekte der sicheren E-Mail-Kommunikation

- Verfügbarkeit
- Verschlüsselung
  Wie wird in Ihrem Unternehmen sichergestellt,
  - dass kein Unbefugter beim Übertragen E-Mails mitlesen kann?
  - dass eingehende E-Mails einfach entschlüsselt werden?
- Authentifizierung + Integrität
  Wie wird in Ihrem Unternehmen sichergestellt, dass
  - der Empfänger E-Mails unverfälscht erhält?
  - die Echtheit des Absenders gewährleistet ist?
- Virenschutz
  Wie wird in Ihrem Unternehmen sichergestellt, dass
  - E-Mails virenfrei versendet werden?
  - eingehende E-Mails virenfrei sind?
- Spam-Filter
  Wie wird in Ihrem Unternehmen sichergestellt, dass Sie keine Spam-Mails erhalten?
- E-Mail-Archivierung
  Wie werden in Ihrem Unternehmen E-Mails lesbar für alle Mitarbeiter archiviert?
- Organisation IT-Infrastruktur
  Wie wird in Ihrem Unternehmen sichergestellt, dass
  - jeder Mitarbeiter E-Mails einfach und effizient verfassen, erhalten und lesen kann?
  - der E-Mail-Verkehr im Einklang mit Datenschutz und Persönlichkeitsrechten erfolgt?

5 Mobile Endgeräte

Im Zuge steigender Mobilität erhöht sich der Einsatz von Notebooks und Arbeitsplätzen, die von außerhalb Zugriff auf das Unternehmensnetzwerk haben müssen. Der Trend geht hier ganz klar zu verteilten Arbeitsumgebungen. Damit die Verantwortlichen jederzeit über relevante Unternehmensdaten verfügen können, liegen Geschäftsinformationen heute auf Smartphones, Notebooks oder in webbasierten Unternehmensportalen bereit. Mit dieser Entwicklung steigt auch die Gefahr, dass Daten verloren gehen oder gezielt gestohlen werden.

Notebook-Verschlüsselung

Der Diebstahl eines Notebooks ist das zweithäufigste Computerdelikt nach Virenattacken. Für maximale Sicherheit bei minimaler Einschränkung des Notebook-Anwenders sorgt eine vollständige Verschlüsselung der Festplatte. Dabei werden auch systembedingte Sicherheitslücken geschlossen, wie z. B. die Speicherung von Daten in temporären Dateien. Auf diese Weise können Sie wie gewohnt weiterarbeiten, ohne Ihre Arbeitsweise umstellen zu müssen. Beim Starten des Rechners ist eine Authentifikation notwendig, z. B. via SmartCard bzw. USB-Stick mit eingebauter SmartCard. Damit erreichen Sie eine weitergehende Absicherung.

Funkverbindung zu den Unternehmensdaten

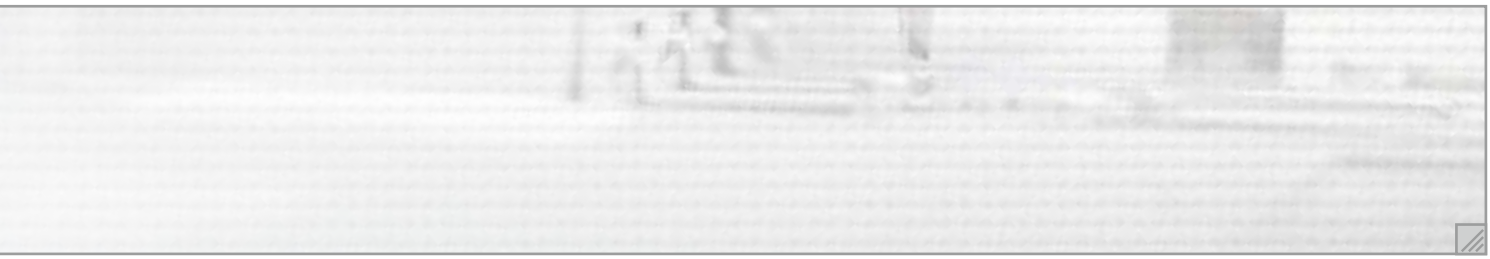
Eine Alternative hierfür ist die permanente Verbindung mit dem Unternehmensnetzwerk via Funknetzwerk. Sollen unterwegs Daten auf einem Notebook verarbeitet werden, bietet sich hierzu eine Telearbeitsplatz-Software an: Programme und Daten von Geschäftspartnern liegen auf dem Server im Unternehmen. Ein Missbrauch durch Fremde ist ausgeschlossen und die Hardware selbst kann gegen Diebstahl versichert werden. Abgesichert werden muss nur die Kommunikationsverbindung, der Online- bzw. Remote-Zugang zum Unternehmensnetzwerk[26].

Notebook – den flexiblen Einsatz vorbereiten

Mobiles Arbeiten mit Notebook und drahtlose Kommunikation erfordern organisatorische Vorkehrungen. Sonst bleibt die Sicherheit auf der Strecke.

Wesentliche Voraussetzung für den universellen Einsatz von Notebooks ist die konkrete Einsatzplanung vor der Integration in die tägliche Arbeit. Soll das Notebook in unterschiedliche Netzwerke integriert werden, steht der Nutzen in direktem Zusammenhang mit der gegenseitigen Verträglichkeit und Stabilität und damit der Betriebssicherheit des Gerätes und des Netzwerkes. Um den Datenschutz einzuhalten, ist ein besonderes Augenmerk auf die sichere Kommunikation zu setzen. Denn der entscheidende Vorteil ist allerdings auch das zentrale Risiko: der drahtlose Anschluss an Netzwerke. Notebooks und Smartphones etc. sind von Haus aus mit unterschiedlichen Kommunikationsschnittstellen ausgestattet. Sie können direkt mit einem Unternehmensnetzwerk verbunden werden und agieren dann wie ein PC. Je nach geplantem Einsatzszenario können Daten entweder auf dem Gerät abgelegt werden oder stehen per Remote-Verbindung zum Unternehmensnetzwerk direkt zur Verfügung. Gerade die hochflexibel einsetzbaren mobilen Geräte besitzen mit WLAN,

[26] vgl. Abschnitt „Administration von Unternehmensnetzwerken“, S. 46 ff.; Kapitel 3 „Internet“, S. 54 ff.; Kapitel 5 „Mobile Endgeräte“, S. 72 ff.



Bluetooth etc. weitere Möglichkeiten, Verbindungen herzustellen. Diese sollten für den jeweiligen Einsatzzweck ausgewählt, konfiguriert und kontrolliert oder abgestellt werden.[27]

Unverzichtbar für die Arbeit mit mobilen Geräten sind Virenscanner und Firewall.

Virenscanner und Firewall sind grundsätzlich unverzichtbar. Dies gilt nicht nur beim Arbeiten im Internet, sondern auch bei Vernetzung des Unternehmens mit Heimarbeitsplätzen, mobilen Geräten oder unterschiedlichen Standorten. Sie schützen die Firmendaten vor Manipulation und Zerstörung sowie vor unberechtigtem Zugriff durch Außenstehende. Sicherheit gewährleisten sie allerdings nur, wenn sie regelmäßig aktualisiert werden. Software-Hersteller stellen in der Regel bedarfsorientiert Sicherheitsupdates zum Download bereit. Benutzerkonten und Passwörter sind ebenfalls ein Muss (siehe auch S. 46 ff.).

Doch Sicherheitssoftware allein kann nicht vor allen Gefährdungen schützen. Ist beispielsweise einem Mitarbeiter im Betriebssystem seines PCs das Recht eingeräumt, die Festplatte zu löschen, könnte ein Angreifer aus dem Internet dies im ungünstigsten Fall ebenfalls. Weniger ist also mehr – bzw. sicherer. Denn: Was der Benutzer nicht darf, darf auch „seine" Software nicht. Die Mitarbeiter sollten sich daher als Benutzer und nicht als Administrator anmelden. Wesentliche Einstellungen und Bestandteile des Betriebssystems können damit nicht mehr manipuliert werden.

Nutzung von Windows Terminal Servern

Ein Windows Terminal Server (WTS) ist eine in mehrfacher Hinsicht interessante Lösung. Das Unternehmen ist flexibel auf den Mischbetrieb von festen, mobilen und ausgelagerten Arbeitsplätzen vorbereitet. Und auch der Datenschutz kommt nicht zu kurz. Im Gegensatz zum Client-Server-Betrieb laufen die Programme nicht mehr auf den einzelnen PCs bzw. Notebooks, sondern auf dem Server. Übertragen werden nur Bildschirminhalte, Tastatureingaben oder Mausbewegungen etc. Datensicherungen und Updates von Programmen können von einem Administrator-PC aus durchgeführt werden. Die Organisation und Verwaltung von Datenhaltung und Programmen findet an zentraler Stelle statt. Auch Verhaltensvorschriften wie die Wahl des Datenverzeichnisses (Datensicherung) oder Virenprüfung können durch zentrales Arbeiten leichter durchgesetzt werden. Eine unerwünschte Programminstallation von Benutzern kann über die Nutzungsrechte leicht unterbunden werden. Positiver Nebeneffekt: Schädliche Programme können sich selbst bei Fehlern der Mitarbeiter nicht installieren bzw. das Betriebssystem lahmlegen.

Mobiler Zugriff auf Unternehmensdaten – auch mit den Kleinsten

Eine Sonderstellung nehmen Smartphone und PDA ein. Ein PDA kann mit einem Mobiltelefon verbunden werden und so auf das Internet bzw. die Daten im Unternehmen zugreifen. Smartphones sind eine Kombination aus Mobiltelefon und PDA. Diese Geräte können zwar ebenfalls direkt und sicher auf das Unternehmen zugreifen, aufgrund von Restriktionen, z.B. des Betriebssystems und der Darstellungsmöglichkeiten, ist dies jedoch nicht zu empfehlen. Der Datenaustausch mit dem Unternehmen kann dagegen via Mail oder per Synchronisation erfolgen.

[27] Die aktuellen Empfehlungen bietet das Bundesamt für Sicherheit: www.bsi.de

Mobile Sicherheit auch für die Kleinsten

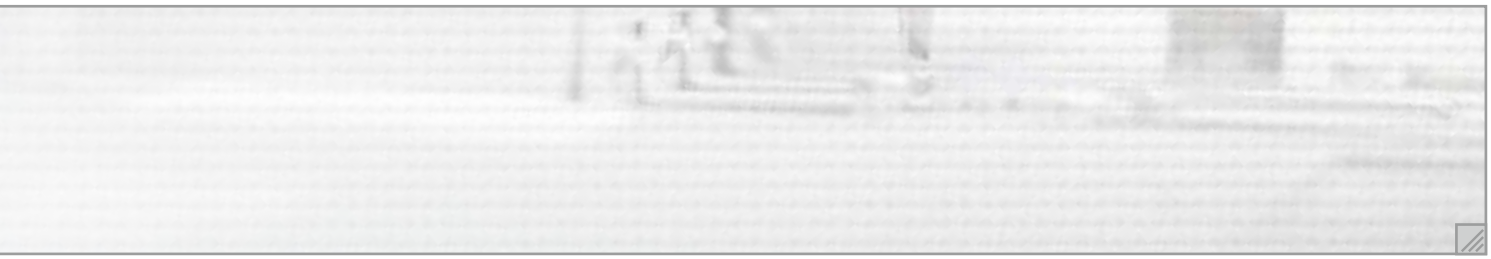
Die zunehmende Anzahl der Applikationen unterstreicht den Trend zu höherer Mobilität und zu kleineren Endgeräten. Mobile Endgeräte wie beispielsweise Smartphones oder BlackBerry sind zunehmend mit vollwertigen Betriebssystemen ausgestattet. Das erhöht ihre Funktionalität, macht sie aber auch wie den PC angreifbar. Durch eine Verbindung mit dem Unternehmensnetzwerk wird das insgesamt vorliegende Sicherheitsniveau durch den schwächsten Partner bestimmt. Mit steigender Mobilität der Berufstätigen erfolgt zudem eine Verlagerung des Arbeitsplatzes und somit auch der unternehmensrelevanten Daten hin zu mobiler Hardware. Die Gefahr ist groß, dass sowohl Daten als auch Hardware dabei verloren gehen. Im Gegensatz zu den üblichen Sicherheitsvorkehrungen beim PC müssen sich diese bei den Kleinrechnern erst noch etablieren. Das hohe Verlustrisiko erfordert ein sicheres Authentisierungs- und Verschlüsselungsverfahren sowie eine penibel durchgeführte Datensicherung. Auch die verschiedenen Schnittstellen wie WLAN oder Bluetooth erhöhen überproportional das Risiko von Schäden durch Angriffe oder Viren. Zugangspasswörter, Virenscanner und Firewall sind auch bei den Kleinen ein Muss.

Risiken bewusst machen

Durch den fließenden Übergang vom Telefon zum „mobilen Computer" ist das Risikobewusstsein der Anwender noch nicht sehr geschärft. Doch wer geschäftlich unterwegs ist, ist gut beraten, sich nicht nur von den umfangreichen Möglichkeiten der Kleinrechner verführen zu lassen, sondern auch ein wachsames Auge auf die Sicherheitsvorkehrungen zu werfen.

Sicher mobil mit WLAN, UMTS und VPN

Ob Handy, PDA, USB-Medien oder Notebook – mobile Hardware ist verlockend: Mitarbeiter können Reisezeiten zur Leistungserstellung nutzen. Das Risiko, Hardware samt Arbeitsergebnissen zu verlieren, ist jedoch deutlich höher als beim Arbeiten im Unternehmen. Verbleiben Daten und Arbeitsergebnisse im Unternehmensnetzwerk und erfolgt der Zugriff darauf lediglich per Funknetzwerk, bietet dies bereits mehr Sicherheit. Auf diese Weise arbeitet man beispielsweise mit dem Notebook so, als wäre man im Unternehmen: jederzeit auskunftsbereit, unabhängig vom Aufenthaltsort und den Öffnungszeiten. Gerade drahtlose Netze wie Wireless LAN oder UMTS machen diesen Einsatz möglich. Für WLAN finden sich in Flughäfen, Bahnhöfen, Restaurants immer mehr öffentliche Zugänge, die sogenannten Hotspots, an denen beispielsweise der Internetzugang möglich ist. WLAN wird vornehmlich im Kurzstreckenbereich eingesetzt. UMTS dagegen bietet direkten Zugang zum Funknetz von Mobilfunkanbietern und ermöglicht ebenfalls den direkten Zugang zum Internet. Unterschiede zwischen UMTS und WLAN bestehen hinsichtlich der Reichweite, Übertragungsgeschwindigkeit, einzelner Sicherheitsaspekte und der damit verbundenen Kosten dieser Systeme. Gerade bei drahtloser Nutzung sollte man aber besonderen Wert auf das Thema Sicherheit legen: Hierbei schneiden



WLAN-Hotspots gegenüber UMTS deutlich schlechter ab, denn bei UMTS gehört die Verschlüsselung der Datenübertragung zur Grundausstattung. Der Einsatz der VPN-Technik hat sich bei Fernzugriffen bewährt: Eine VPN-Lösung bietet den Vorteil, dass hierbei ein sicherer Tunnel zwischen Endgerät und Unternehmensnetzwerk aufgebaut wird. Der Schutz ist dann nicht nur unabhängig von der Wahl des drahtlosen Netzwerks, sondern ist ebenso vorhanden, wenn die Verbindung über eine stationäre DSL-Leitung aufgebaut wird.

Sichere Verbindung mit VPN.

Sicherheit – Gegner des Komforts?

Die Sicherheit tritt leicht in den Hintergrund, wenn die neue Technik begeistert. Wenn Daten beispielsweise per Funk übertragen werden, sind wie beim Radioempfang Störungen oder Funkschatten möglich. Und genau wie beim Radio kann grundsätzlich ein fremder Empfänger die übertragenen Daten ebenfalls „hören". Ohne Sicherheitsmaßnahmen kann beispielsweise jeder WLAN-Nutzer, der sich im Funkbereich des Hotspots oder des Notebooks befindet, das bereitstehende Netzwerk nutzen. Im schlimmsten Fall könnte ein Fremder Daten Ihres Notebooks auslesen.

Aus Gründen des Datenschutzes ist der Einsatz von WLAN nicht zu empfehlen.

Lange Jahre war es üblich, Notebook-Bildschirme so zu entwickeln, dass ein Einblick nur in einem sehr begrenzten Rahmen möglich war. Der eingebaute Sichtschutz bot ein hohes Maß an Sicherheit vor unberechtigter Einsichtnahme. Moderne Notebooks werden gerne als Multimedia-Stationen eingesetzt. Demzufolge haben die Hersteller sich auf diesen Trend eingestellt und die Blickwinkel deutlich vergrößert. Für den privaten multimedialen Einsatz eine Bereicherung, ist diese Entwicklung für den Einsatz in einem Unternehmen aus Datenschutzgründen nicht tragbar. Um den Sichtschutz zu gewährleisten, können jedoch Sichtschutzfolien auf den Bildschirm aufgebracht werden. Mit diesen wird die seitliche Lesbarkeit durch Unberechtigte deutlich reduziert.

Geschützt und verschlüsselt

↗ Viele WLAN-Besitzer sichern die Funkverbindung ihres drahtlosen Netzwerks mittels WEP-Verschlüsselung (Wired Equivalent Privacy), die ursprünglich eine dem Kabel vergleichbare Sicherheit bieten sollte. Für Hacker ist es jedoch ein Leichtes, durch frei verfügbare Tools sich binnen weniger Sekunden Zugriff auf ein solches Netzwerk zu verschaffen. Eine höhere Absicherung bieten andere Verfahren wie WPA, WPA-EAP etc., die ständig weiterentwickelt werden. WPA2 gilt derzeit als ausreichender Schutz. Doch bietet die aktuelle Funktechnik zurzeit nicht die Sicherheit einer Kabelverbindung. Datenschutz im WLAN kann nach dem aktuellen Stand der Technik bestenfalls durch das Verschlüsseln der Daten, beispielsweise mit VPN, bei der Übertragung gewährleistet werden. Ohne diese sind die Daten während der Übertragung für jeden sicht- und lesbar, ähnlich einer Postkarte.

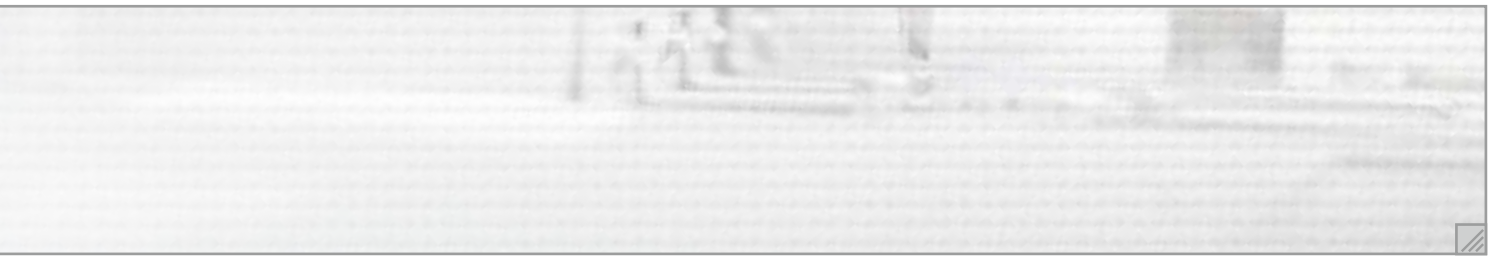
6 Notfallkonzept

Für ein Unternehmen gibt es verschiedene Arten der Bedrohung, etwa technisches Versagen durch Stromausfall oder Hardwaredefekt, höhere Gewalt wie Wasserrohrbruch oder schadhafte Software, die sich etwa über Viren verbreitet. Aber auch vorsätzliches Handeln durch Löschen von Daten durch Mitarbeiter oder Nachlässigkeiten und Fehlbedienung im Unternehmen sind Ursache für viele IT-Sicherheitsprobleme.

Die Bewältigung der täglichen Aufgaben im Unternehmen ist ohne den Einsatz angemessener Hard- und bedarfsgerechter Software in einem geschützten IT-Umfeld kaum denkbar. Mit einer sogenannten Risikoanalyse kann die Gefahr einer „unsicheren" bzw. risikobehafteten IT erkannt und der Ausfall oder die Störung der IT-Infrastruktur in den Unternehmen bewertet werden, sodass darauf aufbauend entsprechende Schutzmaßnahmen zur Risikominimierung abgeleitet werden können. Dies wird gerne als Notfallkonzept bezeichnet.

Fragestellungen zur Ermittlung des eigenen Sicherheitsstandards als Ausgangspunkt für Sicherheitsmaßnahmen

- Wie ist die externe Kommunikation (Internetzugang, Telearbeitsplätze, Fernwartung) abgesichert?
- Kennen Sie die vergebenen Zugriffsberechtigungen auf Daten und Software?
- Ist im Unternehmen auf allen Arbeitsplätzen ein Virenschutz vorhanden und wird dieser laufend aktualisiert? Werden relevante Sicherheitsupdates zeitnah installiert?
- Läuft die Datensicherung vollständig und ohne Fehler? Wird die Datenrücksicherung getestet?
- Versenden und empfangen Sie Daten von extern nur entsprechend abgesichert?
- Sind Daten auf mobilen Geräten gegen fremden Zugriff geschützt? Sind vertrauliche Informationen auf mobilen Datenträgern sicher geschützt?
- Werden die Vorschriften des BDSG eingehalten (Bestellung eines Datenschutzbeauftragten, vertragliche Gestaltung mit externen Partnern, Dokumentation u. v. m.)?
- Ist ein ausreichender Passwortschutz im Unternehmen etabliert?
- Sind die Systeme gegen Zugriff Dritter sowie Diebstahl gesichert?



Ereignisse mit Folgen

Das IT-Notfallkonzept beschreibt die Maßnahmen, die beim Ausfall einzelner IT-Komponenten oder des gesamten IT-Systems ergriffen werden sollen.

Schadensereignisse kommen mit unterschiedlicher Wahrscheinlichkeit und mit sehr unterschiedlichen Ursachen und Folgen vor – vom stundenweisen Ausfall der EDV bis hin zur Existenzbedrohung. Manche Schadensereignisse wie Naturkatastrophen lassen sich nicht verhindern, wobei es dann gilt, die möglichen Folgen und Auswirkungen zu beachten und zu minimieren, damit diese nicht existenzbedrohlich werden können. Eine Möglichkeit ist beispielsweise die abgesicherte Aufbewahrung von Sicherungsbändern auch außerhalb der Räumlichkeiten des Unternehmens.

Für den Geschäftsbetrieb eines Unternehmens ist es notwendig, dass die EDV funktioniert und dass Akten sowie Daten jederzeit verfügbar sind – bei Bedarf auch für Prüfer. Darüber hinaus müssen die Dokumente für die Dauer der Aufbewahrungspflicht vor Vernichtung geschützt werden.

Ein IT-Notfallkonzept sollte deshalb folgende Fragen beantworten: Was passiert, wenn die IT ausfällt? Welche Bereiche sind bei Ausfall welcher Systeme betroffen? Welche Ausfallzeit kann sich das Unternehmen leisten? Welche Maßnahmen werden ergriffen, um die Lauffähigkeit der Systeme wiederherzustellen? Dies ist wichtig zu definieren, da bereits kurzfristige Unterbrechungen zu erheblichen finanziellen Schäden führen können. Ein Notfallkonzept umfasst immer technische und organisatorische Lösungen.

Hierzu gehören beispielsweise: Um für Wasser oder Brandschäden gerüstet zu sein, werden Datensicherungen und Kopien von Programmen auch außerhalb des Unternehmens aufbewahrt. Wer ist für Schlüssel im Notfall verantwortlich? Wer ruft Polizei bzw. Feuerwehr? Wie ist das Vorgehen im Virenfall? Wer muss informiert werden und was ist zu tun, wenn Notebook oder mobile Hardware abhanden gekommen ist? Wer muss informiert werden, wenn Telefone bzw. Server ausfallen? Etc.

Ziel des Notfallmanagements ist es, sicherzustellen, dass wichtige Geschäftsprozesse selbst in kritischen Situationen nicht oder nur temporär unterbrochen werden und die wirtschaftliche Existenz der Institution auch bei einem größeren Schadensereignis gesichert bleibt. Eine ganzheitliche Betrachtung ist daher ausschlaggebend. Es sind alle Aspekte zu berücksichtigen, die zur Fortführung der kritischen Geschäftsprozesse bei Eintritt eines Schadensereignisses erforderlich sind, nicht nur die Ressource Informationstechnik. IT-Notfallmanagement ist ein Teil des Notfallmanagements.[28]

[28] www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Vollständige IT-Notfallpläne beinhalten neben Krisenstab und Alarmierungsplan vor allem Anleitungen zur Wiederherstellung kritischer IT-Anwendungen und -Systeme.

Vorgehen im Notfall[29]

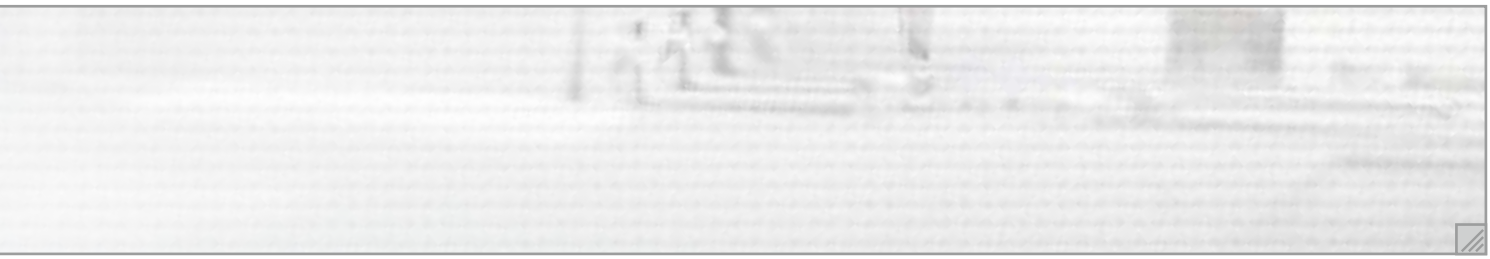
Ein Handlungsplan mit klaren Prioritäten der Sicherheitsziele und -maßnahmen sollte erstellt werden
Wer eine Weile über sinnvolle Schritte zur Erhöhung der eigenen IT-Sicherheit nachgedacht hat, wird sich bald vor mehr Aufgaben gestellt sehen, als er zeitlich und finanziell bewältigen kann. Daher ist eine geeignete Priorisierung identifizierter Sicherheitsziele und -maßnahmen erforderlich. Diese Priorisierung sollte auch unter Abwägung des Kosten-Nutzen-Verhältnisses getroffen werden.

Zuständigkeiten müssen festgelegt werden
Für jede identifizierte Aufgabe muss festgelegt werden, wer für die Durchführung verantwortlich ist. Ebenso sollte für alle allgemein formulierten Sicherheitsrichtlinien genau dargelegt werden, für welchen Personenkreis diese verbindlich sind: Betreffen diese nur festangestellte Mitarbeiter, eine bestimmte Abteilung oder alle? Jeder Verantwortliche braucht einen Stellvertreter. Wichtig ist, dass der Vertreter auch in der Lage ist, seine Aufgaben wahrzunehmen. Wurde er in seine Aufgaben eingewiesen? Sind notwendige Passwörter für den Notfall hinterlegt? Benötigt er Dokumentationen?

Notfallchecklisten sollten erstellt werden und jedem Mitarbeiter bekannt sein
Die Checklisten sollen Mitarbeitern die wichtigsten Handlungsschritte vorgeben. Um im Einzelfall bedarfsorientiert entscheiden zu können, sollten auch Telefonnummern der jeweils Zuständigen dokumentiert sein. Gibt es geeignete Vertretungsregelungen für Verantwortliche und sind die Vertreter mit ihren Aufgaben vertraut? Sind die wichtigsten Passwörter für Notfälle sicher hinterlegt?

Notfallvorsorge
Gibt es einen Notfallplan mit Anweisungen und Kontaktadressen? Werden alle notwendigen Notfallsituationen behandelt? Kennt jeder Mitarbeiter den Notfallplan und ist dieser gut zugänglich?

[29] www.bsi.bund.de/DE/Themen/ITGrundschutz/LeitfadenInformationssicherheit/leitfaden_node.html



7 Rechtliches zum Datenschutz

Abgabenordnung, Strafgesetzbuch, Telemediengesetz oder Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme etc. liefern den rechtlichen Handlungsrahmen für das Unternehmen in der realen sowie in der digitalen Welt.

Experten unterscheiden gerne zwischen Datenschutz und Datensicherheit. Die Datensicherheit steht für eine fehlerfreie Erfassung, Verarbeitung und Speicherung betriebsnotwendiger Daten. Im Rahmen der Buchführung bedeutet dies beispielsweise die ordnungsgemäße, korrekte Verarbeitung der eingegebenen Buchungen. Zu den betriebsnotwendigen Daten gehören auch jegliche Arten von elektronisch abgelegten Verträgen oder auch Kalkulationen, die Kostenrechnung oder Rechnungen etc. Im engeren Sinne bezeichnet Datenschutz den Schutz personenbezogener Daten. Dabei ist es unerheblich, ob es sich hierbei um Daten über Mitarbeiter, Kunden, Lieferanten oder sonstige natürliche Personen handelt.

Datenschutz und Datensicherheit werden in der Fachwelt begrifflich voneinander unterschieden.

Maßnahmen für Datenschutz und -sicherheit

Die regelmäßig auftretenden Ereignisse und Pressemeldungen über Datenschutzvorfälle in Unternehmen zeigen, wie wichtig der Schutz von personenbezogenen Daten sowie von Geschäfts- und Berufsgeheimnissen für ein Unternehmen ist und welcher Schaden bei Verstößen entstehen kann. Unternehmen sind inzwischen auf die Verarbeitung von Daten durch die Informationstechnik angewiesen. Maßnahmen zum Datenschutz und zur Datensicherheit dienen dem Schutz der Mitarbeiter, Kunden und Geschäftspartner – und damit dem Schutz des Unternehmens. Unabhängig davon ist jedes Unternehmen aufgrund von gesetzlichen Vorgaben und insbesondere durch das Bundesdatenschutzgesetz (BDSG) verpflichtet, sich mit Datenschutz und IT-Sicherheit auseinanderzusetzen. Viele Anforderungen des Datenschutzes beziehen sich auch auf die Sicherheit der Informationstechnologie (IT). Nur eine zuverlässig funktionierende und sichere IT-Infrastruktur ermöglicht die reibungslose Abwicklung produktiver und verwaltungstechnischer Geschäftsvorfälle und Prozesse.

Gesetzliche Anforderungen zum Datenschutz

Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS), Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), Sarbanes-Oxley Act (SOX), Bundesdatenschutzgesetz (BDSG), Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) – die Liste von Gesetzen und Regulierungen mit direkten oder indirekten Auswirkungen auf die Firmen-IT wird von Jahr zu Jahr länger. Trotz unterschiedlicher Formulierung bleibt eine Anforderung gleich: die Pflicht, für fundierte IT-Sicherheit zu sorgen. Darüber hinaus sind verschiedene Ausprägungen zu beachten, etwa die Pflicht zur Archivierung von E-Mails (GDPdU), die Implementierung von Kontrollmechanismen (SOX) oder das Führen von Verfahrensverzeichnissen (BDSG). Das rechtskonforme Handeln eines Unternehmens (Compliance) minimiert nicht nur das Risiko, haftungsrechtlich belangt zu werden, durch die hierfür notwendige Prozessanalyse ergeben sich auch Chancen, die Prozesse zu optimieren.

Das Bundesdatenschutzgesetz (BDSG) ist nicht nur eine gesetzliche Pflicht. Werden das Unternehmen und die damit verbundenen persönlichen Existenzen vor den datenschutz- und sicherheitsrelevanten Gefahren besser geschützt, stellt es auch eine hervorragende Chance dar.

Die Regelungen des BDSG

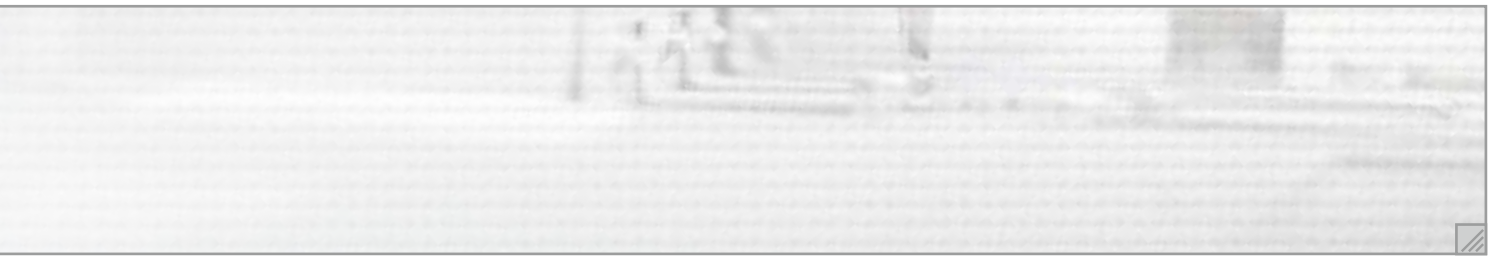
In allen Unternehmen wird eine Vielzahl personenbezogener Daten verarbeitet. Die vertrauliche Behandlung der Daten und die geschützte Verarbeitung wird von den Geschäftspartnern erwartet. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten bergen aber durchaus Gefahren und Risiken. Neben der fehlenden Verfügbarkeit der Daten zur Aufgabenerfüllung kann auch die Beeinträchtigung von Persönlichkeitsrechten der Betroffenen durch die Verarbeitung und Nutzung der Daten eine Bedrohung darstellen. Wie diese Daten zu schützen sind, wird unter anderem durch das BDSG geregelt. Normadressat und damit verantwortlich für die Durchführung der Schutzvorschriften ist immer der Unternehmer.

Datenschutzbeauftragter

Die Bestellung eines Datenschutzbeauftragten ist gesetzliche Pflicht, wenn mehr als neun Personen mit der automatisierten Datenverarbeitung befasst sind.

Fast täglich hört man im Zusammenhang mit IT-Sicherheit von neuen Virenwarnungen oder Hinweisen über gefälschte Internetseiten, die zum Ausspähen von Benutzerinformationen gedacht sind. Die Einhaltung des Datenschutzes stellt für viele Unternehmen eine große Herausforderung dar. Dies zeigt sich bereits bei der organisatorischen Umsetzung der gesetzlichen Pflicht zur Bestellung eines Datenschutzbeauftragten (DSB). Unternehmen, die personenbezogene Daten – dazu zählen Mitarbeiter- als auch Kundendaten – erheben und verarbeiten, sind nach dem Bundesdatenschutzgesetz verpflichtet, einen Datenschutzbeauftragten schriftlich zu bestellen, wenn mehr als neun Personen mit der automatisierten Verarbeitung befasst sind. Das schließt zum Beispiel die Personalabteilung und die im Verkauf tätigen Mitarbeiter ein. Damit dürfte ein Datenschutzbeauftragter also für einen Großteil der Unternehmen Pflicht sein. Er soll sicherstellen, dass die mit den Daten in Berührung kommenden Kollegen über die gesetzlichen und betrieblichen Datenschutzbestimmungen ausreichend informiert sind und gleichzeitig die technischen Einrichtungen des Unternehmens kontrollieren.

Ist es gesetzlich nicht erforderlich, einen betrieblichen DSB zu bestellen, muss der Leiter der verantwortlichen Stelle, in der Regel der Inhaber des Unternehmens, die Erfüllung der gesetzlichen Aufgaben des Datenschutzbeauftragten in anderer Weise sicherstellen. Die Funktion des DSB kann einem Beschäftigten (intern) oder einer Person außerhalb (extern) übertragen werden. Bestellt werden darf jedoch nur, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Nicht bestellt werden dürfen der Inhaber selbst, der Geschäftsführer oder sonstige gesetzlich oder verfassungsmäßig berufene Leiter. Aber auch der IT- oder Personalleiter darf aufgrund bestehender Interessenkonflikte bei der Ausübung der Tätigkeit nicht zum DSB bestellt werden. Im Falle eines Rechtsverstoßes ist die verantwortliche Stelle haftbar, in der Regel der Geschäftsführer.



Aufgaben eines Datenschutzbeauftragten

- Überwachung der Einhaltung von Datenschutzvorschriften
- Prüfung der ordnungsgemäßen Anwendung von Programmen
- Unterweisung der Mitarbeiter in die Anforderungen des Datenschutzes
- Erstellen eines internen und eines externen Verfahrensverzeichnisses auf Basis einer aktuellen Übersicht aller Verfahren mit personenbezogener Datenverarbeitung. Diese Übersicht wird von der Unternehmensleitung zur Verfügung gestellt.

Datenschutz bei Beauftragung eines externen Dienstleisters

Auch bei der Vergabe an externe Dienstleister sind die Unternehmer dafür verantwortlich, dass die Vorschriften des Datenschutzes eingehalten werden.

Wichtig ist auch die Beachtung der Datenschutzvorschriften bei Einbezug von externen Unternehmen zum Zwecke der Datenverarbeitung im Auftrag oder eines System-Partners für Updates und Wartungen im Unternehmen. Bei Einschaltung ist der Unternehmer als Auftraggeber verpflichtet, den Auftragnehmer unter besonderer Berücksichtigung des dort vorhandenen Datenschutz-Standards sorgfältig auszuwählen. Der Unternehmer bleibt jedoch weiterhin „Herr der Daten" und ist damit für die Einhaltung der Datenschutzvorschriften verantwortlich. Die Vorschriften für die Auftragsdatenverarbeitung wurden mit der BDSG-Novelle verschärft. So sind vertragliche Pflichtinhalte zwingend vorgeschrieben. Dazu gehören Umfang, Art und Zweck des Umgangs mit den Daten, die zu treffenden technischen und organisatorischen Maßnahmen, die Kontrollpflichten des Auftragnehmers und die Kontrollrechte des Auftraggebers sowie dessen Weisungsbefugnisse und auch Regelungen für die Löschung gespeicherter Daten beim Auftragnehmer. Die Information der Geschäftspartner über die externe Unterstützung erfolgt empfehlenswerterweise durch einen entsprechenden Passus in den Verträgen oder in den Allgemeinen Geschäftsbedingungen.

Informationssicherheit

Die Datensicherheit wird bereits aus dem eigenen Sicherheitsbedürfnis angestrebt, auch wenn sich ihre Notwendigkeit aus vielen gesetzlichen Anforderungen ableiten lässt.

Eng verbunden mit dem Datenschutz ist auch der Bereich Informationssicherheit bzw. IT-Sicherheit. Die obersten Ziele der IT-Sicherheit sind die Sicherstellung gegen Verlust von Daten, der fehlerhaften Verarbeitung und die Gewährleistung der Verfügbarkeit der IT-Systeme. Die Informationssicherheit bezieht sich nicht nur auf Daten, sondern auch auf alle übrigen Komponenten eines Informationssystems und berücksichtigt neben technischen auch organisatorische sowie personelle Aspekte.[30]

[30] vgl. Kapitel 2 „Elementarschutz IT-Organisation", S. 39 ff.

Tauschen Unternehmen und Geschäftspartner beispielsweise Daten per Datenträger oder Mail aus, so setzt der Geschäftspartner voraus, dass diese frei von Viren sind und der Datenaustausch ausreichend sicher erfolgt. Sollte dies nicht der Fall sein, entsteht ein nur schwer zu behebender Vertrauens- und Imageverlust. Zur Vermeidung von Schadensfällen bzw. zur Reduzierung der Folgen im Schadensfall müssen technische und organisatorische Maßnahmen realisiert werden. Hierbei reicht es nicht aus, die Verfügbarkeit der Systeme zu sichern. Auch die Vertraulichkeit der Informationen zur Vermeidung von Missbrauch, die Integrität von Daten und Programmen sowie die Verbindlichkeit bei der Kommunikation müssen gewährleistet sein.

Die acht Gebote der Datensicherheit

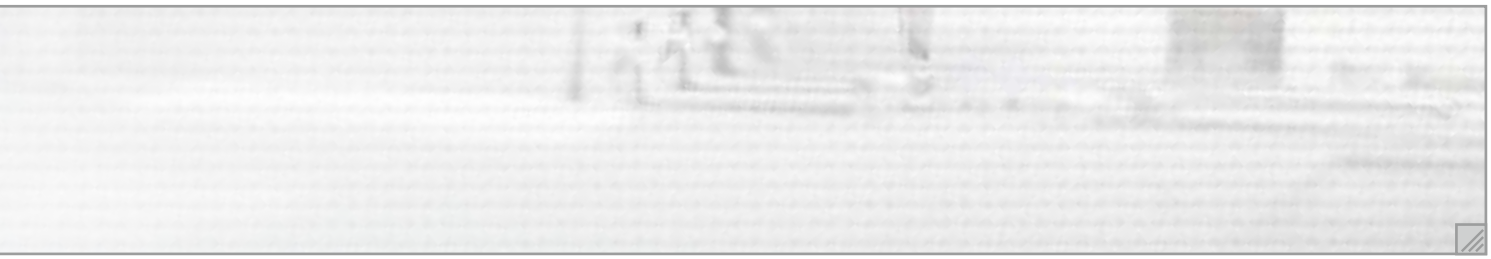
Maßnahmen zur Datensicherheit sind etwa nach dem BDSG in § 9 und Anlage vorgeschrieben. Das BDSG geht dabei von einem zusammenhängenden Schutzsystem von acht Sicherheitsgeboten aus. Diese umfassen neben der Zutritts-, Zugangs- und Zugriffskontrolle unter anderem auch eine Kontrolle der Weitergabe und der Eingabe sowie eine Sicherstellung der Verfügbarkeit der Systeme und Daten. Die Verarbeitung darf nur gemäß den Weisungen des Auftraggebers und nach dem Zweck ihrer Erhebung getrennt erfolgen. Dabei müssen die einzelnen Maßnahmen nur im Verhältnis zum angestrebten Schutzbedarf realisiert werden. Gemessen an der Vertraulichkeit der zu verarbeitenden Daten im Unternehmen zeigt die Praxis allerdings, dass von allen acht Geboten immer ein Mindestmaß umzusetzen ist. Auf diese Punkte wurde bereits im Notfallkonzept hingewiesen.

Datenschutz und IT-Sicherheit: Gefragt ist ein ganzheitliches Konzept[31]

Die Realität sieht jedoch in den Unternehmen anders aus: Häufig fehlt noch das Bewusstsein über mögliche Gefahren hinsichtlich Datenschutz und IT-Sicherheit. Mangels eigener Betroffenheit befasst man sich oft erst damit, wenn ein Schadensfall bereits eingetreten ist.

Ein ganzheitliches Konzept sollte immer durch individuelle Beratungen bei einer Einschätzung der Risiken und Ableitung von Maßnahmen sowie der Erarbeitung, Umsetzung und Weiterentwicklung von Sicherheitsrichtlinien oder Sicherheitskonzepten erfolgen. Der Nutzen eines systematischen Konzeptes, welches Datenschutz und IT-Sicherheit aus einem ganzheitlichen Ansatz heraus betrachtet, liegt auf der Hand. Auch die dynamische technische Entwicklung in den letzten Jahren hat zu immer komplexeren und offeneren Systemen geführt: War beispielsweise vor wenigen Jahren noch eine Unternehmens-Homepage und die Kommunikation per Mail selten, ist dies mittlerweile zur Selbstverständlichkeit geworden. Das Unternehmen hat sich damit nach außen geöffnet und es sind zusätzliche Bedrohungen hinzugekommen.

[31] Sicherheitskonzept: www.bitkom.org, Leitfaden „Sicherheit für Systeme und Netze in Unternehmen", www.bitkom.org/de/themen/54737.aspx



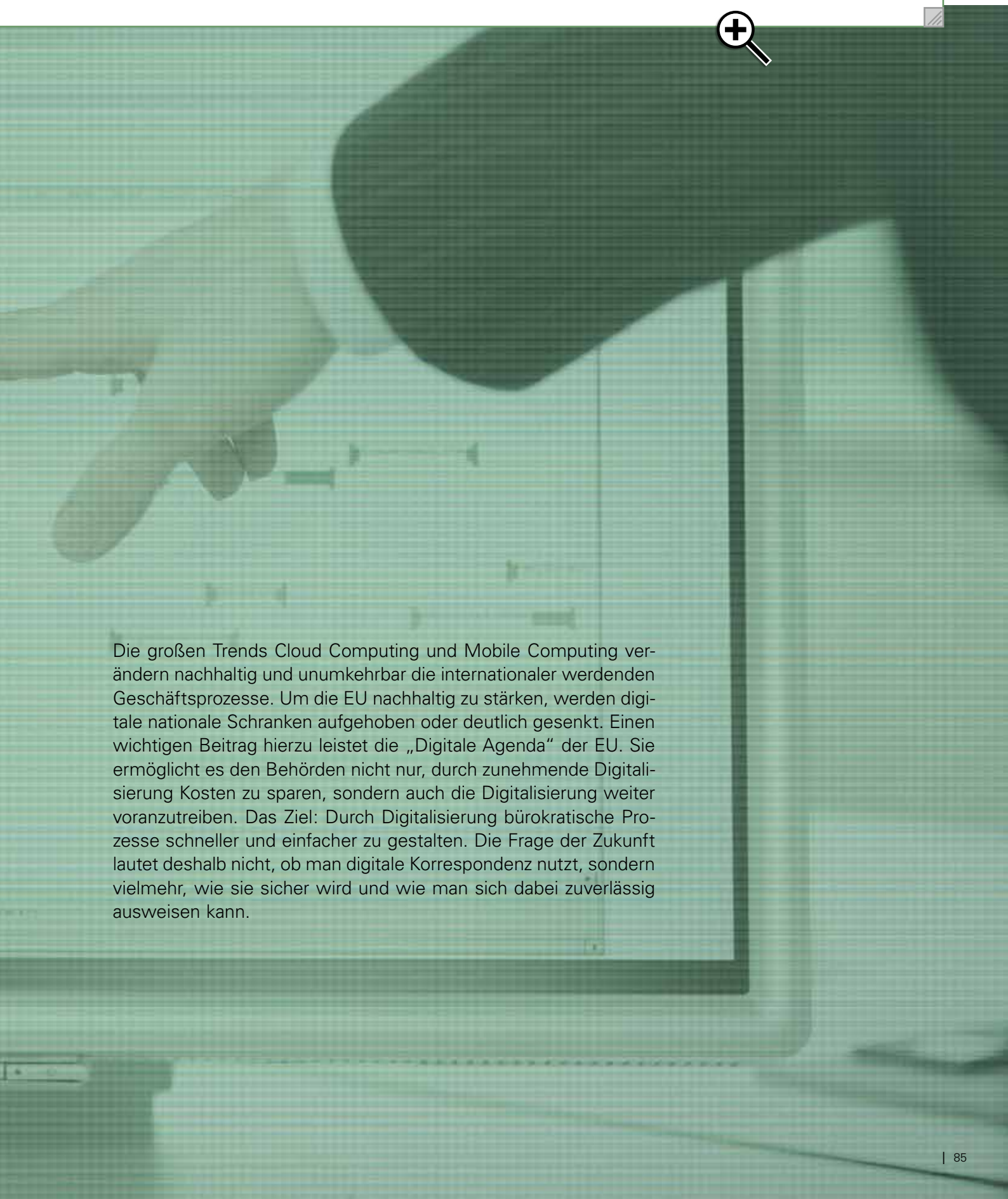
Fazit

Datenschutz und IT-Sicherheit ergänzen sich gegenseitig. Bei der Verarbeitung personenbezogener Daten sind neben dem Datenschutz auch die Ziele der IT-Sicherheit zu gewährleisten. Als Unternehmer ist es daher grob fahrlässig, sich dem Thema nicht zu stellen. Neben den gesetzlichen Vorschriften unter anderem durch das Bundesdatenschutzgesetz ergibt sich die Notwendigkeit bereits aus dem Eigeninteresse an der Existenzsicherung.

Jedes Unternehmen muss ein individuelles Datenschutz- und IT-Sicherheitskonzept erstellen, um sich vor datenschutzrechtlichen Problemen und Schadensereignissen zu schützen bzw. die Folgen daraus zu minimieren.

Digitale Korrespondenz

Teil 3



Die großen Trends Cloud Computing und Mobile Computing verändern nachhaltig und unumkehrbar die internationaler werdenden Geschäftsprozesse. Um die EU nachhaltig zu stärken, werden digitale nationale Schranken aufgehoben oder deutlich gesenkt. Einen wichtigen Beitrag hierzu leistet die „Digitale Agenda" der EU. Sie ermöglicht es den Behörden nicht nur, durch zunehmende Digitalisierung Kosten zu sparen, sondern auch die Digitalisierung weiter voranzutreiben. Das Ziel: Durch Digitalisierung bürokratische Prozesse schneller und einfacher zu gestalten. Die Frage der Zukunft lautet deshalb nicht, ob man digitale Korrespondenz nutzt, sondern vielmehr, wie sie sicher wird und wie man sich dabei zuverlässig ausweisen kann.

↗1 Das Finanzwesen online
↗2 Der Staat online – E-Government
↗3 Privat online
↗4 Geschäftspartner online
↗5 Social Media

01 | Kommunikation online

Noch nie war es so bequem und einfach wie heute, seine geschäftlichen und privaten Angelegenheiten online zu erledigen. Bankgeschäfte lassen sich über das Internet ausführen, Reisen werden im World Wide Web gebucht und sogar Steuererklärungen lassen sich über das Netz an die zuständigen Finanzämter verschicken. Wer dabei ein paar grundlegende Sicherheitsregeln beachtet, muss keine Angst davor haben, dass seine Daten in falsche Hände geraten.

1 Das Finanzwesen online

Der Begriff Phishing bezeichnet die kriminelle Vorgehensweise, mit der versucht wird, über gefälschte WWW-Adressen an sensible Daten eines Internet-Nutzers zu gelangen.

24 Millionen Deutsche erledigen ihre Bankgeschäfte mittlerweile per Internet – zwei Millionen mehr als noch 2007. Damit nutzen derzeit 38 Prozent aller Bundesbürger im Alter von 16 bis 74 Jahren Online-Banking. „Online-Banking ist eine der großen Erfolgsgeschichten des Internets", sagt BITKOM-Präsident Prof. Dr. August-Wilhelm Scheer. „Im Internet hat die Bank stets geöffnet, es gibt keine Wartezeiten und in vielen Fällen sind Ansprechpartner per Telefon auch in den Abendstunden oder am Wochenende erreichbar." Außerdem sei das Online-Banking in der Regel preiswerter. Doch auch hier ist Vorsicht geboten. So wird das Passwortfischen, im Fachjargon „Phishing" genannt, zu einer zunehmenden Bedrohung gerade beim Online-Banking.

Phishing – Auf der Jagd nach dem großen Fisch

Beim Phishing verfolgen Betrüger ein Ziel: Daten von Benutzern zu erbeuten und sie für ihre Zwecke zu missbrauchen. Die Masche ist immer die Gleiche: Durch einen Trick soll das Opfer dazu gebracht werden, persönliche Informationen in ein Formular auf einer gefälschten Internetseite einzutragen. Dazu verfassen die Kriminellen beispielsweise E-Mails, die in Aussehen und Inhalt jenen von Geschäftspartnern oder Banken gleichen. Sie spekulieren dabei darauf, dass der Empfänger der massenweise verschickten Nachrichten auch tatsächlich Kunde dieser Firmen ist. Das Opfer wird dazu verleitet, einen in der E-Mail enthaltenen Internetlink zu verfolgen. Folgt der Nutzer diesem, landet er auf einer perfekt gefälschten Webseite. Gibt er dort nun seine vertraulichen Kontoinformationen ein, „fischen" die Betrüger diese ab und greifen selbst auf das Konto zu.[1]

Generelle Sicherheitsregeln, die auch für das Internetsurfen und den E-Mail-Verkehr gelten:

- Halten Sie Ihre Software immer auf dem aktuellen Stand (Sicherheitsupdates)
- Prüfen Sie den Sicherheitsstatus von Webseiten, bevor Sie persönliche Informationen eingeben (z. B. https)
- Geben Sie Internet-Adressen immer manuell ein
- Niemals aufgrund eines Anrufs PIN oder TAN eingeben
- Funktion „Aktive Inhalte ausführen" grundsätzlich deaktivieren (nur für vertrauenswürdige Seiten ausnahmsweise zulassen)
- Firewall und Virenschutzsoftware einsetzen
- Bei Betrugsverdacht Bank oder Geschäftspartner kontaktieren
- Bei tatsächlichem Betrug Polizei einschalten

[1] www.bsi-fuer-buerger.de/Phishing

Schutzmaßnahmen fürs Online-Banking

Wenn man einige Schutzmaßnahmen beim Online-Banking beachtet, ist der virtuelle Bankbesuch relativ sicher. Oberstes Gebot ist der sorgfältige Umgang mit Zugangsdaten. PINs und TANs sind so aufzubewahren, dass niemand darauf zugreifen kann. Außerdem sollte man diese niemals elektronisch speichern. Daten sollten erst eingegeben werden, wenn der Sicherheitsstatus (z. B. https) überprüft wurde. Eine weitere Sicherheitsmaßnahme stellt die regelmäßige Kontrolle von Kontobewegungen dar. Denn nur dann kann man bei Betrugsverdacht sofort seine Bank informieren, die dann weitere Schritte einleitet.

PINs und TANs sind sorgfältig zu verwahren!

Grundsätzlich sollte jeder PC über funktionsfähige Sicherheitssoftware verfügen. So ist es etwa wichtig, die Virenschutzsoftware, die persönliche Firewall und auch die Sicherheitspatches für das Betriebssystem immer aktuell zu halten. Die meisten Hersteller aktualisieren ihre Software laufend und versuchen damit, bekannt gewordene Lücken zu schließen. Darüber hinaus sollte beim Online-Banking die Internetadresse der Bank jedes Mal wieder von neuem eingetippt oder über „Favoriten" oder „Bookmarks" angewählt werden. Keinesfalls sollte über Verlinkungen eingestiegen werden.

Kreditinstitute und seriöse Wirtschaftsunternehmen wissen, dass E-Mails von Betrügern leicht gefälscht werden können. Daher werden sie ihre Kunden niemals per E-Mail dazu auffordern, darin angeführte Links anzuklicken und dort vertrauliche Daten einzugeben. Das Gleiche gilt für Anrufe. Seriöse Geschäftspartner oder Banken werden sich nie von sich aus telefonisch bei Ihnen melden und Sie zur Eingabe von Passwörtern, PINs oder TANs über die Tastatur oder per Sprachcomputer auffordern!

Banken oder seriöse Firmen fordern ihre Kunden niemals per E-Mail oder per Telefon zur Eingabe vertraulicher Informationen auf!

Telefonbanking und Mobile Banking

Telefonbanking ist eine weitere Möglichkeit, Bankgeschäfte aus der Ferne zu erledigen. Dabei rufen Kunden die Servicemitarbeiter ihrer Bank an oder kommunizieren mit Hilfe der Telefontastatur oder automatisierter Spracherkennung mit einem Computer. Die Absicherung erfolgt dabei über den Einsatz von Passwörtern oder PINs. Da Telefongespräche ohne besonders hohen technischen Aufwand abgehört werden können, ist dieser Kommunikationsweg eher als riskant einzustufen.

Wer Mobile Banking über internetfähige Smartphones ausführt, sollte durch Nutzung von Sicherheitssoftware auf die gleichen Sicherheitsstandards wie beim PC oder Laptop setzen. Da diese Gerätegeneration nicht nur über vollwertige Betriebssysteme, sondern zudem über unterschiedliche Kommunikations-Schnittstellen verfügt, sind weitergehende Vorkehrungen für deren Absicherung sinnvoll: Auch hier sollte auf jeden Fall auf verschlüsselte Kommunikation geachtet werden. Mobile Funknetzwerke (WLAN, Bluetooth) sind zudem besonders anfällig für Angriffe. Daher muss besonders beim Online-Banking darauf geachtet werden, dass Smartphones etc. mit ihren Schnittstellen ausreichend abgesichert sind.

2 Der Staat online – E-Government

E-Government bezeichnet die elektronische Kommunikation zwischen Bürgern und der Verwaltung sowie zwischen den Behörden untereinander. Diese wird europaweit immer beliebter. In Deutschland haben sich Bund, Länder und Kommunen das Ziel gesetzt, alle geeigneten Verwaltungsverfahren online zur Verfügung zu stellen.[2] Dazu gehören zum Beispiel das Melde- und Personenstandswesen, das Bauwesen, die Kfz-Anmeldung oder etwa das BAföG. Die Online-Aktivitäten des Bundes und die allgemein voranschreitenden Digitalisierungsprozesse in der EU haben Methode. Sie sind Teil einer Strategie, die unseren Wirtschaftsstandort und damit unseren Wohlstand nachhaltig sichern soll.

Durch die Digitalisierung müssen auch die etablierten, analogen Verfahren des Ausweisens und der Kommunikation mit Behörden verändert werden.

Doch dieses Unterfangen ist nicht ohne Tücken. Durch die digitale Öffnung bei Behörden und Verwaltung stehen diese vor denselben Problemen wie die Privatwirtschaft: Nicht nur die Einführung eines sicheren digitalen Kanals wie beispielsweise De-Mail zu den Behörden muss etabliert werden. Auch das Ausweissystem muss im Zuge dessen erneuert werden, wie beispielsweise durch Einführung des nPa. Die Jahrhunderte währende Tradition der „Sichtprüfung" und der „manuellen, handschriftlichen Unterschrift" neigt sich dem Ende zu. Bei den Banken hat sich eine elektronische Karte, die EC bzw. die Kreditkarte, als Ausweis für Geldtransaktionen beim Bezahlen durchgesetzt. Im Online-Banking bzw. Online-Shopping hat bereits die Chipkarte als Sicherheitsmedium Einzug gehalten. Im Gesundheitsbereich und mit dem neuen Personalausweis (nPa) stehen auch im E-Government vergleichbare Veränderungen an.

Die durch E-Government ermöglichte Umstellung des E-Commerce bzw. E-Business auf eine vernünftige Identifizierung, Authentifizierung und Autorisation sowie eine sichere und vertrauliche Übermittlung sind aufgrund der technischen Unsicherheiten und der bislang gelebten Praxis überfällig. Umso mehr, weil das Mobile Computing[3] über Smartphones zum Teil unkalkulierbare Risiken in der Absicherung von Endgeräten, Kommunikationsverbindungen und Authentifikation mit sich bringt.

Behördengänge einfach online erledigen

Der elektronische Weg macht Verwaltungsprozesse für die Bürger komfortabler.

Öffentliche Einrichtungen und Behörden setzen zunehmend auf Online-Aktivitäten. Dazu gehört zum einen die Bereitstellung von Informationen wie zum Beispiel zum Bearbeitungsstand eines neuen Personalausweises. Darüber hinaus gibt es aber auch die Möglichkeit, auf elektronischem Weg direkt Kontakt mit Ansprechpartnern in der Verwaltung aufzunehmen. Auch Gebühren lassen sich online entrichten und Formulare übermitteln. Die Vorteile liegen auf der Hand: Zeitaufwendige Behördengänge gehören der Vergangenheit an. So können beispielsweise Meldeanträge oder Steuererklärungen bequem zu Hause ausgefüllt und elektronisch an die zuständigen Ämter gesendet werden.

[2] Informationen zu den aktuellen Internet-Angeboten des Staates: www.bund.de

[3] vgl. Teil 4, Kapitel 3 „Mobilität – ein Muss", S. 139 ff.

Veränderung von Wertschöpfungsketten

Das E-Government ist nur ein Teilaspekt der allgemein voranschreitenden Digitalisierungsprozesse. Wie die Vergangenheit gezeigt hat, können diese Prozesse selbst durch Fehlschläge auf Seiten der Verwaltung nicht mehr aufgehalten werden.

Wenn nun Prozesse neu geplant werden, weil sie beispielsweise digitalisiert werden bzw. auf Grund eines Gesetzes digitalisiert werden müssen, verändern sich sehr oft auch zentrale Wertschöpfungsketten: Wer dann nicht mehr nahe an den (Daten-)Bahnhöfen liegt und frühzeitig die richtigen Weichen stellt, landet mitunter sogar auf dem digitalen Abstellgleis.

Betroffen sind beispielsweise Arbeitnehmer- und Unternehmensdaten, die in unterschiedlichen Datenbanken gesammelt bzw. abrufbereit zur Verfügung gestellt werden. Darüber hinaus geht es auch um Modelle von Zugriffsverfahren und deren Sicherheitsmerkmale: Verschlüsselung, Signatur und Authentifikation, wie sie z. B. der neue Personalausweis bietet. Von ebenfalls großer Bedeutung ist das Thema Kommunikation beim E-Government mittels De-Mail.

Für die Akzeptanz dieser Angebote in der deutschen Bevölkerung ist ausschlaggebend, dass sie nicht nur von zu Hause, sondern auch einfach, sicher und mobil genutzt werden können. Den Trend zu mobilen E-Government-Lösungen, die die Bürgerinnen und Bürger mit Smartphones und Tablet-PC nutzen können, ist auch im E-Government-Monitor 2012 ablesbar. Einfache Bedienung, hohe örtliche Unabhängigkeit und zeitliche Verfügbarkeit machen diese Angebote besonders attraktiv.[4]

Auftragsvergabe

Die öffentliche Auftragsvergabe[5] ist eine gefragte Lösung für viele digitale Prozesse in Unternehmen. Hier sind in naher Zukunft auch die größten Veränderungen zu erwarten. So sollen künftig die Vergabeverfahren von Bund, Ländern und Kommunen elektronisch erfolgen.[6] Voraussetzung dafür ist die fortgeschrittene elektronische Signatur.[7] Diese entspricht in der digitalen Welt einer rechtsverbindlichen Unterschrift.

Bereits die fortgeschrittene elektronische Signatur ist für die Vergabe ausreichend.

[4] www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2012/07/egov.html

[5] www.evergabe-online.de

[6] Angebote nur noch elektronisch: www.evergabe-online.de/jsp/nachricht.jsp?newsid=3

[7] Die elektronische Signatur: www.evergabe-online.info/cln_091/nn_119090/DE/Signatur/artikel__signatur.html?__nnn=true

E-Justice

E-Justice bezeichnet die rechtsverbindliche elektronische Kommunikation im Gerichtswesen.

Der Begriff E-Justice bezeichnet die Möglichkeit zur rechtsverbindlichen elektronischen Kommunikation zwischen Prozessbeteiligten und Gerichten. So haben die Prozessbeteiligten die Möglichkeit, ihrerseits Klageschriften und prozessuale Erklärungen elektronisch einzureichen. Andererseits können die Gerichte ihre Entscheidungen auf gleichem Weg bekannt geben. Innerhalb der Justiz eröffnet die elektronische Aktenführung, -bearbeitung und -archivierung eine erhebliche Erleichterung der organisatorischen Abläufe. Der interne digitale Datenfluss beschleunigt die Arbeitsprozesse und verkürzt damit die Verfahrensdauer. Eine anwenderfreundliche Kommunikation mit der Justiz soll sowohl per De-Mail als auch über das elektronische Gerichts- und Verwaltungspostfach (EGVP) bundeseinheitlich möglich werden.[8]

Digitale Agenda für Europa

Die „Digitale Agenda" der EU hat das Ziel, nachhaltigen wirtschaftlichen und sozialen Nutzen zu schaffen.

Die digitale Welt ist eine internationale Welt. Sie macht nicht an nationalen Grenzen halt. Produkte und Dienstleistungen werden grenzübergreifend angeboten und nachgefragt. Mobilfunk und Internet gewinnen gerade durch ihre globale Reichweite an Attraktivität.[9]

Die „Digitale Agenda für Europa" bestimmt maßgeblich das Vorgehen im Bereich der Informations- und Kommunikationstechnologie (IKT) und löst die Strategie i2010 ab. Sie ist eine der sieben Leitinitiativen der Strategie EU 2020. Die „Digitale Agenda" hat insgesamt das Ziel, aus einem digitalen Binnenmarkt, der auf einem schnellen bis extrem schnellen Internet und interoperablen Anwendungen beruht, einen nachhaltigen wirtschaftlichen und sozialen Nutzen zu ziehen.
Der Abbau der bestehenden Schwachstellen soll das gesamte Potenzial der IKT nutzbar machen. Insbesondere soll ein echter digitaler Binnenmarkt geschaffen und damit die Fragmentierung des Markts überwunden, die Interoperabilität verbessert und das Vertrauen in die Netzwerke gestärkt werden.

E-Government soll in diesem Kontext dazu beitragen, die Vorteile des Einsatzes von IKT für die Gesellschaft auszuschöpfen.

[8] „IT-Gipfel 2011 – Impuls für E-Justice": www.cio.bund.de/SharedDocs/Kurzmeldungen/DE/2011/20111206_it_gipfel_e_justice.html

[9] www.bmwi.de/DE/Themen/Digitale-Welt/internationale-dimension

Deutschland Digital 2015

Die Bundesregierung hat eine neue IKT-Strategie für die digitale Zukunft Deutschlands mit dem Titel „Deutschland Digital 2015“[10] erarbeitet. Vorrangiges Ziel ist es, die großen Potenziale der IKT für Wachstum und Beschäftigung in Deutschland besser zu erschließen. Die IKT-Strategie der Bundesregierung orientiert sich an den Zielstellungen der „Digitalen Agenda für Europa“.

Schwerpunkte der nationalen IKT-Strategie

- Stärkung der Wettbewerbsfähigkeit der Unternehmen
- Ausbau der Infrastrukturen
- Gewährleistung der Schutz- und Individualrechte der Nutzer
- Ausbau von Forschung und Entwicklung im IKT-Bereich und schnellere Umsetzung von F&E-Ergebnissen in Innovationen
- Stärkung von Aus- und Weiterbildung für die Nutzung von IKT
- Nutzung der IKT bei der Lösung gesellschaftlicher Herausforderungen wie Klimaschutz, Gesundheit, Mobilität

Nationaler IT-Gipfel[11]

Die IKT-Strategie („Deutschland Digital 2015“) bildet das „Dach“ für die IKT-Politik der Bundesregierung, unter dem die Ressorts ihre Aktivitäten planen und umsetzen. Die Bundesregierung will die großen Potenziale der IKT für Wachstum und Beschäftigung in Deutschland besser erschließen. Der Nationale IT-Gipfel ist dabei die Plattform, auf der Vertretern von Politik, Verwaltung und Wirtschaft an Konzepten und Lösungen arbeiten.

Der Nationale IT-Gipfel soll Konzepte zur Stärkung des IT-Standortes Deutschland entwickeln.

Innovative IT-Angebote des Staates

Eine Zielsetzung dieser Angebote ist die verstärkte Marktdurchdringung mit elektronischen Behördendiensten. Im Fokus stehen hierzu verbesserte, flexible und medienbruchfreie Prozesse zwischen Wirtschaft und Verwaltung.[12]

Eine wichtige Grundlage hierfür ist das E-Government-Gesetz. Da die vielfältigen Schriftformerfordernisse ein wichtiges Hemmnis für die elektronische Kommunikation mit der Verwaltung sind, soll die Zulassung hinreichend sicherer technischer Verfahren zur Erfüllung der Schriftform neben der qualifizierten elektronischen Signatur (qeS) geregelt werden. Eine der möglichen Lösungen ist hier die eID-Funktion des neuen Personalausweises. Auch wird geprüft, ob De-Mail schriftformersetzend eingesetzt werden kann.

Ziel des E-Government-Gesetzes ist die Unterstützung elektronischer Behördendienste.

[10] www.bmwi.de/DE/Service/suche,did=359924.html

[11] www.bmwi.de/DE/Themen/Digitale-Welt/nationaler-it-gipfel.html

[12] www.bmwi.de/DE/Service/suche,did=454194.html

De-Mail[13]

Mit der De-Mail ist eine sichere und zuverlässige Infrastruktur für E-Mail-Verkehr aufgebaut worden.

Am 3. Mai 2011 ist das De-Mail-Gesetz in Kraft getreten. Auf der Grundlage dieses „Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften" können künftig De-Mail-Dienste angeboten werden.[14]

Das De-Mail-Gesetz regelt die Mindestanforderungen an einen sicheren elektronischen Nachrichtenaustausch. Darüber hinaus sorgt es für ein geregeltes Verfahren, wie diese Mindestanforderungen, die für alle De-Mail-Anbieter in gleicher Weise gelten, wirksam überprüft werden. Das sind wichtige Voraussetzungen für das Entstehen von Vertrauen in die Sicherheit und für die Qualität der De-Mail-Dienste.
Unabhängig davon, welchen De-Mail-Anbieter Sie auswählen: Sie können darauf vertrauen, dass ein einheitliches und geprüftes Sicherheitsniveau gewährleistet ist. Durch die gesetzlichen Regelungen ist zudem sichergestellt, dass alle De-Mail-Nutzer bei allen anderen De-Mail-Anbietern erreicht werden können.[15]

Mit der De-Mail ist damit eine elektronische Kommunikationsplattform im Internet entstanden, über die Bürger, Wirtschaft und Verwaltung künftig sensible Informationen vertraulich, nachvollziehbar und verbindlich austauschen können. Die Dienste dieser Plattform sollen einen sicheren elektronischen Geschäftsverkehr für jeden registrierten Benutzer ermöglichen.

Zu den Erwartungen zählen schnellere und kostengünstigere Bearbeitungsprozesse, weniger Behördengänge sowie eine Entlastung für wenig mobile oder behinderte Menschen. An die elektronische Kommunikation über De-Mail sollen vergleichbare Rechtsfolgen geknüpft werden können wie an die heutigen papierbasierten Verfahren.

[13] www.De-Mail.de

[14] www.cio.bund.de/SharedDocs/Publikationen/DE/Innovative-Vorhaben/de_mail_informationsbroschuere_juli_2012_download.pdf

[15] www.bmi.bund.de/DE/Themen/OeffentlDienstVerwaltung/Informationsgesellschaft/De_Mail/de_mail_node.html

De-Mail – Aspekte[16]

Accounts und Adressen

Ein De-Mail-Account stellt die Basis für die Nutzung der De-Mail-Dienste dar. Ihn erhalten nur diejenigen, die sich im Rahmen einer obligatorischen Erstregistrierung identifiziert haben. Dabei werden verschiedene Pflichtattribute wie Vor- und Nachname, Meldeadresse und Geburtsdatum für natürliche Personen erfasst.

De-Mail-Accounts können sowohl von natürlichen als auch juristischen Personen eröffnet werden.

Postfach- und Versanddienst

Von De-Mail werden verschiedene Versandarten angeboten, die mit einem Brief, einem Einschreiben oder einem Postzustellungsauftrag vergleichbar sind. Dabei können für den Absender Nachweise darüber erstellt werden, wann er die Nachricht verschickt hat und wann sie in das Postfach des Empfängers zugestellt wurde.

De-Safe

Mit De-Mail können in Zukunft wichtige Nachrichten und Dokumente auch elektronisch sicher empfangen und versendet werden. Diese müssen dann natürlich auch veränderungssicher und dauerhaft gespeichert werden können. Daher sieht das Projekt auch einen Dokumentensafe vor, der Unterlagen verschlüsselt und vor Veränderungen geschützt für Sie bereithält. Sicheres Speichern auf dem heimischen PC ist dagegen schwer umzusetzen, denn auch USB-Sticks, CD-ROMs etc. sind nicht langfristig vor Datenverlust sicher.

Wichtige elektronische Dokumente können sicher und langfristig so gespeichert werden, dass sie vor Verlust und Manipulation geschützt sind.

Identitätsnachweis

Auf Verlangen des Nutzers erstellt der De-Mail-Dienstanbieter einen Ident-Nachweis. Die Inhalte werden vom Dienstanbieter qualifiziert elektronisch signiert, um die Korrektheit der übermittelten Daten zu bestätigen.

Der Ident-Nachweis beinhaltet die vom Nutzer ausgewählten überprüften Identitätsdaten.

[16] www.cio.bund.de/DE/Innovative-Vorhaben/De-Mail/de_mail_node.html

De-Mail-Sicherheitsmerkmale [17, 18]

De-Mail: so einfach wie E-Mail und so sicher wie Papierpost.

Mit De-Mail können elektronische Nachrichten so einfach verschickt werden, wie Sie es von E-Mail gewöhnt sind. De-Mail kann einfach mit Standardprogrammen wie Internet-Browser und E-Mail-Clients genutzt werden und bietet verschiedene Versandarten, die mit „Brief" oder „Einschreiben" (mit Zustellbestätigung) vergleichbar sind.

De-Mail ermöglicht unter anderem eine beweiskräftige Versand- und Zustellbestätigung. Diese elektronische Form des Einschreibens ist vor allem bei Terminsachen hilfreich. So werden viele Briefsendungen oder persönliche Besuche im Amt künftig überflüssig. Allein durch wegfallende Porto-, Druck- und Verpackungskosten können nach Berechnungen des Bundesministeriums des Innern pro Jahr Kosten von bis zu 1,4 Milliarden Euro vermieden werden. Der Branchenverband der IKT-Anbieter BITKOM setzt sich mit Nachdruck für die De-Mail ein.

Das Angebot an die Nutzer umfasst neben einem sicheren Postfach und dazugehörigen Versanddiensten auch einen elektronischen Dokumentensafe und die Möglichkeit, im Internet verlässliche Angaben zur eigenen Identität zu machen.

De-Mail-Wege sind vielfach abgesichert. Versand und Empfang sind verschlüsselt.

Im Gegensatz zur E-Mail können bei De-Mail aber sowohl die Identität der Kommunikationspartner als auch der Versand und der Eingang von De-Mails jederzeit zweifelsfrei nachgewiesen werden. Die Inhalte einer De-Mail können auf ihrem Weg durch das Internet nicht mitgelesen oder gar verändert werden. Denn abgesicherte Anmeldeverfahren und Verbindungen zu den De-Mail-Anbietern sorgen ebenso wie verschlüsselte Transportwege zwischen den De-Mail-Anbietern für einen vertraulichen Versand und Empfang von De-Mails.
De-Mail erhöht so die Sicherheit der elektronischen Kommunikation im Vergleich zur herkömmlichen E-Mail und hilft, Spam und Phishing zu vermeiden. [19]

Aus Sicherheitsgründen kann De-Mail kann nur von Providern betrieben werden, die vom Bundesamt für Sicherheit in der Informationstechnologie (BSI) zertifiziert und akkreditiert wurden. Außerdem überprüft das BSI immer wieder die Sicherheit der eingesetzten Produkte sowie die Zuverlässigkeit der Organisation und der Prozesse bei den Providern.

De-Mail bietet zwei unterschiedliche Sicherheitsniveaus: Normale Sicherheit und Hohe Sicherheit.

Abhängig von den unterschiedlichen Funktionen [20] der De-Mail gibt es zwei unterschiedliche Sicherheitsniveaus: Für die „normale Sicherheit" ist Benutzername und Passwort vorgesehen, also die klassische Anmeldung mit Wissenskomponenten. Für die „hohe Sicherheit" ist zusätzlich noch eine Besitzkomponente erforderlich. Diese Besitzkomponente kann entweder der nPa, eine

[17] www.bmi.bund.de/DE/Themen/OeffentlDienstVerwaltung/Informationsgesellschaft/De_Mail/de_mail_node.html

[18] www.cio.bund.de/SharedDocs/Publikationen/DE/Innovative-Vorhaben/de_mail_informationsbroschuere_juli_2012_download.pdf

[19] www.cio.bund.de/DE/Innovative-Vorhaben/De-Mail/de_mail_node.html

[20] vgl. Info-Kasten, S. 97

Signaturkarte oder ein anderes zugelassenes Verfahren sein. Die Anmeldung mit dem „hohen“ Sicherheitsniveau ist vom Gesetzgeber als Standard für den Zugang zum De-Mail-Konto vorgesehen und wird für die meisten De-Mail spezifischen Versandoptionen (Eingangs- und Versandbestätigungen) benötigt.[21] Zusätzlich zur Identität der Kommunikationspartner kann damit auch der Versand und der Eingang von De-Mails jederzeit zweifelsfrei nachgewiesen werden. Dies gilt jedoch nur für hohe Sicherheit, also mit Besitzkomponente.

Sicherheitsmerkmale De-Mail[22]

De-Mails haben – ohne zusätzliche Installationen – wichtige Sicherheitsmerkmale, die der herkömmlichen E-Mail fehlen:

- De-Mails können nicht von Dritten abgefangen und verändert werden, weil sie auf ihrem Weg durch das Internet immer verschlüsselt sind.
- Versender und Empfänger einer De-Mail sind stets nachvollziehbar, weil die Nutzer erst dann ein De-Mail-Konto erhalten, wenn sie sich vorher eindeutig identifiziert haben.
- Nutzer erhalten auf Wunsch Versand- und Eingangsnachweise für ihre De-Mails („elektronisches Einschreiben“).
- Spam wird verhindert, weil die Absender eindeutig identifiziert sind.
- Phishing und Identitätsdiebstahl werden bekämpft, weil sich Nutzer mit einem doppelt gesicherten Verfahren anmelden können
- Schadprogramme in De-Mails können über zentrale Schutzprogramme beim Provider erkannt werden.
- Verbindlicher Versand von E-Mails, soweit kein „Schriftformerfordernis“ vorliegt.[23]

Aufgrund dieser Sicherheitsmerkmale stärkt und unterstützt De-Mail die Möglichkeiten der Nutzer, ihre persönlichen Daten wirksam zu schützen.

[21] www.cio.bund.de/SharedDocs/Publikationen/DE/Innovative-Vorhaben/de_mail_informationsbroschuere_juli_2012_download.pdf

[22] www.cio.bund.de/DE/Innovative-Vorhaben/De-Mail/Sicherheitsmerkmale/sicherheitsmerkmale_node.html

[23] vgl. „Rechtsverbindlichkeit“, S. 98

Rechtsverbindlichkeit[24]

Sowohl die Identität der Kommunikationspartner als auch die Zustellung können mit De-Mail nachgewiesen werden, weil auf Wunsch ein belastbarer Nachweis für die elektronisch übermittelte Nachricht möglich ist. Zudem wird die Integrität der E-Mail, also der Nachweis, dass der Inhalt nicht verfälscht wurde, sichergestellt. Damit bietet De-Mail eine technische Grundlage für den nachweisbaren Abschluss von Rechtsgeschäften.

Mit De-Mail kann man verbindliche Rechtsgeschäfte abschließen, solange keine besonderen Erfordernisse an die Form des Rechtsgeschäftes bestehen. Dies ist jedoch für die Rechtsverbindlichkeit in den Fällen des Schriftformerfordernisses nicht ausreichend!

Die qualifizierte elektronische Signatur (qeS) nach Signaturgesetz (SigG) dient als Äquivalent zur eigenhändigen Unterschrift. Wenn ein Schriftstück eigenhändig unterschrieben werden muss (Schriftformerfordernis), kann dies nach geltender Rechtslage in den meisten Fällen elektronisch nur mit qualifizierter elektronischer Signatur geschehen.

In Kombination erfüllen damit beispielsweise De-Mail und nPa (bzw. SmartCard) die Voraussetzung für die Rechtsverbindlichkeit:
De-Mail sorgt für eine sichere Zustellung, einen sicheren Transport und eine sichere Aufbewahrung von Nachrichten und Dokumenten. Die qualifizierte elektronische Signatur bildet dagegen in der Regel die eigenhändige Unterschrift in der elektronischen Welt ab. Erfordert also eine zu übermittelnde Information eine eigenhändige Unterschrift (d. h. Schriftform), muss zusätzlich zur De-Mail die qualifizierte elektronische Signatur nach Signaturgesetz zum Einsatz kommen. Beide Konzepte ergänzen sich somit sehr gut.

[24] www.cio.bund.de/DE/Innovative-Vorhaben/De-Mail/Haeufig-gestellte-Fragen/haeufig_gestellte_fragen_node.html#doc2201960bodyText5

Datenschutz

Die Verbindung zum De-Mail-Provider und zwischen den verschiedenen Providern ist grundsätzlich verschlüsselt. Eine einfache Kenntnisnahme durch Mitschneiden des Datenverkehrs ist damit nicht möglich. Die De-Mail unterstützt zudem Verfahren, die beispielsweise die E-Mail komplett verschlüsseln und signieren; damit ist die Kenntnisnahme durch unbefugte Dritte praktisch unmöglich. Die Mindestanforderungen an die Kommunikation sind per Gesetz geregelt. Zudem sind im Prozessablauf bei den Providern umfassende Maßnahmen und deren Kontrollen vorgesehen, die von unabhängiger Stelle[25] regelmäßig zertifiziert werden müssen.[26]

Neuer Personalausweis[27]

Seit 1. November 2010 hat der neue Personalausweis im Scheckkartenformat den bisherigen Personalausweis abgelöst.

Die vielleicht interessanteste neue Eigenschaft ist die Online-Ausweisfunktion, die die Sicherheit und den Komfort von E-Business und E-Government für alle deutlich erhöht.

Die neue Generation des Ausweises ergänzt die herkömmlichen Anwendungen um elektronische Funktionen. Personenbezogene Daten, die heute optisch vom Dokument ablesbar sind, werden auch in einem Ausweis-Chip abgelegt. Damit können sich die Ausweisinhaber online ausweisen – sowohl gegenüber Behörden im Bereich E-Government als auch gegenüber privatwirtschaftlichen Dienstleistungsanbietern.

Die Online-Ausweisfunktion basiert auf dem Prinzip des gegenseitigen Ausweisens, wonach beide Seiten auf die angegebene Identität ihres Gegenübers vertrauen können: Nur mit einem staatlich ausgestellten Berechtigungszertifikat ist es für Dienstleister im Internet technisch möglich, auf Ausweisdaten zuzugreifen. Im Berechtigungszertifikat ist zusätzlich hinterlegt, welche Datenkategorien abgefragt werden können. Und nur durch Zustimmung durch den angemeldeten Nutzer werden die angeforderten Daten weitergegeben.

[25] „Zertifizierung als Auditor De-Mail“ https://www.bsi.bund.de/cln_156/DE/Themen/ZertifizierungundAnerkennung/Konformitaetsbewertung/Personen/AuditorDeMail/auditor-demail_node.html

[26] vgl. Abschnitt „De-Mail-Sicherheitsmerkmale“, S. 96

[27] www.bmi.bund.de/DE/Themen/Sicherheit/PaesseAusweise/ePersonalausweis/ePersonalausweis_node.html

Online-Ausweisfunktion

Der neue Personalausweis ist mit der Funktion des elektronischen Identitätsnachweises ausgerüstet. Damit können Prozesse wie z. B. Log-in oder Alters- und Wohnortbestätigung wirtschaftlicher und schneller realisiert werden. Ein besonderer Schwerpunkt wurde auf den Schutz persönlicher Daten gelegt: Nur berechtigte Anbieter von Dienstleistungen dürfen die Daten des Ausweises abfragen. Der Ausweisinhaber selbst behält die volle Kontrolle darüber, welche seiner persönlichen Daten an den Anbieter übermittelt werden. Aufgrund dieses Sicherheitskonzepts hilft der neue Personalausweis, Internetkriminalität zu bekämpfen und das Vertrauen der Bevölkerung in elektronische Transaktionen zu steigern. Er stärkt den Schutz vor Identitätsdiebstahl und bietet neue benutzerfreundliche Möglichkeiten für die Umsetzung des Jugendschutzes, wie er beim Kauf von altersbeschränkten Waren erforderlich ist.

Elektronische Signatur

Die Ausweisinhaber können ein Zertifikat für die qualifizierte elektronische Signatur (Unterschriftsfunktion) auf ihren Personalausweis laden. Damit können auch Dienste, die eine eigenhändige Unterschrift erfordern, medienbruchfrei, sicher und preiswert auf dem elektronischen Wege in Anspruch genommen werden.

Sicheres Reisedokument

Für hoheitliche Kontrollen an Grenzen und im Inland – und nur für diese – ist die Biometriefunktion zur Identitätsfeststellung vorgesehen: Auf dem neuen Personalausweis ist das digitale Lichtbild auch im Chip abgelegt. Zwei Fingerabdrücke können auf freiwilliger Basis ebenfalls im Chip gespeichert werden. Damit kann der elektronische Personalausweis ähnlich wie der elektronische Reisepass als sicheres Reisedokument eingesetzt werden. Beide Merkmale ermöglichen eine effiziente und sichere Unterstützung der Personenkontrolle, insbesondere zur Bekämpfung von Betrugsversuchen, bei denen verlorene oder gestohlene Dokumente gezielt durch fremde Personen verwendet werden.

Sicherheit der Daten im Chip des Ausweises[28]

Die Sicherheitsstandards des neuen Personalausweises sind auf dem höchsten Niveau. Das gilt sowohl für die physikalischen Sicherheitsmerkmale des Sichtdokuments als auch für die Sicherheitstechnologien, die die Daten auf dem Chip des neuen Personalausweises vor unberechtigten Zugriffen schützen. Die verwendeten Protokolle und Mechanismen beim neuen Personalausweis haben sich gegen alle Angriffsversuche bewährt, sind international anerkannt und etabliert. Alle Daten werden „Ende-zu-Ende" – also vom Ausweis bis zum Dienstanbieter – verschlüsselt übertragen.[29] Allerdings muss hierbei beachtet werden, dass nPa und SmartCard etc. ihren Einsatz auch am PC finden. Die resultierende, praktische Sicherheit des Online-Ausweises wird damit durch die am PC durchgeführten Maßnahmen bestimmt.[30] Auch bei hoheitlichen Kontrollen sollten die Lesegeräte sich in einer sicheren Umgebung befinden.

[28] www.cio.bund.de/DE/Innovative-Vorhaben/Neuer-Personalausweis/neuer_personalausweis_node.html

[29] Detaillierte Informationen unter: www.personalausweisportal.de

[30] vgl. „Die derzeit häufigsten Gefährdungen:", S. 62 ff.

3 Privat online

Immer mehr Menschen nutzen auch privat die Möglichkeiten, die das World Wide Web ihnen bietet. Dazu gehört neben dem Senden und Empfangen von E-Mails sowie dem Pflegen und Aufbauen von Kontakten in Chatrooms oder sozialen Netzwerken besonders auch das Online-Shopping.

Einkaufen im Internet

Das Einkaufen im Internet erfreut sich zunehmender Beliebtheit. Gerade vor großen Festen wie Weihnachten gehen viele lieber online shoppen, als sich ins Getümmel der Kaufhäuser zu stürzen. Leider nutzen Internetkriminelle dieses Einkaufsverhalten für ihre Zwecke. Grußkarten, E-Mails oder Internetseiten werden manipuliert und unseriöse Online-Shops eröffnet. Dabei haben es die Angreifer vor allem auf Kreditkarteninformationen, Bank- und Zugangsdaten zu Online-Shops und Bezahlsystemen abgesehen.

https ist ein Verfahren, um Daten im Internet verschlüsselt zu übertragen.

Diese Tatsache muss Einkaufswillige jedoch nicht vom Online-Shoppen abschrecken. Vorkehrungen zum eigenen Schutz sollten jedoch getroffen werden. Wie zum Beispiel das Einkaufen in „sicheren" Shops. Diese erkennt man zum Beispiel daran, dass die Eingabe von Konto- oder Kreditkartendaten nur im verschlüsselten SSL-Modus möglich ist – zu identifizieren am Anfang der Adresszeile mit „https" und einem Schlosssymbol im Browserfenster.

Zeichen für die Seriosität von Anbietern sind darüber hinaus nach Angaben des Branchenverbands BITKOM ein Impressum mit vollständiger Anschrift und Nennung des Geschäftsführers sowie verständliche Geschäftsbedingungen (AGB). Und schließlich sollte es selbstverständlich sein, die Sicherheitssoftware sowie das Betriebssystem des Rechners immer auf dem neuesten Stand zu halten. Zusätzliche Informationen finden Sie im Teil 1, Kapitel 01.03 „Internet als Marktplatz" (S. 14 ff.).

Gütesiegel für Online-Shops

Auch Gütesiegel können ein Zeichen für seriöse Anbieter sein. In der Praxis hat sich gezeigt, dass man nicht allen Anbietern blind vertrauen sollte. Bei manchen Qualitätssiegeln erfolgte die Zertifizierung zu schnell oder die Zulassungskriterien waren zu einfach. So kann es dann trotz Gütesiegel vorkommen, dass die bestellte Ware nicht den Beschreibungen entspricht oder gar nicht erst ankommt. Probleme können darüber hinaus auch bei der sicheren Übermittlung von Konto- oder Kreditkartennummern auftreten. Wer sich aktuell über empfohlene Gütesiegel informieren möchte, kann dies zum Beispiel auf den Internetseiten der „Initiative 21" tun. Dieser gemeinnützige Verein setzt sich zusammen aus Vertretern von Politik und Wirtschaft und hat sich unter anderem zum Ziel gesetzt, wirtschaftliches Wachstum zu fördern.[31] Zusätzliche Informationen finden Sie im Teil 1 „Der sichere Weg zum eigenen Shop" (S. 25).

[31] mehr Informationen dazu: www.internet-guetesiegel.de

Portale für soziale Netzwerke

Die sogenannten Social Networks wie XING, Facebook oder MySpace erfreuen sich zunehmender Beliebtheit. Mit Plattformen wie SchülerVZ, StudiVZ etc. wächst die nachfolgende Generation mit dem Internet auf. Für sie sind die Kommunikationsmöglichkeiten des Internets so selbstverständlich wie für die ältere Generation der Umgang mit Papier und Bleistift.

Der Siegeszug des Internets ist nicht mehr aufzuhalten – unabhängig vom Verhalten und von der Einstellung des Einzelnen. Selbst wer sich nicht aktiv an diesem gesellschaftlichen Wandel beteiligt, sollte sich darüber informieren, was unter Umständen über ihn geschrieben wird oder zu finden ist.

Mehr über die Vor- und Nachteile sozialer Netzwerke finden Sie
im Teil 1 „Gefahren von Social Engineering“ (S. 26).
im Teil 3 „Social Media“ (S. 106 ff.).

4 Geschäftspartner online

Kaum ein Unternehmen, das heute nicht im World Wide Web vertreten ist. Das gilt besonders für Unternehmen, die mit Waren handeln, doch auch Dienstleistungen werden verstärkt im Internet angeboten. Sie alle nutzen vermehrt die Möglichkeit von E-Business. Klar, denn der Einkauf im Web boomt. Virtuelle Shops vermehren sich rasant. Auch hier gibt es ein paar Tricks und Kniffe, wie man diese Online-Shops erfolgreich und sicher gestalten kann.

Web-Portale für E-Business

Über Web-Portale können Verkäufer und Käufer von Waren und Dienstleistungen miteinander kommunizieren und ihre Geschäfte reibungslos abwickeln. Diese Möglichkeit der elektronischen Abwicklung von Geschäftsprozessen ist ein wichtiger Erfolgsfaktor dafür, die Wettbewerbsfähigkeit von Unternehmen zu sichern und auch im internationalen Markt zu bestehen. Besonders für kleine und mittlere Unternehmen eröffnet sich hier eine Chance, im globalen Wettbewerb neue Geschäftsfelder zu erschließen oder bestehende auszubauen.

Dabei sorgen sogenannte E-Business-Standards dafür, dass Unternehmensprozesse automatisiert und damit effizient ablaufen können, sei es bei Bestellung, Lieferung oder Abrechnung. Das Bundesministerium für Wirtschaft und Technologie hat sich die Aufgabe gestellt, die Nutzung von einheitlichen E-Business-Standards in Deutschland zu beschleunigen. Mit der Initiative „PROZEUS – Prozesse und Standards" soll vor allem kleineren und mittleren Unternehmen bei der Einrichtung von E-Business Hilfestellung geleistet werden.[32]

Social Networking

Social Networking gefährdet IT-Sicherheit und Datenschutz – v. a. wenn Bonität und Seriosität des Geschäftspartners vernachlässigt werden.

In der Geschäftswelt ist es unerlässlich, neue Kontakte zu knüpfen, Geschäftsbeziehungen aufzubauen und zu pflegen. Auch hier bietet das Internet mit sozialen Netzwerken die geeignete Plattform. Längst haben Unternehmen die Vorteile erkannt, die Web-Anwendungen bei Geschäftsvorgängen wie Kundensupport, Marktforschung und Werbekampagnen bieten. Doch gleichzeitig unterschätzen sie die Gefahren des Web 2.0.

Im Web 2.0 lauern auch Gefahren

Fraunhofer-Studie entlarvt Sicherheitsmängel von Social-Networking-Portalen.

Viele Firmen gewähren ihren Mitarbeitern uneingeschränkten Web-Zugang – sogar zu Social-Networking-Angeboten, die ihre Inhalte nicht auf Schadcode oder gefährliche Links prüfen. Dies ist insbesondere vor dem Hintergrund gefährlich, dass ein Großteil von Schadprogrammen über das Internet verteilt wird. Doch die Gefahr im Web 2.0 geht insbesondere auf Social-Networking-Portalen nicht allein von Viren, Würmern und Trojanern aus. Vielmehr ist auch der Schutz persönlicher Daten mangelhaft, wie das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) bei einer Untersuchung der gängigsten Kontaktpflege-Plattformen herausgefunden hat. Bevor man „Social Networking" nutzen kann, muss man sich mit Namen, E-Mail-Adresse und unterschiedlich vielen weiteren persönlichen Informationen registrieren. Teilweise werden dort auch Angaben zum Unternehmen abgefragt, in dem man beschäftigt ist, sowie die dort eingenommene Rolle. Was mit diesen Daten geschieht, bemerken viele Anwender erst, wenn es zu spät ist.

[32] Inzwischen stehen zahlreiche Informationen und Anwendungsbeispiele sowie Broschüren und Merkblätter zum Thema E-Business-Standards auf der Transferplattform „www.prozeus.de" kostenfrei zum Herunterladen bereit.

Denn es scheint niemand zu wundern, dass sich die Postfächer nach der Registrierung mit suspekten E-Mails füllen. Bislang ist es noch schwer abschätzbar, welche Folgen es für Internetnutzer haben wird, die sehr freigiebig mit ihren persönlichen Informationen umgehen. Datenschutzbeauftragte warnen besonders davor, harte Fakten wie Namen und Geburtsdatum gemeinsam preiszugeben. Wenn man diese nämlich kombiniert, ist es möglich, die Person zu allen möglichen anderen öffentlichen und behördlichen Datenbanken zuzuordnen. Das macht sie eindeutig identifizier- und damit angreifbar.

Zusätzliche Informationen finden Sie im Teil 1
Web 2.0 – das „Mitmach-Medium“ für geschäftliche Beziehungen (S. 12)
Wo Licht ist, ist auch Schatten (S. 14)

Die Anbieter sind in der Pflicht

Datenschützer fordern, dass sich die Betreiber sozialer Netzwerke ihrer Verantwortung bewusst werden. Sie sind in der Pflicht, über die Verwendung aller Nutzungsdaten wie Profilinformationen oder IP-Adressen Rechenschaft abzulegen und die Anwender über die generellen Risiken von Social Networks bereits vor der Registrierung aufzuklären.

Das Unternehmen online

Besonders kleine Unternehmen zögern noch, sich ihre eigene Homepage zu erstellen. Dabei wird diese zu einem immer wichtigeren Marketinginstrument. Oft spricht ein mangelndes Budget dagegen oder fehlendes firmeninternes Know-how. Dabei gibt es einfache Wege, um im World Wide Web präsent zu sein.

Homepagebaukasten

Ein Homepagebaukasten ist ein relativ kostengünstiger Weg, ins Internet zu gelangen. Die Kosten für die Software liegen bei rund 50 Euro und die Software wird von manchen Anbietern sogar kostenlos zur Verfügung gestellt. Mit diesen Tools lässt sich die eigene Seite komplett selbst erstellen und pflegen. Demgegenüber stehen aber auch einige nicht unerhebliche Nachteile. Oft fehlt es an Bedienfreundlichkeit, es mangelt an guten Anleitungen und auch ein professionelles Layout lässt sich nicht ohne Weiteres erstellen. Wer sich für diese Möglichkeit entscheidet, sollte an einem entsprechenden Workshop teilnehmen. Hier lernt man die Bedienung der Software sowie die Kriterien bei Auswahl der Inhalte und letztendlich auch, wie man die Homepage als verkaufsstarkes Marketinginstrument richtig nutzt. Nach erfolgreicher Fertigstellung der Homepage sollten zusätzlich Sicherheitsaspekte berücksichtigt werden. Auch hier können Softwarelücken die erstellten Internetseiten angreifbar machen. Dies ist insofern problematisch, da solche Seiten mitunter leicht per Suchmaschine gefunden werden.

Ein Homepagebaukasten ist eine mögliche Lösung für kleine Budgets.

Content-Management-Systeme

Professionelle Webseiten erstellt man am besten mit Hilfe eines Content-Management-Systems (CMS). Layout und Einrichtung der Seite werden an externe Dienstleister und damit in professionelle Hände übergeben. Der Betreiber der Seite übernimmt lediglich die Pflege und laufende inhaltliche Anpassung seines Internetauftritts selbst. Unter Umständen müssen eigene Schutzvorkehrungen getroffen werden.

Ein Content-Management-System ermöglicht die dynamische Erstellung und Bearbeitung von Inhalten für Web-Anwendungen.

Selbst programmieren

Wer seine eigene Homepage selbst programmieren und individuell gestalten will, kommt nicht darum herum, eine geeignete Programmiersprache zu lernen. Auch hierbei sollte großer Wert auf Sicherheit gelegt werden: Nichts schadet dem eigenen Ruf mehr als eine Homepage, die Viren etc. verbreitet.

Zusätzliche Informationen finden Sie im Teil 1 „Homepage – Werbung in eigener Sache“ (S. 15).

5 Social Media

Das Internet, früher ein reiner Wissensspeicher, hat sich weiterentwickelt. Durch technische Innovationen ist es zu einer interaktiven Plattform geworden, die vom Nutzer selbst verändert und gestaltet werden kann. Es bietet, und das meint der Begriff Web 2.0, die Möglichkeit zum Dialog. Für die vielen Möglichkeiten des Web 2.0 hat sich in den letzten Jahren der Begriff „Social Media" etabliert. Er bezeichnet weniger den technischen Fortschritt, sondern vor allem den sozialen Charakter der Anwendungen und deren gesellschaftliche Bedeutung. Dies ist besonders deshalb von Bedeutung, da diese neuen Kanäle immer entscheidender für die Verbreitung von Nachrichten werden und eine neue Art der Demokratisierung von Information ermöglichen.

Das Web 2.0

Worauf ist der Erfolg von Social-Media-Plattformen zurückzuführen? Niedrige Einstiegshürden und hohe Schnelligkeit sind zwei der großen Stärken von Twitter, Facebook oder XING. Heute kann jeder leicht Informationen im Internet veröffentlichen. In wenigen Minuten ist man angemeldet und kann eigene Inhalte teilen. Social Media ist daher in zweierlei Hinsicht grenzenlos: Texte, Bilder, Töne und Videos können, einen Internetanschluss vorausgesetzt, weltweit konsumiert werden. Sie können aber auch dank Smartphones und Tablet PC überall produziert werden. Mit anderen Worten: Die Grenzen zwischen Konsument und Produzent wurden aufgehoben. Seitdem ist das Web durch „nutzergenerierte Inhalte" („user generated content") geprägt. Und da die Interaktion mit Dritten nichts anderes als Sozialverhalten ist, spricht man heute eben von „Sozialen Medien" oder „Social Media" im Internet, wenn man Plattformen meint, die diesen Austausch ermöglichen.

Social Media als Vermarktungsinstrument

Die Kommunikation in Web 2.0 und Social Media bietet Unternehmen und Freiberuflern die Möglichkeit, mit Kunden in direkten Kontakt zu treten und verschiedene Ziele zu verfolgen. Social-Media-Marketing konzentriert sich auf die Realisierung klassischer Marketingziele mit Hilfe des Web 2.0: zum Beispiel die Steigerung der Bekanntheit eines Unternehmens, einer Marke, einer Person oder eines Shops. Oder den Aufbau eines positiven Images, eine Verbesserung der Suchmaschinenergebnisse, eine Steigerung der Besucherzahlen auf der Webseite oder eine Interaktion mit der Zielgruppe. Welche Marketingstrategie zur Erreichung der Ziele eingesetzt werden sollte, hängt nicht nur vom Produkt oder der Dienstleistung ab, sondern auch von der jeweiligen Social-Media-Plattform.

Das Web 2.0 kann für Unternehmen ein mächtiges Marketing-Tool sein.

In Zukunft wird es nicht nur um die Meinungsmacht im Social Web gehen, sondern auch um die Mitgestaltung von Produkten. Das Web 2.0 macht Konsumenten zu Co-Produzenten, es ermöglicht die direkte Beteiligung an der Produktentwicklung. Davon können Hersteller und Verbraucher gleichermaßen profitieren. Denn engagierte Kunden haben oft gute Ideen, wie Produkte und Dienstleistungen noch besser werden können.

Authentisch bleiben

Absolut entscheidend für eine erfolgreiche Kommunikation in sozialen Medien ist, dass die Informationen einen Mehrwert haben und sowohl glaubwürdig als auch authentisch sind. Nicht alle Social-Media-Plattformen und -Anwendungsformen sind für jedes Unternehmen und jeden Freiberufler geeignet. Und nicht alle Zielgruppen sind im Social Web vertreten.

Auch die Unternehmenskultur ist ein kritischer Erfolgsfaktor von Social Media. Denn als Konsument von Social Media merkt ein Nutzer sehr schnell, wenn in dem Unternehmen keine offene Kommunikation herrscht. Diese Diskrepanz wird, ob man es möchte oder nicht, schnell nach außen sichtbar. Die Unternehmensleitung muss letztlich darauf vertrauen, dass die eigenen Mitarbeiter die besten Botschafter für das Unternehmen, seine Produkte und Dienstleistungen sind. Dabei muss die Kommunikation im Social Web zuerst intern verstanden und gelebt werden, um extern erfolgreich umgesetzt werden zu können. Im Idealfall setzt ein Unternehmen daher Web-2.0-Instrumente bereits intern ein, wie Blogs im Intranet oder Wikis in Wissensprojekten.

Auch im Social Web gilt: Kommunikation muss authentisch sein, wenn es dem Unternehmen dienen soll.

Der Einsatz von Social Media erfordert also eine sorgfältige Analyse, Planung, Umsetzung und Kontrolle, die in verbindlichen Verhaltensrichtlinien für den Umgang mit Social Media zusammengefasst werden sollten.

Social Media Guidelines

Wie sich Unternehmen in der Kommunikation im Social Web verhalten, sollte klar geregelt sein. Viele Unternehmen gehen davon aus, dass sie keine Social Media Guidelines benötigen, weil sie zwar eine Homepage haben, aber mit Facebook, Twitter und allem, was zu Social Media gehört, bislang nichts zu tun haben. Weshalb also Verhaltensrichtlinien in diesen Medien für die Mitarbeiter festlegen?

Dafür gibt es gute Gründe. Schon allein deshalb, weil vielleicht von eigenen Mitarbeitern oder von Dritten über das Unternehmen geredet wird, auch wenn es bewusst nicht beteiligt ist bzw. das nicht wünscht. Angenommen ein Auszubildender äußert sich auf Facebook negativ über seinen Ausbilder und das ganze Unternehmen. Alle seine Facebook-Kontakte lesen mit. Die Nachricht verbreitet sich, wird kommentiert, bekommt Kraft.

Es braucht klare Spielregeln zum Verhalten in Social Media.

Daher ist es für Unternehmen mit und ohne Internetpräsenz wichtig, sich mit den Auswirkungen von Social Media zu beschäftigen. Klare und einheitliche Unternehmenskommunikation muss durch das verbindliche Einhalten von Social Media Guidelines gewährleistet sein.

Berufliche und private Vermischung

Ein weiterer Aspekt: Immer mehr Menschen nutzen das Social Web sowohl privat als auch beruflich. Berufliche und private Inhalte werden vermischt. Es ist daher notwendig, dem Nutzerverhalten der Mitarbeiter entgegenzukommen, es aber in die richtigen Bahnen zu lenken. Social Media Guidelines können dabei helfen. Auf der nächsten Seite finden Sie einen Formulierungsvorschlag.

Muster für Social Media Guidelines

1. Verantwortung
Sie sind für das, was Sie in sozialen Netzwerken tun und veröffentlichen, selbst verantwortlich. Bitte gehen Sie bewusst mit dieser Verantwortung um, in Ihrem eigenen Interesse und im Interesse Ihres Arbeitgebers.

2. Persönlichkeit
Wenn Sie sich ohne einen dienstlichen Auftrag in sozialen Medien zu einem Thema äußern, machen Sie bitte deutlich, dass Sie hier Ihre persönliche Meinung vertreten und nicht für das Unternehmen sprechen. Verwenden Sie daher immer die Formulierung „ich" statt „wir".

3. Transparenz
Es ist Ihr persönlicher Beitrag, der in den sozialen Medien zählt. Daher bekennen Sie sich auch bitte immer mit Ihrem Klarnamen dazu. Spitznamen, sogenannten Nicknames, begegnet man zwar immer wieder, für den Leser und auch Sie selbst ist es aber hilfreicher und angenehmer, über die Identität des Verfassers Klarheit zu haben.

4. Mehrwert
Auch in Social Media wird, wie in manch anderem Medium, viel redundantes und nutzloses Wissen produziert und reproduziert. Fragen Sie sich also am besten vor jedem eigenen Beitrag, ob er dem Leser wirklich einen Mehrwert bietet. Falls nicht, seien Sie bitte so höflich und lassen Sie von dem Beitrag ab. Wenn Sie sich im Rahmen Ihrer Fachkompetenz in Social Media zu einem Thema äußern wollen und unsicher sind, stimmen Sie sich am besten im Vorfeld mit Ihrem Vorgesetzten ab.

5. Rechtliche Rahmenbedingungen
Machen Sie sich bewusst, dass Sie mit der Nutzung von sozialen Netzwerken keinen rechtsfreien Raum betreten – Sie unterliegen hier ebenso den Gesetzen und Verträgen, zu denen Sie sich bekannt haben, wie wenn Sie an Ihrem Schreibtisch sitzen, im Zug oder in der Kneipe. Davor schützt Sie auch kein Nickname. Auch haben viele Netzwerke eigene Nutzungsbedingungen; mit deren Anerkennung bei der Registrierung werden diese verbindlich. Die Verschwiegenheitspflicht besagt, dass Sie keine Interna nach außen geben dürfen, also vor allem Betriebsgeheimnisse, Wissen über andere Mitarbeiter oder Angelegenheiten, die dem Unternehmen schaden oder sein Ansehen verletzen könnten.

6. Urheberrecht
Ein wichtiger Punkt des Verhaltenskodex betrifft das Urheberrecht: Social Media verleiten nicht selten dazu, Inhalte von anderen einfach zu kopieren. Das ist nach dem Urheberrecht nicht erlaubt. Kopieren Sie also in ihren Beiträgen kein Material von anderen und geben Sie es nicht als ihr eigenes aus. Wenn Sie auf fremde Inhalte verweisen, nutzen Sie Links. Vermeiden Sie auch lange Zitate. Laden Sie nur Bilder oder Videos ins Internet hoch, wenn Sie die nötigen Rechte besitzen, weil sie zum Beispiel über die Zustimmung der Fotografen oder des Filmemachers und auch der abgebildeten Personen verfügen.

7. Die private Nutzung
Die Social-Media-Nutzung bringt es mit sich, dass häufig private und dienstliche Nutzung ineinander übergehen. Halten Sie sich an die vereinbarten Rahmenbedingungen.

8. Privatsphäre und Sicherheit
Eine der größten Sorgen der Menschen beim Umgang mit dem Internet im Allgemeinen und den sozialen Medien im Besonderen ist, dass auf Grund von Pannen, krimineller Energie oder schlicht Unwissen persönliche und vertrauliche Daten offen für jedermann sichtbar werden. Ein weiteres Problem können Viren und Hacker sein. Diese Risiken sind jedoch überschaubar, wenn man gewisse Grundsätze beherzigt und etwa die Einstellungen für die Privatsphäre der gängigen Online-Plattformen kennt. Informieren Sie sich daher genau, welche Einstellungen Ihre Privatsphäre schützen.

9. Besonnenheit
Denken Sie immer daran, dass Ihre Beiträge öffentlich sind – und das unter Umständen sehr lange bleiben. Bewahren Sie also auch in hitzigen Debatten einen kühlen Kopf und lassen Sie sich zu nichts hinreißen. Unterdrücken Sie im Zweifelsfall den Impuls, sich zu äußern, auch wenn Sie sich im Recht sehen. Argumentieren Sie immer sachlich, beleidigen Sie niemanden und seien Sie respektvoll im Umgang mit Ihren Dialogpartnern.

Gefahren und Risiken

Bei all den Vorteilen, die Social Media dem Unternehmen bieten kann, empfiehlt es sich dennoch, potenzielle Gefahren und Risiken nicht außer Acht zu lassen. Neben der Einhaltung von Social Media Guidelines können durchaus noch weitere Sicherheitsvorkehrungen getroffen werden, um sich auf dem Social-Media-Parkett sicher zu bewegen.[33]

Zusätzlich zu den Gefährdungen im Umgang mit dem Internet bietet Social Media noch ein paar andere Stolpersteine und Sicherheitsrisiken. Traditionelle statische Sicherheitslösungen alleine, wie Antiviren-Software und Firewalls, sind hierbei nicht effektiv genug, um fortschrittliche Malware und Datendiebstahl aufzuhalten. Während beispielsweise Facebook und Twitter gesperrt werden könnten, kann der Administrator Social Networks wie Google+ kaum sperren, da er dann auch die Suchmaschinenfunktion im Unternehmen unterbinden würde. Da Social Media auch von mobilen Geräten genutzt werden kann, kommt man nicht um aufeinander abgestimmte Sicherheitsrichtlinien, Social Media Guidelines und laufende Schulungen der Mitarbeiter herum.[34]

Gefahren von außen

Social Engineers spionieren das persönliche Umfeld ihrer Opfer aus, täuschen Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um geheime Information oder unbezahlte Dienstleistungen zu erlangen.

In letzter Zeit nehmen Angriffe auf das Web 2.0 an Intensität und Häufigkeit zu. Soziale Netzwerke geraten verstärkt unter Beschuss von Cyberkriminellen, die es besonders auf geschäftskritische Daten und Informationen abgesehen haben. Über soziale Netzwerke drohen gezieltes Phishing[35] und die Verbreitung von Viren und Trojanern. Hacker geben sich als Bekannte aus und versuchen auf diese Weise, mit einem Nutzer in Kontakt zu treten. Antwortet dieser auf das Kontaktgesuch, schicken die Hacker Schadsoftware oder locken ihn auf infizierte Download-Seiten (Clickjacking). Auch das sogenannte Social Engineering stellt ein großes Sicherheitsrisiko dar. Je mehr persönliche Daten im Spiel sind, desto höher sind die Erfolgschancen der Angreifer. Daher sollte wohl überlegt sein, welche Daten man wo veröffentlicht. Ist man in mehreren Netzwerken aktiv, können Informationen allgemein, aber auch geäußerte Meinungen miteinander zu einem Profil verknüpft werden, das dem Cyberkriminellen tiefe Einblicke gewähren kann. Das schwächste Glied in der Kette ist hier wieder einmal der Mensch. Hier können sogenannte Security-Awareness-Schulungen helfen.

[33] vgl. „Tipps für mehr Sicherheit im Netz“, S. 33

[34] vgl. Teil 4 , Kapitel 03 „Mobilität – ein Muss“, S. 139 ff.

[35] vgl. zum Thema Phishing, S. 88

Rechtssicherheit

Wenn Social Media zur Marketing-Strategie eines Unternehmens gehört, so sind neben den strategischen Aspekten und der Sicherheit auch noch rechtliche Aspekte zu berücksichtigen. Um Haftungsrisiken zu vermeiden, sollte man rechtliche Aspekte vorab sorgfältig prüfen.

Wahl des Account-Namens

Bereits bei Auswahl des Account-Namens ist darauf zu achten, dass nicht Rechte Dritter (z. B. Namens- oder Markenrechte) verletzt werden. Auch unter wettbewerbsrechtlichen Gesichtspunkten kann die Verwendung eines Account-Namens, der Bezüge oder mögliche Verwechslungen zu Wettbewerbern oder bekannten Unternehmen hervorruft, problematisch sein. Die Grundsätze des Domainrechts lassen sich wohl auch auf die Registrierung von Twitter-Namen übertragen.

Impressumspflicht

Für eine Firmenwebseite ergibt sich die Verpflichtung aus § 5 Telemediengesetz (TMG), der auch im Rahmen von Social Media anwendbar ist. Um also rechtlich kein Risiko einzugehen, ist die Angabe eines Impressums jedenfalls für geschäftliche Nutzung zu empfehlen. Das Landgericht (LG) Aschaffenburg hat entschieden (Urteil vom 19.08.2011, Az: 2 HK O 54/11), dass auch bei der Unternehmenspräsentation auf Facebook gemäß § 5 Telemediengesetz (TMG) ein Impressum einzustellen ist. Fehlt dieses, verhält sich der Anbieter wettbewerbswidrig. Die Impressumspflicht besteht nur dann nicht, wenn der Facebook-Account rein privat und überhaupt nicht für Marketingzwecke genutzt werde.

Werbung

Ganz genau prüfen sollte man, ob etwa ein Newsletter an die eigenen Kontakte über das soziale Netzwerk platziert werden kann. Hier sind die jeweiligen Nutzungsbedingungen sowie telemedien- und wettbewerbsrechtliche Grundsätze zu beachten. In den vergangenen Jahren haben mehrere Gerichte entschieden, dass nur das Double-Opt-in-Verfahren tauglich ist, um eine Einwilligung für die Zusendung von Werbe-E-Mails nachzuweisen. Denn rechtlich muss jeder Kunde „ausdrücklich" einverstanden sein. Die Einwilligung (Opt-in) eines Empfängers zum Erhalt von Newslettern und Marketing-Mails muss vom Versender rechtssicher nachweisbar sein.

Urheber- und Persönlichkeitsrechte

Sofern Bilder oder Videos ohne Zustimmung des Urhebers ins Internet eingestellt werden, liegt eine Urheberrechtsverletzung vor. Sie kann Unterlassungsansprüche und Schadensersatzforderungen nach sich ziehen, ja sogar strafrechtlich relevant sein. Auch das Persönlichkeitsrecht kann durch Verwendung von Bildern und Videos in sozialen Netzwerken betroffen sein. Regelmäßig ist die Einwilligung der betroffenen und identifizierbaren Personen erforderlich.

Verlinkung

Generell haftet man auch für fremde Links und deren Inhalte, die auf der eigenen Webseite oder Plattform eingestellt sind. Das kann nur dadurch verhindert werden, dass man sich ausdrücklich von diesen Inhalten distanziert.

Provider und Forenhaftung

Die Bereitstellung von Blogs und ähnlichen Medien, die es Nutzern ermöglichen, eigene Inhalte einzustellen, bringt immer die Gefahr einer Rechtsverletzung durch Beiträge und Inhalte mit sich. Sollte sich also jemand dazu hinreißen lassen, auf einer Facebook-Unternehmens-Fanseite beleidigende oder diffamierende Inhalte einzustellen, so kann das Unternehmen haftbar gemacht werden, wenn es diese Inhalte nicht schnellstmöglich beseitigt.

Fazit

Werden entsprechende Vorkehrungen und Schutzmaßnahmen getroffen, ist Social Media ein durchaus sinnvolles Marketinginstrument für das Unternehmen. Regelungen sollten klar festlegen, ob soziale Medien auch während der Arbeitszeit genutzt werden dürfen und vor allem, welche Plattformen zu welchem Zweck. Eine klare Trennung von privaten und geschäftlichen Inhalten unter Berücksichtigung entsprechender Sicherheitsaspekte sollte selbstverständlich sein. Mitarbeiter sollten über konkrete Gefahren, mögliche Kommunikationsmechanismen und rechtliche Folgen Bescheid wissen. Plaudert ein Mitarbeiter Geschäfts- oder Betriebsgeheimnisse aus, kann das zur fristlosen Kündigung führen. Durch die Einführung spezieller Sicherheitsrichtlinien lässt sich die unerlaubte Nutzung bestimmter Webseiten und Technologien zwar eindämmen. Am wichtigsten jedoch ist, bei den Mitarbeitern ein Bewusstsein für die Verantwortung zu schaffen, die sie im Social Web haben, da technische Vorkehrungen alleine nicht ausreichen.

Technische Entwicklungen und deren Auswirkungen – Geschäftsprozesse im Wandel

Teil 4

Angebote, Auftragsbestätigungen und Rechnungen lassen sich heute bequem online erstellen und verschicken. Ganze Infrastrukturen und Laufzeitumgebungen für Anwendungen können im Internet aus Modulen zusammengestellt und dort genutzt werden. Dabei verwischen die traditionellen Grenzen der eigenen IT-Infrastruktur, die Übergänge zu den Partnern werden fließend. Entwicklungen wie Virtualisierung und Smartphones mit ihren Apps forcieren dies. Gerade auch Cloud-Services eröffnen den Unternehmen viele neue Möglichkeiten. Es geht um eine neue Art und Weise, wie Unternehmen mit ihren Lieferanten und Kunden zusammenarbeiten, auch wenn viele Unternehmen diesen Entwicklungen noch hinterherhinken.

01 | Mobile Computing in der Cloud

Das Internet, Web 2.0, Soziale Netzwerke, Cloud, Mobilität sowie Smartphones und Tablets waren, jedes für sich, wichtige Vorbereiter für den nun stattfindenden Quantensprung in der Arbeitswelt: Durch die Wechselwirkung ergeben sich Möglichkeiten, nicht nur einzelne Prozesse, sondern die Arbeitsorganisation selbst zu verändern. Die Entwicklung geht weg von der standardisierten, industriellen Arbeitsorganisation hin zu neuen, kreativen Arbeits- und Organisationsformen. Mit Mobile Computing in der Cloud geht es um die neue Art und Weise, wie das Internet nun genutzt werden kann.

1 Neue Anforderungen

Mobile Endgeräte fordern eine neue Denkweise von Unternehmen.

Endgeräte liegen heute in verschiedenen Größen und für den unterschiedlichsten Bedarf vor. Apps, Web-Anwendungen, Kollaborationsplattformen im Internet und traditionelle Netzwerke mit ihren lokalen Installationen lassen sich bequem und beliebig miteinander kombinieren. VDSL und LTE liefern Bandbreiten, die in ihren Übertragungsraten vergleichbar sind mit den eigenen Unternehmensnetzen. Es gibt für die verschiedensten Bedarfe Lösungen „in der Cloud". Diese steht für die verschiedensten Produkte und Dienstleistungen, die sich, abhängig vom Sicherheitsbedarf, innerhalb (Private Cloud) oder außerhalb (Exclusive Cloud, Public Cloud) der eigenen, physischen Unternehmensgrenzen befinden. Mit dem Mobile Cloud Computing ist sowohl eine Plattform geschaffen als auch ein Endgeräte-Mix, die es im wechselseitigen Zusammenwirken ermöglichen, IT- und Kommunikationseinrichtungen zu nutzen, die sich außerhalb der phyischen Unternehmensgrenzen befinden.

Neue Arbeitsweisen – neue Gefahren

Die Vereinbarungen zum Service-Level entscheiden über Stabilität, Betriebsfähigkeit und Sicherheit des Angebotes.

Mit der Cloud sind neue Formen des Outsourcings entstanden, die nicht nur beliebige Flexibilität in der Verwendung von Hard- und Software verleihen. Mit den neuen Endgeräten und damit verbundenen neuen Arbeitsweisen gehen auch neuartige Gefährdungen für ein Unternehmen einher. Beispielsweise mussten sich die Verantwortlichen in der Vergangenheit kaum Gedanken darüber machen, ob bei Arbeitsbeginn der PC, der für die Verwendung im Unternehmensnetzwerk bereits eingerichtet ist, überhaupt eine Verbindung zu seinem Server bekommt. Für einen stabilen und sicheren Betrieb ist es wichtig, wie der Dienstleister mit Störungen, Angriffen oder Malware auf die Infrastruktur umgeht. Zugriffsverwaltung, Patchmanangement und Sicherheitssoftware sollten nicht nur vorhanden und funktionsfähig, sondern die Software auch auf dem neuesten Stand in Version und Konfiguration sein. Die Vereinbarungen zum Service-Level sind vergleichbar mit den Wartungsverträgen (Reaktionszeiten!) eines IT-Systempartners. Mangelhafte Vereinbarungen werden im Notfall in einer solchen Geschäftsbeziehung nicht so schnell bzw. leicht zu beheben sein.

Die Vertrauensstellung vom Auftraggeber zum Dienstleister ist von besonderer Bedeutung.

Darüber hinaus ist auch die Vertrauensstellung vom Auftraggeber zum Dienstleister von besonderer Bedeutung, da geschäftskritische Daten in fremde Hände gegeben werden. Dem sollte nicht nur die Vertragsgestaltung, sondern auch der Umgang mit den Kundendaten Rechnung tragen.

Rechtliche Auflagen

Deutsche Datenschutzregelungen gelten auch für Cloud-Angebote.

Die Angebote in der Cloud sind reichhaltig. Doch für Unternehmen kommen aus Gründen des Datenschutzes und weiterer rechtlicher Auflagen eigentlich nur Angebote wie private oder exklusive Cloud-Services in Frage, deren Hardware nicht weltweit, sondern ausschließlich in Europa bzw. Deutschland aufgestellt ist.

2 Cloud Computing

Cloud Computing beschreibt die orts- und zeitunabhängige gemeinsame Nutzung von Daten und Services mit minimalen Anforderungen an die eigene Infrastruktur. Je nach Wahl der Organisationsform sind dabei Daten und Services (Hard- und Software) online verfügbar.

Minimale Anforderungen an eine eigene IT-Infrastruktur: Cloud Computing.

Laut Definition des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien, dem BITKOM, werden beim Cloud Computing IT-Leistungen bedarfsgerecht und flexibel in Echtzeit als Service über das Internet oder innerhalb eines Firmennetzwerks bereitgestellt und nach Nutzung abgerechnet.[1] Die IT-Leistungen können sich auf Software, Plattformen für die Entwicklung und den Betrieb von Anwendungen sowie die Basisinfrastruktur wie beispielsweise Speicherplatz beziehen. Cloud Computing ist also nichts anderes als das Auslagern von IT-Anwendungen an externe Dienstleister, die bislang innerhalb des Unternehmens erledigt wurden.

Cloud-Computing-Vorteil: vollkommen bedarfsgerecht und flexibel.

Beim Cloud Computing handelt es sich um ein Konzept für neue Nutzungsformen von Soft- und Hardware, das die Weichen für Bereitstellung, Betrieb, Support, Management und Verwendung von IT neu stellt. Grundgedanke dabei ist, dass die IT-Landschaft, von Hardware über Software bis hin zur Datenhaltung, nicht mehr durch den Anwender selbst betrieben, sondern bedarfsgerecht via Internet bezogen wird – ohne dass der Anwender einen Unterschied zur bisherigen, lokalen IT feststellen kann.

Im Unterschied zu einer ASP-Lösung können in der Cloud verschiedene Ebenen als Service bezogen werden.[2] Der eine benötigt nur Infrastrukturleistungen, mit Hardwareservices (Speicher, Netzwerk, Rechenleistung) und Betriebssystemen, andere zusätzlich die Anwendungs-Infrastruktur (Abrechnung, Authentifizierung, Datenbank oder Entwicklungsumgebung) in Form von technischen Frameworks (Datenbanken und Middleware), der nächste die gesamte Anwendungssoftware – jeweils als Dienstleistung „as a Service".[3]

Im Unterschied zu ASP ermöglichen Cloud-Services eine differenziertere Steuerung der bezogenen Dienstleistung.

[1] BITKOM-Leitfaden „Cloud Computing", S. 7: www.bitkom.org/de/themen/36129_61111.aspx

[2] vgl. „Servicemodelle des Cloud Computings", S. 128 ff.

[3] vgl. BITKOM-Leitfaden „Cloud Computing": www.bitkom.org/de/themen/36129_61111.aspx

Vorteile

Investitionen in IT können gering gehalten und variabel bezogen werden.

Der Vorteil von Cloud Computing besteht vor allem darin, dass ohne eine hohe Anfangsinvestition modernste IT-Infrastruktur gemietet und diese flexibel geänderten Rahmenbedingungen angepasst werden kann. Je nach Geschäftsentwicklung können zusätzliche Ressourcen „variabel" hinzugezogen oder abbestellt werden und damit sogenannte sprungfixe Kosten deutlich reduziert werden. Ferner entfällt gleichzeitig die fortlaufende Anschaffung neuer Hardware. Dies wird möglich, da die erforderliche Infrastruktur (Software, Teile der Hardware-Ausstattung) nicht mehr am eigenen Rechner vorgehalten, sondern in Echtzeit über das Internet als Dienstleistung bereitgestellt wird. Die eigentlichen Anwendungen, die Verarbeitung der Daten, ihre Speicherung und die Bereitstellung der Ergebnisse, all dies geschieht „in der Wolke", einem „virtuellen Rechenzentrum", um dessen Wartung sich der Nutzer nicht kümmern muss. Die Vorteile liegen auf der Hand: Updates, Versionspflege, Sicherungskopien, Hardware-Voraussetzungen etc. sind kein Thema mehr, stattdessen: unerschöpfliche IT-Ressourcen und ein System, das immer auf dem neuesten Stand ist – dank der „Rechnerwolke", die – bildlich gesprochen – direkt hinter dem Schreibtisch beginnt.

Relation von Aufwand und Nutzen

Dennoch steht der Mittelstand in einigen Fällen der Cloud noch skeptisch gegenüber, weil er bezweifelt, dass der entstehende Nutzen den mitunter aufwendigen Wechsel rechtfertigt. Cloud Computing beschleunigt allerdings das gemeinsame Arbeiten an Inhalten. Ebenso ist eine zeitnahe Unternehmenssteuerung möglich, da zum Beispiel Dokumente zentral gespeichert werden.

Größe des Unternehmens spielt bei Cloud Computing kaum eine Rolle.

Welche Dienste in der Cloud genutzt werden, hängt weniger von der Größe des Unternehmens als davon ab, welche Funktion benötigt wird. So können Programme genutzt oder abonniert werden, die zuvor nur sehr aufwendig in die eigene IT-Infrastruktur integriert werden konnten. Zudem spart man Zeit für Aktualisierungen und muss sich nicht mehr um die Sicherung der Daten im Haus kümmern. Damit können auch kleinere Firmen von Cloud-Diensten profitieren.

IT-Know-how und IT-Sicherheit

Erfahrene Dienstleister erledigen wichtige IT-Aufgaben.

Cloud Computing bietet erhebliche Chancen, auch für die IT-Sicherheit. So kann sich die IT-Sicherheit u. a. weitreichende Standardisierungsbestrebungen und hohe Skalierbarkeit im Cloud Computing zu Nutze machen. Kleinere und mittelgroße Betriebe können durch die Konzentration auf das Kerngeschäft und die Auslagerung von IT-Aufgaben an einen erfahrenen Dienstleister in besonderem Maße profitieren. Ein weiteres schlagendes Argument ist die hohe Ausfallsicherheit der Cloud. Die Sicherheit in der Wolke ist höher, als man intern mit vertretbarem Aufwand gewährleisten kann, sofern man einen seriösen Partner gewählt hat.[4]

[4] DETECON-Studie „Chancen und Risiken des Cloud Computings": www.detecon.com/de/publikationen/studien/studien.html?unique_id=46435

Public Cloud oder Private Cloud

Cloud-Dienste unterscheiden sich nicht nur im Hinblick auf die unterschiedlichen Dienstleistungsebenen von Hard- und Software (IaaS, PaaS und SaaS, also Infrastruktur, Plattform und Software)[5] sondern auch hinsichtlich Betriebs-, Eigentums- und Organisationsaspekten. Dabei unterscheidet man zwischen zwei reinen Cloud-Formen, die letztlich die entgegengesetzten Endpunkte einer Reihe von Möglichkeiten[6] darstellen:

- den Private Clouds (auch Enterprise Clouds genannt) und
- den Public Clouds, wobei sich beide Formen in der technischen Realisierung nicht grundsätzlich unterscheiden.[7]

Die Public oder Öffentliche Cloud ist zunächst einmal jedem zugänglich.
Hier greifen viele verschiedene Nutzer unterschiedlicher Unternehmen jeweils über ihre Internetverbindungen auf Anwendungen und Daten zu.
Die Private Cloud wird auch als Unternehmens-Cloud bezeichnet, in der Dienste auf unternehmenseigener Infrastruktur für die Mitarbeiter und zum Teil auch für Kunden oder Geschäftpartner bereitgestellt werden.

Exclusive Cloud

Eine Sonderform der Public Cloud stellt die Exclusive Cloud dar. An der Open Cloud kann wirklich jeder teilnehmen, während bei der Exclusive Cloud eine enge, vertrauensvolle und vor allem eine vertragliche Beziehung zwischen Anwender und Cloud-Betreiber besteht.

Die Unterscheidung nach dem Kriterium „Sicherheit" erfolgt im Wesentlichen aufgrund der Einschränkung des Nutzerkreises, die auf unterschiedliche Weise und in unterschiedlicher Qualität durchgeführt werden kann. Sei es durch die Nutzung eigener Infrastruktur, sei es durch verschiedene Formen der Authentifikation und Autorisierung.

Authentifikation und Autorisierung erhöhen die Sicherheit für die Private und die Exlusive Cloud.

Hybrid Cloud

Der häufig verwendete Begriff Hybrid Cloud bezeichnet nichts anderes als eine parallele Nutzung von Public und Private, um die Vorteile beider Welten zu nutzen: Sicherheitskritisches liegt in der Private Cloud, weniger Kritisches in der Public Cloud.

[5] BITKOM-Leitfaden „Cloud-Computing", S. 22: www.bitkom.org/de/themen/61492_61111.aspx vgl. auch S. 128 ff.

[6] DETECON-Studie „Chancen und Risiken des Cloud Computings", S. 7: www.detecon.com/de/publikationen/studien/studien.html?unique_id=46435

[7] BITKOM-Leitfaden „Cloud Computing", S. 29: www.bitkom.org/de/themen/36129_61111.aspx

Datenschutz und IT-Sicherheit

Die Berichterstattung in den Medien über Datenschutzskandale und Hackerangriffe ist alles andere als motivierend für die Auslagerung der Daten. Denn es vergeht fast keine Woche ohne neuen Datenschutzskandal. Ein Unternehmen sollte nur dann bereit sein, seine Daten aus der Hand zu geben, wenn beispielsweise eine langjährige Reputation des Anbieters vorliegt und Zertifikate diesem Unternehmen guten Datenschutz- und Datensicherheit bescheinigen.

Zertifizierungen sind ein Muss.

Viele deutsche Cloud-Anbieter begegnen dieser Situation, indem sie sich zertifizieren lassen. Als Beispiel sei hier die Zertifizierung nach der Sicherheitsnorm ISO 27001 genannt, die als De-Fakto-Standard für IT-Sicherheit gilt.[8] So zweckmäßig das Konzept der Cloud ist, so kritisch muss der Schutz der Daten, die Verfügbarkeit der Dienstleistung sowie deren Qualität bzw. Sicherheit hinterfragt werden. Nach welchem Rechtssystem ist der Datenschutz sichergestellt? Kann der Anbieter einer Software sicherstellen, wo Daten abgelegt werden und deren Vertraulichkeit gewährleisten? Wie wird die Dienstleistung abgesichert, wie die Betriebsbereitschaft sichergestellt? Die Beantwortung dieser Fragen sollte über die Akzeptanz eines Angebotes entscheiden, auch wenn bisher die Einführung neuer Technik (Internet, E-Mail, Smartphones, VoIP etc.) die Sicherheit in der Regel erst einmal außen vor ließ.

Rechtssicherheit

Wer sich für eine Cloud-Lösung entscheidet, steht momentan vor dem Problem der „Rechtsunsicherheit" bei der Auswahl geeigneter, international arbeitender Anbieter. Diese wird bedingt durch deren länderübergreifende IT-Systeme, die unterschiedlichen Rechtssysteme der jeweiligen Länder und die Vorschriften für hiesige Unternehmen. Geschürt wird die Unsicherheit durch eine öffentliche Diskussion über die Unvereinbarkeit der Datenschutzregelungen beispielsweise der USA und Europas. Die unterschiedlichen Datenschutzregelungen verhindern etwa eine gleichmäßige globale Verteilung der für Cloud Computing benötigten Ressourcen, da europäische Datenschutzbestimmungen in den USA nicht gewährleistet werden können und somit personenbezogene Daten außerhalb der EU nicht gespeichert werden dürfen.

Eine mögliche Lösung ist die Auswahl eines Private- bzw. Exclusive-Cloud-Anbieters mit Standort in Deutschland der ausschließlich eigene Rechenzentrumskapazitäten nutzt und damit auch den hiesigen strengen gesetzlichen Vorschriften unterliegt.

IT-Risiken in der Cloud

Seine wichtigen Geschäftsdaten aus der Hand zu geben, fällt jedem Unternehmer schwer. Schließlich sind die Geschäftsdaten sein unternehmerisches Kapital. Der Verlust beziehungsweise das Ausspähen dieser Daten hätte weitreichende negative Folgen für den Geschäftsbetrieb.

[8] www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzZertifikat/ISO27001Zertifizierung/iso27001zertifizierung_node.html

Nun ist es ein wesentliches Kriterium der Public Cloud, dass alle Welt gleichzeitig den Zugriff auf die virtuellen Maschinen, deren Programme und Datenbanken in der Cloud besitzt. Stellen Sie sich vor, auf der gleichen Hard- und Software des Cloud-Anbieters lassen nicht nur Sie Ihre Programme laufen, sondern auch Ihre schärfsten Konkurrenten, also in direkter Nachbarschaft. Es liegt nun an den Sicherheitsvorkehrungen des Cloud-Anbieters, ob nicht doch – bildlich gesprochen – ein Blick über den Zaun möglich ist. Oder aber Sie befinden sich in direkter Nachbarschaft mit Cyberkriminellen, die ihr Geschäft über eben diesen Provider abwickeln, und natürlich auch mal wissen möchten, wer in ihrer direkten IT-Nachbarschaft zugange ist.

In der Cloud leben Konkurrenten oder Kriminelle in unmittelbarer Nachbarschaft. Ausgereifte Sicherheitskonzepte müssen implementiert werden.

Bei der Public Cloud liegt das Risiko für den Einzelnen v. a. in der Anzahl der Nutzer, in der nur einfachen Benutzer-Authentifikation und der direkten physischen Nähe. Damit dürfen in der zugrunde liegenden Hard- und Software sowie der Administration praktisch keine Fehler mehr auftreten, beispielsweise bei der Trennung des Datenverkehrs der verschiedenen Nutzer.

Sicherheit durch begrenzten Nutzerkreis

Eine Vorgehensweise, die besonders sicher ist, sind geschlossene Cloud-Systeme (Private bzw. Exclusive Cloud), die zudem über eine Mehr-Faktor-Authentifizierung verfügen. Ein Nutzer erhält nur dann Zugriff auf seine Daten, wenn er sich beispielsweise mittels einer Hardwarekomponente in Verbindung mit einer PIN-Eingabe, also „Besitz und Wissen", authentisiert hat. Die Verbindung mit dem Anbieter wird zudem über ein VPN (Virtual Private Network) geschützt. Es liegt in der Natur der Sache, dass das Risiko umso geringer ist, je weniger verschiedene Parteien ein IT-System nutzen. Aus diesem Grund ist eine sogenannte Private Cloud auch die sicherste Variante. Allerdings sind die Skaleneffekte und damit die Einsparungen hier am niedrigsten. Die Exclusive Cloud bietet dagegen einen guten Kompromiss zwischen Einsparungen und Sicherheit.

Zugriffsschutz: Hardware-Komponente

Ohne zusätzliche Besitzkomponente können Name und Passwort erraten, gestohlen oder geknackt werden. Werden E-Mail-Adressen als Name verwendet, können diese bereits aus einem bestehenden E-Mail-Verkehr oder aus der Homepage abgegriffen werden. Werden die Vorschriften für ein gutes Passwort nicht eingehalten, ist es schnell geknackt: die Dauer, um ein gutes 6-stelliges Passwort zu knacken, liegt beispielsweise auf einem Standard-PC bei 10 Minuten. Die Mehrfachverwendung von Passwörtern bzw. fehlende Passwortwechsel tun hier ihr Übriges: Die Zahl der durch Einbrüche bei großen Anbietern gestohlenen Zugriffsdaten (Name und Passwort) ging alleine im ersten Halbjahr 2012 in die Zigmillionen.

Lösungsansätze für IT-Risiken

Strenge Organisation und klare Richtlinien im Unternehmen machen die Cloud zum mächtigen Instrument.

Ein besonders wichtiger Aspekt bei der zunehmenden Vernetzung ist die Bestandsaufnahme vorhandener Daten und der Programme bzw. Prozesse, die auf diese Daten zugreifen. Wer glaubt, die Cloud helfe Probleme zu lösen, die auf unzureichender Organisation basieren, irrt. Im Gegenteil, die Tragweite unprofessioneller Unternehmensorganisation wird durch unzulängliche Verträge und falsche Rahmenbedingungen bzw. fehlerhafte Implementierung noch verstärkt. Überleben wird auf längere Sicht nur, wer innerhalb seiner Branche seine Prozessabläufe und seine Datenhaltung im Griff hat. Und darauf aufbauend die Kostenstruktur und damit die Form der Arbeitsorganisation den Marktgegebenheiten anpasst.

Spezielle Sicherheitsaspekte für die Auswahl eines Cloud-Dienstleisters

Ein paar spezielle Aspekte für die Auswahl von Cloud-Dienstleistern sollten unbedingt beachtet werden.

Verfügbarkeit

Verfügbarkeit ist ein wesentlicher Grundstein, um überhaupt mit der Cloud arbeiten zu können. Bei eigener IT stellt sich zumeist nicht die Frage, ob der PC den Server erreichen kann. Benötigt das eigene Geschäftsmodell, beispielsweise bei einem Webshop, eine hohe Verfügbarkeit, sollte diese unbedingt im Rahmen der sogenannten SLAs (Service Level Agreements) konkret festgelegt werden. Eine Verfügbarkeit von 97 % bedeutet beispielsweise, dass an knapp 11 Tagen im Jahr der Zugang zum Webshop nicht funktionieren darf. In der heutigen Zeit wäre das voraussichtlich das Ende des Unternehmens. Es sollte auch festgehalten werden, wie viel Zeit bei einer Störung verstreichen darf, bis der Anbieter die Störung beseitigt hat. Dies gilt ebenso für die Häufigkeit der Störungen. Im Zuge der freien Vertragsgestaltung können natürlich auch Konventionalstrafen vereinbart werden.

Verfügbare Bandbreite

Die verfügbare Bandbreite ist eigentlich kein Sicherheitsfeature. Wenn jedoch geneigte Käufer den Server in die Knie zwingen, ist dies kein gutes Aushängeschild für einen Shop-Betreiber. Zumal wenn bei ungenügenden Verträgen im schlimmsten Fall der Wiederanlauf Stunden dauert oder die Datenbanken des Shops Schaden nehmen. Feste Wartungsfenster unterstützen ebenfalls einen stabilen Betrieb.

Vereinbarungen

Besonders wichtig sind die Vereinbarungen bzw. die Klärung von Aspekten der Administration, da diese letztlich über den Sicherheitsstandard des Angebots entscheiden. Gerade durch die Auslagerung und physische Nähe der Daten und Programme zu anderen Anbietern und Nutzern muss eine Trennung der Datenströme sichergestellt werden. Dies kann nur durch zeitnahes Patchmanagement sichergestellt werden. Durch Analysen der Patches können Kriminelle sehr schnell die Schwachstellen herausfinden, die durch den Patch geschlossen werden. Jeder, der hier zu spät kommt, ist potenziell anfällig für Malware. Dies ist insofern wichtig, da heute allein aufgrund der schieren Menge an Malware (>50.000 neue Malware/Tag)[9] die Erkennungsleistung der Virenscanner an ihre Grenzen stößt. Jede geschlossene Lücke unterstützt damit den Virenscanner, da selbst unbekannte Schadsoftware hier nicht mehr angreifen kann.

Qualitätssicherung durch Sicherheitsanalysen

Penetrationsanalysen, also vorbeugende Einbruchsversuche, des Anbieters sorgen für die Aufdeckung von Schwachstellen des Konglomerates aus Infrastruktur, Plattform und Anwendungssoftware. Dabei werden auch mögliche administrative Schnittstellen zur Wartung und Pflege des Auftritts bzw. der Software untersucht. Derartige Maßnahmen unterstützen die eingesetzte Sicherheitssoftware, da selbst bei unbekannter Malware und neuartigen Angriffen die möglichen Angriffsflächen verringert werden: Ein Benutzer könnte beispielsweise durch Ausnutzung von Sicherheitslücken administrative Rechte auf der (virtuellen) Maschine des Anbieters erlangen. Dies hätte zur Folge, dass dieser Einsicht in fremde Daten erhält bzw. diese benutzen kann.

In Summe betrachtet muss sich letztlich jedes Unternehmen vor einer Auslagerung über genau die organisatorischen Dinge im Klaren sein, die bei lokalem Betrieb im Rahmen der lokalen Administration anfallen.[10] Wer auslagert, um sich nicht damit auseinandersetzen zu müssen, macht den Bock zum Gärtner. Ist die Auslagerung durchgeführt, führt dies in der Folge jedoch zu beträchtlichen Einsparungen, da dann tatsächlich nur noch das Kerngeschäft zählt.

Sicherheitsaspekte

- Verfügbarkeit der Dienstleistung
- Wartungsfenster
- Verfügbare Bandbreite
- Administration
  - Patchmanagement
  - Sicherheitsupdates
  - Penetrationsanalysen o.Ä.
  - Trennung der Datenströme unterschiedlicher User
  - Zuteilung und Verwaltung von Benutzer-/administrativen Rechten

[9] www.av-test.org

[10] vgl. Teil 2, S. 36 ff.

Datenschutz in der Cloud

Die Einhaltung der Vorschriften zum Datenschutz und zur gesetzeskonformen Aufbewahrung muss der Cloud-Anbieter gewährleisten. Belegen kann der Anbieter entsprechende Maßnahmen mit Nachweisen wie beispielsweise Zertifikaten und freiwilligen Audits, die den hohen Sicherheitsstandard dokumentieren. Liegen Zertifikate vor, können Kunden diese auch selbst als Nachweis dafür verwenden, dass mit den Daten, die sie dem Cloud-Provider anvertraut haben, sicher umgegangen wird.

Auftragsdatenverarbeitung

Cloud-Anbieter müssen kritisch geprüft werden.

Die Auslagerung von Verarbeitung und Speicherung von personenbezogenen Daten an ein anderes Unternehmen ist nach dem Bundesdatenschutzgesetz (BDSG) als Auftragsdatenverarbeitung definiert. Dort findet sich auch die Regelung, dass der Auftraggeber für die Datenschutz- und Datensicherheitsmaßnahmen verantwortlich bleibt. Der Auftraggeber sollte daher seinen Cloud-Betreiber sorgfältig auswählen und dessen Sicherheitsniveau kritisch prüfen. Hierzu gehört, dass der Auftraggeber weiß, wo seine Daten verarbeitet werden und ob sowie welche technischen und organisatorischen Maßnahmen zu deren Schutz bestehen.

Ein Zertifikat nach ISO 27001 belegt, dass ein wirksames Sicherheitsmanagementsystem vorhanden ist.

Sind Unternehmer beispielsweise durch Auftragsdatenverarbeitung verpflichtet, sich von der Ordnungsmäßigkeit der Datenverarbeitung eines Cloud-Anbieters zu überzeugen, helfen unabhängige Prüfungen und Zertifikate. Bei der Auswahl eines Anbieters ist es daher hilfreich, auf derartige Prüfbescheinigungen zu achten. Das Sicherheitsniveau kann regelmäßig durch Audits bescheinigt werden. Neben einem eigenen Datenschutztetat sollte auch eine Zertifizierung nach der Sicherheitsnorm ISO 27001 vorliegen. Diese belegt die Qualität und Wirksamkeit des Informationssicherheitsmanagementsystems (ISMS) des Cloud-Angebotes.

Für die Wahl des Anbieters ist der Standort des Rechenzentrums wichtig: Eine Auftragsdatenverarbeitung innerhalb der Europäischen Union ist aufgrund des gemeinsamen Standards der EU-Datenschutzrichtlinie privilegiert. Außerdem ist eine Verlagerung von Buchhaltungsdaten auch nach § 146 der Abgabenordnung an bestimmte Voraussetzungen gebunden, für die der Ort der Aufbewahrung eine wichtige Rolle spielt.

Wenn die Auftragsdatenverarbeitung im Ausland erfolgt, sind darüber hinaus spezielle Vorgaben der Abgabenordnung (§§ 146, 147 AO) zu beachten, die es den Finanzbehörden ermöglichen sollen, Kontrollen und Zugriffe auf die Unternehmensdaten durchführen zu können.

Die Abgabenordnung enthält Vorgaben für die Auftragsdatenverarbeitung im Ausland.

Nicht zuletzt die Verschwiegenheitsgebote der Berufsordnungen einzelner Berufsstände und die strafbewährte Geheimhaltungspflicht nach § 203 Strafgesetzbuch bei bestimmten Berufsgruppen legen weitere Maßstäbe an, die bei der Überlegung, Daten einer Cloud anzuvertrauen, zu berücksichtigen sind.

↗1 Klassifizierung der Services
↗2 Virtualisierung
↗3 (Out-)Sourcing
↗4 Application Service Providing (ASP)
↗5 Managed Security Services
↗6 Hosting und Housing
↗7 Software on Demand
↗8 Software as a Service

02 | Servicemodelle des Cloud Computings

Cloud Computing ist nicht gleich Cloud Computing. Es muss sehr genau definiert werden, welche Cloud Services dem Unternehmen nutzen. Am Anfang steht daher eine genaue Bedarfsanalyse. Welche Verfügbarkeit wird benötigt? Welche Skalierbarkeit?

1 Klassifizierung der Services [11]

Üblicherweise werden Produkte und Lösungen aus dem Cloud-Umfeld drei Ebenen zugeordnet. Diese Ebenen bauen funktional aufeinander auf und beinhalten die jeweils darunter liegende Dienstleistung.

Funktionale Ebenen

- **Infrastructure as a Service (IaaS):** Bei IaaS werden grundlegende Infrastrukturleistungen zur Verfügung gestellt (z. B. Rechenleistung, Speicherplatz), auf deren Basis der Nutzer individuelle Software wie Betriebssysteme oder Anwendungsprogramme betreiben kann. Der Nutzer ist nicht für das Management oder die Wartung der Infrastruktur zuständig, hat aber dennoch die Kontrolle über Betriebssysteme, Speicherverwaltung und Anwendungen. Auf die Konfiguration bestimmter Infrastrukturkomponenten, wie beispielsweise Host-Firewalls, hat er eventuell eine beschränkte Einflussmöglichkeit.
- **Platform as a Service (PaaS):** Nutzer können auf Basis einer Cloud-Plattform Anwendungen entwickeln oder bereitstellen. Dazu werden entsprechende Frameworks und Entwicklungswerkzeuge zur Verfügung gestellt. Dabei hat der Nutzer die Kontrolle über die Anwendungen und individuelle Konfigurationsparameter der Bereitstellungsumgebung.
- **Software as a Service (SaaS):** Bei SaaS wird dem Nutzer eine Anwendung als Dienst zur Verfügung gestellt. Die Änderung nutzerspezifischer Konfigurationseinstellungen ist evtl. nur eingeschränkt durch den Nutzer möglich.

Je nach Cloud-Computing-Servicemodell unterscheiden sich nicht nur die Dienste in ihrer Funktionalität. Bei den einzelnen Angeboten ist auch von unterschiedlichen Sicherheitsphilosophien auszugehen. Infrastruktur-Provider (IaaS) bieten Sicherheitsfeatures lediglich auf Hardware bzw. Infrastrukturebene an, z. B. mittels geeigneter Maßnahmen gemäß BSI-Grundschutz, und garantieren somit eine Basissicherheit und -verfügbarkeit. Für das Management und die Umsetzung der darüber hinausgehenden Sicherheitsmaßnahmen ist der Kunde verantwortlich. Bei PaaS verantwortet der Anbieter i. d. R. Plattformdienste, wie z. B. Datenbanken und Middleware. SaaS Provider regeln Details der Applikationsnutzung vertraglich, beispielsweise geltende Service Level, Sicherheit und Compliance. Soll im Zusammenspiel mit der eigenen IT nicht nur die Funktionalität, sondern auch die Sicherheit gewährleistet sein, ist ein Gesamtkonzept erforderlich, das die einzelnen Dienste in ihrem Zusammenwirken umfasst.

[11] DETECON Studie „Chancen und Risiken des Cloud Computings“, S. 6: www.detecon.com/de/publikationen/studien/studien.html?unique_id=46435
BITKOM-Leitfaden „Cloud Computing“, S. 22: www.bitkom.org/de/themen/36129_61111.aspx

2 Virtualisierung

Das Konzept der Virtualisierung ist ein Meilenstein für eine völlig veränderte Organisation von Software. Durch die Virtualisierung wird die Rolle des Betriebssystems massiv verändert: Es ist künftig nicht mehr für die Hardwareverwaltung zuständig. Diesen Teil übernimmt die Virtualisierungs-Software. Diese macht es möglich, mehrere sogenannte virtuelle Maschinen auf einem einzigen PC zur Verfügung zu stellen. Damit können mehrere virtuelle PCs installiert und gleichzeitig betrieben werden.

Weniger Hardware, weniger Aufwand

Reduzierung der Kosten durch bessere Auslastung physikalischer Server.

Dies führt zwangsläufig zu einer elementaren Veränderung bei Organisation der Hardware: Durch die Konsolidierung von Servern und PCs wird spürbar weniger Hardware und weniger administrativer Aufwand erforderlich sein. Neue Geschäftsmodelle der Hard- und Softwareanbieter berücksichtigen dies bereits: Werden mehrere (Software-)Server oder auch Internetauftritte auf einem physikalischen Server angeboten, lassen sich Speicherplatz und Performance skalieren. Die sich hieraus ergebenden Möglichkeiten in der Zusammenarbeit mit Partnern konnten durch die im Internet angebotenen Bandbreiten bisher nicht genutzt werden. Durch die anfallenden Datenmengen war dies bisher auf Web-Applikationen beschränkt.

Kosten durch Auslagerung sparen

Der Ausbau des Breitbandnetzes wird diese Lösungen stärker forcieren: Virtualisierung steht dann für das Auslagern der kompletten IT oder einzelner Teilbereiche in virtuelle Umgebungen. Diese können sowohl im eigenen Unternehmen als auch in fremden Rechenzentren stehen: Hosting, Housing, Software as a Service, Cloud Computing usw. werden durch die Möglichkeiten zur Reduzierung der Kosten bei gleichzeitig professioneller IT im Wettbewerb eine große Rolle spielen. All diese neuen Konzepte umschreiben letztlich die unterschiedlichen Arten und Ausgestaltungen vom Auslagern einzelner oder kompletter IT-Leistungen an externe Dienstleister. Dies ist bei der aktuellen Entwicklung von Soft- und Hardware-Zyklen eine sinnvolle Alternative: Immer kürzere Update-Zyklen, hohe Sicherheitsanforderungen sowie mögliche Festplatten- bzw. Hardwaredefekte – die lokale Installation von Softwareprodukten auf einem persönlichen Arbeitsplatzrechner ist immer mit einem gewissen Risiko verbunden. Auch Upgrades, Patches und Backups können durch die Auslagerung zuverlässiger erfolgen als im eigenen Netzwerk.

3 (Out-)Sourcing

Outsourcing senkt die Kosten und ermöglicht die Fokussierung aufs Kerngeschäft.

IT-Outsourcing ist ein viel diskutiertes Thema, das durch die Entwicklungen im Umfeld der Virtualisierung stark an Bedeutung gewinnt. Durch die neuen Geschäftsmodelle der Anbieter können Angebote bedarfs- und kostenorientiert unterbreitet werden. Im sich verstärkenden Wettbewerb ist Outsourcing eine Möglichkeit, sich verstärkt auf das Kerngeschäft zu konzentrieren und vor allem die Geschäftsprozesse zu rationalisieren, für die nur geringes Know-how vorhanden ist. Aufgaben, die neben dem Kerngeschäft liegen, gibt das Unternehmen an spezialisierte Dienstleister ab. Die Auseinandersetzung mit dem komplexen Thema EDV kostet Zeit und die Entscheidung für die richtigen Systeme kostet Geld, zumal Anschaffungen, die man heute tätigt, schnell wieder von Neuerungen überholt sind. Auch bindet der Wartungs- und Pflegeaufwand für den störungsfreien Betrieb beträchtliche Kapazitäten, die bei der Ausübung des Kerngeschäftes fehlen.

Gute Gründe für Outsourcing

Die Bedingungen für Wartung und Pflege der IT müssen im Vorfeld vertraglich geregelt werden.

Der Branchenverband BITKOM versteht unter Outsourcing die „vollverantwortliche Übertragung betrieblicher Funktionen an rechtlich selbstständige – d. h. externe – Dienstleister über einen definierten Zeitraum auf Basis festgelegter Service Level Agreement(s) (SLA)". Diese SLAs beschreiben beispielsweise, in welchem Umfang und mit welcher Reaktionszeit Unterstützung geleistet wird. Die Outsourcing- Leistungen können die Infrastruktur- und die Applikations- bzw. Anwendungsebene beinhalten. Erfahrungsgemäß können die IT-Betriebskosten durch IT-Outsourcing zwischen 15 % und 40 % reduziert werden. Für Existenzgründer und Freiberufler gibt es immer weniger Gründe, Server, Speicher und Applikationen selbst zu kaufen, zu pflegen und zu betreiben.

Eine große Bandbreite an Möglichkeiten

Die Angebote von IT-Outsourcing unterliegen einem ständigen Wandel und variieren von Anbieter zu Anbieter zum Teil erheblich. Unterschiede finden sich sowohl im Leistungsumfang, zum Beispiel bei der Qualität der bereitgestellten Datenleitung oder der Servicequalität, als auch in den allgemeinen Vertragskonditionen wie der Vertragslaufzeit und in mehr oder minder transparenten Preismodellen. Die Wahl des richtigen Anbieters ist eine grundlegende Entscheidung, da der Anwender eine langfristige Bindung eingeht. Doch zuvor sollten wesentliche Kriterien berücksichtigt werden: Ein besonders kritischer Aspekt ist der Schutz des Know-hows. Ein weiterer wichtiger Aspekt ist die Qualitätssicherung bei ausgelagerten Prozessen. Kurzfristige Eingriffe bzw. Änderungen im Prozessablauf sind nur erschwert möglich. Vor allem aber sollte die Sourcing-Strategie an der Geschäftsstrategie ausgerichtet werden: Anforderungen an Verfügbarkeit, Qualität, Vertraulichkeit und eine aufeinander abgestimmte Organisation müssen zum eigenen Geschäftsbetrieb passen, kompatibel sein. Deshalb sollten einige wichtige Aspekte bei der Auslagerung beachtet werden. Auch sollte ein Anbieter über ausreichend Branchenerfahrung verfügen bzw. mit Referenzen seine Qualifikation für Projekte nachweisen können, die in Art und Umfang der Auslagerung entsprechen.

Was ist bei IT-Outsourcing zu beachten?

Nur wenn administrative Tätigkeiten, Störungsbeseitigung und die Hilfe bei Fragen zum eingesetzten Programm reibungslos funktionieren, rechnet sich IT-Outsourcing.

Folgende Fragen sind entscheidend:

- Gibt es eine klare Zieldefinition?
- Welches ist die richtige Sourcing-Strategie?
- Nach welchen Kriterien erfolgt die Auswahl des externen IT-Dienstleisters?
- Welche Aspekte enthält der Outsourcing-Vertrag?
- Wie gestalten sich die Service Level Agreements (SLA) für technische Faktoren wie Performance und Verfügbarkeit?
- Sind die Angebote vergleichbar und marktgerecht?
- Wie erfolgt das Sourcing- und Vendor-Management?
- Welche Servicezeiten werden angeboten?
- Existiert eine Notfall-Hotline außerhalb der regulären Servicezeiten?
- Stehen verschiedene Kommunikationswege für Anfragen zur Verfügung?
- Welche Rückrufzeiten und welche Verfügbarkeitsgarantien werden zugesagt?
- Liegt der Service für die eingesetzten Programme beim selben Anbieter, sodass eine reibungslose Kommunikation zwischen den IT-Mitarbeitern und den Programmspezialisten gewährleistet ist?
- Steht mir ein Team von Spezialisten zur Verfügung oder bin ich von einem einzelnen Ansprechpartner abhängig?
- Gibt es eine lückenlose Dokumentation aller Anfragen und Vorfälle? Denn nur so können schnelle Reaktionen und Nachvollziehbarkeit gewährleistet sein.
- Welche Informationen werden in welcher Form zur Verfügung gestellt? Gibt es die Möglichkeit, wichtige Fakten online nachzuschauen, und wie dokumentiert der Anbieter die Verfügbarkeit seiner Dienstleistung für den Kunden?

4 Application Service Providing (ASP)

DV-technische Funktionen und Anwendungen werden von zentraler Stelle außerhalb des Unternehmens bereitgestellt, administriert und aktualisiert. In den Unternehmen stehen nur noch Geräte für die Erfassung und Darstellung der Ergebnisse. Alle Verarbeitungen, Wartungs- und Unterhaltungsarbeiten sowie die gesamten Datensicherungen erfolgen zentral in einem Rechenzentrum. Der Leistungsumfang kann dabei gestaffelt werden, um den unterschiedlichen Anforderungen gerecht zu werden.
Im Idealfall greifen Unternehmen über eine abgesicherte Verbindung auf die von ihnen eingesetzten Programme und Daten zu. Von dem aufwendigen IT-Support sind sie dann entlastet: EDV-Experten administrieren, überwachen und warten die Server, installieren Programm-Updates und sorgen für eine verlässliche Datensicherung. Auch das Lizenzmanagement für Server-Betriebssysteme und Microsoft Office erledigt der Dienstleister ebenso wie die bedarfsorientierte Aufrüstung bzw. Erneuerung der Server-Systeme.

5 Managed Security Services

Managed Services bezeichnet das professionelle Management von IT-Services für Unternehmen durch externe Dienstleister.

Ob IT-Arbeitsplatz, Netzwerk oder Rechenzentrum – der Begriff Managed Security Services umfasst den IT-Infrastrukturbetrieb über alle Plattformen. Laut einer Studie setzen deutsche Unternehmen im Bereich Sicherheit immer häufiger auf Unterstützung durch externe Dienstleister. Wie weit sie mit dem Outsourcing gehen, hängt jedoch stark vom jeweiligen Thema ab. Etwa jedes dritte Unternehmen nutzt mittlerweile Managed Security Services (MSS), sprich: lässt Betrieb und/oder Konfiguration bestimmter Sicherheitssysteme überwachen.

6 Hosting und Housing

Beim Hosting bezieht der Kunde über einen Mietvertrag die Rechenleistungen eines Service-Providers. Darüber hinaus erfolgt eine Bereitstellung von Webspeicher, Webhosting und Webdatenbanken zur Datenhaltung im Internet. Hosting-Services haben den großen Vorteil, dass mit klar definierten Kostenstrukturen gerechnet werden kann und diese bedarfsgerecht nutzbar sind. Diese Anbieter legen üblicherweise auf ihren Webservern die durch den

Kunden hochgeladenen Webseiten ab, übernehmen gegebenenfalls auch die Registrierung von Domains und die Bekanntmachung per Domain Name System (DNS). Zu den Hosting-Dienstleistungen gehören üblicherweise E-Mail-Hosting, Bereitstellung kompletter Shopsysteme sowie Content-Management-Systeme und Web-Applikationen. Eng mit dem Hosting ist auch das Housing verbunden, wie zum Beispiel das sogenannte Serverhousing. Damit ist die physische Unterbringung und Netzanbindung eines Kundenservers im Rechenzentrum eines Providers gemeint. Vorteile liegen in der Regel in wesentlich höheren Datenübertragungsraten, speziellen Sicherheitsvorkehrungen sowie einer hohen Verfügbarkeit der Server.

7 Software on Demand

Software on Demand läuft über die Server des Anbieters.

Software on Demand ist ein Service, bei dem der Kunde eine bestimmte Software bei einem Anbieter betreiben lässt, der diese je nach Anfrage staffelt. Dieses erlaubt flexible Lizenzierungsformen, bei denen nach Datenvolumen, Anzahl der Benutzer oder Ähnlichem abgerechnet werden kann. Im Gegensatz zur hausinternen Softwarelösung mit üblichem Kaufvertrag wird Software on Demand nicht beim Anwender, sondern auf den Servern des Softwareanbieters, des Application Service Providers, betrieben. Der Anwender greift meist über ein öffentliches Rechnernetz darauf zu. Dies ermöglicht dem Benutzer einer solchen Anwendung den weltweiten Zugriff auf seine meist browsergestützte Softwarelösung[12].

Besonders für kleine und mittlere Unternehmen geeignet

Software wird nicht mehr gekauft und auf eigenen PCs installiert, sondern nach Bedarf genutzt.

On-Demand-Lösungen richten sich vornehmlich an kleine und mittlere Unternehmen, die mit niedrigen Einführungs- und Betriebskosten rechnen möchten, denn es entstehen keine hohen Kaufinvestitionen bei Lizenzierung der Software und Hardware, da diese beim Anbieter stehen. Darüber hinaus sind sowohl Service wie auch Aktualisierungen oder Hotline in der Regel im Mietpreis inbegriffen. Ein weiterer Vorteil ist die zeitnahe Implementierung in den laufenden Betrieb, da oftmals keine speziellen Anpassungen an die bestehende IT-Infrastruktur vorgenommen werden müssen. Ein Nachteil besteht allerdings durch die Abhängigkeit von Anbietern und von funktionierenden Internetanbindungen. Die Auslagerung interner Daten in die Hände Dritter ist eine große psychologische Hemmschwelle. Die Nutzung der Anwendung ist auf Standardfunktionalitäten beschränkt. Mögliche Nachteile sehen viele aber auch bei der Anbindung: Was passiert beispielsweise, wenn die Internetverbindung unterbrochen ist?

[12] http://de.wikipedia.org/wiki/Software_on_demand

8 Software as a Service

Mit dem Kauf einer Software erwirbt man lediglich das Recht auf deren Nutzung.

Wer bisher eine Software „gekauft" hat, hat im Prinzip die Lizenz zu ihrer Nutzung erworben. Diese wird im Rahmen eines Installationspaketes zur Verfügung gestellt. Dem Käufer obliegt es dann, für eine entsprechende EDV-Umgebung zu sorgen und diese zu betreuen. Dazu gehören Wartung, Installationen, Aktualisierungen, Anschaffung sowie Erneuerung der Hardware. Der Hersteller der Software ist nur verantwortlich für das fehlerfreie Arbeiten dieser Software unter den von ihm beschriebenen Systemarchitekturen.

Das Modell Software as a Service verfolgt im Gegensatz dazu den Ansatz, dass die Software bei einem Dienstleister betrieben wird. Software as a Service, kurz SaaS, ist nichts anderes als ein Software-Distributions-Modell. Bei diesem Modell ist es möglich, Softwarekomponenten mit spezifischen Eigenschaften auszustatten – in der Installation, im Erscheinungsbild, in der konkreten Programmauswahl, im Design etc. Der Endnutzer benötigt nur noch eine minimale EDV-Infrastruktur für den Zugriff auf die bereitgestellte Software: PC oder Notebook mit Internetanbindung oder ein Endgerät, das terminal-, webbrowser- oder javafähig ist und keine Festplatte besitzt.

Die Preismodelle von SaaS

SaaS wird auch oft als Softwaremiete oder Leasing bezeichnet.

Alle anfallenden Kosten von Software as a Service werden in den meisten Fällen auf eine monatliche Rate umgerechnet, die sämtliche Kosten abdeckt. Der Dienstleister übernimmt somit das Risiko für den Kunden. Das betrifft z. B. Hardware-Ausfälle mit der damit verbundenen Beschaffung von Ersatzgeräten, Auslastung der Infrastruktur, Wartung und Datensicherung. Auch möglich sind Zahlungen in Abhängigkeit von der Nutzung, erfolgsbasierte oder auch umsatzabhängige Bezahlung. Diese Preismodelle sind vor allem für gelegentliche Nutzer von Vorteil.

Stärken des SaaS-Modells

Als wichtigster Vorteil für den Kunden gilt, dass er sich nicht um den Betrieb der Applikation oder der gesamten EDV-Umgebung kümmern muss. Alle EDV-relevanten Vorgänge werden vom Dienstleister übernommen.

Schwächen des SaaS-Modells

Während der Vertragslaufzeit besteht eine Abhängigkeit vom Dienstleister. Darüber hinaus ist eine funktionierende Internetanbindung unerlässlich, da ohne Netzverbindung kein Arbeiten mit der SaaS-Anwendung möglich ist. Die Übertragung der Daten über die Internetanbindung eines Unternehmens bringt Einschränkungen in der Übertragungsgeschwindigkeit der Daten mit sich.

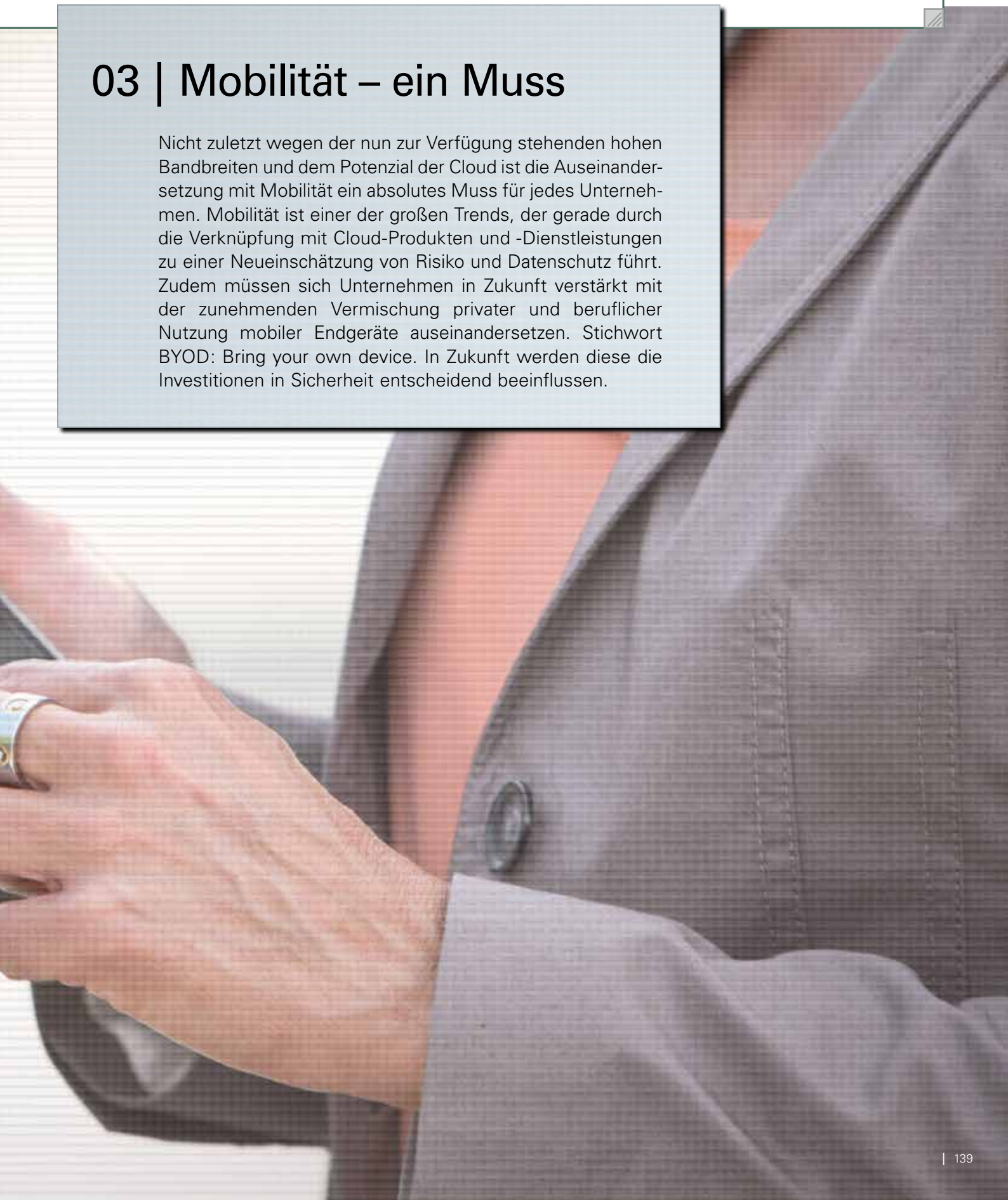
Für Anwendungen, die eine schnelle Datenübertragung benötigen, ist oft eine Lösung im lokalen Unternehmensnetz zu bevorzugen.

Vertrauen ist die Basis

Werden sensible oder unternehmenskritische Daten beim Dienstleister gelagert, ist ein besonderes Vertrauensverhältnis zwischen Dienstleister und Kunde nötig. Insbesondere bei personenbezogenen Daten sind auch die rechtlichen Aspekte mit dem Datenschutzbeauftragten zu klären. Als Partner empfehlen sich deshalb zum Beispiel zertifizierte Rechenzentren.

03 | Mobilität – ein Muss

Nicht zuletzt wegen der nun zur Verfügung stehenden hohen Bandbreiten und dem Potenzial der Cloud ist die Auseinandersetzung mit Mobilität ein absolutes Muss für jedes Unternehmen. Mobilität ist einer der großen Trends, der gerade durch die Verknüpfung mit Cloud-Produkten und -Dienstleistungen zu einer Neueinschätzung von Risiko und Datenschutz führt. Zudem müssen sich Unternehmen in Zukunft verstärkt mit der zunehmenden Vermischung privater und beruflicher Nutzung mobiler Endgeräte auseinandersetzen. Stichwort BYOD: Bring your own device. In Zukunft werden diese die Investitionen in Sicherheit entscheidend beeinflussen.



1 Voraussetzungen

Breitbandiger Internetzugang und leistungsstarke Endgeräte ermöglichen neue Arbeitsformen.

Ermöglicht wird der Trend zum Mobile Computing von technischer Seite zum einen durch einen breitbandigen Zugang zum Internet, zum anderen durch immer leistungsstärker werdende Endgeräte. Bemerkenswert ist hier v. a. die Entwicklung der Smartphones, die bereits die Möglichkeiten eines PC bieten.

Von Seiten der Nutzer führen diese Möglichkeiten überhaupt erst zu einer flexiblen, mobilen Nutzung von Web-Applikationen und sogenannter Apps, die das Pendant zu Programmen auf dem PC bilden. Die „sozialen Medien" wie Facebook, Twitter & Co. sorgen darüber hinaus bereits für eine neue Form der Kommunikation.

Konsequente Folge dieser Entwicklung ist der Ruf nach Öffnung von Firmennetzwerken für den „mobilen Außendienst". Die im Privaten genutzten Geräte sowie die Einfachheit und Flexibilität deren Benutzung drängt zusehends in die Unternehmen. Leistungsstarke, innovative Mitarbeiter fordern heute die Möglichkeit, das ihnen vertraute Arbeitsumfeld aufzubauen. Ebenso wie dies bei Einführung von Microsoft-Produkten in den 90ern oder dem Anfang des Internets 2000 der Fall war. Dies bedeutet die Gestaltung des Arbeitsplatzes mit Internet-/Cloud-Funktionen, Software und Endgeräten. Und wie bereits in der Vergangenheit scheint es auch Erfolg versprechend, wenn es um die Entwicklung von Standards geht.

2 Mobilität als Standard

Mobilität ist kein Hype.

Mobilität ist keine Modeerscheinung, die nach einer kurzen Hochphase wieder verschwinden wird. Dafür sorgen schon alleine das Social Web[13] und der Umfang der privaten Nutzung des mobilen Internets. Darüber hinaus drängt mit der aktuellen Generation von Arbeitnehmern eine neue Kultur der Erreichbarkeit und der Kommunikation in die Unternehmen. Mobilität ist aus dieser Sichtweise heraus kein technischer Trend mehr, sondern ein Wandel in der Kommunikationskultur, aus dem sich neben Komfort auch wirtschaftliche Vorteile ergeben.[14]

Verzahnung von mobilen und stationären Arbeitsplätzen

Für Unternehmen ist der Wandel weg von der Internet-Nutzung mit dem Handy hin zum mobilen Computing mit Smartphones und Tablets zukunftsweisend.

Die Cloud stellt mit Online-Diensten und Web-Anwendungen die perfekte Ergänzung zu mobilen Endgeräten zur Verfügung. In ihrem Zusammenwirken kann mit den unterschiedlichen mobilen Endgeräten in der Cloud fast ebenso gearbeitet werden, wie an einem PC in einem Terminal-Server-Netzwerk.

Eine wichtige Funktion für den Erfolg von Smartphone und Tablet-PC stellen nicht nur die Apps dar, sondern die damit verbundene Möglichkeit, praktisch in jeder Lebenslage erreichbar zu sein, auf Unternehmensdaten zugreifen zu können oder Dienste der Cloud zu nutzen.

Die permanente Erreichbarkeit und leistungsstarke Geräte ermöglichen ortsungebundenes Arbeiten.

Dies ermöglicht vom Chef bis zum Mitarbeiter eine neue Form der Kommunikation und der Arbeitsorganisation. Können Daten ohne Medienbruch und Zeitverzug an beliebigen Orten nahezu gleichzeitig bearbeitet und zur Verfügung gestellt werden, wird sich in Folge dessen auch die Prozesslandschaft des Unternehmens verändern. Bei Schnittstellen zu vorgelagerten „Datenlieferanten" bzw. digitalen Abnehmern verändert sich dadurch die komplette Wertschöpfungskette.

Abhängig von Branche und Unternehmen können sowohl die traditionelle Kollaboration mit Office-Anwendungen als auch ganze Prozesse aus dem Unternehmensnetzwerk herausgelöst und in die Cloud „outgesourced" werden. Der Vorteil liegt direkt auf der Hand: keine langwierigen Installationen oder Unverträglichkeiten mehr mit Software.
Zur zentralen Administration gesellt sich der schnelle Online-Zugriff von mobilen Endgeräten ebenso wie eine zentrale Datensicherung bzw. Archivierung in der Cloud.

Der bedarfsorientierten Verzahnung von stationären und mobilen Arbeitsplätzen steht technisch und organisatorisch nichts mehr im Wege.

[13] vgl. Teil 3, Kapitel 5 „Social Media", S. 106 ff.

[14] Accenture-Studie „Mobile Web Watch 2011", S. 36:
www.accenture.com/de-de/Pages/insight-mobile-web-watch-2011.aspx

3 Wandel auf drei Ebenen

Der Wandel der Arbeitsformen, Organisationsstrukturen und Unternehmenskulturen vollzieht sich auf verschiedenen Ebenen gleichzeitig.

Die Usability für den jeweiligen Zweck entscheidet über die Wahl des Endgerätes.

Die Endgeräte werden kleiner und leistungsstärker. Es findet ein Verdrängungswettbewerb statt, bei dem sich Smartphones, Tablets und Netbooks, je nach Lebens- bzw. Arbeitsbereich und den dort vorherrschenden Anforderungen neu verteilen werden. Gerade die einfache Bedienung führt dazu, dass die Hürden zum Einstieg ins Internet fallen. Kontaktmanagement und E-Mail auf dem Handy, Berichte und Übersichten auf dem Tablet, kompakte Auswertungen auf dem Note- bzw. Netbook. Die Usability für den jeweiligen Zweck entscheidet über die Wahl des Endgerätes.

(De)zentrale Ressourcennutzung je nach Anforderung.

Gleichzeitig entstehen rund um die neue Generation von Smartphones und Tablets Tausende Apps, Cloud-Dienste und Web-Anwendungen für jede Lebenslage und Anforderung. Ist der Arbeitsspeicher oder die Rechenkapazität nicht ausreichend, kann auf Cloud-Funktionen zugegriffen werden. Werden Informationen aus dem eigenen Unternehmen benötigt, wird einfach remote darauf zurückgegriffen.

Die Usability dominiert erstmalig die Anforderungen an die Sicherheit.

Die bestechende Benutzerfreundlichkeit lässt die Schranken fallen – zumal plötzlich alles einfacher ist als auf dem PC mit seinen komplexen und z. T. schwerfälligen Anwendungen. Zudem schlagen gerade bei der PC-Nutzung im Unternehmen die Restriktionen der IT-Sicherheit und des Datenschutzes für die Nutzung von Geräten, Programmen und Daten mit voller Wucht zu. Dagegen wirken unterwegs die kleinen Helfer locker und leicht in ihrer Bedienung – fast befreiend für die modernen Arbeitsprozesse. Kein Wunder also, dass derart befreit und damit motiviert jeder, vom Chef bis zum Mitarbeiter, diese neue Freiheit nutzen möchte. „Bring your own Device" ist ein Schlagwort der aktuellen Stunde, das eigene Gerät nicht nur für die persönliche Kommunikation zu nutzen, sondern auch geschäftlich einzusetzen und damit auf die Informationen des Unternehmens zuzugreifen, zu jeder Zeit und von jedem Ort. Natürlich stets auf dem aktuellen Stand der Informationen aus dem Unternehmen.

So wie Studierende daran gewöhnt sind, im Internet zu arbeiten, werden sie dies auch mit in ihren Arbeitsalltag integrieren wollen.

Auch an den (Hoch-)Schulen, also bei den Arbeitnehmern der Zukunft, ist dieser Trend zur mobilen Nutzung des Internets allzeit und überall sichtbar. Sind es dort noch die Communities und Netzwerke, so werden die Unternehmen als Arbeitgeber mit der Forderung konfrontiert, Smartphones, Tablets & Co. als festen Bestandteil des Arbeitsplatzes zu stellen; selbstverständlich in freier Auswahl des Herstellers und Betriebssystems.

4 Gefährdungen

Fehlende Zugriffsberechtigungen als Risikofaktor.

Trotz der Anstrengungen der Hersteller existieren zu jeder Zeit sowohl Sicherheitslücken als auch Fehler und Fehlfunktionen ebenso wie Fehlverhalten der Benutzer. Darüber hinaus stellen fehlende bzw. unzureichende Zugriffsberechtigungen eine zusätzliche Gefährdung dar, die unberechtigten Zugriff, Manipulation und Datenabfluss ermöglicht. Daher sollten Unternehmen stärker auf die Feinsteuerung der Zugriffsberechtigungen achten. Sei es zum eigenen Schutz von sensiblen Daten des Unternehmens oder sei es aufgrund gesetzlicher Verpflichtung.

Neue Geräte und Arbeitsweisen ermöglichen die Erstellung und direkte Zuordnung von individuellen Nutzungsprofilen.

Das Gefährdungspotenzial zum Ausspionieren vertraulicher Informationen ist besonders hoch bei Funkverbindungen. Sei es durch automatisches Einbuchen in vorhandene Netze oder durch neue Mechanismen für die Nutzung von sozialen Netzen. Gerade diese Funkverbindungen sind jedoch Standard bei mobilen Endgeräten. Als vertrauliche Information gelten nicht nur geschäftskritische Daten, sondern auch Zugangsdaten zum Unternehmensnetz bzw. zu Cloud-Diensten. Besonders im mobilen Bereich ist die persönliche Zuordnung des Nutzungsverhaltens, also die Profilerstellung des Nutzers nach abgerufenen Inhalten, App-Nutzung oder Bewegungsmustern zusammen mit der Ortsbestimmung durch eine feste Geräte-ID möglich.
Eben diese Profilerstellung des Nutzers muss kritisch gesehen werden, da diese nicht nur zu Werbezwecken missbraucht werden kann, sondern auch Bestandteil von „Social Engineering" ist und zur Vorbereitung von Angriffen dient.

Darüber hinaus müssen auch mobile Speichermedien im Rahmen der Sicherheitsbetrachtung eines Unternehmens entsprechend berücksichtigt werden. Diese werden beispielsweise erheblich häufiger liegengelassen, mitgenommen oder werden durch die physische Beanspruchung defekt. Dies gilt es bei Datenerfassung und Datenhaltung und Datensicherung zu beachten.

Defizite in Sicherheit und Datenschutz durch mobile Computing.

Wenn es um den Schutz des eigenen geistigen Eigentums, der Firmenwerte, Absprachen mit Lieferanten, Preisabsprachen, Kalkulationen etc. geht, müssen sich zur Benutzerfreundlichkeit auch Sicherheitsmechanismen gesellen, die im geschäftlichen Bereich entweder gesetzlich vorgeschrieben sind oder dem Selbstschutz dienen.
Wann wäre es jemals einem Unternehmer in den Sinn gekommen, eine bunte Mischung von verschiedenen Programmen, vom Kontaktmanagement über Börsenticker hin zu Spielen und Multimedia unterschiedlichster Hersteller aus unterschiedlichen Nationen auf einem produktiven PC zu installieren – und sich dabei nicht die Frage zu stellen, auf welche Daten all diese Programme zugreifen können, geschweige denn, ob diese Programme selbstständig alle Daten des PCs beliebig an Adressen auf der ganzen Welt versenden können – und dies, ohne die Möglichkeit, es festzustellen?

Der Mangel an zentraler Administration führt zu verstärkter Attraktivität bei Kriminellen.

Analog zum stationären PC führt der Mangel an zentraler Administration nicht nur zu hoher Verbreitung auf dem Markt mit entsprechend leistungsstarken und vielseitigen Apps, sondern eben auch zu verstärkter Attraktivität bei Kriminellen.

App-Plattformen – Wettlauf zwischen Anbietern und Kriminellen

Mehr Sicherheit durch geschlossene Marketplaces.

Einen wesentlichen Unterschied hat die App-Entwicklung im Vergleich zu PC-Programmen dann doch. Die Anbieter versuchen auf ihren Marketplaces nur sichere Software anzubieten. Mit mehr oder weniger Engagement – und mit mehr oder weniger Erfolg. Immer wieder erreichen uns Meldungen über Apps, die in fremden Daten wildern oder von Malware befallen sind.

Im Vergleich zum PC ist Malware kaum zu finden. Dennoch ist Sicherheitssoftware zur App-Kontrolle gegen unerwünschten Datenabfluss sinnvoll.

Gut und Böse zu unterscheiden ist jedoch bei den Apps deutlich schwieriger. Zumal auch die Bewertungen im Internet prinzipiell jeder erstellen kann – auch bezahlte Autoren. Neutrale Dritte, die Sicherheitssoftware anbieten und ein Gegengewicht darstellen könnten, sind bislang nur auf den marktführenden Betriebssystemen zu finden. Dies erfolgt jedoch auch nur dort, wo die Hersteller dies zulassen. Mancher Anbieter von Hardware lässt sich z. B. nicht gerne in die Karten schauen und eröffnet Anbietern von Sicherheitssoftware nicht die Möglichkeit, ihre Software in die Tiefen des Betriebssystems zu integrieren, um die dortigen Vorgänge zu überwachen. Andere hinken beim Patchmanagement hinterher, sodass Sicherheitslücken lange ausgenutzt werden können.

Schnittstellen auf mobilen Endgeräten sind schwer zu kontrollieren.

Werbung, eingebetteter Code von sozialen Netzen, Web 2.0 in Verbindung mit JavaScript, dynamische Webseiten, aktive Inhalte und Inline-Frames auf einer „einzelnen Internetseite" haben nicht nur zur Folge, dass es praktisch keine „vertrauenswürdigen Internetseiten" mehr gibt. Mit Werbung und je nach Betriebssystem bei Smartphones umfangreichen Freigaben bei der Installation bzw. Betrieb von Apps existieren sicherheitskritische Schnittstellen, die schwer zu kontrollieren sind. Schwer deshalb, da ein unkontrollierter Kanal auf unkontrollierte Quellen verweist, von denen auch bei Tests durch die Marketplace-Anbieter nur Momentaufnahmen gemacht werden können.

Für die neuen Arbeitsformen sind neue Sicherheitskonzepte erforderlich.

Die etablierten Sicherheitskonzepte und -strategien für ITK in Unternehmen greifen bei den Smartphones und Tablets ins Leere, da sich deren funktionale Konzepte am privaten Nutzer orientierten und damit anders aufgebaut sind. Das aktive Mitarbeiten und das Verständnis des Nutzers sind auch hier wichtige Aspekte, um Sicherheit zu gewährleisten.

App-Controlling und Konfiguration

Wenn der Einsatz der mobilen Geräte nicht verhindert oder im klassischen Sinne abgesichert werden kann, muss eine andere Strategie für mehr Sicherheit sorgen.

Mit einem sogenannten Whitelisting können spezielle Apps für die Installation freigegeben werden. Negativ bekannt gewordene können gezielt auf eine Blacklist gesetzt werden. Gerade in Verbindung mit BYOD (Bring your own Device)[15], also der Verwendung von privaten Mobilgeräten im dienstlichen Kontext, kann verhindert werden, dass durch unzählige, ungeprüfte oder kritische Apps die Angriffsfläche künstlich erhöht wird.

[15] BYOD ist die Abkürzung für das Englische „Bring your own Device". Das meint, dass Mitarbeiter ihre privaten Geräte geschäftlich nutzen können.

Durch Werbung und aktive Elemente wie JavaScript [16] etc. können natürlich nicht alle Schnittstellen zentral im Marketplace [17] kontrolliert werden. Auch hier ist eine firmeninterne Kontrolle und Studium einschlägiger Tests erforderlich, um die Seriosität einer App beurteilen zu können. Gerade bei Zulassung von werbefinanzierten Apps ist eine Prüfung erforderlich, da auf den kleinen Mobilteilen doch schnell der Werbebanner gedrückt werden kann und dies für Abofallen mittels Werbung ausgenutzt wird.

Vor dem Einsatz von Apps sollten diese kritisch geprüft werden.

Sinnvoll und auch sicherer ist die Installation ausschließlich von offiziellen Plattformen der Hersteller, da diese in eigenem Interesse versuchen, Malware oder kritische Apps auszusondern. Dennoch können durch die Marketplace-Anbieter nur Momentaufnahmen gemacht werden.

Für die unerschrockenen Experimentierfreudigen gibt es zumindest bei Android eine Einstellung, um die Installation von beliebigen Quellen zu ermöglichen. Im Unternehmensumfeld sollte diese Einstellung als potenzielle Schwachstelle unter ständiger Beobachtung stehen.

Bei der Auswahl der Geräte und der Nutzung von Apps müssen sich gerade Manager disziplinieren: Der hohen Usability wird gerne der Sicherheitsaspekt untergeordnet. Ein vernünftiger Konsens, mit dem beide Ziele in Einklang gebracht werden können, ist wünschenswert. Denn: Je höher die Position im Unternehmen, desto kritischer ist meist die Information. Dies gilt für Marketingstrategien gegenüber dem Wettbewerb ebenso wie für neue Produkte. Hinzu kommen rechtliche Verpflichtungen wie beispielsweise der Datenschutz. Die Einwände von Seiten der IT-Sicherheit und des Datenschutzes kommen ja nicht von ungefähr. Auf der anderen Seite ist es manchmal, oberflächlich betrachtet oder aus den Formulierungen der ITler heraus, nicht nachvollziehbar, warum gerade diese App nicht eingesetzt werden darf oder der Hotspot in der Bahn oder dem Hotel nicht benutzt werden sollte, wenn die Alternative bedeutet, für einen Tag nicht erreichbar zu sein.

Gerade Manager neigen dazu, die Usability über die erforderliche Sicherheit bzw. Compliance zu stellen.

Die neue Mobilität erfordert hier eine neue Kommunikationskultur, in der nicht nur einer Recht haben darf. Es gilt, Risiko und Nutzen neu zu bewerten und abzuwägen. Nicht alles, was geht, ist auch für den Fortbestand des Unternehmens vernünftig – und Sicherheit ist auch kein Selbstzweck, zumal absolute Sicherheit nicht erreichbar ist.

Es gibt genügend Angebote zur sogenannten Endpoint Security oder einem Mobile-Device-Management. Ein neuer Ansatz berücksichtigt die Mischung aus verschiedensten Geräten, Betriebssystemen und Apps. Grundvoraussetzung für eine solche Lösung ist jedoch eine Bestandsaufnahme von Daten und Prozessen sowie deren Zuordnung zu Sicherheitsklassen – und auf lange Sicht die Datenhygiene. Auf einer solchen Basis können je nach Endgerät und Verwendungskontext die unterschiedlichen Nutzer mit ihren unterschiedlichen Rollen/Berechtigungen Zugriff auf unterschiedliche Datenklassen erhalten. Automatismen überwachen den Zustand des Gerätes, der Apps, der Berechtigungen und der Daten, sodass bei Verstößen Geräte auch ausgesperrt werden können.

Endpoint Security ist eine gängige Methode zum Überwachen von Datenübertragungen nach innen und außen.

[16] JavaScript ist eine Skriptsprache, die es Webseiten z. B. ermöglicht, Inhalte nachzuladen.

[17] Mit Marketplace ist der virtuelle „Marktplatz" gemeint, auf dem Nutzer je nach operierendem Betriebssystem, passende Apps kaufen können.

Soweit möglich sollte der Datenverkehr durch Firewalls abgesichert werden, da nur so Apps, Cloud-Anwendungen, lokale Programme und Netzwerkaktivitäten vernünftig kontrolliert werden können.

Sicherheitsupdates

Auch beim Einsatz der modernen Smartphones und Tablets kommt der Anwender nicht um Updates für seine Apps bzw. sein Betriebssystem herum.

Bei der Entscheidung für ein Gerät sollte berücksichtigt werden, ob dessen Hersteller die Updates für das Betriebssystem zeitnah bereitstellt.

Gerätehersteller glänzen nicht unbedingt darin, das auf ihr Gerät zugeschnittene Betriebssystem auf dem aktuellen Stand zu halten. Es lohnt sich, bereits im Vorfeld der Anschaffung von Hardware zu klären, wie lange es je nach Hersteller und Modell dauert, bis bekannt gegebene Lücken durch Updates behoben werden. Augenscheinlich wird dies, wenn das Betriebssystem der von Google vertriebenen Hardware bereits gepatcht ist, während die Anpassungen der anderen Hardwarehersteller noch ausstehen. Wie am PC sind natürlich für die Apps die jeweiligen Hersteller verantwortlich. Treten Sicherheitslücken auf, zeigt sich die Qualität des Anbieters an der Geschwindigkeit, mit der Schwachstellen behoben werden.

Problematisch bei einem Zeitverzug ist, dass genügend Tools über das Internet verfügbar sind, mit deren Hilfe Programmcode analysiert werden kann, und mit den Sicherheitsupdates gleichzeitig die Lücken frei Haus geliefert werden.

Ort der Datenhaltung

Keine Datenhaltung auf mobilen Endgeräten.

Unabhängig von den Verfahren und Angeboten zur Endgerätesicherheit ist ein Aspekt für die Sicherheit besonders wichtig: Wo findet die Datenhaltung statt? Werden Daten auf dem Endgerät abgelegt, müssen diese zum einen laufend synchronisiert werden. Zum anderen bleiben gerade Smartphones – ebenso wie andere kleine mobile Datenträger – gerne liegen, werden verloren oder auch gestohlen.

Problematisch wird der Verlust, wenn wichtige Daten ausschließlich auf dem Gerät vorliegen, aber auch, wenn Daten unverschlüsselt abgelegt werden.

Ein weiterer wichtiger Punkt ist die Herkunft bzw. Zugehörigkeit der Daten: Handelt es sich nur um geschäftliche Informationen oder wird das mobile Endgerät im „Dual-Betrieb" genutzt, also privat und dienstlich? Während im rein dienstlichen Umfeld Vorschriften eher durchgesetzt werden können, ist es im Mischbetrieb deutlich schwieriger, den Anwender davon zu überzeugen, nicht jede scheinbar interessante App zu installieren oder gar einen Jailbreak durchzuführen.

Die Meldungen der Vergangenheit haben leider gezeigt, dass trotz aller Softwareprüfung von Seiten der offiziellen Marketplaces immer wieder installierte Software unberechtigt auf gespeicherte Daten, Kontakte oder Geoinformationen etc. zugreift bzw. diese auslesen kann.

Sicherheitssoftware

Es ist sicher keine schlechte Lösung, über eine Firewall zu kontrollieren, welche App sich an welchen Daten zu schaffen macht und auf welchen Kanälen diese wann und wohin im Internet kommuniziert.

Antivirensoftware hat auch bei mobilen Endgeräten ihre Berechtigung.

Auch Virenscanner sind kein Allheilmittel, sorgen jedoch dafür, dass weitverbreitete Malware, also Viren und Trojaner, gefunden wird. Jedoch muss sich jeder spätestens seit Stuxnet darüber im Klaren sein, dass gut gemachte Malware, die nur auf einzelne Systeme oder Unternehmen zielt, ebenso wenig durch die Standardmechanismen von Sicherheitssoftware gefunden werden kann wie ein gut gemachter Hacker-Angriff.

Wie bereits im Abschnitt zu den App-Plattformen erwähnt, lassen manche Hersteller mal mehr, mal weniger systemnahe Programmierung zu. Diese ist jedoch für gute Sicherheitssoftware erforderlich. Nichtsdestotrotz gibt es bereits Sicherheitssoftware. Manche Anbieter richten sich bei Erstellung ihres Portfolios strikt nach der aktuellen Marktlage und erstellen nur für die marktführenden Betriebssysteme Antiviren-Apps. Auf viel genutzte Betriebssysteme ist ein Viren-Angriff lohnender und somit der wahrscheinliche Absatz der Antivirensoftware höher.

Dabei wäre gerade die Entwicklung von Firewalls im Interesse der gewerblichen Nutzer von mobilen Endgeräten. So könnte jeder selbst schnell feststellen, wie umtriebig manche Apps sind. Im offiziellen Google-Market kommt beispielsweise vor der Installation einer App u. a. ein Listing, welche sicherheitskritischen Funktionen enthalten sind, wie z. B. Zugriff aufs Adressbuch oder selbstständiger Internetaufbau der App. Dass mit dem lesenden Zugriff auf das Adressbuch die vollständige Kontakt-Sammlung auf den Server des Programm-Herstellers geladen wird, ist so nicht zu entnehmen.

Firewalls helfen bei der Kontrolle allzu neugieriger Apps.

Beim Einsatz von Firewalls ist allerdings zu beachten, dass die recht kryptischen Regeln zwar ein hervorragendes Steuerinstrument für Apps und Prozesse auf einem Gerät darstellen – jedoch auch gutes technisches Know-how erfordern.

BYOD: Übertragung ins Firmen-Netz

Auch im Mischbetrieb von privat und dienstlich gibt es Möglichkeiten, die gewünschte Sicherheit durchzusetzen. Dies bedarf im Vorfeld jedoch der Auseinandersetzung mit dem Anwender, seinen Wünschen, seinen Gewohnheiten und dienstlichen Erfordernissen.

Private Endgeräte müssen kein Sicherheitsrisiko sein. Klare Regelungen und Richtlinien können hier Abhilfe schaffen.

Eine Whitelist der IT-Sicherheit weist beispielsweise Apps aus, deren Verwendung unbedenklich ist. Richtlinien zum Datenzugriff können festlegen, dass ein Remote-Zugriff aufs Unternehmensnetzwerk nur dann stattfinden kann, wenn alle Apps auf dem aktuellen Stand sind. Der Verbindungsaufbau ins Firmen-Netz erfolgt nur über gesicherte Kanäle und gibt unter Umständen nur die Daten frei, die je nach Prüfung des angemeldeten Anwenders, der Anwendung und des Gerätekontextes zulässig sind. So kann beispielsweise der Zugriff auf Auftragsdaten für BYOD-Geräte unterbunden werden, während firmeninterne Informationen zugänglich sind: direkter Zugriff für niedrige Datenschutzklasse, virtueller Zugriff bei höherer Schutzklasse.

Dies setzt natürlich voraus, dass sich die Verantwortlichen bereits vor der Einführung mobiler Endgeräte mit Datenzuordnungen in Datenklassen unterschiedlicher Vertraulichkeit, Datenhygiene sowie den darauf zugreifenden Verarbeitungsprozessen auseinandergesetzt haben.

Wer diese vorbereitenden Tätigkeiten für die Absicherung der Unternehmenswerte bisher nicht vorgenommen hat, muss sich keine Sorgen darüber machen, dass die mobilen Endgeräte eine besondere Gefahr für das Unternehmen darstellen. Die Probleme des Informationsabflusses liegen dann an anderer Stelle.[18]

Geräteverlust und Zugangsdaten

Der Verlust eines Gerätes ist ein finanzieller Schaden, aber verschmerzbar. Kritischer ist es, wenn Informationen zu Geschäften bzw. Geschäftspartnern nicht synchronisiert wurden, also nur auf dem Gerät vorlagen.

Die PIN schützt vor unberechtigtem Zugriff.

Ist dann aus Bequemlichkeit keine PIN verwendet worden, ist das Gerät nicht vor unberechtigtem Zugriff geschützt. Auch wenn es auf Youtube genügend Videomaterial gibt, wie welches Smartphone-Modell etc. geknackt werden kann, schützt die PIN doch vor dem zufälligen Finder oder dem Gelegenheits-Cracker.

Um schnell auch auf Apps zuzugreifen, die eine Anmeldung erfordern, werden Zugangsdaten wie Benutzername und Passwörter fest in Apps hinterlegt. Kommt ein Gerät abhanden, können, gerade bei unverschlüsselt abgelegten Daten, die Zugangsdaten schnell in fremde Hände gelangen. Mit der Folge, dass sowohl auf das Unternehmensnetzwerk zugegriffen werden kann als auch im Namen des Geschädigten Geschäfte getätigt, Malware versendet, kostenpflichtige Dienste in Anspruch genommen oder mit Finanz-Apps Geld verschoben und gewaschen werden kann.

[18] Bring your own Device – BYOD (Horst Speichert): www.citrixonline.de/aktuelles/whitepaper
DirektLink: http://learn.gotoassist.com/DE-G2A-WP-BYOD-Speichert?ID=70150000000Y7IB

Bei Verlust des Gerätes sollten unbedingt Verfahrensabläufe im Unternehmen vorhanden sein, die eine schnelle Deaktivierung des Zugangs für das verlorene Gerät ermöglichen. Eine Fernlöschung bzw. Lokalisierung kommt hier ebenfalls in Betracht.

Bei Geräteverlust sollte eine Fernlöschung unverzüglich durchgeführt werden.

Funkverbindung ausspioniert

Die mobilen Begleiter haben darüber hinaus ein grundsätzliches Problem: die Sicherheit der Funkverbindung. Im Bereich der drahtlosen Datenübertragung stehen WLAN und Bluetooth bzw. UMTS und LTE im Vordergrund. Sie stellen sicher, dass Mitarbeiter jederzeit und überall erreichbar sind.

Dass WLAN-Hotspots unsicher sind, leuchtet vielen noch ein, da die einzelnen eingewählten Nutzer in einem großen Netzwerk nebeneinander liegen und nicht besonders gut gegeneinander abgesichert sind – eben ein öffentliches Netzwerk. Andere Funkverbindungen bergen jedoch vergleichbare Risiken.

Um die Angriffsflächen so gering wie möglich zu halten, sollten sämtliche Datenverbindungen auf das Notwendigste beschränkt werden.

Bluetooth-Verbindungen sind eine schicke Sache. Ohne großen Aufwand suchen und finden sich mitunter die Geräte selbstständig. Mit den richtigen Apps oder auch Tools auf einem Notebook kann man schon einmal einen neugierigen Blick in das andere Gerät werfen.

Funktastaturen an Smartphones, Tablets oder Notebooks werden selten als besonders gesprächig wahrgenommen. Doch wer nicht beim Anschluss für eine verschlüsselte Übertragung sorgt, liefert einem Lauscher schnell Informationen, u.a. auch Zugangsdaten für unterschiedliche Dienste oder das eigene Unternehmensnetzwerk.

Nicht nur staatliche Stellen können sich das erforderliche Equipment für das vollständige Abhören von Funkverbindung zwischen Endgerät und Funkmast leicht besorgen. Mittels Störsender wird UMTS in die Knie gezwungen, sodass das Smartphone automatisch auf GSM herunterregelt. Mittels ISMI_Catcher wird dann eine Man-in-the-Middle-Attacke auf die Funkverbindung gestartet. Damit können Gespräche und Datenübermittlung unverschlüsselt mitgehört bzw. mitgeschnitten werden.

Grundsätzlich sollten daher Datenverbindungen auf das Notwendige beschränkt werden, um die Angriffsfläche so gering wie möglich zu halten.

Jailbreak / rooten

Von Haus aus ist Smartphones & Co. eine Sicherheitsarchitektur mitgegeben worden, die manchem PC-Nutzer der Vergangenheit gut gestanden und Schlimmes verhindert hätte. Der Nutzer kann das Gerät nur nutzen und verfügt nicht über administrative Möglichkeiten. Für Bastler und Tüftler eine Herausforderung.

Jailbreaks stellen immer ein Sicherheitsrisiko dar.

Doch Jailbreak ist nicht nur etwas für Technikfreaks. Wer selbst etwas an seinem Gerät herumbasteln möchte, erhält hierdurch Vollzugriff auf das Gerät. Schlimm ist ein Jailbreak, wenn er unerwünscht stattgefunden hat, beispielsweise beim Besuch einer präparierten Webseite.

Mobile-Device-Management überwacht Zugriffsberechtigungen.

Im Unternehmen sollte ein Mobile-Device-Management beim Zugangsversuch feststellen können, ob ein Jailbreak vorliegt. Und, wenn dies der Fall ist, das Gerät in Quarantäne nehmen, da in diesem Zustand nicht sichergestellt werden kann, ob im Zuge dessen schädliche Software aus ungeprüften bzw. unseriösen Quellen auf das Gerät installiert wurde. Im Auslieferungszustand können die mobilen Geräte nur aus den Hersteller-Marketplaces bestückt werden. Hier ist zumindest ein Mindestmaß an Sicherheit gewährleistet. Wie die Vergangenheit zeigte, können von Seiten der Hersteller im schlimmsten Fall Apps sogar ohne Rückfrage und Zutun des Anwenders entfernt werden.

Entsorgung

Am Ende des Lebenszyklus auch eines mobilen Endgerätes steht die Entsorgung. Was aus Sicht des Anwenders ein trivialer Vorgang ist, ist aus Sicht der IT-Spezialisten etwas komplizierter.

Die Sicherung der Daten ist eine einfache Übung, wenn sie originär und nur auf dem Gerät abgelegt und nicht nur durch Synchronisation darauf kopiert wurden.

Das vollständige Löschen sensibler Daten ist nicht immer möglich.

Schwieriger wird es, wenn es um das sichere Löschen sensibler Informationen aus dem Unternehmen geht. Ganz zu schweigen von gesetzlichen Auflagen bei personenbezogenen Daten Dritter, die unter Umständen sogar strafrechtliche Relevanz besitzen. Mancher Hersteller ermöglicht es Anwendern, Administratoren oder Technikern nicht, direkt auf Hardwareteile zuzugreifen. Ein Ausbau der integrierten Speicher, vergleichbar dem Ausbau von Festplatten, kommt damit nicht in Frage. Spezialisten empfehlen hier, den kompletten Speicher mehrmals komplett mit leeren Bildern oder Zahlensalat zu überschreiben. Allerdings kommt man bei geschlossenen Systemen einzelner Hersteller als Nutzer, bedingt durch deren Konzept/Geschäftsmodell, nicht ans Betriebssystem und die Systembereiche heran, die ebenfalls Daten enthalten können. Auch bei anderen Herstellern ist der Zugriff auf das System und dessen Daten nicht ganz so einfach und setzt technisches Know-how voraus.

Die physische Zerstörung ist die sicherste Lösung.

In Folge müsste man, wie auch zum Tausch eines defekten Akkus, spezialisierte Filialen des Anbieters aufsuchen, um dort Teile entfernen bzw. ersetzen zu lassen. Die sichere Alternative: physische Zerstörung des Gerätes.

Nun ist jedoch das Ende des Lebenszyklus im Unternehmen nicht das „Verfallsdatum" des Gerätes selbst. Da die in der Anschaffung nicht ganz billigen Endgeräte weiterveräußert werden könnten, sollte dieser Aspekt bei der Anschaffung berücksichtigt werden. Auch wenn dies unter Umständen bedeutet, dass besonders schicke und besonders einfach zu bedienende Geräte nicht angeschafft bzw. bei BYOD nicht zugelassen werden können.

Der Faktor Mensch

Wo Sicherheitsstandards fehlen, kommt dem Sicherheitsbewusstsein der Mitarbeiter besondere Bedeutung zu.

Das mangelnde Risikobewusstsein der Mitarbeiter ist als gravierende Sicherheitslücke einzustufen. Wenn das Telefon quasi im Internet surfen kann, sollte es über eine Firewall verfügen. Können Bilddateien, Musik oder Videos per MMS, Fax oder E-Mail versendet werden, ist ein Virenscanner erforderlich. Kann die Kalkulation ins firmeneigene Netzwerk übertragen werden, sollte eine sichere Einwahl ins Netzwerk möglich sein. Zudem muss ein Passwortschutz für die Nutzung des Gerätes vorhanden sein, falls es entwendet wird oder verloren geht. Ein unberechtigter Dritter könnte sich sonst im Namen des Eigentümers ins Firmennetz einwählen.

Neben den eingesetzten Produkten, die zur Sicherheit beitragen, sollte vor allem das Sicherheitsbewusstsein der Mitarbeiter geschärft werden. Diese bedienen letztendlich die eingesetzte Software. Hat der Nutzer administrative Rechte, entscheidet er nicht nur über sein eigenes Verhalten, sondern auch über den Grad an Sicherheit, den die Software bietet.

5 Folgen bei Infektion

E-Mail-Adresse und Passwort sind eine begehrte Ware.

Die Folgen einer Infektion sind ähnlich denen des PCs: Gerne werden beispielsweise Zugangsdaten, also Benutzernamen und Passwörter für den Firmenzugang oder diverse Dienste im Internet bzw. der Cloud in den Apps fest hinterlegt. Dies sorgt für eine sehr schnelle und bequeme Verwendung. Sind allerdings durch Befall mit Malware die Passwörter abhanden gekommen, ist ein schneller Wechsel der Passwörter angeraten.

Identitätsklau hat für das Opfer Konsequenzen.

Kriminelle sind schnell und einfallsreich. Accounts bei sozialen Medien wie Twitter oder Facebook werden ebenso wie Mailaccounts benutzt, um sämtliche Kontakte des Mobilgerätes mit Nachrichten zu beglücken, deren Absender der ohnehin Geschädigte ist. Spam, Scareware und Malware jeglicher Art werden so über seriöse Absender dem Kreis der Bekannten und Geschäftspartner zugesendet, die dann arglos ebenfalls zu Opfern der Kriminellen werden. Unter Geschäftspartnern muss ein Unternehmen sich dann die Frage nach der im Geschäftsbetrieb erforderlichen Sorgfalt und der gebotenen Sicherheit gefallen lassen.

Der eigene PC als Malwareverteiler und Hacker.

Eine besondere Art der Infektion stellt das Botnetz dar. Hierbei werden die Opfer durch eine Art „Fernbetreuungs-Software" zum Teil eines großen Netzwerkes, in dem der „Administrator" die befallenen Geräte nicht nur dauerhaft nach interessanten Kontakten und Informationen durchsucht. Der Kriminelle kann nach Belieben über das Gerät verfügen: Sei es zum Verteilen von Malware und Spam, sei es zum Angriff auf Internetseiten, deren Anbieter erpresst werden sollen, sei es für illegale Finanztransaktionen oder gar zum Knacken von Passwörtern. Die so gebildeten Netzwerke können – als lukratives Geschäftsmodell – im Internet auch nach Bedarf angemietet werden.

Darüber hinaus können bequem Abos auf Kosten des Nutzers abgeschlossen oder teure Servicenummern angerufen werden.

Je nach den durch Malware erhaltenen Zugangsdaten können im Namen der Geschädigten auch Online-Geschäfte getätigt werden; sei es durch Verkauf von Produkten und Dienstleistungen oder sei es durch deren Ankauf.

Der Verlust des Gerätes kann durch Missbrauch teuer werden.

Ein besonderes Bonbon stellen in diesem Zusammenhang die Zugangsdaten zu einem Unternehmensnetzwerk dar. Wer als Berechtigung nur die Wissenskomponenten Name und Passwort einfordert, öffnet einem Kriminellen schnell Tür und Tor.

Besondere Beachtung sollte daher den je nach Gerätehersteller und Betriebssystem unterschiedlich vorhandenen Sicherheitslösungen für Smartphone & Co. gewidmet werden.

6 Tipps und Lösungsansätze

Der Anspruch an Sicherheit muss sich dieser Entwicklung anpassen.

IT-Verantwortliche und Geschäftsleitung müssen sich künftig auf eine neue Art von Konsens verständigen. Der Anspruch an Sicherheit kann in dieser neuen vernetzten Arbeitswelt nicht mehr in der traditionellen Weise aufrechterhalten werden. Die bisher übliche Fiktion von Sicherheit kann nicht mehr aufrechterhalten werden. Der Anspruch an Sicherheit muss künftig niedriger angesetzt werden. Allerdings nur so weit, dass ein effektives und effizientes Arbeiten möglich ist. Es darf jedoch nicht dazu führen, vollständig auf Sicherheit zu verzichten, auch wenn diese ohnehin nicht vollständig erreicht werden kann.

Fehlende Sicherheitsfeatures der mobilen Geräte müssen durch Sicherheitsbewusstsein ausgeglichen werden.

Grundsätzlich wird beim mobilen Endgerät der Faktor Mensch in besonderer Weise in den Fokus rücken müssen, da die aktuellen Geräte noch nicht über die ausgefeilten Automatismen des PCs verfügen. Essenziell ist das Verständnis der Beteiligten nicht nur für die Funktionen, die als leistungserstellend angesehen werden, sondern auch für die Sicherheit. Bei Verlust des Gerätes sollten unbedingt Verfahrensabläufe im Unternehmen vorhanden sein, die eine schnelle Deaktivierung des Zugangs für das verlorene Geräte ermöglichen. Eine Fernlöschung bzw. Lokalisierung kommt hier ebenfalls in Betracht.

Die Zugangsberechtigungen zum Unternehmensnetz müssen differenziert ausgearbeitet werden. So sollten u. a. nur verschlüsselte Verbindungen zugelassen werden. Darüber hinaus muss Sicherheitssoftware angepasst bzw. passende angeschafft werden. Bei Geräteverlust muss umgehend der Account deaktiviert und ggf. das Gerät aus der Ferne gelöscht werden können, um Missbrauch von Informationen und Zugangsdaten zu verhindern.[19]

Klassische Sicherheitsvorkehrungen gelten auch für mobilie Geräte.

Eine Whitelist von Apps minimiert die Risiken von unseriösen Apps und Werbefallen etc. Zudem wird die Angriffsfläche verringert. Grundsätzlich sollte, soweit verfügbar, Sicherheitssoftware installiert und vernünftig konfiguriert werden. Für das Prozedere von Downloads sind Richtlinien zu erstellen.

Das Update- bzw. Patchmanagement muss auf die mobilen Endgeräte ausgedehnt werden – und ggf. den Zugang zum Unternehmensnetz so weit verhindern, dass Updates durchgeführt werden können, ein Zugriff auf Daten aber so lange verwehrt wird, bis das Gerät den Mindestanforderungen der Sicherheit entspricht.

[19] vgl. Kapitel 4 „Gefährdungen", Abschnitt „Geräteverlust und Zugangsdaten", S. 148

Müssen Daten auf dem Gerät abgelegt werden, sollte dies immer in einen verschlüsselten Container erfolgen. Es muss eine neue Sicherheitsstrategie erarbeitet werden, die abhängig ist von den Schutzklassen der Daten und Informationen, der Gerätetypen, des Einsatzkontextes bzw. Einsatzortes der mobilen Geräte, der Person und der Rollen, die der Anwender einnimmt. Dabei muss ebenfalls beachtet werden, wo die Verarbeitung und Speicherung von Daten stattfinden soll, auf dem Gerät, in der Cloud oder im Unternehmen. Werden Datenzugriffe protokolliert, sichert dies nicht nur rechtliche Auflagen, sondern führt bei Mitarbeitern auch zu einem anderen Bewusstsein im Umgang mit Gerät, Daten und Apps, da im Haftungsfall der Verursacher belangt werden kann.

Noch vor der Anschaffung eines mobilen Endgerätes sollte jedes Unternehmen sich klar über dessen Einbettung in das vorhandene IT-Umfeld sein. Hierzu gehört an erster Stelle, Unternehmenswerte zu definieren und vorhandenen Daten Schutzklassen zuzuordnen. An sich sollte dies bereits bei der Einführung von IT stattgefunden haben. Doch jedes Unternehmen verändert sich im Laufe der Zeit, sodass mit der Einführung neuer IT-Komponenten und neuer Arbeitsprozesse der Gesamtkomplex überprüft werden sollte. Dies gilt insbesondere für die Einführung der aktuellen, mobilen Gerätegeneration, die direkt mit Cloud-Angeboten einhergeht und damit z. T. fest verbunden ist. Insbesondere, da sich durch Apps und Clouds neue Formen der Datenhaltung, der Datenverarbeitung und neue Kommunikationsformen etabliert haben, die neue Formen der Arbeit nach sich ziehen.

Der Schutzbedarf der Daten entscheidet über die Sicherheitsvorkehrungen.

Die neuen Schnittstellen zu staatlichen Stellen erfordern zudem auf gesetzlicher Basis eine verstärkte Auseinandersetzung mit Schutzklassen von gespeicherten Informationen und deren Verarbeitungsprozessen.

1 DATEV Sicherheitscheck
2 Deutschland sicher im Netz
3 Leitfäden des BITKOM
4 BSI für Bürger
5 Das Bürger-CERT

04 | Informationen im Netz

Wer richtig vorsorgt, kann bereits mit wenig Aufwand beruhigt arbeiten. Der Einsatz von Sicherheitssoftware ist wichtig, kann aber allein nicht vor allen Gefährdungen schützen. Wer darüber hinaus einige Regeln beachtet, verringert seine Risikopotenziale ganz erheblich. Im Folgenden geben wir Ihnen einige Tipps, wo Sie weitere Informationen zu mehr Sicherheit im Netz finden.

1 DATEV Sicherheitscheck

Der DATEV Sicherheitscheck bietet Ihnen eine erste Einschätzung Ihrer Datenschutz- und IT-Sicherheitslage. Auf www.datev.de/sicherheit können Sie selbst schnell, unverbindlich und kostenlos prüfen, welche sicherheitsrelevanten Aspekte Ihr Unternehmen betreffen und wie stark der Handlungsbedarf ist. Sie erhalten Handlungsempfehlungen zur Verbesserung Ihrer Sicherheit.

Für weitere Schritte stehen wir Ihnen gerne als kompetenter Partner zur Verfügung.[20]

2 Deutschland sicher im Netz e. V.

Deutschland sicher im Netz ist die erste Adresse für Verbraucher und mittelständische Unternehmen zu Fragen der IT-Sicherheit.

Der Verein Deutschland sicher im Netz e. V. ist die erste Adresse für Verbraucher und mittelständische Unternehmen zu Fragen der IT-Sicherheit. Er stärkt das Vertrauen in neue Technologien durch verständliche Botschaften zu einem sicheren Umgang mit Internet und Informationstechnik.

Deutschland sicher im Netz e. V. steht unter der Schirmherrschaft des Bundesministeriums des Innern und kooperiert eng mit der Bundesregierung und seinen Mitgliedern mit dem gemeinsamen Ziel, das Sicherheitsbewusstsein von Anbietern und Verbrauchern beim Umgang mit dem Medium Internet zu erhöhen. Als übergreifende Institution bündelt der Verein die Aktivitäten von Unternehmen, Branchenverbänden sowie Vereinen und bietet der Bundesregierung herstellerunabhängig und produktneutral einen zentralen Ansprechpartner.

Der Verein Deutschland sicher im Netz e. V. möchte mit dieser Informationsbroschüre und mit dem IT-Sicherheitspaket für den Mittelstand von der Notwendigkeit von Sicherheitsmaßnahmen überzeugen und zugleich bei deren Umsetzung unterstützen. Dieses Paket gibt konkrete Hilfsmittel an die Hand, die Sie sofort im Unternehmen umsetzen können. Für den täglichen Gebrauch haben wir Ihnen eine umfangreiche Sammlung an Sicherheitsrichtlinien, Verfahrensanweisungen, Checklisten und Notfallplänen zusammengestellt und bedarfsgerecht aufbereitet.

Zur besseren Unterstützung sind die Informationen auf die jeweiligen funktionalen Rollen im Unternehmen abgestimmt:

Geschäftsführer

Als Geschäftsführer finden Sie einen kompakten und verständlichen Überblick über die neuesten Sicherheitstechnologien und die aktuellen rechtlichen Rahmenbedingungen, damit Sie die erforderlichen Prozesse in Ihrem Unternehmen in die Wege leiten und notwendige Entscheidungen treffen können.

[20] www.datev.de/sicherheit

IT-Verantwortliche

Als IT-Verantwortlicher erhalten Sie konkrete Hilfsmittel, die Ihnen die Arbeit erleichtern und Ihnen Argumente für die Kommunikation mit der Geschäftsleitung, Mitarbeitern und Kollegen liefern.

Mitarbeiter

Als Mitarbeiter bilden Sie zusammen mit Ihren Kollegen die wichtigste Firewall in Ihrem Unternehmen. Die richtige Passwortwahl und umsichtiges Verhalten beim E-Mail-Versand helfen, Schäden zu vermeiden. Poster, Mustervorlagen und ein Bildschirmschoner sind nur einige der Materialien, die Ihnen „Deutschland sicher im Netz" hierfür zur Verfügung stellt.[21]

Unter http://www.sicher-im-netz.de finden sich leicht verständliche Informationen zum Thema IT-Sicherheit, praxisrelevante Checklisten und konkrete Empfehlungen für mehr Sicherheit im Internet.

3 Leitfäden des BITKOM

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) ist der Branchenverband der deutschen Informations- und Telekommunikationsbranche.

BITKOM ist die Abkürzung für Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Der BITKOM ist das Sprachrohr der IT-, Telekommunikations- und Neue-Medien-Branche. Der BITKOM vertritt mehr als 1.300 Unternehmen, davon gut 950 Direktmitglieder. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

Die Schaffung innovationsfreundlicher Rahmenbedingungen hat für den BITKOM höchste Priorität. Bildung und Fachkräftenachwuchs, Green-ICT, E-Government, E-Health, Mittelstandspolitik, Urheberrecht, Sicherheit und Vertrauen, Softwaretechnologien, Consumer Electronics, Klimaschutz und Nachhaltigkeit sowie eine neue Telekommunikations- und Medienordnung sind Kern der politischen Agenda des BITKOM. Im Sinne der digitalen Konvergenz fördert der BITKOM die Zusammenarbeit aller Unternehmen mit ITK-Bezug.

Die Leitfäden des BITKOM bieten Informationen für die Praxis zu Themen wie IT-Sicherheit, Outsourcing-Projekten oder Surfen am Arbeitsplatz. Sie richten sich vorrangig an Fach- und Führungskräfte in den ITK-Unternehmen.[22]

[21] www.sicher-im-netz.de

[22] www.bitkom.org

4 BSI für Bürger

Das Bundesamt für Sicherheit in der Informationstechnik gibt Tipps für mehr Schutz im Internet.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gehört zum Geschäftsbereich des Bundesministeriums des Innern. Das BSI ist eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft. Das BSI untersucht Sicherheitsrisiken bei der Anwendung der Informationstechnik und entwickelt Sicherheitsvorkehrungen. Es informiert also über Risiken, Gefahren und Befürchtungen beim Einsatz der Informationstechnik und versucht, Lösungen dafür zu finden.

Wie viel Aufwand Sie zum Schutz Ihres PC – und somit natürlich auch zum Schutz Ihrer Privatsphäre – betreiben wollen, hängt in erster Linie von Ihren persönlichen Anforderungen ab. Es gibt jedoch Schutzmaßnahmen, die Sie in jedem Fall treffen sollten.

Die zehn wichtigsten Tipps, die Internetnutzer für ein ungetrübtes Surf-Vergnügen immer beherzigen sollten, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) übersichtlich zusammengestellt.

Basisschutz leicht gemacht![23]

- Installieren Sie ein Virenschutzprogramm und ein Anti-Spyware-Programm und halten Sie diese immer auf dem aktuellen Stand.

- Setzen Sie eine Personal Firewall ein und aktualisieren Sie diese regelmäßig. Sie schützt bei richtiger Konfiguration vor Angriffen aus dem Internet und verhindert zudem bei einer Infektion des PCs mit einem Computerschädling, dass ausspionierte Daten an einen Angreifer übersendet werden können.

- Achten Sie darauf, ob es Sicherheitsupdates für Ihr Betriebssystem und sonstige von Ihnen installierte Software gibt, und führen Sie diese durch.

- Arbeiten Sie nach Möglichkeit nicht als Administrator an Ihrem PC, denn so können Schadprogramme noch mehr Unheil anrichten. Richten Sie für alle Nutzer eines PCs unterschiedliche Benutzerkonten ein. Vergeben Sie für diese Konten nur die Berechtigungen, die der jeweilige Nutzer für seine Arbeit braucht. So werden auch private Dateien vor dem Zugriff anderer geschützt.

- Gehen Sie sorgfältig mit Ihren Zugangsdaten um: Halten Sie Kennwörter und Benutzernamen sowie Zugangscodes für Dienste (z. B. beim Online-Banking) unter Verschluss. Wechseln Sie Passwörter in regelmäßigen Abständen.

- Seien Sie vorsichtig beim Öffnen von E-Mail-Anhängen. Schadprogramme werden oft über Dateianhänge in E-Mails verbreitet. Im Zweifelsfall fragen Sie vorsichtshalber beim Absender nach, ob der Anhang tatsächlich von ihm stammt.

- Seien Sie vorsichtig bei Downloads von Webseiten. Vergewissern Sie sich vor dem Download von Programmen aus dem Internet, ob die Quelle vertrauenswürdig ist, und bringen Sie Ihr Virenschutzprogramm auf den aktuellsten Stand.

[23] www.bsi-fuer-buerger.de

↗ Seien Sie zurückhaltend mit der Weitergabe persönlicher Informationen. Online-Betrüger steigern ihre Erfolgsraten, indem sie individuell auf ihre Opfer zugehen: Zuvor ausspionierte Daten wie etwa Surfgewohnheiten oder Namen aus dem persönlichen Umfeld werden dazu verwandt, Vertrauen zu erwecken.

↗ Nutzen Sie Übertragungstechnologien wie Voice over IP (VoIP) oder Wireless LAN (WLAN), dann achten Sie besonders auf eine Verschlüsselung Ihrer Kommunikation, damit die Übertragung Ihrer Daten nicht von Dritten mitgelesen bzw. Gespräche nicht abgehört werden können.

↗ Kommt es trotz aller Schutzmaßnahmen zu einer Infektion des PCs mit einem Schädling, können wichtige Daten verloren gehen. Um den Schaden möglichst gering zu halten, sollten Sie regelmäßig Sicherungskopien Ihrer Dateien auf CD-ROM/DVD oder externen Festplatten erstellen.[5]

5 Das Bürger-CERT

Das Bürger-CERT[6] informiert und warnt Bürger und kleine Unternehmen schnell und kompetent vor Viren, Würmern und Sicherheitslücken in Computeranwendungen – kostenfrei und absolut neutral. Die Experten analysieren rund um die Uhr die Sicherheitslage im Internet und verschicken bei Handlungsbedarf leicht verständliche Warnmeldungen und Sicherheitshinweise per E-Mail für den technischen Laien. Das Bürger-CERT ist ein Projekt des Bundesamtes für Sicherheit in der Informationstechnik. Wer auf Nummer sicher gehen möchte, kann einen Newsletter abonnieren.

[5] www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/BasisschutzComputer/basisschutzComputer_node.html

[6] www.buerger-cert.de

DATEV eG
90329 Nürnberg
Telefon +49 911 319-0
Telefax +49 911 319-3196
E-Mail info@datev.de
Internet www.datev.de
Paumgartnerstraße 6–14

Art.-Nr. 10102 2012-10-01