VÄGLEDNING INFORMATIONS- OCH IT-SÄKERHET SAMT SÄKERHETSSKYDD

MARS 2014

SVENSK energi

SVENSKA KRAFTNÄT

Omslagsfoto: Hasse Eriksson

Foton, illustrationer och kartor har tagits fram av
Svenska kraftnät om inte annat anges.

Org.Nr 202 100-4284

Svenska kraftnät
Box 1200
172 24 Sundbyberg
Sturegatan 1

Tel 010 475 80 00
Fax 010 475 89 50

www.svk.se

FÖRORD

En väl fungerande elförsörjning är en nödvändig förutsättning för ett modernt samhälle. Företag verksamma inom elförsörjningen utsätts varje dag för olika slags angrepp, bland annat i form av inbrott, skadegörelse eller IT-angrepp. Hot inom IT- området måste ägnas särskild uppmärksamhet, eftersom i stort sett all informationshantering i dag sker med stöd av IT.

Under 2013 har Svenska kraftnät gett ut nya föreskrifter och allmänna råd om säkerhetsskydd (SvKFS 2013:1).

En arbetsgrupp inom Svenska kraftnät har tillsammans med representanter från Svensk Energi arbetat med att ta fram denna vägledning. Vägledningen syftar till att hjälpa alla företag verksamma inom elförsörjningen i säkerhetsarbetet i allmänhet och det som rör nämnda föreskrifter i synnerhet.

Denna vägledning är inte främst ett dokument som är avsett att läsas från pärm till pärm, utan syftar mer till att utgöra ett uppslagsverk. De säkerhetsrelaterade områden som beskrivs utgörs av vedertagna ramar och kriterier för ett strukturerat säkerhetsarbete. Ett huvudsyfte med denna vägledning är alltså att beskriva hur man kan arbeta för att uppfylla det gällande regelverket.

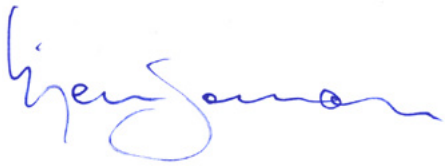
Det är vår förhoppning att denna vägledning ska stödja säkerhetsarbetet hos elföretagen i Sverige och även tjäna som källa till inspiration för detta viktiga arbete.

Vi tackar dem som deltagit i arbetsgrupp och referensgruppen och övriga som lämnat värdefulla bidrag för att göra vägledningen till ett användbart hjälpmedel i vårt gemensamma säkerhetsarbete.

Sundbyberg, mars 2014
Svenska kraftnät

Mikael Odenberg
Generaldirektör

Stockholm, mars 2014
Svensk energi



Kjell Jansson
Verkställande direktör

INNEHÅLL

1 INLEDNING

1.1 ALLMÄNT OM VÄGLEDNINGEN

1.2 UPPBYGGNAD AV RESPEKTIVE KAPITEL

Varje kapitel i vägledningen som rör ett specifikt säkerhetsområde, exempelvis förvaring av handlingar, är indelat så att sådant som direkt rör säkerhetsskydd finns under ett eget delkapitel, sådant som befunnits vara skyddsvärt utifrån andra aspekter under ett annat delkapitel och så vidare. Tanken med detta är att det ska vara lättare att hitta vad som är tillämpligt i det specifika fallet.

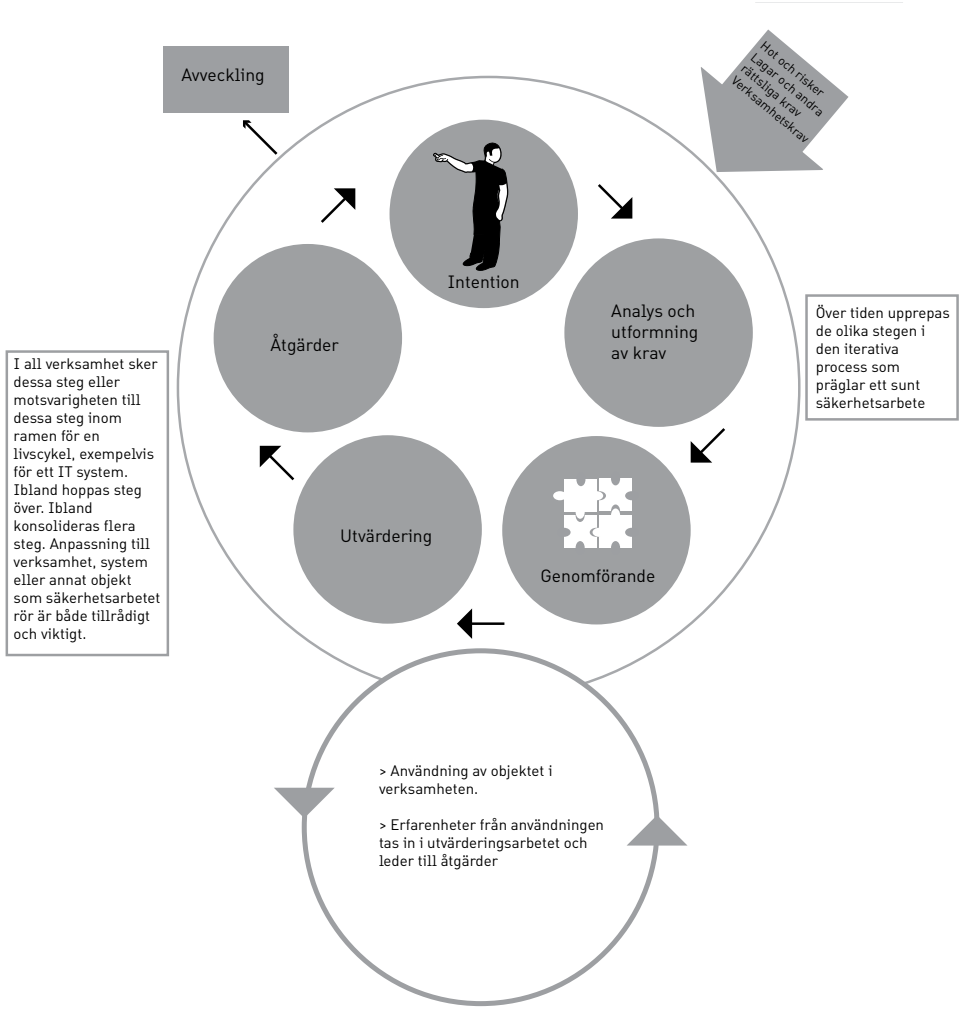
Om man exempelvis letar efter information om förvaring av handlingar som rör skyddet mot terrorism ska man således titta under kapitel 8 och där under 8.5 Förvaring av handlingar (även i IT-system)

1.3 VÄGEN TILL GOD SÄKERHET

Alltför många gånger har säkerhetsarbetet i olika organisationer präglats av att det arbete som utförs för att etablera eller skärpa säkerheten i en verksamhet för ett system eller en anläggning inte förvaltas på ett bra sätt. Detta kan bero på många saker men en av de vanligaste är att säkerhetsarbetet ofta genomförs som en ”engångsinsats”, inte sällan som ett projekt med tillfälligt engagerad personal. Det är inte fel att engagera extern personal, särskilt om företaget självt saknar kompetens eller utsedda befattningar för säkerhetsarbetet. Vad som måste beaktas och säkerställas är dock att det inom säkerhetsarbetet etableras en fungerande organisation inom verksamheten som fortsatt kan förvalta säkerhetsarbetet. Ofta genomförs en säkerhetsinsats endast en gång för att sedan bli stående som ett monument över att man vid ett enskilt tillfälle nått ett bra säkerhetsläge. ”Hyllvärmare” är tyvärr ett begrepp i nästan alla verksamheter då man talar om olika dokument och rutiner som rör säkerheten.

Sanningen är dock naturligtvis lika självklar som att man tittar åt båda hållen innan man går över gatan. Ett annat exempel är att man funderar både en och två gånger kring alla tänkbara scenarier innan man släpper iväg sin tonåring på en föräldrafri fest. Säkerhetsarbetet är en ständigt pågående process som i olika faser kräver uppmärksamhet på regelbunden basis. Syftet med denna ständigt pågående process är att löpande över tiden minimera ett mätbart skadeutfall av något slag. Om man tar till sig det och funderar lite över hur ett resonemang som att korsa gatan eller tänka på sin tonårings bästa skulle kunna appliceras på säkerhetsarbetet i en verksamhet så måste man bryta ned processen i lite mindre beståndsdelar för att göra detta begripligt.

Det finns olika definierbara skeenden och faser i processer. Oavsett om det handlar om att



Figur1. Säkerhetsarbetet – en iterativ process.

korsa gatan, att tonåringen ska på fest, att ta fram ett nytt IT-systemstöd för ett informationsflöde, att göra ändringar i en anläggnings beskaffenhet eller exempelvis att anställa någon för en specifik uppgift så kan dessa faser definieras innehållsmässigt på en lite mer abstrakt nivå. Detta är nyttigt för att öka förståelsen för hur en väl fungerande process i allmänhet, och säkerhet i synnerhet, kan uppnås.

De flesta medvetna handlingarna börjar med en idé. En önskan, vilja och intention att göra något. Därefter sker olika typer av analyser i syfte att ha ett så gott underlag som möjligt att agera utifrån. Sedan kommer implementationen. I det här läget skiljs agnarna från vetet. Många kommer inte längre än så, men behovet föreligger ändå. Låt oss kalla dessa första tre steg i processen för **intention, analys och kravutformning** samt **genomförande.**

Inom ramen för verksamhetsprocesser, exempelvis vad gäller hanteringen av IT-system finns ytterligare ett steg att ta hand om, **avveckling.** Således har vi nu **intention, analys och kravutformning, genomförande, utvärdering och åtgärd** samt **avveckling** att ta hänsyn till. Denna process kan beskrivas i en bild enligt figur 1.

Sett mot ovanstående resonemang ter det sig självklart att säkerhetsarbetet är en iterativ process som måste ges den uppmärksamhet och regelbundenhet som föremålet för säkerhetsarbetet kräver, oavsett vad föremålet för säkerhetsarbetet är. Det kan vara skillnad i behov vad gäller både uppmärksamhet och frekvens mellan exempelvis en obemannad automatiserad anläggning och ett IT-system som används av många personer och som interagerar med andra

nät och system men utan regelbunden uppmärksamhet kommer säkerheten att degenerera oavsett vilket objekt det rör.

Den iterativa processen återfinns förutom i vår vardag när vi korsar gator och bedömer risken att bli påkörd också i de olika ramverk som finns för säkerhetsarbete. Från tillämpliga lagar och standarder till företagsspecifika instruktioner. Den finns där av ett mycket gott skäl.

2 GRUNDER

2.1 INDELNING AV SÄKERHETSARBETET

2.1.1 ALLMÄNT

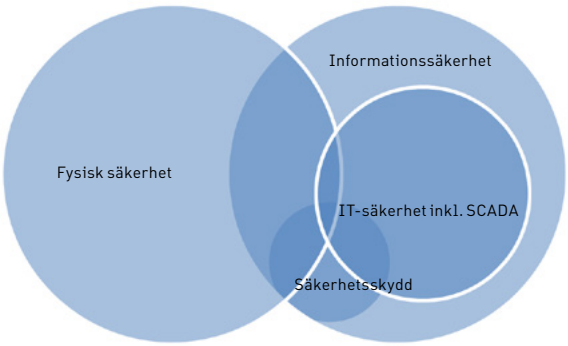
Säkerhetsarbete indelas vanligtvis i tre till fem huvudsakliga kategorier. Säkerhetsskydd, informationssäkerhet, IT-säkerhet, övrig fysisk säkerhet och personsäkerhet. Personsäkerhet är ett specifikt säkerhetsområde som inte belyses särskilt i denna vägledning. Vägledningen berör dock perifert personsäkerhet så till vida att visst skydd som beskrivs även, i vissa sammanhang, ger skydd åt medarbetare.

Säkerhetsskydd relaterar sig till uppgifter som rör rikets säkerhet eller skyddet mot terrorism.

Informationssäkerhet är sådant som rör hantering av, och säkerhet kring information. Detta gäller oavsett i vilken form informationen existerar och hanteras. Pappersbunden, digital information eller övriga uppgifter. Av detta följer att informationssäkerheten utgör det största säkerhetsområdet med beröringspunkter i alla de andra säkerhetsområdena.

IT-säkerhet är samlingsnamnet på sådan säkerhet som rör tekniskt skyddande funktioner av exempelvis system. Häri ingår exempelvis SCADA-säkerhet som en delmängd då SCADA-system är just IT-system.

Övrig fysisk säkerhet avser sådan säkerhet som enklast beskrivs som lås och larm, men då i sammanhanget att det inte omfattar säkerhetsskydd utan rör övrig säkerhet. Ett exempel på detta kan vara uppgifter om hur en reception för besöksmottagning är uppbyggd och utformad i en anläggning som inte rör säkerhetsskydd.



Figur 2. Bild över sambandet mellan olika säkerhetsområden.

2.1.2 SÄKERHETSSKYDD

Med säkerhetsskydd avses enligt 6 § säkerhetsskyddslagen:

1. Skydd mot spionerи, sabotage och andra brott som kan hota rikets säkerhet,
2. skydd i andra fall av uppgifter som om fattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet, och
3. skydd mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott

(terrorism), även om brotten inte hotar rikets säkerhet.

För att förstå innebörden av detta och då särskilt vad som menas med rikets säkerhet hänvisas till följande förklaring som står att läsa i Kommittédirektiv Dir. 2011:94 En modern säkerhetsskyddslag.

Säkerhetsskyddets syfte

Säkerhetsskyddslagen är i första hand inriktad på att skydda rikets säkerhet. I förarbetena till lagen anges att det visserligen inte finns någon legaldefinition av begreppet rikets säkerhet, men att begreppet kan sägas avse såväl den yttre säkerheten för det nationella oberoendet som den inre säkerheten för det demokratiska statsskicket (prop. 1995/96:129 s. 22 och 74).

Skyddet för den yttre säkerheten tar framför allt sikte på totalförsvaret, dvs. den verksamhet som behövs för att förbereda Sverige för krig. Ett hot mot rikets yttre säkerhet anses dock kunna förekomma även om det inte hotar totalförsvaret. Skyddet av rikets yttre säkerhet anses omfatta uppgifter och förhållanden av rent militär betydelse eller av betydelse för totalförsvaret i övrigt och andra uppgifter som har betydelse för rikets nationella oberoende (prop. s. 23).

Också rikets inre säkerhet kan vara hotad utan att totalförsvaret berörs. Angrepp på det demokratiska statsskicket kan förekomma från grupperingar utan förbindelse med främmande makt. Det kan vara fråga om försök att ta över den politiska makten genom våld eller att använda våld, hot eller tvång mot statsledningen i syfte att påverka politikens utformning. Försök att systematiskt hindra medborgarna från att utnyttja sina demokratiska fri- och rättigheter räknas också till hoten mot rikets inre säkerhet (prop. s. 23).

Även om begreppet rikets säkerhet inte är reserverat för förhållanden som har betydelse för totalförsvaret har det i hög grad kommit att förknippas med framför allt militära förhållanden. Samtidigt har utvecklingen gått mot att andra samhälleliga verksamheter fått en allt större betydelse från säkerhetsskyddssynpunkt, något som bl.a. lyfts fram i Säkerhetspolisens förstudie. Ett uttryck för detta är den förändring som hotbilden genomgått under de senaste tio åren. I förarbetena till säkerhetsskyddslagen konstaterades att hotbilden mot Sverige förändrats efter det kalla krigets slut. Trots det gjordes bedömningen att det nya säkerhetspolitiska läget inte hade inneburit några radikala förändringar av förutsättningarna för en ny säkerhetsskyddsreglering, se Säkerhets-5 skyddsutredningens betänkande Säkerhetsskydd (SOU 1994:149 s. 14 f.). Det nya regelverket utarbetades mot den bakgrunden.

Sedan säkerhetsskyddslagen trädde i kraft har hoten mot rikets säkerhet ytterligare förändrats. Ett enskilt militärt angrepp direkt mot Sverige bedöms som osannolikt under överskådlig tid. Kriser eller incidenter, som även inbegriper militära maktmedel kan dock uppstå i vår region, och på längre sikt kan militära angreppshot aldrig uteslutas, se propositionen Ett användbart försvar (prop. 2008/09:140 s. 28). Dagens säkerhetspolitiska hot, eller howtt de kan få säkerhetspolitiska konsekvenser, är ofta gränsöverskridande, icke-militära och utgår inte sällan från icke-statliga aktörer. Som exempel kan nämnas internationell terrorism och andra typer av grov internationell brottslighet, spridning av massförstörelsevapen samt framställning och transport av vapen, komponenter och teknologi, jfr propositionen En anpassad försvarsunderrättelseverksamhet (prop. 2006/07:63 s. 17). Säkerhetspolisen har också noterat att främmande staters underrättelseverksamhet de senaste decennierna har breddats mot forskning och utveckling inom civila områden samt mot politiska frågor och information som rör samhällsviktiga system, jfr regeringens direktiv till Utredningen om förstärkt skydd mot främmande makts underrättelseverksamhet (dir. 2010:35). Vidare betraktar Säkerhetspolisen elektroniska angrepp i olika former som ett av de allvarligaste hoten. Även den ökade internationaliseringen innebär nya förutsättningar för säkerhetsskyddet. En särskild fråga är de svårigheter som kan uppstå från säkerhetsskyddssynpunkt

vid utflyttning av verksamheter till utlandet, bl.a. inom energiförsörjningen.

Det är mot bakgrund av ovanstående rimligt att anta att den kommande förändringen i säkerhetsskyddslagstiftningen på ett mera nyanserat sätt kommer att ge stöd i bedömningar som också handlar om svåra påfrestningar för samhället oavsett aktör och militärt säkerhetsläge i övrigt.

Säkerhetspolisen har ett lite modernare och enklare sätt att väcka tanken kring vad som kan röra rikets säkerhet. Där fokuserar man på ett antal frågeställningar kring konsekvenser av inträffade händelser enligt följande.

- Påverkas ett större antal människors liv och hälsa?
- Påverkas ett större geografiskt område? Är denna påverkan långvarig och/eller inträffar den vid en olämplig tidpunkt?
- Får händelsen allvarliga sociala, ekonomiska och/eller politiska konsekvenser för samhället?
- Påverkas andra samhällsviktiga verksamheter allvarligt?
- Finns det risk att allvarliga negativa konsekvenser uppstår i framtiden?

När det gäller terroristbrott anger 2 § i Lag (2003:148) om straff för terroristbrott följande:
2 § För terroristbrott döms den som begår en gärning som anges i 3 §, om gärningen allvarligt kan skada en stat eller en mellanstatlig organisation och avsikten med gärningen är att:

1. injaga allvarlig fruktan hos en befolkning eller en befolkningsgrupp,

2. otillbörligen tvinga offentliga organ eller en mellanstatlig organisation att vidta eller att avstå från att vidta en åtgärd, eller

3. allvarligt destabilisera eller förstöra grundläggande politiska, konstitutionella, ekonomiska eller sociala strukturer i en stat eller i en mellanstatlig organisation.

Vid denna vägledningens skapande pågår revidering av säkerhetsskyddslagstiftningen. För mer aktuella uppgifter konsultera gällande lagstiftning.

Exempel på händelser som kan utgöra terroristbrott under ovan angivna förutsättningar.

Mord, dråp, grov misshandel, människorov, olaga frihetsberövande, grov skadegörelse, mordbrand, allmänfarlig ödeläggelse, sabotage, kapning, spridande av gift eller smitta, olaglig befattning med kemiska vapen, uppsåtligt vapenbrott, hantering och framställning av CBRN-vapen, smuggling, olaga hot.

Ovanstående frågor och kriterier kan användas som lathund för att få en indikation på om de konskevenser man för tillfället analyserar rör rikets säkerhet eller skyddet mot terrorism.

Oavsett vilket stöd man använder för att nå sina slutsatser är det viktigt att tänka på implicita förhållanden. En mindre, till synes harmlös eller av ringa vikt, händelse kan ge upphov till, eller möjliggöra, större och allvarligare händelser.

2.1.3 INFORMATIONSSÄKERHET

Som tidigare nämnts så är informationssäkerhet allt sådant som rör hantering av, och säkerhet kring information. Detta gäller oavsett i vilken form informationen existerar och hanteras. Det är på grundval av detta faktum som informationssäkerhetsområdet blir så stort och berör alla övriga säkerhetsområden. Det anförs inte sällan från konservativa håll att exempelvis fysisk säkerhet inte har något med informationssäkerhet att göra. I vår upplysta tid är det lätt att avfärda ett sådant resonemang då fysisk säkerhet ofta inbegriper lås-, inpasserings- och larmfunktioner. Av detta följer att hantering av IT-baserad information är en nödvändighet och därmed är informationssäkerheten befintlig i området.

Många organisationer använder sig av ISO 2700x standard inom ramen för informationssäkerhetsarbete. De delar som praktiskt brukar användas av organisationer som tillämpar standarden är:

> SS-ISO/IEC 27001 Ledningssystem för informationssäkerhet – Krav.

> SS-ISO/IEC 27002 Riktlinjer för styrning av informationssäkerhet.

Som brukligt är med standarder så är de synnerligen omfattande. Detta har både för- och nackdelar. Fördelen är att den är just så omfattande så att den täcker in det allra mesta av informationssäkerhetsområdet och den som följer standarden kan då vara någorlunda säker på att få en bra täckning på sitt informationssäkerhetsarbete. Vidare finns det fördelar med standarden om man exempelvis interagerar med leverantörer och entreprenörer som själva tillämpar och använder standarden. Nackdelen är att den, likt andra standarder, är komplex och innebär mycket administrativt arbete. Det bör här särskilt påpekas att det finns en ISO/IEC TR 27019:2013 Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. Denna är specifik för energiindustrin och ett komplement till den befintliga standarden.

Alternativ till standard är att själv designa informationssäkerheten för sin organisation. Detta medför dock att resultatet, då särskilt den tillämpliga omfattningen, blir direkt beroende av erfarenhet och kompetens hos den eller de som utför en sådan uppgift.

Det är vanligt förekommande att plocka valda delar av standarden och tillämpa inom sin organisation. Många organisationsföreträdare brukar använda uttryck som ”Vi följer ISO-standarden i valda och tillämpliga delar”. Att inte slaviskt följa en standard utan att utvärdera tillämpligheten i delarna är ett bra sätt att utnyttja standarden.

ISO 27002 består av ett antal olika delområden enligt följande:

> RISKBEDÖMNING OCH RISKBEHANDLING
Innefattar bland annat riskanalys, åtgärder, utvärdering och riskhantering.

> SÄKERHETSPOLICY
Ett inriktningsdokument för informationssäkerheten.

> ORGANISATION AV INFORMATIONSSÄKERHETEN
Ska styra informationssäkerheten inom organisationen.

> HANTERING AV TILLGÅNGAR (ENG.)ASSET MANAGEMENT
Syftar till att uppnå och upprätthålla lämpligt skydd av organisationens tillgångar.

> PERSONALRESURSER OCH SÄKERHET
Målet här är att säkerställa att anställda, uppdragstagare och tredjepartsanvändare förstår sitt ansvar och är lämpliga för de roller de avses ha och för att minska risken för stöld, bedrägeri eller missbruk av resurser.

> FYSISK OCH MILJÖRELATERAD SÄKERHET
Här avses att förhindra obehörigt fysiskt tillträde, skador och störningar i organisationens lokaler och information

> STYRNING AV KOMMUNIKATION OCH DRIFT
Syftar säkerställa korrekt och säker drift av informationsbehandlingsresurser.

> STYRNING AV ÅTKOMST
Syftar till att styra åtkomst till information.

> ANSKAFFNING, UTVECKLING OCH UNDERHÅLL AV INFORMATIONSSYSTEM
Målet här är att säkerställa att säkerheten är en integrerad del av informationssystem.

> HANTERING AV INFORMATIONSSÄKERHETSINCIDENTER
Syftar till att säkerställa att informationssäkerhetshändelser och svagheter hos informationssystem kommuniceras på ett sådant sätt att korrigerande åtgärder kan vidtas i rätt tid.

> KONTINUITETSPLANERING FÖR VERKSAMHETEN
Målet med kontinuitetsplanering är att motverka avbrott i organisationens verksamhet och att skydda kritiska verksamhetsprocesser från verkningarna av allvarliga fel i informationssystem eller katastrofer och att säkra återstart inom

rimlig tid.

> EFTERLEVNAD
Syftar till att undvika överträdelser av lagar, författningar eller avtalsförpliktelser, samt andra säkerhetskrav.

Som synes är standarden omfattande. Vissa områden innehåller mera material än andra, exempelvis styrning av kommunikation och drift, styrning av åtkomst och anskaffning, utveckling och underhåll av informationssystem.

Denna vägledning innehåller information som faller inom de olika respektive områdena i standarden. I de flesta fall är det självförklarande, i andra fall inte fullt så uppenbart men där det är tillämpligt framgår hänvisningar till motsvarande område inom ISO 27002. Detta kommer sig främst av att denna vägledning är branschspecifik och präglas av ett antal särskilda omständigheter. Ett exempel på en sådan omständighet är hur tillämpligheten måste differentieras i styrning av åtkomst till information, se figur 3.

Sammanfattningsvis kan sägas att denna vägledning i möjligaste mån står i harmoni med ISO-standarden och ger exempel på hur tolkningar kan ske branschspecifikt där det annars inte är uppenbart.

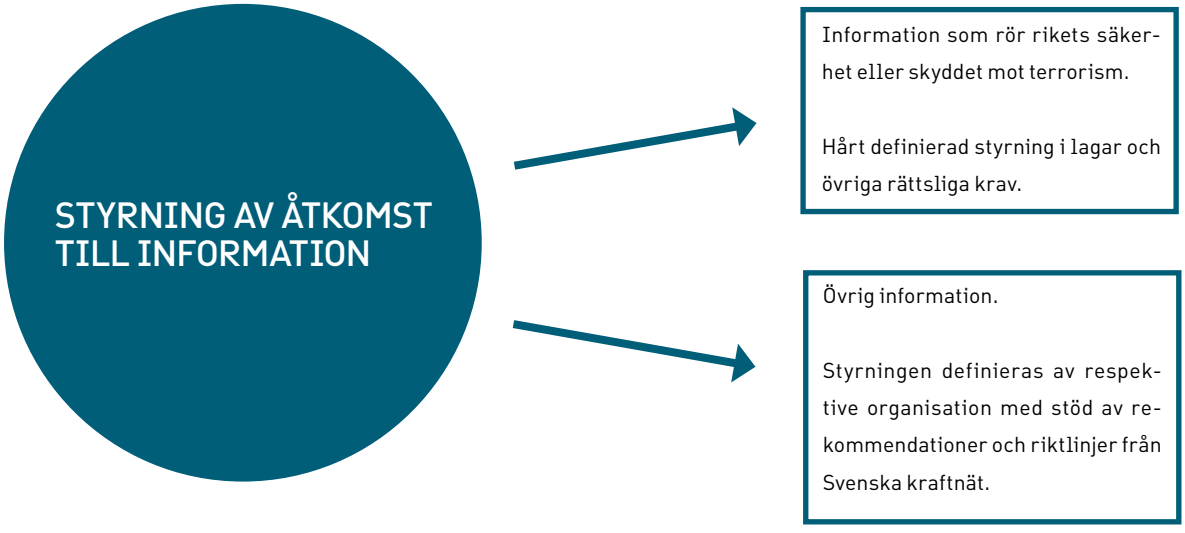
2.1.4 IT-SÄKERHET

IT-säkerhet inordnas taxonomiskt som en del av informationssäkerheten. Detta följer per automatik av det faktum att i all verksamhet och alla processer som använder IT som stödfunktion, exempelvis i form av ett för uppgiften dedicerat system, förekommer, bearbetas, lagras och sprids information. I branschen är dessutom IT hårt förknippat med styrsystem av olika slag. Härvid bör särskilt nämnas SCADA (eng.) Supervisory Control And Data Acquisition. SCADA är benämningen på system för övervakning och styrning av processer. Se figur 4 som åskådliggör hur dessa olika säkerhetsområden hänger ihop.

IT-säkerhet utgörs av en mängd olika tekniska delområden. Nedan följer en uppräkning med beskrivning av de vanligaste delområdena.

> DESIGN AV SYSTEM OCH INFRASTRUKTUR
Här menas att säkerheten beaktas och tillämpas i designprocessen och utformningen av såväl system som infrastruktur.

> AUTENTISERING OCH AUKTORISATION (BEHÖRIGHETSHANTERING)
Med autentisering menas att en användare är säkert identifierad av ett system. Med auktorisation avses styrning av åtkomst till information och andra resurser kopplade mot den specifika identiteten.



Figur 3. Exempel på hur tillämpligheten måste differentieras i styrning av åtkomst till information.

> KRYPTERING
Avser tekniska funktioner för att skydda data och information mot obehörig insyn genom matematisk förvanskning av informationen i en given tid och rymd. Rör såväl hårdvarubaserade som mjukvarubaserade lösningar.

> SPÅRBARHET
Rör främst olika typer av logghantering i system i syfte att kunna svara på frågorna; vem, var, när, hur och med vad. Detta är ett område som ofta brister då det är vanligt att (eng.)default inställningar används med bristfälligt resultat som följd.

> SKYDD MOT SKADLIG KOD
Brukar i dagligt tal kallas för antivirusprogram. Detta är dock endast en delmängd, om än nog så viktig, av det totala skyddet mot skadlig kod.

> HÄRDNING AV SYSTEM
Detta är ett begrepp som ofta används av personer med förankring i IT-säkerhetsbranschen och avser processen med att göra IT-system mera tåliga mot olika typer av IT-relaterade hot. Detta kan bestå i allt från att göra adekvata säkerhetsinställningar i standardsystem till att använda särskilt säker hårdvara och mjukvara eller tillämpa segmentering, s.k. zoner.

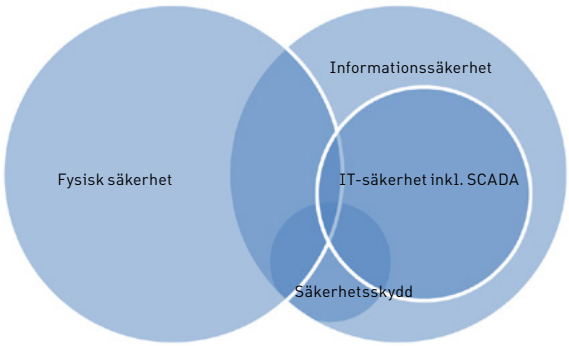
> SYSTEMSKYDD
IDS (intrångsdetekterande system), brandväggar, datadioder m.m.

> SÄKERHETSKOPIERING AV INFORMATION OCH DATA
(eng.)Back-up. Syftar till att skapa kopierade instanser av information och dataavbildningar på media som inte störs eller på annat sätt påverkas av händelser i den ordinarie driftmiljön och som medger återställning av system och lagrad information.

> INCIDENTHANTERING, AVBROTTSPLANERING OCH CERT (ENG.)COMPUTER EMERGENCY RESPONSE TEAM
Dessa begrepp rör främst åtgärder och rutiner kopplade till olika typer av incidenter, olyckor och angrepp på IT-system. För små och medelstora företag är oftast avbrottsplanering det mest tillämpliga begreppet och handlar då främst om att identifiera problem som orsakar störning eller avbrott, åtgärda detsamma och återställa system till ordinarie driftnivå. CERT används mest i större centraliserade sammanhang såsom Sveriges nationella CERT som har till uppgift att uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter.

> AVVECKLING AV IT-SYSTEM
Detta är ett område som ofta glöms bort. Det finns information i alla datamedia som kan leda till oönskade incidenter och röjande av skyddsvärd information i samband med avveckling. Säkra rutiner för att avveckla system är därför viktiga.

> SÄKERHET I STYRSYSTEM OCH SCADA – SÄKERHET
Området är av yttersta vikt för elbranschen då i stort sett alla produktions- och distributionsanläggningar är direkt beroende av sådana system för sin funktion. Säkerhet i styrsystem och SCADA – säkerhet regleras särskilt i flera olika regelverk och riktlinjer. I takt med ökad integration mellan styrsystem och andra typer av IT-system så ökar kraven på att säkerheten i dessa system motsvarar den i andra skyddsvärda IT-system. Med äldre system kan detta vara problematiskt då säkerheten i dessa ofta har berott på att de varit åtskilda från övriga system.



Figur 4. Illustration över hur de olika säkerhetsområdena hänger ihop.

IT-säkerhet i denna vägledning kommer att fo-

kusera på praktiska frågor om tillämpningar i olika sammanhang. Detta främst i syfte att ge stöd åt små och medelstora företag som strävar efter en god IT-säkerhet i sin verksamhet.

Där så är tillämpligt kommer även referenser till andra styrande eller vägledande dokument att ges.

2.1.5 ÖVRIG FYSISK SÄKERHET

Som vägledning för fysiskt skydd finns dokumentet; Fysiskt grundskydd – en vägledning för elbranschen (dnr: 2012/540) utgiven av Svenska kraftnät i samarbete med Svensk Energi. Den finns bland annat tillgänglig på Svenska kraftnäts hemsida. Den tar på ett omfattande, pedagogiskt och bra sätt upp aspekter som rör elbranschen vad gäller fysiskt skydd av elanläggningar.

I denna vägledning kommer därför fokus att ligga på sådant fysiskt skydd som rör den dagliga verksamheten, lokaler och andra utrymmen där skyddsvärd verksamhet pågår eller skyddsvärd information eller andra objekt finns.

Då denna vägledning utgör en rekommendation så kommer ett flertal exempel att ges på hur små och medelstora företag med relativt enkla medel kan förbättra sitt fysiska skydd där behov finns.

3 HOT, HOTBILD OCH HOTBESKRIVNING

3.1 INLEDNING

Läsaren bör ge akt på att Svenska kraftnät även har gett ut en hotkatalog för elbranschen. Denna exemplifierar konkret en stor mängd hot och kan med fördel användas som referens, källa eller inspiration i säkerhetsarbetet i allmänhet och i riskanalyser i synnerhet.

Säkerhetsexperter och riskanalytiker talar ofta om dimensionerande hotbild, dimensionerande hotbeskrivning, hotanalys och liknande uttryck. Med dimensionerande hotbild avses då en beskrivning av hot, och möjligen risker, som vid en **given tidpunkt** utgör de hot och risker mot vilka man avser att dimensionera sitt skydd. Det är därför inte svårt att förstå varför många har en idé om att få en definierad dimensionerande hotbild då det skulle medföra en förenklad, och möjligen standardiserad, procedur för att tillämpa sitt skydd.

Verkligheten är emellertid mera komplex än så. Aldrig tidigare i historien har hotbilden varit så föränderlig, ändrats så snabbt, eller ändrats så ofta som nu. Det finns inget som tyder på att denna utveckling avstannar, tvärtom. Den ökar. En dimensionerande hotbild beror heller inte bara på vilken bransch den avser, vilket förefaller vara en vanlig missuppfattning. Den är beroende av flera faktorer som kan väga olika beroende på exempelvis den geografiska placeringen av objektet man söker skydda eller i vilken utsträckning och tillämpning IT-system används integrerat med verksamheten.

För att erhålla en rimlig bild av de hot och risker man löper i sin verksamhet finns inga genvägar än att själv göra grovjobbet att sätta sig in i sin verksamhet, inventera de fysiska, mänskliga och elektroniska resurser man har, samt se vilka hot som finns samt vilka konsekvenser olika realiserade hot kan medföra. Dynamisk hot-, risk- och sårbarhetsanalys är och förblir det bästa sättet. Kvaliteten i analysen är alltid avhängig analysens avnämnare. Alltså är det av yttersta vikt att involvera verksamheten i det löpande riskanalysarbetet. Detta torde egentligen vara en självklarhet då i stort sett varje människa i vårt samhälle redan har de kunskaper som finns för att vara kvalificerad inom riskanalysområdet, se nedanstående informella exempel.

> Varje person som innehar körkort och kör bil genomför, oftast utan att ens tänka på det, löpande riskanalys under varje bilfärd. Det sker med olika frekvens och djup beroende på den omgivande situationen, precis som det borde ske i de verksamheter som denna vägledning riktar sig till. Om du som förare av en bil kommer till en korsning i en tätort så påbörjar du din riskanalys redan när du ser korsningen. Du letar efter hinder eller potentiella problem och är hela tiden beredd att bromsa hårdare än vad du redan gör. När du kommit fram till punkten ligger summan av dina analysintryck till grund för beslut om huruvida du ska

> fortsätta genom korsningen eller stanna och fortsätta analysera. Är det stopplikt? Kommer det bilar som kan korsa min väg, och är de i så fall så nära att jag beslutar vänta till dem korsat min väg. Finns det cyklister eller barn som plötsligt kan komma ut i vägbanan. Är det möjligt att det kan finnas vilt som står dolt i buskage och kan komma ut framför min bil i rörelse. Etc. etc.

Exemplet ovan kan förefalla vara enkelt och en smula larvigt men sanningen är att de allra flesta människor genomför dynamiska riskanalyser dagligen i olika frekvens, djup och tillämpningsområden. Detta sätt att tänka och agera är det som behöver förmedlas till personal i och kring berörda verksamheter. Då och först då kan man säga att man har en verksamhetsförankrad riskanalys som kan ligga till grund för löpande beslut om säkerhet, oavsett tillämpning. Exemplet ovan visar också på en annan viktig sak. Behovet av att genomföra riskanalys som ett led i den ordinarie verksamheten. Det är inte en pålaga som ska utföras för att en föreskrift eller regel säger det utan ett sätt att på bästa sätt, och framförallt säkraste sätt, nå verkan med det man gör.

Det går att dela in hot i olika typer av kategorier som kan vara på en mer övergripande, **strategisk** nivå men även på mer detaljerad och **taktisk** nivå. Detta kapitel handlar mer om hot på ett allmänt och övergripande plan i kombination med att diskutera metodik för analys av hoten. Svenska kraftnät har även producerat en hotkatalog. Hotkatalogen innehåller hotbeskrivningar på en mer tillämpad och detaljerad nivå. Den är tänkt att användas för att ge inspiration och ingångsvärden i samband med genomförande av riskanalyser inom branschen. Av namnet kan man utlösa att hotkatalogen beskriver just olika hot mot objekt och verksamheter inom branschen. Det är inte en risk- eller sårbarhetskatalog utan fokus ligger på att hjälpa till att identifiera olika problemområden för ett stort antal givna och till branschen kopplade objekt och verksamheter. Den kopplar hot till objekt och verksamheter på flera olika nivåer och med olika detaljgrad, allt för att tillhandahålla så mycket hjälp som möjligt till branschen i samband med genomförande av riskanalyser. Det är ju trots allt så att de flesta människor ständigt strävar efter att verka för att en verksamhet eller ett objekt ska fungera som avsett och inte det omvända. Det är således därför som hotkatalogen är ett så viktigt stöd. För att väcka de tankar som kan leda till identifierandet av tillämpliga risker och adekvata sårbarhetsbedömningar.

I denna del av vägledningen kommer olika problemområden att beskrivas övergripande i syfte att öka förståelsen för hur olika hot i hotkatalogen kan vara möjliga och existera i olika sammanhang.

Att läsa igenom de olika underkapitlen nedan kan också ge en lämplig invisning i hotkatalogen för fördjupning inför en riskanalys. Detta kan vara värdefullt då hotkatalogens innehåll är mycket omfattande och informationsvolymen är stor.

3.2 AKTÖRSRELATERAD HOTBILD

Med aktörsrelaterade hotbild avses här en sådan hotbild som är direkt beroende av att människor faktiskt utför den gärning som renderar själva hotet. I talspråk; människorna är skurkarna i dramat. Detta ska jämföras med andra typer av hot som inte kräver mänsklig hand för att realisera, exempelvis naturkatastrofer och miljörelaterade hot, eller mekaniska fel.

Det finns en inneboende fara i att låsa upp sig på en viss typ eller nivå av hotbilder när man genomför sina analyser. Härvid kan särskilt nämnas just aktörer. Ett gammalt talesätt är; en olycka kommer sällan ensam. Så är naturligtvis även den värsta typen av skeenden som kan identifieras med riskanalys. Kombinationer av händelser som på ett olyckligt vis samverkar ger oftast de värsta konsekvenserna. Således är det av vikt att tänka inte bara på vad en person kan hitta på och sätta i eller ur spel.

Aktörer är dock en betydande faktor inom riskanalysområdet, inte minst som följd av att de förutsätter någon typ av **uppsåt** och **förmåga** att genomföra något som får eller kan få negativa konsekvenser för objektet eller verksamheten. Det måste här alltså förutsättas att den gärning som iscensätts i någon mån har utformats för att åsamka skada just för det objekt eller den

verksamhet som angrips. Aktörsrelaterade hot är oftast förknippade med antagonistiska hot, då vi tänker oss att de har ett uppsåt. En aktör kan dock även vara en person som på grund av inkompetens, slarv eller på annat sätt, gör att ett hot realiseras. En typ av aktör som inte kan bortses ifrån i ett modernt samhälle är en främmande statsmakt som använder sig av cyberkrigföring, exempelvis mot teknisk infrastruktur såsom elförsörjning, för att påverka en annan stat.

Förmågan är ofta kopplad till såväl aktörens kompetens, men även olika typer av resurser som den förfogar över. Tumregeln är att en aktör som förfogar över större resurser:

> har kapacitet att tillföra större skada,

> kan utföra mer omfattande eller avancerade typer av angrepp,

> kan söka efter, hitta och använda mer esoteriska[1] svagheter och därmed realisera "omöjliga" hot.

Nedan beskrivs ett antal olika aktörer övergripande. Syftet är att öka förståelsen för var, när och hur sådana aktörer kan förekomma och verka.

3.2.1 INSIDERS

En insider kan kortfattat definieras enligt följande.

> Insider är den som har tillgång till ett objekt eller en verksamhet, planerar eller genomför en handling som kan få negativa konsekvenser och som genom sitt värv eller utförande av gärning inte väcker uppmärksamhet eller misstänksamhet.

En insider kan således utgöras av exempelvis anställda, entreprenörer, städpersonal, vakter, konsulter, ja i stort sett alla som har tillgång till det som är föremål för påverkan inom ramen för sitt värv.

Problemet med att bedöma insiderrelaterade hot är huvudsakligen tre.

1. Frekvensen av insiderrelaterade händelser.
2. Allvarlighetsgraden i de planerade eller utförda gärningarna.
3. Okända eller oönskade resteffekter av utförd gärning. Ofta kallade residuala effekter.

1: Frekvens

Det går aldrig att med säkerhet säga vilken frekvens en insiderrelaterad händelse har eller kommer att ha. Detta beror på många var för sig verkande eller samverkande faktorer. Inom polisiärt utredningsarbete används ofta minnesordet BESKT för att täcka in de vanligaste orsakerna. BESKT står för:

B = Besvikelse (exempelvis missnöje med lön eller annan förmån eller befordran).

E = Ekonomi (exempelvis utebliven eller för lite löneförhöjning).

S = Stimulantia (Exempelvis att någon betalar för att gärningen ska utföras).

K = Kollegor/Kamrater (Exempelvis mobbning på arbetsplats).

T = Tillfälle (Som talesättet; tillfället gör tjuven).

När man granskar innehållet i ovanstående minnesord och samtidigt lägger till det faktum att en insider mycket sällan behöver ta några allvarliga risker för att utföra sin gärning så blir det lättare att förstå att insiderrelaterade hot är en realitet. Att komma till denna insikt är viktigt i sig då de flesta människor i grund och botten är godtrogna och ärliga. I den kontexten är det svårt att föreställa sig att insiders finns och verkar i ens egen verksamhet.

Ett sätt att mäta frekvensen av insiderverksamhet är statistik. Polisen anger bland annat att de alltmer populära stölderna ur parkerade lastbilstransporter till 70 procent bygger på insidertips. Detta vederlägger även påståendet att insidern oftast tar en mycket liten risk för egen del.

En löpande informell återkoppling av

1. Svagheter och sårbarheter som för en aktör som betraktar ett objekt utan medgiven insyn förutsätts vara okända.

resultatet från flera hundra riskanalyser över en lång tidsperiod ger vid handen att ett rimligt värde att ansätta för insiderfrekvens i en godtycklig verksamhet är 1 händelse per 300-400 personer och kalenderår. Anledningen till att återkoppling är informell är helt enkelt att ingen, oavsett om verksamheten är statlig, kommunal eller privat, skyltar med att man varit offer för insiderrelaterad verksamhet. Om det går att hålla i det fördolda så blir det så. Det gör att sådan statistik som redovisas officiellt ofta är gravt missvisande. När man beaktar frekvensen som här anges måste man även betänka att det avser alla insiderrelaterade händelser oavsett allvarlighetsgrad. Det ger dock en fingervisning om en mer rättvisande frekvens än vad som normalt redovisas.

2: Allvarlighetsgraden i de planerade eller utförda gärningarna.
För att få en bild av bredd och djup på insiderrelaterade händelser redovisas här, utan prioritering eller inbördes ordning, ett litet urval av vanliga händelser som kan härledas till insiders.

> STÖLDER
Exempelvis kontorsmaterial, IT-utrustning, drivmedel, telefoni, sanitetsartiklar, transporter, information.

> FALSK AVNÄMNING
Till exempel att någon anger felaktiga ingångsvärden eller data till ett IT-system som senare leder till eller kan leda till problem eller dyrbara återställningar. Detta är en vanlig händelse som kan kopplas till B i BESKT (Besvikelse).

> FRÄMJANDE AV KONKURRENT ELLER ANNAN OBEHÖRIG
Detta kan bestå i att exempelvis lämna ut uppgifter som är av proprietär art för företaget. Mönsterritningar, prisuppgifter, patentuppgifter, uppgifter om befintligt skydd och sårbarheter på objekt eller i verksamhet.

> FRÄMJANDE AV EGEN VERKSAMHET
Förfördelande av personer eller verksamheter står i konkurrens eller annan form av rivalitet med egen verksamhet. Exempelvis underentreprenörer, bygglov, expropriation.

> SABOTAGE
Avsikten kan vara att infiltrera en verksamhet eller ett objekt enkom i syfte att sabotera denna eller detta.

När man gör sina bedömningar kopplade till insiderrelaterade händelser är det av vikt att använda sin egen och sina kollegers sunda förnuft, samlade kompetens och bedömningsförmåga. Insiderverksamhet är inte en kollegial förekomst och motverkas därför bäst genom bred förankring av åtgärder i verksamheten.

3: Residuala effekter.
En sak som måste tas i beaktande när det gäller insiderrelaterad verksamhet är en ökad risk för residuala effekter. Detta gäller särskilt insiderhot som rör påverkan, exempelvis de som anges efter punkten stölder i uppräkningen ovan.

Residuala effekter kan beskrivas som det som uppstår som följd av den händelse som en insider hade för avsikt att skapa men vars residuala konsekvenser denne inte kunnat förutse.

Förenklat ger följande exempel en bild av residuala effekter.

> Någon som känner sig förfördelad på sin arbetsplats kan och väljer att koppla bort larm- och övervakningsfunktioner på sin arbetsplats och återkommer då arbetsplatsen är obemannad och genomför en stöld. Då stölden utförs och avslutas observeras denne av en annan kriminell som drar slutsatsen att inbrott kan utföras utan att utlösa larm eller insats. Då insidern avlägsnat sig genomför den kriminelle en mycket mera omfattande stöld och väljer därefter att sätta eld på arbetsplatsen för att dölja eventuella spår.

De residuala effekterna i det förenklade exemplet ovan är alltså totalt bortfall av arbetsplatsen och däri ingående inventarier, information och system. Ytterst kan i detta fall konkurs bli effekten.

3.2.2 KRIMINALITET

När begreppet kriminalitet förs på tal i bran-

schen tänker de flesta först och främst på stölder. Det vanligaste handlar naturligtvis om kopparstölder även om mer pikanta varianter, som stöld av transformatorolja, har förekommit på senare tid. Det är naturligtvis så att inom ramen för kriminalitet så är stölder den stora posten. Man ska dock vara försiktig med att generalisera. Kriminalitet är egentligen samma sak som brottslighet och det ordet har en mer vardagligt laddad karaktär. Kriminalitet/Brottslighet som är tillämplig för och påverkar eller kan påverka elbranschen är främst följande.

> Stölder
> Utpressning eller motsvarande
> Sabotage

Stölder

Kopparstölder är klart överrepresenterade vad gäller stölder inom elbranschen. Det finns dessutom flera exempel där gärningsman har avlidit som följd av skador denna ådragit sig i samband med försök till kopparstölder. I bakgrundsarbetet till denna vägledning har inte påträffats något fall där anläggningsägare ställts till ansvar för försummelse av tillträdesskyddet, i.e. att gärningsmannen haft alltför lätt att komma in på ett område där livsfara råder, alternativt att detta inte har framgått på ett tydligt sätt. Det går dock inte att utesluta att en sådan fråga kan komma att prövas rättsligt. Vilken nivå på ett adekvat skydd som förväntas ur ett rättsligt perspektiv kan bara spekuleras om men det går inte att utesluta att gällande föreskrifter för tillträdesskydd kan befinnas vara otillräckliga. Det finns även exempel där oskyldiga transportarbetare fallit offer för gärningsmän som rånat dem på koppar och bragt dem om livet.

På senare år har stöldernas förslagenhet ökat liksom variationen i det som stjäls. Här kan nämnas såväl transformatorolja som hela transformatorer.

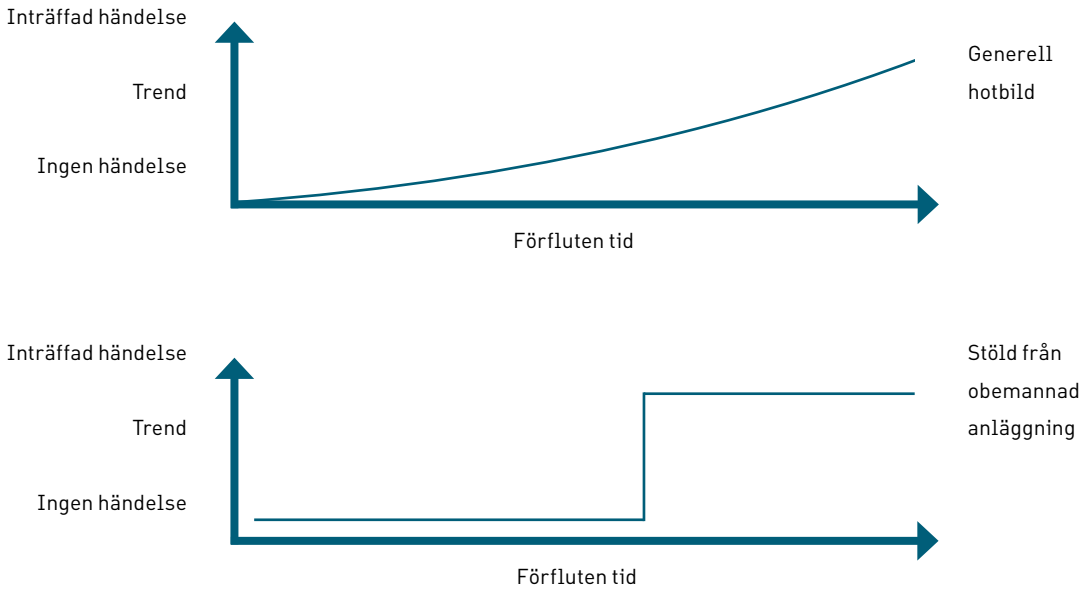
En snabb genomgång av hur det ser ut vid olika obemannade anläggningar, som inte sällan helt saknar larm, ger vid handen att exempelvis följande material och utrustning är föremål för potentiella stölder.

> Drivmedel ur fordon och tankar.
> Kabel, löst liggande eller på trumma.
> Specialfordon eller andra fordon som parkerats på området.
> Elektriska ställverks- och transformatorkomponenter.
> Byggnadsmaterial och inventarier från själva anläggningen.
> Anläggningens staket/stängsel.

Vad gäller stölder generellt så måste grundförutsättningen vara att allt som De-Facto går att stjäla kommer att stjälas. Det är helt enkelt en tidsfråga. Hotbilder som relaterar sig till stöld från exempelvis obemannade anläggningar skiljer sig från övriga i ett speciellt avseende. För många hotbilder kan sannolikheten beskrivas som en funktion som beror på många olika faktorer och som visar på en trend, ofta i tid för att reagera på trenden och motverka den. Vad gäller stölder och då särskilt från obemannade anläggningar ser samma funktion annorlunda ut. Se figur på nästa sida.

När det gäller generella hotbilder inom andra områden kan ofta sannolikheten över tid förändras på ett sätt som, åtminstone till del, kan förutses. Intrångsförsök i IT-system brukar exempelvis föregås av ökad aktivitet med portscanningar och (eng.)probing. Moderna IT-baserade skyddsmekanismer kan varna för detta och tränad personal kan se förändringar i tendenser och trender. I fallet med stöld från en obemannad anläggning däremot så gäller kortfattat. Så länge ingen person som skulle vara beredd att begå brott för att tillförskansa sig det som finns på den berörda anläggningen vet; att och var den finns, att den saknar ett adekvat skydd och att där finns utrustning eller material som denne genom brott är beredd att ge sig tillgång till så kommer inget att hända. När villkoren förändras inträffar händelsen utan förvarning, ofta som följd av en slump.

Man måste även beakta risken för residuala effekter av stölder från sådan anläggning. Det går inte att utesluta att dessa direkt eller indirekt kan påverka elförsörjningen, exempelvis om transformatorolja stjäls från aktiva och inkopplade transformatorer, såsom i fallet med



Figur 5. Bild över funktion generell hotbild och hotbild stöld från obemannad anläggning.

stöld av transformatorolja i Kronobergs län 2012.

3.2.3 TERRORISM OCH MOTSVARANDE

Sverige har länge betraktats som befriat från terrordåd, åtminstone sett i ett globalt perspektiv. Bilden är dock inte helt rättvisande. Som exempel på tidiga, renodlade, terrordåd kan nämnas terrorgruppen Röda arméfraktionens ockupation av den västtyska ambassaden i Stockholm 1975. Men löpande över åren har ett antal händelser inträffat som kan betraktas som terroristbrott eller motsvarande, dock har en eskalering märkts på senare år med kulmen då Sverige officiellt fick sin första självmordsbombare i centrala Stockholm i december 2010.

Nedan återfinns ett utdrag ur Lag (2003:148) om straff för terroristbrott.

2 § För terroristbrott döms den som begår en gärning som anges i 3 §, om gärningen allvarligt kan skada en stat eller en mellanstatlig organisation och avsikten med gärningen är att;

1. injaga allvarlig fruktan hos en befolkning eller en befolkningsgrupp,
2. otillbörligen tvinga offentliga organ eller en mellanstatlig organisation att vidta eller att avstå från att vidta en åtgärd, eller
3. allvarligt destabilisera eller förstöra grundläggande politiska, konstitutionella, ekonomiska eller sociala strukturer i en stat eller i en mellan statlig organisation. 3 § Följande gärningar utgör terroristbrott under de förutsättningar som anges i 2 § i denna lag:

...

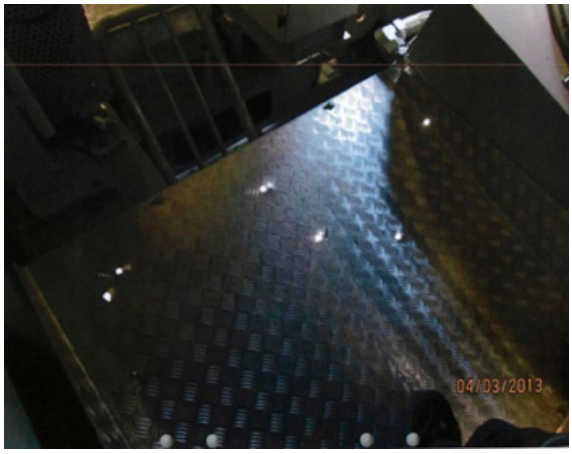
9. sabotage och grovt sabotage,

...

Observera att för att klassa sådan gärning som terroristbrott krävs dessutom att gärningen allvarligt kan skada en stat eller mellanfolklig organisation. Vid denna vägleddnings skapande pågår revidering av säkerhetsskyddslagstiftningen. För mer aktuella uppgifter konsultera gällande lagstiftning.

Vad som utgör ett terroristbrott i praktiken avgörs av rättsliga instanser men det är intressant att bära med sig lagtexten när man tittar på de exempel som löpande inträffar i vårt samhälle.

Ett annat mera konkret och närliggande fall



Interiör vindkraftverket. Bilden visar hur ett flertal skott penetrerat durkplåten. Foto: POLISEN.

av påverkan av energisförsörjningen inträffade i början av mars 2013 utanför Norrtälje. Ett vindkraftverk i Kullsta, Estuna utanför Norrtälje utsattes för beskjutning från någon typ av handeldvapen.

Mer än tio skott har avlossats mot vindkraftverkets kontrollrum, placerat 95 meter över marken av en eller flera gärningsmän. Om kontrollrummet varit bemannat vid tillfället hade personen sannolikt skadats svårt eller omkommit. Värdet på skadorna uppgår till miljonbelopp. Sabotaget påverkade alltså elproduktionsutrustning, men hade kunnat sluta ännu värre. Polisen rubricerar brottet som grovt sabotage.

[Källa: Norrtelje Tidning 14 Mars 2013]

3.2.4 ELEKTRONISKA HOT

Exemplen som anges i detta avsnitt är i vissa fall över tio år gamla. Anledningen till detta är att det tar tid för olika berörda svenska myndigheter att ensa uppfattningen om ett händelseförlopps faktiska skeende. I denna vägledning ska inte exemplen kunna leda till tvetydigheter och kontrovers utan utgöra just vederlagda exempel. Se även not i slutet på detta avsnitt.

En annan aspekt på terrorism är cyberterrorism, det vill säga att någon medvetet och avsiktligt påverkar system så att deras funktion blir otillgänglig eller på annat sätt förfelas. Detta kan ske på många olika sätt såsom intrång i realtid s.k. (eng.)hacking men också med hjälp av skadlig kod som sprids och infekterar system med olika metoder. Det som gör att cyberterrorism är ett så allvarligt hot är främst tre saker.

1. Gärningsmannen kan befinna sig var som helst geografiskt när objektet påverkas och på grund av avsaknaden av närhet till objektet upplevs inte gärningen som så allvarlig som den egentligen är.
2. Verktyg, kunskap och spridningsmetoder finns lätt tillgängliga på Internet.
3. Kvalificerade attacker går att genomföra utan krav på att gärningsmannen har djupare kunskaper om vare sig attackmetoden eller objektet mot vilket attacken riktas.

I en rapport från MSB (dåvarande KBM) återfinns ett flertal exempel på faktiska vederlagda händelser som inträffat där händelsen kan klassificeras som en cyberattack.

> Mars 2000. En missnöjd tidigare konsult tar över kontrollsystemet för ett vattenreningssystem i Australien. Konsekvensen av attacken blir att tusentals kubikmeter obehandlat vatten översvämmar området.

> December 2000. En grupp hackare angriper ett datornätverk i en elkraftanläggning i USA genom att utnyttja svagheter i ett använt protokoll. Sedan används de övertagna nätverksresurserna för att spela datorspel. Detta utnyttjande av dator- och nätverksresurser hindrar påtagligt möjligheten för anläggningen att bedriva affärer med sin elektricitet (electricity trading

> Januari 2003. Driftsäkerhetsövervakningssystemet vid kärnkraftverket Davis-Besse i USA, som vid tillfället är avställt för revision, infekteras med SLAMMER-masken. Systemet är ur funktion i nära fem timmar. Orsaken är dels en felaktigt uppsatt förbindelse in i kärnkraftverkets datornät, dels en dator utan virusskydd eftersom den betraktas som fristående och därmed inte i behov av skydd. Det finns redundanta, analoga reservsystem som är opåverkade av masken men operatörerna vid verket får en avsevärt ökad arbetsbelastning.

> Augusti 2003. En amerikansk tågoperatörs datornätverk för signalering infekteras av

en mask vilket leder till att alla operatörens tåg står stilla i en halv dag.

> Maj 2004. SASSER-masken infekterar ett signal- och kontrollsystem hos den australiensiska lokaltågsoperatören Railcorp. Följdeffekten blir att 300 000 pendlare till och från Sydney saknar transportmedel under en dag.

Det är viktigt att notera att alla dessa antagonistiskt relaterade incidenter härrör från icke kvalificerade antagonister. Källa: Aspekter på antagonistiska hot mot scada-system i samhällsviktiga verksamheter (msb)

Ovanstående utgör endast exempel på vederlagda händelser. Det finns naturligtvis fler aspekter att beakta. För att tillgodogöra sig kunskap om vad en kvalificerad motståndare kan iscensätta rekommenderas en sökning efter information om STUXNET.

> Läsaren kan med fördel själv söka nyare exempel på elektroniska hot som medfört händelseförlopp med negativa konsekvenser. Exempel på sökord är "IT-incident", "Cyberincident", "IT + bedrägeri", "IT + spioneri", "IT + sabotage" m.m. Läsaren uppmanas dock att ta till sig sådan information med ett betydande mått av källkritik.

3.2.5 SPIONERI OCH SABOTAGE

För en lekman kan det förefalla osannolikt att under sin livstid, ens perifert, komma i kontakt med sådana saker som spioneri och sabotage. Verkligheten är dock en annan även om formerna för sådan verksamhet förändrats och följt utvecklingen i samhället över tiden. När man hör ordet spioneri tänker man oftast på män i mörka rockar med slokhattar som stjäl hemlig information, utför sabotage och lönnmord. En viss sanning måste fortfarande sägas gälla i detta avseende. Den största skillnaden är dock målet för sådan verksamhet. Tidigare var det stora fokusområdet militär verksamhet, utrustning och förmåga. I dagsläget är det mera fokus på proprietär information, jmf företagsspioneri, och på funktioner som ser till att samhället fungerar.

Efter Berlinmurens fall och Sovjetunionens kollaps blev hundratusentals personer med kunskaper om spioneri och underrättelsetjänst utan arbete. Många av dessa fortsatte sedan sitt värv i privat regi. Det finns många sätt att vederlägga detta men ett målande exempel på att sådana personer verkar är den lagstiftning som antogs 1998 i Litauen som syftar till att förhindra forna KGB-agenter från att få jobb inom förvaltningen och många sektorer av det privata näringslivet trots risken för att beslutet strider mot författningen. Man kan således konstatera att det finns en väl etablerad förmåga att utföra såväl spioneri som sabotage tillgänglig på den fria marknaden. Var och när den utnyttjas, och till vad, går det bara att spekulera om men i ett hårt marknadsklimat räknas alla fördelar.

Inte sällan bedrivs företagsspionage numera elektroniskt och med hjälp av IT. Att med olika metoder, ibland mycket avancerade, sammanställa och analysera publika uppgifter är ett tillvägagångssätt, som ofta används. Ett steg längre är att aktivt stjäla information och elektroniska uppgifter från företag, myndigheter eller andra organisationer. Via datorintrång, att avlyssning av data- och telekommunikationer eller att på annat sätt inhämta information är några få exempel på de många olika sätt att bedriva elektronisk informationsinsamling och spionage. Ibland bedrivs denna typ av verksamhet av enskilda individer, ibland av företag som vill göra någon konkurrensanalys, men också andra typer av grupperingar och intressegrupper samt nationsstater.

Det finns så pass många exempel på företagsspioneri i Sverige de senaste åren att det inte lönar sig att räkna upp exempel här. Om man vill få vederlagt att det sker och förkovra sig i ämnet föreslås en sökning på ordet företagsspioneri på Internet, läsa säkerhetspolisens årsrapporter eller följa nyhetsflödet gällande nya fall eller försök till företagsspionage.

Vad som dock bör ges särskild uppmärksamhet är att nästan alla fall, åtminstone av de som upptäckts eller för den delen kommit till allmän kännedom, inbegriper någon form av dataintrång. Detta är naturligtvis en följd av att nästan all information som används i vårt samhälle i dagsläget hanteras i IT-system. Det är lätt att man drar snabba slutsatser som följd av den något sneda statistiken över förekomster

av dataintrång i syfte att på något sätt spionera. Då bör man dock betänka att ett mera traditionellt sätt att utföra underrättelsetjänst i form av spioneri är infiltration och (eng.)social engineering. Beroende på hur skicklig gärningsmannen är så är ofta risken för upptäckt i dessa sammanhang lägre. Ett någorlunda färskt exempel på en mera handfast form av spioneri är en 48-årig man som i juli 2008 häktades misstänkt för grovt företagsspioneri mot Saab Microwave Systems i Göteborg. Mannen arbetade som konsult, alltså på "insidan" och kunde på detta sätt disponera den information som berörs. Mannen ifråga genomförde även utpressningsförsök mot Saab vilket skulle kunna peka på att huvudsyftet med dennes verksamhet var ett annat än det rena spioneriet. Icke desto mindre, och oavsett vad sanningen bakom fallet egentligen är, så utgör detta ett konkret exempel på en mera traditionell tillämpning av spioneri.

Faktum är att spioneri och sabotage är företeelser som finns i vårt samhälle och förekommer i större omfattning än vad man som lekman skulle förmoda.

3.2.6 CIVILA OROLIGHETER

Civila oroligheter är ett vitt begrepp som vanligtvis används av polisen för att beskriva en eller flera typer av oroligheter orsakad av en grupp människor. Civila oroligheter är ofta ett symptom på och en form av protest mot, stora sociala och politiska problem. Exempel på civila oroligheter är illegala demonstrationer, i förekommande fall med våldsamma inslag, ockupation av politiska och samhällsviktiga byggnader och andra objekt samt andra former av upplopp, sabotage och brottslighet. Det är från början ofta tänkt att vara en demonstration för allmänheten mot statsmakt eller politiska beslut, men kan trappas upp till allmänt kaos.

Ett exempel på civila oroligheter i Sverige är de så kallade Göteborgskravallerna som ägde rum i juni 2001 i samband med ett EU-toppmöte. Under tiden som mötet och oroligheterna pågick greps mer än 500 personer. Mer än 50 poliser och upp emot 100 demonstranter skadades under sammandrabbningarna. Polisen var stundom så pass trängd av demonstranterna att de flera gånger öppnade eld med sina handeldvapen. Minst en demonstrant skadades härvid allvarligt. Göteborgskravallerna är det allvarligaste exemplet på civila oroligheter som Sverige upplevt på flera decennier.

En viktig aspekt att dra lärdom från är i detta sammanhang formerna för hur kravallerna uppstod. Flera extremistiska grupper bidrog till att piska upp stämningen och eskalera allvarlighetsgraden i de från början tämligen fredliga demonstrationerna. Dessa extremistgrupper är ofta löst sammansatta och präglas av en samhällsfientlig inställning. Detta bör särskilt beaktas när analys av hot och risker mot en verksamhet genomförs. Inom elenergibranschen finns exempel på antagonism exempelvis mot eltaxor och vindkraft. Noggrannhet och öppenhet för det oväntade är framgångsfaktorer vid riskanalys när dessa frågor kan vara aktuella.

3.3 MILJÖRELATERAD HOTBILD

Med miljörelaterad hotbild avses sådana hot som härrör sig till naturfenomen. Exempel på miljörelaterade hot kan vara jordbävningar, tsunamis, geomagnetiska stormar och isstormar. Miljörelaterade hot kan vara mycket oförutsägbara. Detta medför att det är svårt att skydda sig mot alla eventualiteter av miljörelaterade hot. Elsystemets olika aktörer och deras verksamhet är spridd över stora geografiska områden så stora variationer av miljöer och natur kan förekomma. Likaså består elsystemet av ett stort antal anläggningar, utrustningar och fasta installationer, vilka lokalt, regionalt – eller i enstaka extrema fall nationellt – kan påverkas av ett antal olika miljörelaterade hot.

En framgångsfaktor när det gäller att skydda sig mot miljörelaterade hot är, precis som i andra hotbedömningar, att hålla ett öppet sinne. Vi lever i en tid med föränderligt klimat, extremt väder och miljöhändelser som vi inte tidigare upplevt. Ett påtagligt exempel är att antalet takras i offentliga och privata byggnader som följd av extrema snömängder har ökat de senaste åren. För att skydda sig på ett adekvat sätt krävs att skyddet dimensioneras utifrån det föränderliga miljöläge som råder nu och i framtiden.

Islager på bilar och kraftledningar till följd av den isstorm som drabbade Kanada 1998.

3.3.1 STORMAR OCH MOTSVARANDE

Gudrun, Per, Dagmar och Emil är namn som för lång tid framöver kommer att kommas ihåg med förskräckelse. De utgör exempel på stormar som orsakat enorma skador och dödsfall. De rykten om en våg av självmord som skulle ha följt i stormens spår är dock överdrivna. Det finns endast ett dokumenterat fall där en person tog sitt liv som följd av stormens konsekvenser. Det bör dock påpekas att stormens effekter fick katastrofala följder för ett stort antal människor inom skogsbruket.

För människor som bor eller verkar i områden som inte direkt varit drabbade av sådana här stormar kan det vara svårt att på allvar ta in omfattningen och magnituden av konsekvenserna från dessa stormar. Här följer att par målande exempel från stormen Gudrun.

- Den samhällsekonomiska kostnaden för stormen beräknas uppgå till mellan 3 och 4 miljarder kronor. Då är inte kostnader för skogsskador inräknade. Det motsvarar den totala utvecklingskostnaden för X-38 Crew Return Vehicle, den nya ”livbåten” till den internationella rymdstationen ISS.
- Om man använder det stormfällda timret till att göra en vedstapel som är 3 meter hög och 6 meter bred så räcker den från Jönköping till Madrid i Spanien...och tillbaka hela vägen. En sträcka på ungefär 460 mil!
- Om man tänker sig en kub med någorlunda kvadratiska sidor av den storlek, volym, som det stormfällda timret utgör så skulle denna kub kunna inrymma arenan Globen i Stockholm. 120 stycken Globen närmare bestämt och då skulle de ändå ligga som bollar i lådan med luft emellan.

Nämnda stormar är exempel på väder som i närtid har drabbat Sverige. Det finns dock andra skrämmande exempel i länder med snarlikt klimat. Kanada drabbades i januari 1998 av en isstorm då en varmfront långsamt förflyttades från Texas och vidare mot nordost mot nordöstra USA och östra Kanada, här mötte den varma luften kall arktisk luft i ett högtryck. När luftmassorna stötte ihop pressades den varma luften upp över den kalla arktiska luften. Snön som bildades uppe i atmosfären smälte i det varma luftlagret för att åter avkylas i den kalla luften närmare markytan där den föll som underkylt regn. Samtidigt var vindarna svaga i området, det gjorde att vädersituationen inte förändrades på flera dygn. Det bildades ett islager som täckte i stort sett allt i dess väg. Islagrets tjocklek var ca 100 mm.

Fredagen den 9 januari beräknades att tre

Bild: MSB

miljoner människor var utan ström, efter det att elnätet kollapsat på grund av ismassorna. Bara i Ottawa beräknades kostnaden för de materiella skadorna uppgå till ca 3 miljarder kronor. 30 människor fick sätta livet till i isstormen 1998.

När riskanalyser genomförs, och då särskilt för anläggningar, så bör stormeffekter vägas in med stor eftertanke. I många fall har byggnader som varit utförda helt i enlighet med gällande normer för det område de har uppförts drabbats hårt, exempelvis av tak-ras. Sista gången Sverige drabbades av en svår isstorm var 1921. Kanadensiska myndigheter uppger att en svår isstorm inträffar ungefär vart hundrade år.

3.3.2 ÖVERSVÄMNINGAR

Sverige drabbas årligen av översvämningar, ofta i samband med den så kallade vårfloden. Översvämningar inträffar dock även på ett mera oförutsägbart sätt, exempelvis i samband med skyfall. Sådana översvämningar kan vara svårare att reaktivt skydda sig emot då händelseförloppet är avsevärt hastigare.

Det pågår många debatter och mycket forskning kring om och hur klimatet förändras. Den allmänna uppfattningen är dock att antalet väder och klimatrelaterade händelser som påverkar samhällsfunktioner och privata egendomar har ökat de senaste decennierna. Det är inte fastställt om detta är en naturlig variation i klimatet eller om det beror på klimatförändringar.

En faktor som MSB påpekar är havsnivåhöjningen som ökar risken för erosion och översvämningar längs delar av landets kuster.

Några saker att beakta i samband med att risken för översvämningar bedöms, exempelvis inom ramen för en riskanalys är följande.

- Då en översvämning inträffar kan infrastruktur drabbas så att det försvårar eller omöjliggör åtkomst till olika anläggningar beroende på placering och tillresevägar.
- Sekundära effekter på anläggningar kan inträffa när bråte, delar av eller hela fastigheter förs med en översvämning. Härvid kan svåra mekaniska påfrestningar uppstå på en anläggning.
- Andra effekter av översvämningar kan vara att elnät eller kommunikationsnät drabbas av avbrott då stolpar undermineras, träd faller över ledningar eller att exempelvis en bro rasar som följd av vattenmassors påverkan.

En framgångsfaktor för att bedöma och förebygga risker som relaterar sig till översvämningar är att göra bedömningar på plats i terrängen och längs de rutter som man är eller kommer att bli beroende av.

3.3.3 JORDBÄVNINGAR OCH JORDSKRED

Sverige har historiskt varit förskonat från svåra jordbävningar. De inträffar dock varje år, dock med en betydligt lägre magnitud än vad som är brukligt i länder där jordbävningar orsakar skador. Jordbävningar med en magnitud upp till drygt fyra på Richterskalan inträffar dock i Sverige. En fyra på Richterskalan definieras enligt följande; Kännbar skakning av inomhusföremål, skakande ljud. Större skador osannolika.

Det finns för närvarande inget som talar för att Sverige skulle drabbas av någon svårare jordbävning, detta främst på grund av att Sverige är beläget långt från gränsen mellan olika kontinentalplattor där de stora skalven inträffar. Det går dock inte att utesluta att känslig, eller dåligt monterad, utrustning kan påverkas i samband med ett skalv av med Nordliga mått mätt stor magnitud. Åtgärder härvid bör dock kunna begränsas till att följa gällande normer för byggnad och montage av berörd utrustning.

Jordskred skiljer sig från jordbävningar så tillvida att de uppkommer när hållfastheten i marken försämras såpass att marken inte längre är i jämvikt utan börjar röra på sig. Jord-

Jordskred från 2008 nära Granån i Granbäckstorp, Gräsmark, Värmland.

skred kan inträffa som följd av ett flertal faktorer. De vanligaste är följande.

- > Förändringar i marken som följd av ihållande eller kraftigt regn.
- > Ökat marktryck då byggnader eller andra former av anläggningar uppförs.
- > Erosion eller vittring vid stränder där vågor påverkar marken.

I Sverige finn ett flertal exempel på jordskred som gett upphov till stora materiella skador. Ett av de mer kända exemplen i närtid är Skredet i Vagnhärad var ett jordskred som inträffade 00.59 den 23 maj 1997 i Ödesby i Vagnhärad. Skredet omfattade en cirka 200 meter lång sträcka längs Trosaån och sträckte sig cirka 60 meter upp i en bebyggd lerslänt. Som en följd av skredet raserades eller revs totalt 29 villor i det drabbade området.

Ett jordskred behöver inte alltid utgöras av en kant eller strandbank med det drabbade området helt parallellt med en å, älv eller annat vattendrag. Notera formen och storleken på nedanstående ras i Värmland. Observera mannen som står vid bortre raskanten.

Vid uppförande av byggnader och anläggningar bör man alltid beakta riskerna för ett jordskred. Detta bör göras fackmannamässigt med stöd av exempelvis kommunala resurser eller specialister inom det geologiska området.

3.3.4 EXTREMT RYMDVÄDER, GEOMAGNETISKA STORMAR OCH MOTSVARANDE

En kategori särskild hot mot elsystemet är olika typer av allvarligare naturfenomen som kan störa jordens magnetfält, skapa elektriska strömningar som uppstår i atmosfären eller i jordskorpan, som eller på annat sätt påverkar utrustning och fasta installationer inom elproduktion och eldistribution.

En särskild egenskap med just denna typ av miljörelaterade hot är att de kan ha en mycket omfattande geografisk spridning, vilket kan innebära att de kan påverka regioner, nationer eller till och med större delen av en kontinent.

Ett följdproblem av eventuella naturfenomen av denna kategori är att skadorna kan bli permanenta och omfattande, vilket i sin tur leder till att många drabbade elbolag samtidigt försöker

- > beställa ersättningsutrustning vilket inte finns i de volymer som behövs eller att utrustningen enbart tillverkas efter order, vilket leder långa eller extrema ledtider,

> Anlita reparationspersonal, vilka normalt jobbar åt flera uppdragsgivare, vilket naturligtvis innebär att dessa är en trång resurs.

Svenska kraftnät har tagit fram såväl en FAQ, (eng.)Frequently asked questions, som en rapport om skydd i detta ämne. Dessa återfinns på följande länkar.

FAQ
http://www.svk.se/general/Modulen-Genvagar/Vanliga-fragor-FAQ/Fragor-om-solstormar/

Rapport om skydd
http://www.svk.se/Global/02_Press_Info/Pdf/120330-Skydd-mot-geomagnetiska-stormar.pdf

3.4 HOTBILD RELATERAD TILL OLYCKOR OCH MOTSVARANDE

Merparten av händelser som inträffar och som påverkar eller kan påverka verksamheten negativt är olycksrelaterade. Det är således av vikt att ur ett riskperspektiv analysera såväl var, hur och när sådana händelser kan inträffa som vilka konsekvenser de kan få.

De underrubriker som redovisas här utgör ett exempel på områden där olycksrelaterade risker är tillämpliga. Det finns dock naturligtvis fler områden och vad analys bör man inte begränsa sig till dessa utan möjligen utgå ifrån dem.

3.4.1 BRISTANDE KOMPETENS

Bristande kompetens kan ses som ett samlingsnamn på okunskap, dålig utbildning på en specifik produkt eller i en specifik verksamhet, avsaknad av eller brister i formell utbildning m.m. En annan orsak till att denna problematik uppstår kan vara att verksamheten har långa intervall mellan handgrepp och att mellanliggande utbildning och övning saknas.

I många fall där verksamheten innefattar handgriplig verksamhet sker den specifika utbildningen oftast som en form av lärlingskap eller mentorskap. Inte sällan inbegriper detta kritiska åtgärder och verksamheter såsom åtgärder i ett ställverk under olika omständigheter eller i samband med incidenter. Det är mycket viktigt att den som leder och lär någon på detta sätt dels har mandat att avgöra om och när någon får anses kunna en verksamhet och dels ges den extra resurstid som så ofta krävs för att på ett bra och pedagogiskt sätt kunna lära ut verksamheten. Alltför ofta inträffar olyckor som följd av att utbildande verksamhet på detta sätt forceras och att den utbildade inte besitter förmåga att hantera särskilda eller kritiska situationer. Detta medför en ökad grad av allvarlighet i potentiella incidenter eftersom sådana situationer oftast uppstår just då något allvarligt går fel. Alltför ofta saknas dokumentation som på ett begripligt och pedagogiskt sätt beskriver hur olika händelseförlopp, handgrepp, situationer m.m. ska hanteras. Det medför ökad risk för att en given situation hanteras olika och/eller felaktigt då den uppstår.

I sådan verksamhet som har ett stort beroende till styrsystem och andra typer av IT-system är beroendet av verksamhetsspecifik utbildning stort. Vidare är sådana system kritiskt beroende av en korrekt och tillgänglig dokumentation. Sådan dokumentation förpliktigar dock ett ansvar om att hålla denna uppdaterad. Det finns alltför många exempel där dokumentation en gång har upprättats på ett bra sätt men över tiden blivit inaktuell, exempelvis som följd av byte av system eller annan utrustning.

Många olyckor som skylls för bristande kompetens har i själva verket sin orsak i det faktum att såväl intern, systemspecifik och verksamhetsspecifik utbildning brister som att dokumentation saknas eller är behäftad med allvarliga brister eller ibland rena felaktigheter.

3.4.2 EKONOMISKA NEDSKÄRNINGAR SOM PÅVERKAR SÄKERHETEN

Det är svårt att mäta vilken ekonomisk vinning som nås genom god säkerhet. Detta kommer sig främst av att god säkerhet förhindrar ekonomisk förlust som följd av olyckor och andra incidenter. Således är det svårt att kvantifiera de bakomliggande ekonomiska aspekterna som blir resultatet av god eller dålig säkerhet. Detta resulterar

Resandetåg 505 efter att ha kolliderat med en grävlastare på Kimstads driftplats.

inte sällan i att säkerhetsrelaterade verksamheter blir föremål för medskärningar, främst ekonomiska sådana.

Om verksamheten inte har drabbats av någon större olycka eller incident som direkt kan hänföras till nedskärningar i säkerheten så finns det i stort sett endast två sätt att belysa behoven av att säkerheten vidmakthålls på en nivå som ur ett säkerhetsperspektiv är sund.

1. RISKANALYS
Att genom väl genomförda och grundliga analyser påvisa potentiella skeenden som kan påverka verksamheten negativt och att på ett pedagogiskt, professionellt och trovärdigt sätt presentera dessa. Redovisade risker måste ha en förankring i verksamheten.

2. PÅVISA EXEMPEL
Bara för att den egna verksamheten inte drabbats av en allvarlig olycka så betyder inte det att motsvarande händelse inte har inträffat någon annanstans. I de allra flesta fall har den det och materialet finns oftast lätt sökbart.

3.4.3 PRESSADE LEDTIDER

Moderna organisationer består ofta av en liten personalstyrka som ska arbeta effektivt, både i det löpande arbetet men också under andra förhållanden, till exempel inom projekt och förändringsarbeten, men också under särskilda händelser såsom under säkerhetsincidenter. Detta leder ibland till pressade ledtider. Det är inte ovanligt med att människor som jobbar under press tar felaktiga beslut, begår misstag eller på annat sätt medför ökade risker.

Projektarbete mäts ofta utifrån tre mätetal: ekonomi, tid och kvalitet. Ekonomi innebär oftast att den budget som är fastställd för projektet hålls. Tid är att projekttidplan och därmed viktigare hålltider såsom beslutsmöten, utvärderingstillfällen och leveransdatum hålls. Dessa två första mål är konkreta och relativt lätta att mäta med gängse metoder och medel såsom budgetuppföljning. Det tredje målet, kvalitet, är oftast mycket svårare att såväl definiera som att utvärdera om det nåtts. Det är naturligt att dessa tre mål ställs emot varandra, vilket leder till situationer där exempelvis för att hålla ledtid så måste kvaliteten försämras eller budget överskridas. Då kvalitet är ett mer svårmätt mål, så kan pressade ledtider eller budgetproblem ofta leda till att kvaliteten tummas på, då kvalitetsförsämring ofta inte kan bevisas få en direkt negativ inverkan på själva projektet, utan snarare dess eftermäle.

Det finns exempel när en organisation valt att forcera projekts ledtid på ett sådant sätt att flera projektledare avsagt sig projektet och den produkt som projektet presenterat vid leveransdatum saknat mer än två tredjedelar av den planerade funktionaliteten och många av de obligatoriska säkerhetsfunktionerna.

Ovanstående exempel är extremt och naturligtvis helt oacceptabelt men problemet är befintligt och ska tas på allvar. Ofta när ledtider pressas så är det synonymt med att säkerhetsfunktioner får stryka på foten. Det hela blir en ond cirkel när väl den dåliga säkerheten medger att olyckor och andra incidenter inträffar.

Pressade ledtider, oavsett om det är i ordinarie verksamhet eller inom exempelvis projekt, är en vanligt förekommande typ av problem, och en risk, som definitivt bör tas upp och belysas i riskanalyser.

3.4.4 AVSAKNAD AV PERSONELLA OCH MATERIELLA RESURSER

Som tidigare påpekats, så är moderna organisationer pressade vad det gäller kostnader, vilket i sin tur leder liten personalstyrka som ska arbeta effektivt, men också att övriga materiella resurser hålls efter av kostnadsskäl. Hot som kan komma av detta är flera, exempelvis:

- Nyckelpersonberoenden, då få personer är tillgängliga, och dessa måste finnas tillgängliga för viktiga funktioner eller som kritiskt verksamhetsstöd.
- Användning av utrustning som inte längre är säker att använda, då den borde ersättas med modernare utrustning som har modernare skydd.
- Avsaknad av vissa skydd som inte installerats, då besparingskrav gjort att investeringar inte tagits.

Inte sällan är hoten kända på en allmän nivå bland de som arbetar inom organisationen, även om de inte har strukturerats, inventerats, dokumenterats eller analyserats av organisationens företrädare. Hoten blir dock mer tydliga i efterhand när de lett till en olycka eller incident. När olyckor och andra incidenter granskas närmare påträffas ofta formuleringar av typen:

- ...den tjänsten hade emellertid ersatts med ett övervakningssystem för att...
- ...brandsläckningsutrustning saknades i utrymmet vi d det aktuella tillfället då bedömningen var att...
- ...förmågan att dyka i kallt vatten och rädda någon som gått genom isen fanns vid olyckstillfället 134 km ifrån olycksplatsen...
- ...den döde saknade vid olyckstillfället adekvat skyddsutrustning...
- ...någon brovakt fanns inte på plats vid olyckstillfället och då bron fjärrmanövrerades från annan plats täckte inte övervakningskameran in området där den förolyckade klämdes till döds...

Olyckor som beror på att nedskärningar gjorts i bemanning eller att material, administrativa rutiner, kontroll och uppföljning, system eller annan typ av utrustning saknas är mycket vanliga och utfaller inte sällan på ett mycket allvarligt sätt vilket ovanstående exempel visar.

Söndagen den 12 september 2010 inträffade en kollision på Kimstads driftplats mellan resandetåg 505 och en spårgående grävlastare. Olyckan medförde att en person omkom och 20 personer skadades, varav 9 allvarligt.

Olyckan skedde på grund av att en grävlastare fördes upp på spåret utan att A-skydd[2] etablerades på intilliggande spår.

En bakomliggande orsak till att A-skydd inte etablerades är brister i skydds- och säkerhetsplaneringen inför arbetet, vilket i sin tur beror på brister i projektets planering. Bristerna i projektets planering kan i sin tur härledas till otillräckligt projektunderlag.

Brister av det slag som orsakat olyckan och som finns i flera olika nivåer inom Trafikverkets projektorganisation, ska kunna upptäckas och åtgärdas inom ramen för en normal revisions- och avvikelsehantering. Några sådana upptäckter har inte gjorts varför den grundläggande orsaken till olyckan kan anses vara bris-

2. Trafikverksamhet för att förhindra eller begränsa rörelser med spårfordon inom ett bestämt område. Spärrfärd och växling får förekomma efter samråd.

ter i Trafikverkets uppföljnings-, avvikelse- och riskhantering. [Källa: Statens haverikommission RJ 2012:03]

Exemplet ovan är bara ett i raden av liknande händelser som inträffar i olika branscher och verksamheter. Det belyser på ett bra sätt behovet av att analysera, dokumentera och åtgärda brister som identifieras.

4 RISKANALYS

4.1 INLEDNING

Läsaren bör ge akt på att Svenska kraftnät även har gett ut;

- en hotkatalog för elbranschen. Denna exemplifierar konkret en stor mängd hot och kan med fördel användas som referens, källa eller inspiration i säkerhetsarbetet i allmänhet och i riskanalyser i synnerhet,
- en vägledning för riskanalys som även tar upp formella aspekter och bygger på ISO 31000 och ISO 30101.

I detta kapitel ges exempel på en enkel metod att genomföra riskanalys. Metoden är tillämplig på godtyckliga objekt, dvs. den kan användas för exempelvis IT-system, verksamheter, lokaler, anläggningar etc.

Det finns exempel på metoder som bland annat räknas upp i bilaga 1, metodreferenser, till denna vägledning.

4.2 CENTRALA BEGREPP

Här redovisas de mest centrala begreppen i scenariobaserad riskanalys. För varje begrepp ges en förklaring som bidrar till att hålla genomförandet och resultatet av riskanalys enkelt och effektivt.

Det finns ett antal källor till definitioner av begrepp men de är ofta akademiska eller vetenskapliga i sitt uttryck. De begrepp som redovisas här anges med praktisk tillämpning och den enkla metodiken i åtanke.

4.2.1 HOT/RISKKÄLLA

Det talas i olika sammanhang om riskkällor. De är definitionsmässigt samma sak som hot som härefter kommer att vara det begrepp som används i denna beskrivning.

> Ett hot är en möjlig oönskad händelse, företeelse eller förekomst som har eller kan få negativa konsekvenser.

Hot tas fram först i analysen genom en kreativövning, ofta kallad (eng.)Brainstorming.

Det finns flera exempel när organisationer definierar att ett hot måste vara skapat av eller bero på en person med avsikt, så kallade aktörsrelaterade hot. Detta medför begränsningar i analysen och kommer inte att tillämpas i denna beskrivning. Ett hot kan således utgöras av **exempelvis** följande:

- Blixtnedslag i ...
- Dataintrång i ...
- Skadlig kod inkommer i systemet ...
- Insider röjer uppgiften x till obehörig ...
- Oönskad vätskeinträngning i datahallen.
- Data förfelas i överföringen mellan ...

De avslutande trippelpunkterna i några av exemplen ovan avser en godtycklig tillämpning

beroende på vilket analysobjekt som hotet avser. I det första exemplet i punktsatsen skulle det således kunna vara datahall, kontor, manskapsbod, ställverk, transformator eller något annat tillämpligt objekt.

Det som är signifikant i en hotformulering är att den är enkel och inte är flerbottnad, dvs. att den består av multipla händelser. Exempel på en flerbottnad hotformulering är; **Blixten slår ned i datahallen samtidigt som en långtradare kraschar in i datahallsbyggnaden.** Det är lätt att förstå att det inte går att bedöma sådana hotformuleringar. Hot ska således formuleras enkelt och med en singulär händelse i fokus. Följder, skador och andra resteffekter redovisas i scenariot som upprättas för vart och ett av hoten i ett annat skede av analysen.

4.2.2 RISK

En risk är ingenting annat än ett hot som har bedömts avseende två kriterier. Sannolikheten för att hotet ska inträffa och skadan/konsekvensen av hotet givet att det har inträffat.

Detta innebär att om vi har hotet -

- **Insider röjer uppgiften x till obehörig person hos konkurrent**

  – och kompletterar detta med -

- **Hotet bedöms inträffa en gång under en treårsperiod och betinga skadekostnader om minst 1MKr och maximalt 2MKr**

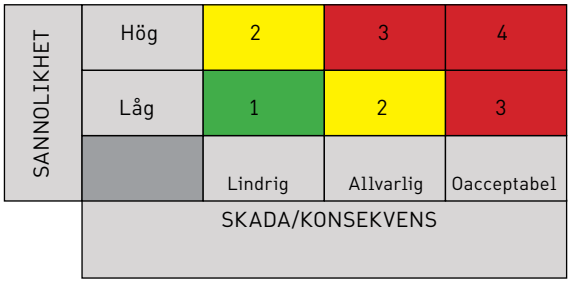
  – så har vi begreppsmässigt gått från att beskriva ett hot till att beskriva en risk.

Riskbedömningen av hoten sker oftast i matrisform där y-axeln i matrisen representerar sannolikheten för att hotet ska inträffa och x-axeln representerar skadan/konsekvensen av det inträffade.

Det spelar egentligen ingen roll hur man utformar sin riskmatris men det finns några saker att tänka på och ta hänsyn till:

- Under senare tid har flera säkerhetstunga myndigheter och organisationer tonat ned betydelsen av att noggrant bedöma sannolikheter för olika hot utan mer fokusera på skadeverkningar.
- Oavsett hur man utformar sin matris så ska det finnas en beskrivning för varje nivå av sannolikhet och skada som är begriplig och tillämplig. Begreppen **"hög sannolikhet"** eller **"betydande skada"** betyder inget eller olika saker för olika personer om de inte på något sätt beskrivits eller definierats.
- Ju fler nivåer riskmatrisen har, oavsett om det gäller sannolikhet eller skada/konsekvens, desto högre komplexitet och risk för tidsödande diskussioner som i sak inte tillför något till analysen.
- Det finns flera sätt att ange ett riskvärde, alltså definiera ett abstrakt värde i respektive ruta av matrisen som anger hur pass allvarlig kombinationen av sannolikhet och skada/konsekvens bedöms vara. Gemensamt är att om matrisen är utformad enligt de kriterier som anges i denna metod så är den allvarligaste rutan i matrisen den som är högst upp till höger och den lindrigaste längst ned till vänster.

Figuren nedan beskriver en väldigt enkel riskmatris som i de allra flesta fall går att använda i riskanalyser av ett godtyckligt objekt.



I denna beskrivning av riskanalys exemplifieras definition/beskrivning av nivåerna för sannolikhet och skada/konskevens enligt följande:

SANNOLIKHET	
Hög	Hotet bedöms inträffa mer än en gång var sjätte månad.
Låg	Hotet bedöms inträffa mindre än en gång var sjätte månad.
SKADA/KONSEKVENS	
Oacceptabel	Skadan/Konsekvensen av ett inträffat hot är så allvarlig att den inte på något sätt kan accepteras utan åtgärder för att eliminera eller minimera effekter av ett sådant hot måste företas.
Allvarlig	Skadan/Konsekvensen av ett inträffat hot medför kraftiga verksamhetsstörningar, omfattande merarbete eller verksamhetsbetydande drivande kostnader som får sekundära effekter.
Lindrig	Skadan/Konskevensen är befintlig men kan hanteras inom ramen för den dagliga verksamheten eller med ringa extra insatser.

Det bör särskilt noteras att i exemplet ovan ingår en nivå på skada/konsekvens som heter "oacceptabel". Detta är ett sätt att säkerställa att verkningsfulla åtgärder sätts in för att bemöta hotet/risken.

Varje företag kan, och bör, särskilt utvärdera och själva välja antal nivåer och definition/beskrivning av respektive nivå för såväl sannolikhet som för skada/konsekvens. Det kan exempelvis finnas anledning att använda olika definitioner/beskrivningar av såväl sannolikhet som skada/konsekvens beroende på vilken typ av analysobjekt som berörs. I ett IT-system är hotbilden snabbt föränderlig över tiden och därför kan det vara värt att välja korta intervall i sannolikhetsbedömningen. När det exempelvis gäller en fast anläggning kanske intervallen kan väljas något frikostigare.

Under alla omständigheter bör stora komplexa matriser undvikas. Detta kommer främst av två anledningar.

1. Varje utfall i matrisen ska ha en egen betydelse, annars är den ju faktiskt överflödig och tillför i praktiken ingenting!
2. Varje tillförd nivå på sannolikhet eller skada/konskevens kommer ofelbart att ge upphov till tidsödande diskussioner som i slutändan inte förändrar åtgärders insättande, utformning eller uteblivande.

I alla avseenden är det viktigt att dokumentera vilka överväganden som görs inom ramen för vald metod och utformning av riskmatris.

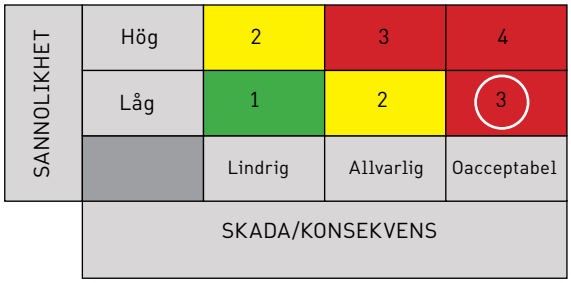
4.2.3 SCENARIO

Ett scenario är teoretiskt sätt en beskrivning som innehåller flera element som tillsammans samverkar för att dokumentera ett tänkt eller inträffat händelseförlopp. Ett mera praktiskt och tillämpligt sätt att beskriva scenario är att det innehåller hotformulering, någon kategorisering[3] av hotet, riskbedömning (sannolikhet och skada/konsekvens), brister och svagheter, följder, skadeverkningar och förslag till åtgärder. Riskanalysmetoden kallas i säkerhetskretsar för "scenariobaserad" av just denna anledning.

Liksom med riskmatrisen så är det viktigt att välja vilken typ av innehåll man vill ha i scenariobeskrivningen. Utöver vad som anges ovan är det inte ovanligt med att ange kostnader, ansvariga, tidsplaner m.m. i separata textfält. Oftast klarar man sig dock utmärkt med de som anges ovan då dessa värderingar kan läggas in i redan befintliga textfält.

Nedanstående tabell visar hur ett scenario kan vara uppbyggt med tidigare angivna textfält och ett fiktivt ifyllt scenario.

3. Exempelvis hot mot sekretess, tillgänglighet, riktighet eller spårbarhet. Vidare kan det vara fysiskt, administrativt, tekniskt eller organisatoriskt. Om ett hot spänner över flera kategorier brukar det anges som ett generellt hot.

SCENARIO NUMMER: 1	KATEGORI: TEKNISKT HOT / TILLGÄNGLIGHETSHOT
Hot:	Vatteninträngning i datahallen.
Brister och svagheter:	Datahallen ligger i källarplan i souterräng och grundväggarna är bristfälligt skyddade mot fuktinslag i samband med skyfall eller vårflod.
Följdverkningar:	Översvämning i datahall, troligen kortslutning i elektronisk utrustning.
Skador/ Konsekvenser:	Avbrott i IT-driften intill det att utrustning återställts eller ersatts och återställts.
Förslag till åtgärder:	Besiktiga grunden och vidta adekvata åtgärder mot fuktinslag. Pumpgrop ska tillföras så att även större vattenmängder kan avvärjas. Uppgiften tilldelas fastighetsavdelningen och ska vara avslutad före den 20 mars.
Riskvärdering	

Metodmässigt är det som ledare för en riskanalys viktigt att kunna förklara innebörden i de olika fälten i scenariot på ett begripligt sätt så att deltagarna i analysen förstår vilken information som hör hemma i respektive fält. De fält som redovisas i ovanstående exempel, utöver nummer och kategori, kan förklaras enligt följande:

> HOT
Är själva formuleringen av hotet som en eller flera deltagare har identifierat och formulerat.

> BRISTER OCH SVAGHETER
Det lättaste sättet att identifiera brister och svagheter är att ställa sig frågan; Vad, vilka brister och/eller svagheter, möjliggör att hotet/risken kan inträffa eller att hotet får redovisade skador?

> FÖLJDVERKNINGAR
Ofta är det viktigt att hålla isär följder och skador. Följder är vad som konkret inträffar om hotet/risken inträffar.

> SKADOR/KONSEKVENSER
Här ska eventuella värderingar fram. Oavsett om de är abstrakta, ekonomiska eller av personell, fysisk eller annan verksamhetsanknuten karaktär.

> FÖRSLAG TILL ÅTGÄRDER
Åtgärdsförslag formuleras enklast genom att titta på vad som angetts under brister och svagheter och på ett enkelt men tydligt sätt bemöta dessa med verkningsfulla åtgärdsförslag.

> RISKVÄRDERING
Sker i enlighet med kriterier och nivåer i vald matrismodell.

En riskanalys består av flera eller många hot/risker som ska dokumenteras så för var och en av dessa så upprättas ett scenario. Dokumentationen av analysen kan således ses som ett

bläddерblock som innehåller ett antal scenariobeskrivningar.

Det går att upprätta scenarier på papper, i vanliga program (Word, Excel m.m.) samt i verktyg för riskanalys.

4.2.4 INSIDER

I samband med riskanalys är det viktigt beakta insiderproblematik. Erfarenhet från många analyser ger vid handen att detta är ett befintligt problem.

En insider kan kortfattat definieras enligt följande.

> Insider är den som har tillgång till ett objekt eller en verksamhet, planerar eller genomför en handling som kan få negativa konsekvenser och som genom sitt värv eller utförande av gärning inte väcker uppmärksamhet eller misstänksamhet.

Mer om insiders finns att läsa i Kap. 3.2.1 Insiders i denna vägledning.

4.3 ANALYSOBJEKT

Med analysobjekt avses det som ska analyseras med avseende på hot och risker.

Ett sätt att exemplifiera olika sorters analysobjekt vilka metoden är tillämplig för är följande.

- SYSTEM
  Med system avses här olika typer av system såsom IT-system, informations- och ledningssystem, systemutrustningar m.m. Man kan här exempelvis se en radaranläggning eller en bomkonstruktion med transponderigenkänning för insläpp i ett garage som system.
- ANLÄGGNINGAR
  Alla former av lokaliteter som huserar en verksamhet och är konfigurerad för ändamålet kvalificerar sig i denna kategori. Exempel härvid är kontorskomplex, kontorslokal, skyddad anläggning och mobil anläggning såsom exempelvis en mobil ledningsplats.
- PERSONAL
  Detta kan utgöras av en personalfunktion i en organisation. Exempel på detta kan vara personal som i sitt värv riskerar hot av utomstående såsom personal vid skattekontor och socialkontor. Andra exempel är personal i call-centers som ibland råkar ut för stalkers[4] och motsvarande för enskilda anställda. OBS. I personskyddsverksamhet förekommer behov av särskild riskanalys i samband med exempelvis transporter, skydd på arbetsplats, i hemmet m.m.
- VERKSAMHET
  Med verksamhet kan avses en löpande eller specifik händelse som planlagts och utförs. Det kan till exempel vara en singulär händelse såsom en utrullning av en systemuppdatering eller ett systembyte. Vidare kan det vara en regelbundet återkommande eller löpande verksamhet. Exempel härvid kan vara uttransport och påfyllning av kontanter i bankomater.

Generellt för alla tillämpliga analysobjekt är att man måste kontrollera om det finns tillämplig lagstiftning som är styrande för analysobjektet i något avseende. Detta blir då ett styrande ingångsvärde att beakta då man definierar analysobjektet.

I samband med seminariegenomförandet av analysen bör någon med god insikt i analysobjektet ifråga föredra detta för deltagarna och redovisa om det finns några särskilda avgränsningar.

4.4 GENOMFÖRANDE

4.4.1 ANALYSGRUPP

Få saker betyder så mycket för kvaliteten i resultatet av analysen som analysgruppens sammansättning och analysledarens förmåga.

Personer som alltid bör ingå i analysgruppen är personer med säkerhetsansvar kopplat mot det berörda analysobjektet samt personer med kunskaper om objektet, tillämpliga interna och

4. Person som ensidigt uppvaktar eller förföljer en person mot dennes vilja eller utan dennes kännedom och medgivande.

externa faktorer som kan påverka objektet samt till objektet kopplade miljörelaterade aspekter och andra aspekter.

Oavsett vilket objekt som ska riskanalyseras så är det viktigt att för analysen sätta samman en analysgrupp med såväl bred som djup kunskap om objektet ifråga. Om man exempelvis ska göra en riskanalys på en datahall så kan dessa roller och befattningar utgöra exempel på lämpliga personer att ha med i analysgruppen.

- SÄKERHETSEXPERTIS
  Kan utgöras av företagets säkerhetschef, Informationssäkerhetschef, IT säkerhetschef, säkerhetsskyddschef eller inhyrd kompetens.
- BYGGNADSTEKNISK EXPERTIS
  Beroende på storlek och utförande kan det röra sig om person med uppgifter som rör fastighetens skötsel och integritet samt har kunskap om närliggande miljöaspekter som kan påverka objektet.
- IT KOMPETENS
  Någon eller några som vet vilka system som ska inrymmas eller finns i datahallen och hur de är beskaffade, vilka krav som ställs etc.
- EL, VVS, TELE
  Någon som deltar bör kunna svara på försörjningsfrågor eller besvara frågor som rör farhågor om vattengenomföringar, avlopp, ventilation, reservkraft, kanalisationer m.m.
- LÅS OCH LARM
  Tillträdesteknisk kompetens bör närvara vid seminariet.
- VD ELLER EKONOMISK FÖRETRÄDARE
  I riskanalysen krävs ofta att avdömningar om insatser grovt skattas och beslutas redan vid seminariet. Då är det lämpligt att ha någon med ekonomiskt beslutsmandat närvarande.
- FÖRETRÄDARE FÖR SLUTANVÄNDARE
  Slutanvändarna bör alltid vara representerade. I detta fall skulle de kunna representeras av drifttekniker som ska verka i datahallen och eventuellt någon som ska nyttja system som driftas i datahallen.

I alla lägen är det viktigt att inte dagtinga med sammansättningen av analysgruppen. Seminariet i analysen bygger på gruppdynamik och resultatet är beroende av att alla eventuella problemområden belyses och bedöms.

Det bör särskilt påpekas att om inte seminariet i analysen ska ta flera dagar att genomföra så bör storleken på analysgruppen inte överstiga 12 personer.

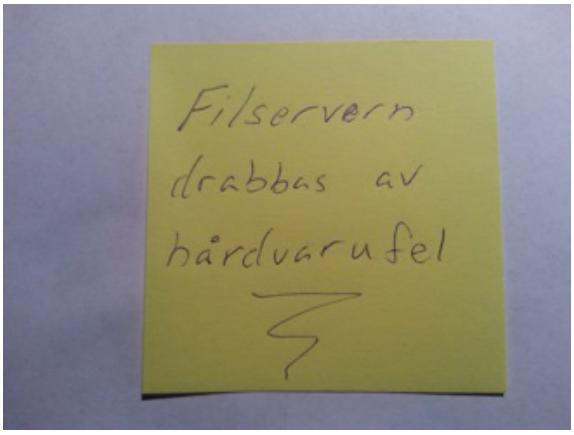
4.4.2 SEMINARIET

Analysseminariet utgör själva kärnan i analysen. Det är vid seminariets genomförande som grundmaterialet i analysen tas fram och fastställs. Seminariets genomförande utgörs huvudsakligen av:

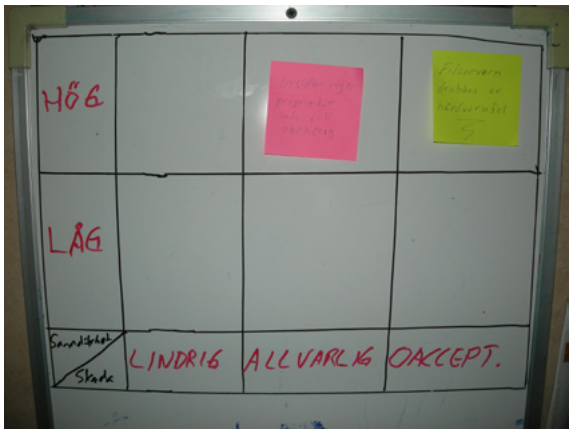
- Inledning med presentationer. Här presenteras deltagarna och deras roller beskrivs. Analysobjektet presenteras, definieras och vid behov dras riktlinjer för avgränsningar upp. Metodiken presenteras och deltagarna får till sig erforderliga begrepp och definitioner för att kunna delta aktivt i seminariet.

- Hotframtagning genom kreativövning, s.k. brainstorming. Denna övning är den viktigaste delen i analysen och kan kräva ett särskilt mått av uppmärksamhet från analysledaren. Det är viktigt att alla deltar aktivt och intresserat för att få ut så mycket som möjligt av deltagarna. Det är där den kunskap om analysobjektet som efterfrågas finns och det är analysledarens jobb att se till att den enskilde känner sig bekväm och säker i sitt sätt att förmedla

den. Normalt arbetar deltagarna inledningsvis ensamma och tecknar ned sina hotformuleringar, lämpligen på anteckningsblock eller post-it lappar. Därefter uppmuntras diskussion i delar av eller hela gruppen för att tillse att problemområden snarare överlappas än att ”saker faller mellan stolarna”.



> Riskvärdesframställning är när hoten bedöms avseende sannolikheten att inträffa samt skadan givet att hotet har inträffat. Detta sker i forum med alla deltagare. Det kommer an på analysledaren att vara uppmärksam på att bedömningarna är rimliga och att deltagarna är överens eller åtminstone till största delen överens om bedömningarna. Lämpligen ritas den riskmatris man valt för analysen upp på en whiteboard och post-it lapparna grupperas efter bedömt riskvärde.



> Detaljanalys genomförs efter riskvärdesframställning. Detaljanalysen omfattar bland annat orsaker och verkan av den specifika risken, men även förslag på åtgärder. Det är i detaljanalysen som scenarierna, som beskrivits ovan, upprättas. Detta kan ske i exempelvis Word, Excel eller i ett verktyg för riskanalys. Normalt genomförs inte detaljanalys på hela mängden framtagna och definierade risker. Denna avgränsning görs av två skäl. 1) Tidsbrist, detaljanalysen är normalt sett mycket tidskrävande. 2) reellt behov av detaljanalys. Risker som värderas lågt föranleder ofta inga aktiva åtgärder då de har begränsad skadeverkan eller låg sannolikhet att inträffa. Kriterier för avgränsningar av denna typ bör tillämpas eller upprättas i samband med analysgenomförandet.

Avslutande av seminariet med genomgång av konfidentialitetsbehov m.m. Innehållet i den färdiga analysen utgör i allt väsentligt en instruktion i hur man förstör eller på annat sätt negativt påverkar objektet eller därtill beroende verksamhet, det är därför viktigt att för deltagarna påtala det behov av konfidentialitet som föreligger.

4.5 EFTERBEARBETNING

4.5.1 RAPPORT

Efterbearbetningen utgörs som tidigare nämnts främst av framställning av rapport efter genomförd analys. Normalt sett utgörs rapporten av två huvudsakliga delar. Rapport och scenarier. I rapporten bör all information framgå som en läsare som inte själv deltagit i analysen behöver för att förstå innehållet, metoden, resultatet och behovet av åtgärder. Vidare bör det framgå vilka som deltagit och om några särskilda beslut fattats angående analysens innehåll. För att öka förståelsen för analysens utfall avseende riskvärdering och sårbarheter så bör det finnas en grafisk representation av dessa. En sammanställning av riskerna med därtill hörande riskvärden bör finnas i tabellform med möjlighet att sortera efter exempelvis kategori eller risk-

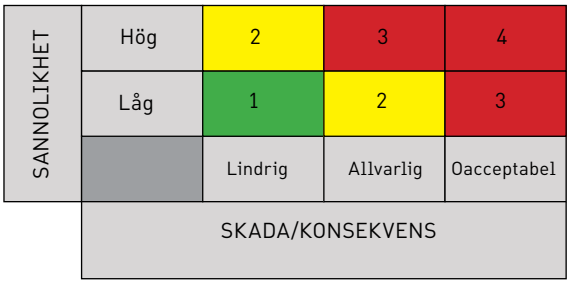
värde.

Nedan följer ett förenklat exempel på en disposition av en rapport efter en riskanalys.

1. Inledning
    a. Analysgrupp och objekt
        Deltagare
        Analysledare
        Objektbeskrivning med ev. avgränsningar
    b. Beskrivning av metoden
        Generell beskrivning av metoden och eventuella tillförda definitioner
        Utformning och kriterier för riskmatris
2. Utfall
    a. Risktabell

NR.	KAT.	HOT	RISKVÄRDE
1	Se	Insider röjer information	3
2	Ti	DDoS-attack mot servicefront	3
3	Ri	Handläggare gör fel	1

    b.Riskmatris



    c. Särskilda beaktanden
        Här anges exempelvis om något som ligger utanför metodiken eller definitionerna tillämpats och varför. Andra särskilda händelser, exempelvis kan analysledaren ha färdigställt lågprioriterade scenarier själv och endast delgivit dem på "remiss" till deltagare.

3. Sammanfattning och slutsatser
    a. Sammanfattning
        En sammanfattande bild av vilka risker som identifierats och analyserats. Ska svara på frågan – Hur ser det ut hot- och riskmässigt?

    b. Slutsatser
        Slutsatser som framförallt analysledaren drar från resultatet med rekommendationer riktade utifrån de sammantagna förslagen till åtgärder och erfarenhet.

4. Scenarier

De färdiga scenarierna sammanställs i ett appendix som ingår i dokumentet eller i en bilaga till detsamma. Analysledaren ska efter analysen inte påverka innehållet i scenarierna annat än en stavnings- och grammatikkontroll. Detta i syfte att alla som läser analysrapporten ska kunna bygga en egen bild utifrån det som de-facto dokumenterats direkt i samband med analysseminariet.

När analysen är färdigbearbetad bör den föredras för den som beordrat eller beställt genomförandet. Detta främst i syfte att undanröja eventuella orsaker till missuppfattningar i exempelvis språkliga formuleringar eller sakinnehåll. Härvid bör även rapporten formellt bedömas avseende konfidentialitetsnivå och vilka delgivningsregler som ska gälla för den.

4.5.2 ÅTGÄRDER SOM FÖLJD AV RESULTATET

Efter genomförd analys bör man upprätta en åtgärdsplan. Här bör man formulera åtgärder som låter sig förstås även av personer som inte deltog vid seminarietillfället. Det är således bra att ange en ansvarig befattning och eventuell tidplan. Vidare kan finansiering av åtgärder beröras. Man bör dock tänka på att hålla formuleringarna någorlunda korta och kärnfulla.

Det är viktigt att åtgärdsplanen följs upp och att framtida revisioner av redan genomförda riskanalyser återspeglar eventuella förbättringar i redan identifierad hot- och riskbild.

4.6 SAMMANFATTNING

För att underlätta genomförandet av riskanalys så finns det två saker som bör belysas i sammanhanget.

- Det underlättar genomförandet avsevärt om man har tillgång till ett verktygsstöd, program, för genomförandet och dokumentationen av riskanalysen.
- Om man inte själv har en person i företaget som regelbundet genomför sådana riskanalyser och är van vid detta så kan man överväga att köpa in ledning av riskanalys som en tjänst.

Vidare är det är en bra idé att skapa någon typ av förvaltningsprocedur för riskanalyser i sin verksamhet så att regelbundenhet i revidering av dessa blir ett modus operandi i verksamheten. Regelbundenheten borgar dessutom för att verksamheten efter en viss inlärningsperiod kommer att känna sig hemma i metodiken som används. Detta kommer i sin tur att leda till att analyserna genomförs snabbare och ändå med bättre kvalitet och precision.

En riskanalys är att betrakta som en färskvara, den har ett bäst-före datum. Avståndet tidsmässigt till sådant datum kan dock skilja sig åt beroende på vilken typ av analysobjekt som avses. Med den teknikutveckling som råder när denna vägledning skrivs är exempelvis en tumregel att riskanalys för ett godtyckligt IT-system har ett bäst-före datum som sträcker sig ca 6 månader framåt i tiden från det att den upprättats. Detta naturligtvis under förutsättning att inga omvälvande händelser som kan komma att påverka systemet inträffar under tiden, exempelvis ett paradigmskifte i tekniken. Fördelen med att regelbundet uppdatera sina riskanalyser är utöver de som nämnts i föregående stycke att riskerna hålls bevakade genom ett ökat mått av påminnelse och medvetandegörande hos de som berörs av dem.

5 STYRDOKUMENT

I detta avsnitt anges vilka styrande dokument som ligger till grund för detaljerade krav på säkerhet inom olika områden. Det är viktigt att påpeka följande. Med styrdokument avses sådana dokument som genom sin rättsliga status legalt styr verksamheten. Det är således ett tjänstefel, en förseelse eller ett brott att inte uppfylla krav som bygger på sådana styrdokument.

Inom olika tillämpliga standarder används ofta begreppet policy. Det bör här påpekas att en policy inte utgör ett styrdokument enligt vad som anges ovan utan oftast definieras som ett dokument som anger ledningens viljeinriktning och stöd för informationssäkerhet i enlighet med verksamhetskrav och relevanta lagar och föreskrifter. Ett företag kan dock i sitt interna regelverk ange att en policy är styrande och ska följas. Frågan måste då ställas om namnet policy är tillämpligt då det ofta definieras som en avsiktsförklaring och riktlinjer för att styra beslut och uppnå önskade mål.

5.1 FÖRFATTNINGAR SOM STYR IS/IT-SÄKERHETSARBETET SAMT SÄKERHETSSKYDDET

5.1.1 INLEDNING

Det är inte alltid helt uppenbart hur styrande regelverk kommer till eller vari de har sin validitet. Som en orientering redovisas därför detta här.

De svenska reglerna består av lagar, förordningar (regeringsförordningar) och föreskrifter beslutade av myndigheter. Det samlade begreppet för dessa olika sorters regler är författningar.

En lag är beslutad av riksdagen, till exempel säkerhetsskyddslagen. Den har ofta karaktären av "ramlag", som innehåller få detaljer och måste fyllas ut med utförligare regler.

En förordning har beslutats av regeringen och innehåller mer detaljerade regler. Säkerhetsskyddsförordningen säger också att myndigheter får utfärda ytterligare föreskrifter.

Föreskrifter beslutas av myndigheter.

I detta kapitel anges endast sådana lagar, förordningar och andra krav som är direkt tillämpligt inom IS/IT-säkerhetsarbetet samt säkerhetsskyddet för företag över vilka Svenska kraftnät utövar tillsyn. Det finns ytterligare beroenden till andra lagar och rättsliga krav men för att höja kapitlets läsbarhet återges här endast utdrag ur Skyddslagen, säkerhetsskyddsförordningen, personuppgiftslagen och Svenska kraftnäts föreskrifter.

5.1.2 LAGSTIFTNING OCH FÖRORDNINGAR

Skyddslag (2010:305):
http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Skyddslag-2010305_sfs-2010-305/?bet=2010:305

Skyddslagen innehåller bestämmelser om åtgärder som syftar till förstärkt skydd för byggnader, andra anläggningar, områden och andra objekt. Svenska kraftnät har i samarbete med Svensk Energi tagit fram en vägledning för skyddsobjekt.
http://www.svk.se/Global/01_Om_oss/Pdf/Sakerhetsskydd/Vagledning-skyddsobjekt-inom-energiforsorjningen.pdf

Nämnda vägledning innehåller en information som ett elbolag kan behöva i samband med bedömningar om vad som bör utgöra ett skyddsobjekt. Vägledningen belyser tydligt problemet med att lagtexter inte följer hotbildens snabba och föränderliga utveckling över tiden. Det ankommer således på respektive ägare av " byggnader, andra anläggningar, områden och andra objekt" som avses i lagen att göra adekvata analyser av deras betydelse, och då inte endast med stöd av betydelseklassificeringen utan även med tanke på vilken påverkan exempelvis ett sabotage kan få givet vissa förutsättningar såsom säsongsbaserade förändringar. Ett geografiskt område kan beroende på säsong motsvara endera glesbygd eller å andra sidan en hårt belastad tätort med försörjningsleder (el, tele, VA, logistik) som är av typen (eng.)Single Point Of Failure. Exempel härvid kan vara populära skidorter där hotbilden måste bedömas mot såväl anläggningarnas kapacitet och skydd som mot exempelvis hot om allvarlig miljöhändelse (exempelvis svår storm) eller sabotage.

Ägaren till en anläggning eller motsvarande som anges i första stycket bör alltid där så är tillämpligt göra bedömningen om objektet ifråga ska bli föremål för ansökan om skyddsobjektsklassificering. Denna bedömning bör även göras för varje objekt som framstår som intressant i samband med genomförande av säkerhetsanalys enligt säkerhetsskyddsförordningen (1996:633).

Säkerhetsskyddsförordningen (1996:633) :
http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Sakerhetsskyddsforordning-199_sfs-1996-633/

Säkerhetsskyddsförordningen ger bestämmelser till säkerhetsskyddslagen (1996:627). Det innebär att säkerhetsskyddsförordningen anger mer detaljerade regler och även ger myndigheter möjligheter till utökade regler i form av föreskrifter för säkerhetsskyddet.

Säkerhetsskyddsrelaterade publikationer på Svenska kraftnäts webbplats:
http://svk.se/Om-oss/Var-verksamhet/Sakerhetsskydd/

Vad gäller hantering av personuppgifter så har detta sedan slutet på 1990-talet reglerats i personuppgiftslagen.

Personuppgiftslagen (1998:204) :
http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Personuppgiftslag-1998204_sfs-1998-204/

5.1.3 SVKFS

Affärsverket Svenska kraftnäts föreskrifter och allmänna råd om säkerhetsskydd SvKFS 2013:1 är föreskrifter som Svenska kraftnät utfärdar och som gäller för enskilda och juridiska personer som bedriver elförsörjningsverksamhet vilken omfattas av säkerhetsskyddslagen (1996:627).

De nya föreskrifterna, SvKFS 2013:1, präglas till fullo av en företagsinriktad tillämpning både i sak och i språk. Allt i syfte att minimera risken för missuppfattningar.

> OBS! Företag för vilka Svenska kraftnät är tillsynsmyndighet är skyldiga att följa föreskrifterna.

5.2 POLICYDOKUMENT OCH MOTSVARANDE

ISO 27000 standarden anger informationssäkerhetspolicy som ett central styrande dokument.

Målet med informationssäkerhetspolicyn är att ange ledningens viljeinriktning och stöd för informationssäkerhet i enlighet med verksamhetskrav och relevanta lagar och föreskrifter.

Ledningen bör fastställa en tydlig policyin-

riktning i enlighet med verksamhetsmål och visa sitt stöd och engagemang för informationssäkerhet genom att utfärda och underhålla en informationssäkerhetspolicy för hela organisationen.

6 SÄKERHETSANALYS ENLIGT 5 § SÄKERHETS-SKYDDSFÖRORDNINGEN

6.1 INLEDNING

Säkerhetsanalys definieras enligt 5 § säkerhetsskyddsförordningen (1996:633) enligt följande.

> Myndigheter och andra som förordningen gäller för skall undersöka vilka uppgifter i deras verksamhet som skall hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism. Resultatet av denna undersökning (säkerhetsanalys) skall dokumenteras.

Viktigt att notera här är bland annat skrivningen "och andra som förordningen gäller för". Att genomföra säkerhetsanalys enligt förordningen åligger de företag för vilka Svenska kraftnät äger föreskriftsrätt.

Svenska kraftnät har gett ut en vägledning om Säkerhetsanalys. Den finns publicerad på Svenska kraftnäts webbplats och kan hittas genom följande länk.

http://www.svk.se/Global/01_Om_oss/Pdf/Sakerhetsskydd/Sakerhetsanalys.pdf

Detta kapitel i vägledningen är mera komprimerat och förenklat i sitt utförande av säkerhetsanalysen. Vidare läggs här mer fokus på teknikutveckling som kan ha bäring på arbetet med säkerhetsanalysen i en mera samtida version. Kapitlet består i valda delar av utklipp från nämnda vägledning.

6.2 TILLÄMPLIGHET OCH GENOMFÖRANDEKRAV

Enligt SvKFS 2013:1 ska bl.a. företagen inom elförsörjningen genomföra en säkerhetsanalys. Analysen ska klarlägga vilka uppgifter i verksamheten som ska hållas hemliga med hänsyn till rikets säkerhet och vilka anläggningar som kräver ett säkerhetsskydd med hänsyn till rikets säkerhet eller skyddet mot terrorism. Resultatet av säkerhetsanalysen ska dokumenteras.

Enligt Svenska kraftnäts föreskrifter (SvKFS 2013:1) om säkerhetsskydd ska en säkerhetsanalys genomföras minst vartannat år.

Som komplement för att underlätta bedömning om tillämplighet har en checklista upprättats. Checklistan innehåller ett stort antal kriterier som lätt kan gås igenom och bockas av. På detta sätt kan företag, med stöd av checklistan, få en invisning om det är lämpligt att genomföra en dokumenterad säkerhetsanalys enligt gängse dokumentationspraxis, alltså minst i nivå med exempeldisposition i denna vägledning eller Svenska kraftnäts vägledning för säkerhetsanalys.

Det bör här påpekas att checklistan också minner om att ta hänsyn till hot och risker mot verksamheten. I Svenska kraftnäts vägledning för säkerhetsanalys kan följande utläsas. "Delar av underlaget för säkerhetsanalysen kan

inhämtas även från företagens riskanalysarbete". I de metoder, utbildningar, instruktioner och vägledningar som olika myndigheter upprättat för säkerhetsanalys och därtill kopplat genomförande anger i stort sett alla att säkerhetsanalysen ska bygga på adekvata bedömningar av hot och risker mot verksamheten. Det kan sägas att en säkerhetsanalys inte kan genomföras på ett korrekt sätt om sådana beaktanden inte har genomförts.

Riskanalys beskrivs bland annat vidare i kapitel 4 Riskanalys i denna vägledning samt i bilaga 1, metodreferenser, till denna vägledning.

6.3 GENOMFÖRANDE AV SÄKERHETSANALYS

Det yttersta ansvaret för att genomföra säkerhetsanalys åvilar företagets VD. Naturligtvis är utfallet och kvaliteten på säkerhetsanalysen direkt avhängig att kompetenser och erfarenhet från hela företagets verksamhet deltar i arbetet. Härvid bör särskilt påpekas att IS/IT-resurser deltar aktivt i arbetet då i stort sett all hantering och förvaring av information idag sker i någon form av IT-system.

Frågan som ska besvaras i en säkerhetsanalys är; Rör detta rikets säkerhet eller skyddet mot terrorism? Det blir i detta sammanhang väldigt tydligt att det behövs olika typer av kriterier för att göra sådana bedömningar. Till stöd för detta finns Svenska kraftnäts vägledning för säkerhetsanalys som innehåller listor med information av olika slag. Dessa listor har även plats för egna kommentarer om man vill använda dem som arbetsmaterial i säkerhetsanalysen. Vidare bör tillgängliga riskanalyser och checklistan för säkerhetsanalys användas.

Det viktigaste att tänka på i samband med genomförandet är att alla delar av företagets verksamhet belyses, granskas och bedöms inom ramen för säkerhetsanalysen. Detta gäller oavsett om säkerhetsanalysen utgörs av ett PM som kort konstaterar att sådana uppgifter inte finns i företagets verksamhet eller om analysen är ett omfattande dokument med många ingående delar.

Det går inte nog att understryka behovet av att beakta IS/IT-säkerheten vid genomförandet av säkerhetsanalys. I efterföljande punktsatser anges några nyckelord och frågor som endast syftar till att väcka eftertanke i samband med genomförandet av säkerhetsanalys. Upptäckta diskrepanser kan behöva undersökas ytterligare i sammanhanget och/eller i en kompletterande riskanalys.

- Hur står sig det tekniska skyddet av information i IT-system gentemot den skyddsnivå som råder för motsvarande eller omgivande anläggning?
- Uppgifter om eller förmåga till dödnätsstart.
- Regional, gränsande till nationell, betydelse.
- Flaskhals, (eng.)Single Point Of Failure, i nätet som kan påverka andra aktörer på ett mer eller mindre okänt sätt.
- Hantering av information i och utanför IT-system (USB-minnen, e-post, delning, gallring, förvaring, hemarbete etc.)

Sammanfattningsvis kan genomförandet i korthet sägas vara:

- Inventera resurser, information och anläggningar.
- Bedöm typen och egenskaperna utifrån kriterier.
- Bedöm betydelsen utifrån begreppen rikets säkerhet eller skyddet mot terrorism (glöm inte att beakta riskanalysen).
- Dokumentera utfallet.
- Upprepa processen vid behov eller vartannat år.

6.4 DISPOSITION AV SÄKERHETSANALYS

I Svenska kraftnäts vägledning för säkerhetsanalys finns ett bra exempel på en disposition för säkerhetsanalys. Som bilaga 2 till denna vägledning finns ett exempel på en fiktivt genomförd säkerhetsanalys för ett mindre företag att titta på för inspiration och idéer om det egna

utförandet.

I korthet och det enkla fallet räcker dock normalt sett följande.

- Inledning med formalia.
- Beskrivning av företaget och tillämpligheten.
- Utfallet, exempelvis i tabellform.
- Planerade åtgärder eller referens till åtgärdsplan.
- Angivet datum eller kriterium för att upprepa genomförandet av säkerhetsanalysen.

6.5 ÅTGÄRDER EFTER GENOMFÖRD SÄKEHETSANALYS

SvKFS 2013:1 ställer krav på att en säkerhetsanalys genomförs och dokumenteras. Naturligtvis ska företaget efter genomförd analys upprätta en handlings- och åtgärdsplan samt vidta åtgärder för att öka säkerhetsskyddet i enlighet med analysresultatet och kraven i säkerhetsskyddslagen (1996:627).

Som bilaga 2 till denna vägledning finns ett exempel på en fiktiv åtgärdsplan.

7 ORGANISATION

Kapitlet syftar till att ge exempel på hur en fungerande säkerhetsorganisation för ett företag i elbranschen kan uppnås och vidmakthållas. Vidare syftar kapitlet till att beskriva en del av de problem som finns och som kan uppstå i samband med utformning av eller förändringar inom säkerhetsorganisationen i elbranschföretag.

Vissa befattningar som beskrivs i kapitlet är inte tillämpliga för alla företag. Exempel på detta är befattningen säkerhetsskyddschef som är tillämplig om företaget äger eller på annat sätt hanterar ett skyddsobjekt, anläggning som rör skyddet mot terrorism och/eller hanterar information eller uppgifter som rör rikets säkerhet eller skyddet mot terrorism.

7.1 ALLMÄNT OM ANSVARSFÖRHÅLLANDEN

7.1.1 INLEDNING

Inom elbranschen varierar storleken mellan olika företag från några få personer till stora globala koncerner med tiotusentals anställda. Detta medför att sättet att besätta olika befattningar varierar kraftigt beroende på storleken på företaget. För ett litet företag kan det i extremfallet vara så att en enda person ensam har alla säkerhetsrelaterade uppdrag, i.e. tillikabefattningar. En person kan således vara Säkerhetsskyddschef tillika informationssäkerhetschef tillika IT-säkerhetschef etc. I sådana fall är det vanligt, och lämpligt, att befattningen endast benämns säkerhetschef vilket i sådana fall ger en tydligare beskrivning av ansvarsområdet. För stora företag är det inte ovanligt att det finns koncernbefattningar och befattningar på delföretagsnivå vilket gör att det på samma företag exempelvis kan finnas flera IT-säkerhetschefer men som vardera är ansvariga för olika organisationsenheter eller funktionsområden inom företaget. I dessa fall är det också vanligt att det finns en övergripande säkerhetschef som har ett helhetsansvar gentemot ledningen. Läsaren bör ge akt på att i de fall det inte finns någon säkerhetsskyddschef så är det vanligt, och lämpligt, att det ändå finns en säkerhetschef.

Ett område som ofta blir föremål för kontrovers är placeringen och mandatet för respektive befattning/ansvarsområde vad gäller säkerhetsarbetet. Generellt är det en sak som måste påpekas; säkerhetsorganisationen måste ges möjlighet att föra upp frågor till ledningen, såväl för avdömning då mandatet inte räcker till som i rent informerande syfte för att stötta den strategiska verksamhetsledningen med beslutsunderlag i olika sammanhang.

Ett vanligt problem med placeringen av och mandatet för respektive befattning/ansvarsområde är att säkerhetsfunktionen som sådan, helt eller delvis, förläggs organisatoriskt under ett annat ansvarsområde. Det är då viktigt att kommunikationen mellan säkerhetsfunktionen och övriga verksamhetsområden inte häm-

mas som följd av detta. Erfarenheten ger vid handen att en kommunikationskanal till den operativa ledningen gör att säkerhetsarbetet totalt sett främjas. Detta oavsett var i organisationen säkerhetsfunktionen formellt befinner sig. Beroende på storlek på företag så kan en sådan kommunikationskanal till och med vara informell men den bör vara dokumenterad och beslutad på rätt nivå. På detta sätt minskas riskerna att säkerhetsrelaterade ärenden förfelas genom långa handläggningskedjor.

Ledningen för ett företag har å sin sida en uppgift i att mål för säkerheten finns, är tillgängliga, uppdaterade och fastställda. Vidare är det ledningens uppgift att säkerställa att säkerhetsarbetet ges tillräckliga resurser för att utföra det säkerhetsarbete som krävs för att uppnå och vidmakthålla de mål som finns för säkerheten.

7.2 VANLIGT FÖREKOMMANDE ROLLER INOM SÄKERHETS-ORGANISATIONEN

De ansvarsområden som beskrivs är de som traditionellt säkerhetsmässigt är tillämpliga och vanligt förekommande i all säkerhetsrelaterad verksamhet. Det går dock inte att utesluta att det finns andra behov inom verksamheter av särskild karaktär. De ansvarsområden som här redovisas ska således ses som en lämplig generell uppdelning av områden som kan utökas om det finns behov.

För små och medelstora företag är det inte ovanligt att resurser saknas för att ha en säkerhetsorganisation där olika roller är knutna till olika personer med specialistkompetens inom respektive område. Det är snarare mer vanligt att en person har flera eller alla säkerhetsrelaterade ansvarsområden i sina arbetsuppgifter, vanligen kallat tillika-befattningar. Detta behöver inte medföra några nackdelar så länge man ser till att den som har dessa uppgifter också har möjlighet att lösa ålagda uppgifter inom ramen för sin befattning. Ett sätt att skapa mätbarhet och framförallt tydlighet är att se till att det finns uppdaterade och korrekta roller beskrivna som kan knytas till befattningar för sådana tjänster Se vidare 12.7.1 Befattningar, roller och rollbeskrivningar i denna vägledning. Det finns några vanliga fallgropar som kan kopplas till tillika-befattningar, se vidare 7.2.6 Kommentarer kring tillika-befattningar nedan.

Ett problem som förekommer i alla verksamheter, statliga som civila, är segmentering mellan ansvarsområden som vanligen kallas stuprörsproblematik. Stuprörsproblematik går i korthet ut på att respektive ansvarsområde verkar autonomt och samverkan mellan ansvarsområdena är minimal. Detta leder ofelbart till missförstånd, merarbete eller dubbelarbete samt ineffektivitet i säkerhetsarbetet. Det finns traditionellt sett en huvudsaklig uppdelning som återfinns i de flesta organisationer som har dessa ansvarsområden. Säkerhetsskydd och annan fysisk säkerhet utgör ett läger medan informationssäkerhet och IT-säkerhet utgör ett annat. Inte vid något tillfälle i tiden torde denna uppdelning ha medfört några fördelar men nu mer än någonsin är den rent av farlig. Dagens hotbilder spänner över flera olika ansvarsområden och påverkar samtliga dessa i större eller mindre omfattning. Här krävs en samverkan mellan de olika ansvarsområdena som inte bara är etablerad utan väl prövad genom exempelvis övningar. Vidare bör det finnas någon typ av forum som löpande och med en hög frekvens av regelbundenhet möts och samverkar om hotbilder, incidenter av olika slag samt planerar säkerhetsverksamheten över tiden. Ärenden kommer alltid att organisatoriskt och verksamhetsmässigt höra hemma i ett av de berörda ansvarsområdena men säkerheten totalt kommer att gynnas ju högre graden av samverkan mellan de olika ansvarsområdena är. Ett hinder mot nämnda samverkan som anförts i flera fall är att det föreligger sekretess för uppgifter inom säkerhetsskyddet och således har på denna grund andra ansvarsområden stängts ute. Detta är ett exempel på en direkt dålig lösning som dessutom saknar saklig grund. Behörig är den som bedömts som lämplig, är placerad i säkerhetsklass och behöver uppgifterna för sin tjänst. Med de asymmetriska hotbilder som präglar samhället i dag måste risken för implicita hot och risker, (eng.)cascading events, utgöra grund för att information mellan de olika ansvarsområdena delas inom lämpliga forum för att nå synergieffekter i det totala säkerhetsarbetet. Detta

medför inget brott mot sekretessen utan utgör ett adekvat exempel på en korrekt tillämpning av densamma.

En framgångsfaktor är att samverkan sker mellan de olika ansvarsområdena på ett sätt som gör att hela säkerhetsfunktionen har en ständig uppdaterad bild av säkerhetsläget som helhet för företaget och dess verksamhet. Härvid erinras också om att det är av yttersta vikt att befattningar befästs med mandat som ger den aktuella befattningen en lämplig handlingsfrihet inom sitt ansvarsområde. Detta är inte minst viktigt sett mot exempelvis snabba IT-hot som kan kräva omedelbara handlingskraftiga åtgärder.

7.2.1 SÄKERHETSCHEF / SÄKERHETSSKYDDSCHEF

7.2.2 SÄKERHETSCHEF

Begreppet och tillika befattningen säkerhetschef kan åsyfta flera saker. Å ena ändan på skalan kan den åsyfta en global koncerns högsta säkerhetsansvarige. Denne kan i sin tur ha flera säkerhetschefer av olika art underställda, exempelvis säkerhetsskyddschef(er) eller informationssäkerhetschef(er). Å andra ändan på skalan återfinns exempelvis mindre elföretag där en enskild person kan ha flera befattningar i företaget varav säkerhetschef utgör en tillika-befattning.

I det första fallet där säkerhetschef utgör en koncerns högst säkerhetsansvarige kan man förutsätta att arbetet bedrivs på en strategisk nivå med en holistisk syn på säkerhetens alla områden sett över en längre tidsperiod.

I det andra fallet där det handlar om en säkerhetschef för ett lite mindre företag så kan de ingående arbetsuppgifterna i stort sett utgöras av en mix av arbetsuppgifter från alla säkerhetsmässiga ansvarsområden. Erfarenheten och utfall från olika typer av analyser ger vid handen att säkerhetschefer av den här kategorin ofta har en mycket hög arbetsbelastning och att fokus ofta inriktas på det fysiska skyddet såsom lås, larm och byggnadstekniska åtgärder. Dessa präglas dessutom inte sällan av ett reaktivt beteende istället för ett proaktivt dito. Anledningen kan naturligtvis härledas till arbetsbelastning och faktorer kopplade till problematik med tillika-befattningar. Det bör här påpekas att mindre företag nogsamt bör följa upp och utvärdera hur utfallet av tillika-befattningar eller ett sammantaget säkerhetsansvar samlat hos en person faller ut i verkligheten. Om det finns tvivel huruvida en tillika-befattning eller singulär person kan hantera det totala säkerhetsarbetet vid företaget så bör förändringar (utökningar) i säkerhetsorganisationen kraftigt övervägas.

Begreppet säkerhetschef kan naturligtvis innebära ett spann av uppgifter mellan de här angivna exemplen vilket i sig påvisar behovet av att, oavsett om man är ett stort eller litet företag, formulera noggranna rollbeskrivningar som kan knytas till befattning och vad viktigare är; att se till att dessa följs. Om det uppstår behov som ligger utanför beskrivningarna som ska omhändertas av samma befattning inom given ram så medför det nästan alltid att arbetsbelastningen blir ohållbar med kvalitetsbrister och fel som följd och ökad risk för, och inträffande av, incidenter som yttersta följd.

7.2.3 SÄKERHETSSKYDDSCHEF

För att grundläggande förstå säkerhetsskyddschefens roll erinras inledningsvis om följande:

Med säkerhetsskydd avses enligt 6 § säkerhetsskyddslagen:

1. skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet,
2. skydd i andra fall av uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) och som rör rikets säkerhet, och
3. skydd mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott (terrorism), även om brotten inte hotar rikets säkerhet.

Begreppet säkerhetsanalys är definierat i säkerhetsskyddsförordningen (1996:633) och utgör ett verktyg för att kontrollera vilka uppgifter som berörs inom en verksamhet.

Här kan man omgående vederlägga behovet av en väl etablerad samverkan mellan olika säkerhetsområden då flera av formuleringarna

ovan kan innefatta exempelvis planläggning och genomförande av någon typ av aktion riktad mot ett kraftverk. I planläggningen kan detta omfatta elektroniska åtgärder, IT-baserat spionage eller (eng.)social engineering. Vidare kan detta omfatta antagonistiska åtgärder med förstörande verkan som påverkar såväl fysisk integritet som elektronisk dito.

Traditionellt brukar säkerhetsskydd handla det fysiska skyddet med fokus på byggnadstekniska åtgärder, lås och larm samt perimeterskydd. Vidare omfattas även hantering av handlingar som rör rikets säkerhet eller skyddet mot terrorism.

I dagens samhälle är det lätt att inse att samverkansbehovet över ansvarsområdena präglas av att hela den säkerhetsrelaterade verksamheten diskuteras i sådana samverkansforum så att alla aspekter, risker och konsekvenser av exempelvis ett hot ges uppmärksamhet och utreds ur alla synvinklar.

Ett tungt ansvar vilar på säkerhetsskyddschefen som utöver de egna föreskrifterna och styrande regelverk styrs av lagstiftning och andra myndighetsförfattningar. Tillsyn och kontroller av verksamheten sker med stöd av olika statliga myndigheter beroende på verksamhetens art. För en förteckning över tillämpliga lagar och andra rättsliga krav som är tillämpliga för säkerhetsskyddet hänvisas till 5 Styrdokument i denna vägledning.

7.2.4 INFORMATIONSSÄKERHETSCHEF

Informationssäkerhetschefen ansvarar för styrningen av all säkerhet som rör hantering av information. Informationssäkerhetschefen ansvarar bland annat för att se till att det finns ett styrande företagsspecifikt regelverk som omfattar all informationshantering. Vidare ansvarar informationssäkerhetschefen för att regelverket förmedlas och efterlevs. Således ingår även utbildning, uppföljning och kontroll i informationssäkerhetschefens arbetsuppgifter. Det är således ett omfattande ansvarsområde som kan åskådliggöras av följande nyckelord för information oavsett den är pappersbunden eller digitalt hanterad.

- UPPRÄTTANDE
  Innefattar all form av skapande av information.
- INFORMATIONSKLASSIFICERING
  Bedömning av informationens skyddsvärde och indelning efter detta.
- FÖRVARING OCH ANNAN HANTERING
  Exempelvis vilken nivå på skydd ett förvaringsskåp ska ha.
- UTLÄMNING OCH DELGIVNING
  Regler som rör behörigheter för att ta del av olika typer av information.
- KVITTERING OCH FÖRTECKNING
  Metodik för att säkerställa spårbarhet. Ger svar på frågan vem, var och när?
- SPRIDNING
  Hur ska information av olika typer spridas och delges exempelvis större grupper?
- INVENTERING
  Kontrollfunktion för att säkerställa att viktiga handlingar hanteras på rätt sätt och ej har förkommit.
- ARKIVERING
  Hur ska information som ej längre används eller är aktuell hanteras? Arkivering för eftervärld, forskning eller andra ändamål.
- FÖRSÄNDNING
  Innebär regler för all typ av skickande av information. Vad ska exempelvis gälla om man försänder en skyddsvärd handling med posten?
- MEDFÖRANDE INOM OCH UTOM RIKET
  Regler för hur information får flöda både nationellt och internationellt samt vad som särskilt gäller personlig hantering i sådana fall.
- FÖRSTÖRING
  Viss information ska förstöras när den inte längre behövs. Vilka regler ska gälla för förstöring av olika typer av information?

Det är mot ovanstående lätt att inse vidden av det ansvar som åvilar informationssäkerhetschefen. Vidare är det likaledes lätt att se att samverkansbehovet med andra ansvarsområden är stort, i dagens samhälle inte minst med

IT-säkerhetschefen men även med säkerhetsskyddschefen.

En annan viktig uppgift som ligger inom informationssäkerhetschefens område är ansvar för att tillhandahålla eller styra metodik som ska användas i olika tillämpning där information hanteras, exempelvis hot-, risk- och sårbarhetsanalys.

7.2.5 IT-SÄKERHETSCHEF

IT-säkerhetschefen ansvarar för säkerheten i och kring de IT-system som företaget hanterar och förfogar över. IT-säkerhetschefens arbete styrs härvid av det regelverk som styr informationshanteringen. Det är således IT-säkerhetschefens uppgift att översätta och upprätta motsvarande regelverk för berörda IT-system. Detta kan vara en grannlaga uppgift då olika informationsklassificeringar motsvarar olika hanteringsregler. Det innebär kortfattat att olika IT-system kan ha olika skyddsnivå beroende på vilken typ av information de är avsedda att hantera. Exempel på ett säkerhetsrelaterat beslut i ett IT-system kan röra dess konduktivitet, i.e. om det exempelvis ska vara anslutet till Internet eller inte.

En stor del av IT-säkerhetschefens arbete rör tillgänglighet i de system som används för informationshantering. Med tillgänglighet avses här att systemen fungerar på avsett sätt och att de som arbetar i systemen kan verka där på avsett sätt. En annan uppgift som åligger IT-säkerhetschefen är spårbarhet i IT-systemen. Med spårbarhet avses här bland annat all form av logghantering som återspeglar användares och programs aktiviteter i ett IT-system.

En annan viktig uppgift för IT-säkerhetschefen är arkitektur. Det kan skilja avsevärt i utformningen av IT-system beroende på vilken typ av information systemet är avsett att hantera samt vilka andra krav på säkerhet som ställs på ett IT-system, då främst tillgänglighet men även riktighet och spårbarhet.

IT-säkerhetschefen samverkar främst med informationssäkerhetschefen men kan även behöva samverka med säkerhetsskyddschefen i olika sammanhang. Oavsett vilken information som ska hanteras så är det snarast ett axiom i dagens samhälle att den kommer att hanteras i ett IT-system. Att vara IT-säkerhetschef för ett företag som hanterar mer än ringa mängder information är ett omfattande arbete.

7.2.6 KOMMENTARER KRING TILLIKA-BEFATTNINGAR

En sak som man dock bör företa i samband med utformning av tillika-befattning är en analys av vilka risker, och även möjligheter, ett beslut om tillika-befattning medför. En sådan analys bör om möjligt genomföras av en oberoende part för att inte färgas av jäv och personliga viljor inom företaget.

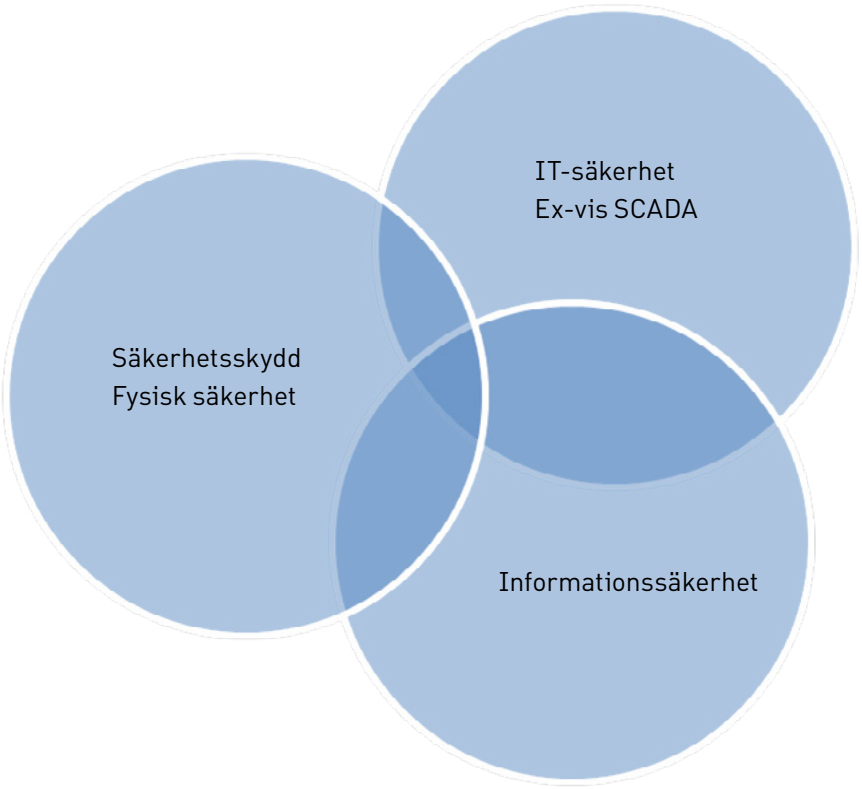
Om man väljer att ha tillika-befattningar så är det av yttersta vikt för säkerheten att roller som knyts till sådan befattning följs upp regelbundet. Så fort en avvikelse från befintliga rollbeskrivningar kan konstateras så måste man överväga att man tar risker som inte analyserats då befattning/en/arna skapades.

En vanlig fälla i organisationssammanhang är att den som ställer kraven på en funktion eller motsvarande också är den som realiserar lösningen. Det innebär i praktiken att kravställning och utförande sker av samma person/er. Således finns ingen egentlig, trovärdig, möjlighet till formell granskning eller formellt godkännande av lösningen från kravställarens sida. Detta problem bör särskilt uppmärksammas i samband med att tillika-befattningar skapas.

Det måste här framhållas att en noggrann, och framförallt regelbunden, uppföljning sker av tillika-befattningar i syfte att tidigt upptäcka avvikelser som kan medföra onödiga risktaganden.

7.2.7 OMRÅDESUPPGIFTER OCH ORGANISATIONSENHETSUPPGIFTER

Som tidigare nämnts kan det finnas särskilda behov av andra befattningar än ovan uppräknade. Exempel på detta kan vara en befattning som har ett säkerhetsansvar för ett geografiskt objekt eller en särskild organisationsenhet. Nedan följer en uppräkning som utgör exempel på sådana befattningar.



Figur 6. Beroenden.

- Säkerhetssamordnare[5] för ett laboratorium eller en forskningsenhet
- Områdesansvarig för ett företags utlokaliserade resurs, exempelvis en konferensanläggning.
- Säkerhetsansvarig i utvecklingsprojekt, exempelvis för framtagning av egenutvecklade IT-system.
- Dammsäkerhetsansvarig. En befattning som har ansvar för en damms integritet och generella säkerhet.
- Bevakningsansvarig. Exempelvis säkerhetsansvar för inpasseringen till ett större anläggningskomplex.

Läsaren bör ge akt på att i alla ovan uppräknade fall så måste man räkna med att alla säkerhetsområden kan komma i fråga. En person som får en sådan befattning måste således kunna hantera frågor inom alla dessa områden. Se figur 6.

7.3 SAMMANFATTNING

Att utforma eller förändra sin organisation för att förbättra eller rent av upprätta en fungerande säkerhetsorganisation är en uppgift som bör tas på största allvar och ges erforderlig eftertanke innan beslut fattas. Man bör beakta att allt säkerhetsarbete utgår från de krav som ställs på organisationen dels i form av lagar och andra rättsliga krav och dels i form av ledningens vilja och inriktning, s.k. (eng.)policy.

Fallgropar som bör undvikas är bland andra att blanda samman kravställande och utförande roller samt att tilldela för stora eller omfattande arbetsuppgifter inom ramen för tillika-befattningar.

Ansvar, mandat, befattning, rollbeskrivningar och uppgifter bör alltid dokumenteras.

Det bör finnas möjlighet till regelbunden aktiv samverkan mellan de olika säkerhetsområdena.

5. Detta är ett typiskt exempel på en ROLL. En person som har en befattning i ett sådant laboratorium kan även få rollen som säkerhetssamordnare.

8 UPPGIFTER SOM RÖR RIKETS SÄKERHET ELLER SKYDDET MOT TERRORISM

8.1 BEGREPPSFÖRKLARING

Begreppet uppgifter som rör rikets säkerhet eller skyddet mot terrorism motsvarar i allt väsentligt den definition som för myndigheter anger vad en hemlig uppgift är.

I praktiken betyder detta att uppgifter som rör rikets säkerhet eller skyddet mot terrorism, exempelvis konstaterade genom säkerhetsanalys, är av samma typ som de uppgifter som hos myndigheter kallas hemliga uppgifter.

8.2 HEMLIGA UPPGIFTER OCH ÖVRIGA UPPGIFTER

Det finns i huvudsak tre kategorier av skyddsvärda uppgifter som kan beröra företag i elbranschen.

- Hemliga uppgifter, dvs. uppgifter som är hemliga enligt offentlighets- och sekretesslagen (2009:400).
- Uppgifter som rör rikets säkerhet eller skyddet mot terrorism som konstaterats genom säkerhetsanalys.
- Övriga skyddsvärda uppgifter som förekommer i ett företags verksamhet.

Hemliga uppgifter kan endast upprättas och ägas av en myndighet. Det är således definitionsmässigt omöjligt för ett företag att själva äga hemliga uppgifter. Ett företag kan däremot ta del av, hantera och förvara, hemliga uppgifter inom ramen för ett SUA[6]-uppdrag. I dessa fall är företaget skyldigt att följa de hanterings- och förvaringsregler som anges i avtalet. Dessa regler är och ska vara lika som för svensk myndighet.

Uppgifter som rör rikets säkerhet eller skyddet mot terrorism och vars förekomst konstaterats genom säkerhetsanalys vid företag i elbranschen ägs av det berörda företaget. Dessa uppgifters hantering och förvaring regleras i Svenska kraftnäts föreskrifter SvKFS 2013:1. Här lämnas möjligheter för företagen att inom givna ramar i enlighet med nämnda föreskrifter utforma säkerheten som omgärdar sådana uppgifter.

Övriga skyddsvärda uppgifter som förekommer i ett företags verksamhet kan exempelvis utgöras av proprietär information som skyddas av Lagen om skydd för företagshemligheter (1990:409). För sådana uppgifter beslutar företaget självt om vilket skydd som ska tillämpas.

8.3 FÖRHÅLLANDET MYNDIGHET – FÖRETAG

Svensk säkerhetsskyddslagstiftning medger inte att en hemlig uppgift, per definition, upprättas av, och ägs av, annan än myndighet. Alltså inte ett företag. Detta innebär dock inte att vare sig uppgifternas betydelse eller skyddsvärde

6. Säkerhetsskyddad upphandling med säkerhetsskyddsavtal.

är annorlunda än för motsvarande hemliga uppgifter.

För uppgifter som rör rikets säkerhet eller skyddet mot terrorism så är Svenska kraftnäts förskrifter 2013:1 Affärsverket svenska kraftnäts föreskrifter och allmänna råd om säkerhetsskydd tvingande.

Detta innebär att skyddsåtgärder som tas fram eller finns och som syftar till att ge ett skydd åt uppgifter som rör rikets säkerhet eller skyddet mot terrorism, oavsett vilken form sådan uppgift förekommer i, ska stå i paritet med säkerhetsskyddsåtgärder såsom de regleras i nämnda föreskrifter. Sådana skyddsåtgärder omfattar:

- FYSISKT SKYDD
  Hur uppgifter ska skyddas mot otillbörlig åtkomst med stöd av byggnadstekniska åtgärder.
- ADMINISTRATIVT SKYDD
  Att det finns dokumenterade och tillämpliga rutiner för hur hantering av uppgifter får ske.
- TEKNISKT SKYDD
  Uppgifter som hanteras i exempelvis IT-system ska omges med ett därför tillämpligt skydd och tillämplig segmentering från andra system och uppgifter.
- ORGANISATORISKT SKYDD
  Det ska finnas en säkerhetsorganisation som är utsedd för att reglera hanteringen av uppgifter som rör rikets säkerhet eller skyddet mot terrorism.

8.4 REGISTERKONTROLL OCH SUA (SÄKERHETSSKYDDAD UPPHANDLING MED SÄKERHETSSKYDDSAVTAL)

8.4.1 SUA

Utdrag ur Säkerhetspolisens vägledning för säkerhetsskyddad upphandling med säkerhetsskyddsavtal, SUA.

> En myndighet som avser att begära in anbud eller genomföra en upphandling måste ta ställning till om det i anbudet eller upphandlingen förekommer hemliga uppgifter. Om så är fallet, ska dessa uppgifter ha samma säkerhetsskydd hos företaget där uppdraget eller tjänsten utförs som hos myndigheten. Ansvaret för detta ligger på myndigheten.

Detta innebär i praktiken att säkerhetsskyddsavtalet är en handling som Svenska kraftnät ansvarar för i samband med att Svenska kraftnät ingår avtal med företag där uppgifter som rör rikets säkerhet eller skyddet mot terrorism kan förekomma.

En följd av detta är att det är ytterst viktigt att företagen genomför och dokumenterar säkerhetsanalys enligt 5§ säkerhetsskyddsförordningen (1996:633) och informerar Svenska kraftnät om utfallet från denna, eller förändringar i densamma i samband med revision. Med revision avses här förnyelse, förnyad analysgenomgång, av säkerhetsanalysen som enligt gällande föreskrifter ska ske minst vartannat år.

8.4.2 REGISTERKONTROLL

Säkerhetsprövning är en kontroll av en person som ska befatta sig med verksamhet eller få ta del av uppgifter som berör ett rikes säkerhet eller skyddet mot terrorism. Syftet med kontrollen är att bilda sig en uppfattning om personens lämplighet för uppgiften och om denne kan anses vara lojal och pålitlig.

Nedan följer ett utdrag ur Svenska kraftnäts föreskrifter som beskriver vilka befattningar som ska registerkontrolleras, och för vilken säkerhetsklass de ska registerkontrolleras.

Inplacering i säkerhetsklass 2 inom elförsörjningen

Nedanstående befattningar eller annat deltagande i verksamhet inom elförsörjningen ska placeras i säkerhetsklass 2.

- Säkerhetsskyddschef som i sin tjänsteutövning får del av uppgifter som har betydelse för rikets säkerhet.
- Verksamhetens chef (VD eller motsvarande) som i sin tjänsteutövning får del av uppgifter som har betydelse för rikets säkerhet.

- Befattningar vid säkerhetsskyddad upphandling jämlikt 8 § säkerhetsskyddslagen som får del av uppgifter som omfattas av sekretess och som är av synnerlig betydelse för rikets säkerhet.
- Befattningar som ingår i elförsörjningens gemensamma krisorganisation.
- Befattningar som regelmässigt hanterar uppgifter som rör rikets säkerhet eller som särskilt behöver skyddas mot terrorism, t.ex. beredskapsplanläggning.
- Befattningar som får del av uppgifter som rör rikets säkerhet eller som särskilt behöver skyddas mot terrorism vid utredning, utbildning eller övning.
- Befattningar som utför ej enbart tillfälliga arbeten vid ett flertal sådana anläggningar som förklarats som skyddsobjekt enligt 4 § 4 skyddslagen (2010:305) och som därvid kan få del av uppgifter som rör rikets säkerhet eller som särskilt behöver skyddas mot terrorism.
- Befattningar som i arbete med IT-system, tele/datakommunikation eller på annat sätt får en sådan insyn i överföringssystem av el att de vid utförande av sina arbetsuppgifter kan få del av uppgifter som rör rikets säkerhet eller som särskilt behöver skyddas mot terrorism.

Till befattningar i säkerhetsklass 2 hänförs också vikariat och/eller ersättare om denne får ta del av uppgifter i samma omfattning som den ordinarie innehavaren av befattningen.

Inplacering i säkerhetsklass 3 inom elförsörjningen

Nedanstående befattningar eller annat deltagande i verksamhet inom elförsörjningen ska inplaceras i säkerhetsklass 3.

- Befattningar som omfattar tillfälliga arbeten vid ett flertal sådana anläggningar som förklarats som skyddsobjekt enligt 4 § 4 skyddslagen (2010:305) och som därvid kan få del av uppgifter som rör rikets säkerhet eller som särskilt behöver skyddas mot terrorism.
- Befattningar som innefattar besök eller på annat sätt tillträde till ett flertal sådana anläggningar som förklarats som skyddsobjekt enligt 4 § 4 skyddslagen (2010:305) och som därvid kan få del av uppgifter som rör rikets säkerhet eller som särskilt behöver skyddas mot terrorism.
- Befattningar hos enskilda eller juridiska personer som har träffat säkerhetsskyddsavtal med Svenska kraftnät och/eller andra myndigheter och som innebär att man kan få del av uppgifter som rör rikets säkerhet eller som särskilt behöver skyddas mot terrorism.
- Befattningar i lednings-, styrelsefunktion eller motsvarande som medför att innehavaren i sin utövning kan få del av uppgifter som rör rikets säkerhet eller som särskilt behöver skyddas mot terrorism.
- Personer som i utbildning vid universitet, högskolor eller motsvarande vid examens-, special- eller tentamensarbete kan få del av uppgifter som rör rikets säkerhet eller som särskilt behöver skyddas mot terrorism.

Till befattningar i säkerhetsklass 3 hänförs också vikariat och/eller ersättare om denne får ta del av uppgifter i samma omfattning som den ordinarie innehavaren av befattningen.

8.5 FÖRVARING AV HANDLINGAR (ÄVEN I IT-SYSTEM)

Med förvaring avses här lagring av uppgifter som rör rikets säkerhet eller skyddet mot terrorism oavsett vilken form eller vilket medium som uppgifterna berör.

I allt väsentligt så hanteras uppgifter som rör rikets säkerhet eller skyddet mot terrorism endera i IT-system eller i pappersbunden form. Det kan förekomma sådana uppgifter i annan form, exempelvis en beskaffenhet eller egenskap på en anläggning.

I SvKFS 2013:1 9§ framgår följande:

> Handling som rör rikets säkerhet eller skyddet mot terrorism, i skrift eller bild, ska förvaras i ett förvaringsutrymme med en sådan skyddsnivå att den inte obehörigen röjs, ändras eller förstörs. Endast behörig personal får ha tillgång till dessa utrymmen.
>
> Handling som är av synnerlig betydelse för rikets säkerhet ska förvaras i utrymme till vilket endast behörig personal i säkerhetsklass 1 och 2 har tillgång.
>
> Skyddsnivån ska motsvara lägst säkerhetsskåp Svensk Standard SS 3492.
>
> Ytterligare säkerhetsskyddsåtgärder för förvaringen ska vidtas om säkerhetsanalysen ger anledning till det.

Det bör i detta sammanhang påpekas att för myndigheter som exempelvis Försvarsmakten så gäller förvaring i säkerhetsskåp enligt Svensk Standard SS 3492 även för handlingar som inte är av synnerlig betydelse för rikets säkerhet.

SvKFS ger företagen ett visst utrymme för tolkning av vad som avses med en ”sådan skyddsnivå”. Generellt påpekas dock följande.

En skyddsnivå som medger att en handling **inte obehörigen röjs, ändras eller förstörs** är beroende av flera faktorer som måste beaktas noggrant i varje enskilt fall.

De mest tongivande faktorerna att väga in i bedömningen är följande: **[Med uppgifter avses här uppgifter som rör rikets säkerhet eller skyddet mot terrorism]**

- Om uppgifter förvaras i markplan i ett normalt kontorskomplex eller motsvarande lokaler och utrymmet där uppgifterna förvaras inte särskilt har skyddats bör förvaring ske i förankrat säkerhetsskåp SS3492 där larm utlöses vid otillbörlig åtkomst. Med särskilt skyddat utrymme avses exempelvis plåtslagning av standardväggar med 2 mm stålplåt och säkerhetsdörr istället för vanlig dörr. Om sådana särskilda åtgärder vidtagits kan förvaring i låst tunnplåtsskåp medges under förutsättning att utrymmet är larmat.
- Om flera handläggare eller motsvarande hanterar och förvarar uppgifter så bör respektive kontorsutrymme eller motsvarande förses säkerhetsskåp SS3492 där larm utlöses vid otillbörlig åtkomst, exempelvis volymlarm i rum eller larmkontakt på dörr och andra larmdetektorer på fönster eller andra tillämpliga åtkomstmöjligheter till utrymmet. Om utrymmet är beläget med nedre del av fönster närmare mark än 4 meter så bör fönstret förstärkas med exempelvis intrångsfördröjande film eller lexanplast.
- Om handläggare eller motsvarande hanterar uppgifter på en bärbar dator så ska datorn, eller om datorn är försedd med löstagbar hårddisk eller motsvarande, hårddisk eller motsvarande i sig betraktas som den uppgift som ska skyddas och förvaras enligt de två föregående punkterna. Här bör särskilt beaktas att i berörd dator ska alla ingående databärande media (multipla hårddiskar, (eng.)flashdrives eller motsvarande) betraktas som, och hanteras som uppgifter enligt de två föregående punkterna.
- Om uppgifter förvaras och hanteras i IT-system, exempelvis traditionellt klient-server system för kontorsstöd så ska även databärande centrala resurser (servrar, NAS, SAN etc.) förvaras i ett utrymme som motsvarar erforderlig skyddsnivå. Detta kan uppnås genom en kombination av flera åtgärder. Fysiskt skydd (plåtslagna väggar eller betongväggar, -golv och –tak samt lämplig säkerhetsdörr i klass 2 eller högre) Inre skydd i form av inlåsning av resurser i säkerhetsklassat dataskåp (SS3492), datorskyddsskåp (lägre skyddsnivå än SS3492 men högre än låst rack eller tunnplåtsskåp) eller låsta rackkonstruktioner. Tillämplig larmning av utrymme och resurser. Se även 13 IT-säkerhet.
- Säkerhetskopior, oavsett mediatyp, som innehåller uppgifter ska omges med ett skydd som motsvarar 1 och 2 punkterna. När det gäller säkerhetskopior så är

rekommendationen förankrat säkerhetsskåp SS 3492 i ett larmat och brandskyddat utrymme eller skyddsskåp i ett larmat, brandskyddat och på annat sätt skyddat (plåtslagna väggar eller betongväggar, -golv och –tak samt lämplig säkerhetsdörr i klass 2 eller högre) utrymme.

Ofta betraktas kostnad för säker förvaring som en avskräckande faktor. Sanningen är dock att de bonuseffekter som säker förvaring ger oftast mer än väl uppväger eventuella kostnader. Vidare är det viktigt att anpassa storleken på eventuella skåp och utrymmen efter behov. Många med branscherfarenhet tänker omedelbart på ett manshögt kylskåpsbrett säkerhetsskåp (SS3492) när begreppet kommer på tal. Det finns dock i dagsläget många leverantörer och modeller att välja emellan. Nedan följer några exempel på prisuppgifter för olika förvaringar från 2013-2014.

Mindre säkerhetsskåp (SS3492) mindre än 5000 SEK

Större säkerhetsskåp (SS3492) ca 8000 SEK

Brandsäkra dokumentskåp som också medger ett skydd där de kan kallas skyddsskåp (dock ej till nivå SS 3492) kostar ungefär lika mycket.

Datorskyddskåp (dock ej till nivå SS 3492) kostar för inrymmande av några få servrar eller motsvarande ca 5000 SEK. För skyddsnivå SS 3492 kostar ett sådant skåp ca 15000 SEK.

Datorskyddskåp SS 3492 och för inrymmande av tiotalet servrar kostar ca 20000 SEK.

Det är, sett mot ovanstående prisexempel, inte särskilt dyrt att etbalera ett lämpligt förvaringsskydd för uppgifter som rör rikets säkerhet eller skyddet mot terrorism. Man bör dock beakta att förvaringen bara utgör en del av skyddet och att administrativa, tekniska och organisatoriska åtgärder också måste vidtas för att uppnå ett acceptabelt skydd.

Förvaring av uppgifter som rör rikets säkerhet eller skyddet mot terrorism bör alltid ske så att den sammantagna skyddsnivån motsvarar SS 3492. Det innebär således att i många fall kommer detta att ske genom kombinationer av olika åtgärder. Generellt gäller dock att det inte ska vara möjligt att otillbörligt ge sig tillgång till sådana uppgifter utan att larm utlöses och åtgärd initieras.

8.6 INVENTERING

Enligt SvKFS 2013:1 ska uppgifter som rör rikets säkerhet eller skyddet mot terrorism inventeras.

Företag ska besluta om med vilken periodicitet inventering ska genomföras, det synes dock olämpligt att låta denna period överstiga två år vilket är den maximala kalendertid en säkerhetsanalys gäller innan den måste revideras (förnyas).

Resultatet av inventeringen ska dokumenteras och sparas minst till dess att förnyad inventering genomförts.

Fel och brister som upptäcks i samband med inventering ska hanteras som incident och i tillämpliga fall rapporteras till Svenska kraftnät i enlighet med 12 § SvKFS 2013:1.

8.7 KVITTERING OCH UPPFÖLJNING

För att inventering ska vara möjlig att genomföra så måste kvittering av uppgifter som rör rikets säkerhet eller skyddet mot terrorism ske.

Detta innebär att den som förvarar eller på annat sätt tar del av eller hanterar en uppgift som rör rikets säkerhet eller skyddet mot terrorism ska kvittera detta.

Kvittering sker på lista (tabell eller motsvarande) där minst följande framgår:

- Vilken uppgift som avses (Dokument-ID, diarienr eller motsvarande).
- När uppgiften lämnats ut eller upprättats.
- Vem som kvitterat, mottagaren.
- Vem som bemyndigat utlämnandet eller upprättandet.
- Datum/Tid för upprättande eller utlämnande.
- Datum/Tid för återlämnande.
- Om uppgiften destruerats.

Följande kan med fördel också anges på kvittenslistan:

> När inventering ska ske/har skett.
> I förekommande fall vilken informationsklassificering som gäller.
> Om det är lämpligt, kontaktuppgifter till mottagaren.

För uppgifter som ska delges flera personer ansätts lämpligen en kvittens/delgivningslista på uppgiften som kvitteras i samband med överlämnande/cirkulering och som arkiveras när delgivning eller cirkulation av uppgiften är slutförd.

Om information som berörs av kvittering och uppföljning enligt ovan är digitalt hanterad och förvarad så krävs vissa funktioner och aktiva handgrepp i det aktuella systemet för att nå motsvarande effekt.

> Inventering i sådant system sker i stort sett som med pappersbundna handlingar, dvs. en aktiv kontroll av att uppgiften är befintlig i systemet, på den logiska area som den avses hanteras och lagras på samt att den endast är åtkomlig för den som är behörig att ta del av densamma.
> Användning av systemet och åtkomst till sådana uppgifter ska tekniskt loggas på en sådan nivå att det kan motsvara en manuell kvittering av pappershandling. Detta innebär att personlig identifieringsinformation, behörighetsinformation, information om ändringsarbete (jmfr. RWX på operativsystemnivå) och tidsstämplar måste loggas.
> Information till användaren om att systemet hanterar berörd information, att loggning sker och i vilket syfte loggningen sker bör automatiskt förmedlas exempelvis i samband med inloggning. Se även Kap. 12.6 Hantering av tillgångar (eng.)Asset management.
> Uppföljning av loggar ska ske på regelbunden basis där åtkomst till berörda uppgifter kontrolleras. Beroende på volymer och omfattning så kan sådan uppföljning ske på stickprovsbasis. Regelbundenheten måste dock motsvara syftet med uppföljningen och bör bygga egen analys av behovet. Den bör dock aldrig överstiga ett år.

8.8 DESTRUKTION AV HANDLINGAR OCH UPPGIFTER

8.8.1 PAPPERSBUNDNA HANDLINGAR

Pappersbundna handlingar destrueras i dokumentförstörare.

Efter destruktion i sådan dokumentsförstörare ska restprodukter utgöras av spån med en bredd av högst 1,2 mm och en längd av högst 15 mm alternativt högst 2 x 2 mm kvadratiska spån.

8.8.2 UPPGIFTER LAGRADE PÅ IT-MEDIA

Hårddiskar och andra digitala lagringsmedia innehåller ofta ämnen som är miljöfarliga eller på annat sätt giftiga eller hälsovådliga. Destruktion av sådana datamedia bör därför överlåtas på återvinningsföretag som specialiserat sig på detta.

Det finns återvinningsföretag som kommer till kunden med utrustning för destruktion på plats under kundens överinseende så att det inte finns någon risk för otillbörlig åtkomst av information i samband med hanteringen.

Det finns en fördel i att välja en leverantör, eller utrustning, som redan används av organisationer eller myndigheter med höga säkerhetskrav för motsvarande tjänster. Fördelen med att göra detta är att organisationer och myndigheter såsom exempelvis Försvarsmakten och Polisen redan har lång erfarenhet på området och har valt leverantörer som svarar upp mot deras krav. Då leverantörsberoendet varierar över tiden rekommenderas att kontakta sådan myndighet för att kontrollera vilka leverantörer som används i detta avseende. Ett annat alternativ är att själv analysera leverantörers förmåga, pris och tillgänglighet och välja utifrån resultatet av den egna analysen.

8.9 MEDFÖRANDE AV HANDLINGAR

8.9.1 ALLMÄNT

Här avses alla tillämpliga fall då uppgifter tas med på tjänsteförrättning eller motsvarande, av personer som är behöriga till uppgifterna.

Det som ska styra hanteringsregler när det gäller medförande är att det inte ska vara möjligt att stjäla uppgifterna genom spontant tillgrepp eller motsvarande. Särskilda hanteringsregler ska beslutas av varje enskilt företag men det går inte att frångå att uppgifterna, oavsett i vilken form de hanteras, ska hållas under ständig uppsikt och skyddas mot spontant tillgrepp. Observera att tillämpningen av nedanstående kan variera beroende på vilken typ av transportmedel som används, om man är flera behöriga personer som reser tillsammans och om man färdas utom riket. Det är dock avsikten med typfallen som ska styra hanteringen. Således gäller exempelvis i samband med flygtransport, ständig uppsikt och kontroll över berörda handlingar, uppgifter eller databärande media.

De typfall som kan förekomma är följande.

Medförande av uppgifter i det dagliga värvet.

Här avses i allt väsentligt besök vid egna anläggningar, förflyttning inom verksamhetsområden eller motsvarande.

Här gäller att de berörda uppgifterna är under ständig uppsikt av den som hanterar dem. Här följer några exempel på hur hanteringen kan gå till och hur den inte får gå till.

- Pappershandlingar och datorer, surfplattor eller motsvarande bärs med i samband med att arbete utförs.
- Pappershandlingar och datorer, surfplattor eller motsvarande förvaras tillfälligtvis i fordon eller motsvarande i där inbyggt, fastskruvat, låst utrymme. Detta kan exempelvis vara en låst plåtlåda. Fordon eller motsvarande ska vara larmad och hållas under uppsikt hela tiden.
- Pappershandlingar och datorer, surfplattor eller motsvarande förvaras tillfälligtvis i låst tunnplåtsskåp eller motsvarande inuti anläggningsbyggnad som i övrigt är låst. Om byggnaden är olarmad ska den hållas under uppsikt.
- Man får **inte** lämna, ens tillfälligtvis, pappershandlingar och datorer, surfplattor eller motsvarande i fordon eller motsvarande.
- Man får **inte** lämna, ens tillfälligtvis, pappershandlingar och datorer, surfplattor eller motsvarande i anläggningsbyggnader som inte i sig själva motsvarar hela säkerhetsskyddet (inklusive krav på administrativ, teknisk och organisatorisk säkerhet).
- Man får **inte** förvara pappershandlingar och datorer, surfplattor eller motsvarande i förvaringsbox i offentliga utrymmen eller motsvarande.

Medförande av uppgifter på tjänsteresa inom landet.

Här avses i allt väsentligt besök, möten eller annan samverkan vid samverkansparters eller myndigheters anläggningar, kontorsbyggnader eller motsvarande. Här avses även övernattning på hotell eller motsvarande anläggning.

- Pappershandlingar och datorer, surfplattor eller motsvarande bärs med i samband med att arbete utförs.
- Pappershandlingar och datorer, surfplattor eller motsvarande förvaras tillfälligtvis i fordon eller motsvarande i där inbyggt, fastskruvat, låst utrymme. Detta kan exempelvis vara en låst plåtlåda. Fordon eller motsvarande ska vara larmad och hållas under uppsikt hela tiden. Detta kan således endast ske i samband med verksamhet som innebär att stora delar av verksamheten ska ske med stöd av fordon.
- Pappershandlingar och datorer, surfplattor eller motsvarande förvaras tillfälligtvis i låst tunnplåtsskåp eller motsvarande inuti anläggningsbyggnad som i övrigt är låst. Om byggnaden är olarmad ska den hållas under uppsikt. En förutsättning här är att det inte finns obehöriga personer som har tillgång till utrymmet.

- Man får **inte** lämna, ens tillfälligtvis, pappershandlingar och datorer, surfplattor eller motsvarande i fordon eller motsvarande.
- Man får **inte** lämna, ens tillfälligtvis, pappershandlingar och datorer, surfplattor eller motsvarande i anläggningsbyggnader som inte i sig själva motsvarar hela säkerhetsskyddet (inklusive krav på administrativ, teknisk och organisatorisk säkerhet). En förutsättning här är att det inte finns obehöriga personer som har tillgång till utrymmet eller att delningsutrymme eller eget utrymme tilldelas i skyddsskåp eller säkerhetsskåp.
- Man får **inte** förvara pappershandlingar och datorer, surfplattor eller motsvarande i förvaringsbox i offentliga utrymmen eller motsvarande.

Medförande av uppgifter på tjänsteresa eller förrättning utom landet.

Här avses i allt väsentligt besök, möten eller annan samverkan vid samverkansparters eller myndigheters anläggningar, kontorsbyggnader eller motsvarande i utlandet. Här avses även övernattning på hotell eller motsvarande anläggning.

- Pappershandlingar och datorer, surfplattor eller motsvarande bärs med i samband med att arbete utförs.
- Datamedia bör vara krypterat. (Hårddisk i bärbar dator eller motsvarande. USB-minne etc.)
- Pappershandlingar och datorer, surfplattor eller motsvarande får inte lämnas på hotellrum eller utrymme hos organisation som besöks.

Det går att exemplifiera en sund hantering av uppgifter, oavsett lagringsmedia, på följande enkla sätt:

Ponera att uppgifterna du bär med dig är en väska innehållande en tipsvinst på en kvarts miljon kronor i kontanter, din plånbok, dina bankuppgifter och bank-ID, dina nycklar hem med adresslapp, dina bilnycklar samt en lapp innehållande alla dina lösenord och övriga inloggningsuppgifter.

Sättet du hade valt att hantera en sådan väska kommer förmodligen att hamna nära den eftersökta hanteringen för uppgifter som rör rikets säkerhet eller skyddet mot terrorism.

8.9.2 MEDFÖRANDE TILL LÄNDER SOM INTE ”GODKÄNNER” KRYPTERING

Det finns idag ett antal länder som kräver att en inresande person på anmodan ska lämna ut lösenord, kryptonyckel, token eller motsvarande till medfört datamedia (exempelvis bärbar dator eller USB-drive). På detta vis ger sig dessa länders säkerhetstjänst tillgång till den information som du medför in i det landet.

Idag är de två mest framträdande exemplen på detta USA och Storbritannien. Här tillämpas lagstiftning med hårda straff om man inte på anmodan ger ut nämnda lösenord etc.

Även om en sådan anmodan inte sker regelmässigt så bör man beakta denna risk då man reser till sådana länder. I företrädande fall bör en annan kanal för informationshantering väljas som exempelvis (eng.) Dead-Drop funktion på Internet, krypterad förbindelse med egna resurser i hemlandet m.m.

Man bör i sammanhanget alltid beakta att många säkerhetstjänster, bland annat den amerikanska, har uttalade mål att aktivt hjälpa och främja domestiska företag i sina affärer utanför USA. Detta kan vara ett ingångsvärde i den analys man bör göra innan man fattar beslut om vilken, och i vilken form, information ska medföras till annat land. En sådan analys bör även innefatta en menbedömning som pekar på vilket men

som kan uppstå om uppgifterna röjs till obehöriga. Fördelen här är att menbedömningen kan göras i förväg genom att ponera att uppgifterna röjs i samband med en resa till annat land. På detta sätt erhålls ett mycket bra beslutsunderlag om huruvida berörda uppgifter ska medföras eller inte och i så fall i vilken omfattning.

Det enklaste sättet att genomföra en menbedömning är att tillämpa ett "värstafallsantagande", (eng.)Worst case scenario. Anta att vi ska resa till ett land där vi kan tvingas att lämna ifrån oss uppgifter vid inpassering över landets gräns. Anta vidare att det sociala klimatet kan innebära en hög risk för rån och andra former av spontant tillgrepp av stöldbegärlig utrustning såsom exempelvis bärbara datorer eller mobila surfplattor. Det ger oss två enkla fall att ta ställning till.

- Uppgifter kopieras av landets säkerhetstjänst och delges sedan andra organisationer i syfte att främja domestiska intressen och/eller motverka våra intressen.
- Uppgifter som finns på utrustning som stjäls kommer kriminella tillhanda som sedan kan sälja eller på annat sätt delge och distribuera den vidare.

I båda fallen ovan så är konsekvensen att vi måste anta att berörda uppgifter röjs till obehörig och att det inte går att utesluta att de sedan används i ett för oss kontraproduktivt syfte. Det går således heller inte att utesluta att förlusten av uppgifterna innebär men för rikets säkerhet eller för skyddet mot terrorism.

Mot bakgrund av ovanstående analys fattas sedan ett riskhanteringsbeslut om huruvida uppgifter ska medföras och i så fall i vilken omfattning.

9 PERSONAL

9.1 INLEDNING

Inom elbranschen varierar storleken mellan olika företag från några få personer till stora globala koncerner med tiotusentals anställda. Detta medför att det svårligen går att definiera riktlinjer som är fullt ut tillämpliga oavsett storlek på organisationen.

Detta kapitel strävar mot en allmängiltig tillämpning även om kapitlet är skrivet med små och medelstora företag i åtanke.

9.2 MEDARBETARE

Med medarbetare avses här personer som är anställda i företaget, inhyrd personal, såsom personal hos entreprenörer, konsulter på långtidsbasis, eller annan personal från exempelvis bemanningsföretag som föranleder att en medarbetarliknande roll måste antas.

I det moderna arbetslivet sker många aktiviteter och verksamheter med stöd av projekt, tillfälligt sammansatta grupper eller dito på längre sikt. I slutändan bör sådana personer som aktivt deltar i företagets verksamhet i mer än ringa omfattning och/eller med någon regelbundenhet betraktas som medarbetare.

I fall som ovan kan det vara motiverat att i **tillämpliga** delar använda vad som anges i detta stycke.

9.2.1 UTBILDNING

Som nämnts tidigare i denna vägledning är Sverige i arbetslivet, internationellt sett, milt drabbat av olyckor som kan kopplas till direkt inkompetens eller oaktsamhet. Det kan antas att detta följer av ett generellt gott medvetande om ett säkert beteende i olika situationer. Det är exempelvis lätt att se en stor skillnad i beteende i hur gemene man i Sverige uppträder i trafiken kontra hur detta sker i många andra länder. Detta kan naturligtvis underbyggas med statistik men vägledningen gör inte anspråk på att leda alla påståenden som relaterar sig till sunt förnuft i bevis. Det generellt höga säkerhetsmedvetandet kopplat till faror i vardag och arbetsliv till trots så sker ändå tillbud, incidenter och olyckor. Ofta kan sådana tillbud, incidenter och olyckor undvikas genom att fortlöpande utbilda personal och sprida kunskap om förändringar i system, tillämpningar och rutiner.

Vad är då en adekvat utbildning för en medarbetare, såväl inför anställning som fortlöpande i uppdaterande syfte? För att svara på frågan så ställs lämpligen ett antal andra kontrollfrågor, i likhet med en checklista.

- Har företaget förändrat system, oavsett vilka system det rör, eller andra komponenter på ett sätt så att det kan antas att en medarbetare som var familjär med "före"-läget nu har problem att känna igen sig?
- Har företaget förändrat sina anläggningar eller andra lokaler på ett sätt så att det

kan antas att en medarbetare som var familjär med ”före”-läget nu har problem att känna igen sig?

> Finns det ny lagstiftning eller andra rättsliga krav som kan påverka läget? **En bra bilförare behöver inte nödvändigtvis vara innehavare av ett körkort men får då faktiskt inte framföra en bil trots sin kompetens. Jmfr. exempelvis heta arbeten.**

> Har en medarbetare varit frånvarande en längre tid? Exempelvis långtidssjukskriven, sabbatsår etc.

> Finns det ny omvärldsinformation om rutiner, system eller andra komponenter i verksamheten som också är tillämpliga? **Jmfr. Gottröra-olyckan med SAS där piloten inte var informerad om automatiska funktioner i flygplanet som starkt ansågs bidra till olyckans utgång.**

Om svaret är ja på någon eller flera av dessa frågor så kan det antas att det föreligger ett reellt behov av någon typ av utbildning eller fortbildning. Det är här viktigt att påpeka att ett jakande svar inte per automatik innebär att utbildningspaket ska tas fram, designas, köpas in eller att personal måste gå kurser vid utbildningsinstitutioner. I många fall räcker det med att lösa ut sådana frågor internt och med egna resurser. Exempel:

> Ett företag har byggt om sitt kontor och som följd tvingats ändra utrymningsvägar. I detta fall torde det vara tillräckligt att genomföra säkerhetsgenomgångar med personalen samt öva densamma i de nya utrymningsvägarna.

Som med allt annat krävs ett mått av administration för att ha god kontroll på utbildningsnivåer. En funktion vid företaget bör ha som uppgift att föra journal över utbildningsläget och planera för fortbildning, repetition, övning och uppföljning.

9.2.2 UPPFÖLJNING OCH KONTROLL

I elbranschen förekommer många arbetsuppgifter som kan vara förknippade med fara eller som innebär att personal hanterar skyddsvärd information. Ett sunt säkerhetstänkande är således att löpande kontrollera att personalen dels känner att de har företagets stöd i sitt värv och dels att personalen inte upplever sin situation som negativ ur exempelvis ett socialt perspektiv.

När rutiner blivit inövade och upprepats en tid så är det lätt att vid stressade eller pressade tillfällen göra avkall på dessa rutiner. Det kan exempelvis vara att personal lämnar grind till ställverksområde öppen medan ett kortare arbete genomförs på plats där uppsikt och kontroll över grinden saknas. Det är av denna anledning som det är viktigt att regelbundet genomföra uppföljning och kontroll.

Kontrollverksamhet kan lätt få en negativ klang i arbetsmiljösammanhang. Det är då viktigt att hitta former för att denna kontrollverksamhet sker med lämpliga intervall och framförallt under lämpliga former. Ingen fördel kommer av att med närmast formella metoder ingripa mot medarbetares eventuella bristande efterlevnad.

> Kontrollverksamhet som utförs i samförstånd om varför kontrollen är nödvändig, exempelvis p.g.a. rättsliga krav eller för att förebygga personskada når oftast både högst acceptans och bästa resultat

Med information och utbildning nås oftast det bästa resultatet. I exemplet ovan där en ställverksgrind lämnats öppen och obevakad torde en påminnelse om vad som kunnat inträffa om någon obehörig förirrat sig in på området vara lämplig. Naturligtvis kan dock inte ett konstant upprepat ignorerande av regelverk och rutiner accepteras utan i sådana fall måste disciplinära åtgärder vidtas.

9.2.3 REGISTERKONTROLL OCH SUA

För uppgifter som rör rikets säkerhet eller skyddet mot terrorism så är Svenska kraftnäts författningar 2013:1 Affärsverket svenska kraftnäts föreskrifter och allmänna råd om säkerhetsskydd tvingande.

Detta innebär att skyddsåtgärder som tas fram

eller finns och som syftar till att ge ett skydd åt uppgifter som rör rikets säkerhet eller skyddet mot terrorism, oavsett vilken form sådan uppgift förekommer i, ska stå i paritet med säkerhetsskyddsåtgärder såsom de regleras i nämnda föreskrifter. Sådana skyddsåtgärder omfattar:

- FYSISKT SKYDD
  Hur uppgifter ska skyddas mot otillbörlig åtkomst med stöd av byggnadstekniska åtgärder.
- ADMINISTRATIVT SKYDD
  Att det finns dokumenterade och tillämpliga rutiner för hur hantering av uppgifter får ske.
- TEKNISKT SKYDD
  Uppgifter som hanteras i exempelvis IT-system ska omges med ett därför tillämpligt skydd och tillämplig segmentering från andra system och uppgifter.
- ORGANISATORISKT SKYDD
  Det ska finnas en säkerhetsorganisation som är utsedd för att reglera hanteringen av uppgifter som rör rikets säkerhet eller skyddet mot terrorism.

Om ett företag som omfattas av SUA ska engagera underleverantörer, se även Kap. 9.3.5 Registerkontroll och SUA i denna vägledning.

9.2.4 AVSLUTANDE AV ANSTÄLLNING ELLER TJÄNST

Ett område som berör säkerheten och som ofta försummas är vad som sker i samband med att en person avslutar sin tjänst eller byter befattning eller genomgår betydande förändringar i tilldelade roller. VD eller motsvarande vid elföretag bör se till så att endera VD, utsedd säkerhetschef eller båda genomför ett säkerhetssamtal med medarbetare som slutar eller på ett betydande sätt byter befattning/roll.

Vid ett avslutande säkerhetssamtal bör exempelvis följande saker tas upp, diskuteras och i förekommande fall erinras om.

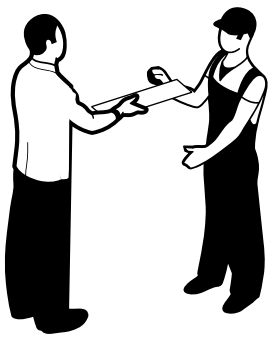
- Erinra om sekretess för uppgifter som den enskilde kan ha tagit del om som rör rikets säkerhet eller skyddet mot terrorism.
- Erinra om skydd för företagets proprietära uppgifter.
- I samtal säkerställa att den enskilde inte lämnar befattning, roll eller anställning som följd av otillbörlig påtryckning.
- Intervjua den enskilde i syfte att säkerställa att denne informerar om sådant som kan vara singulära arbetsuppgifter eller unika kunskaper om företagets verksamhet som i samband med detta kan behöva dokumenteras.

Det bör påpekas att beroende på vilken storlek företaget har så föreligger olika behov av säkerhetssamtal även i samband med byte av vissa befattningar och roller.

Ett säkerhetssamtal ska inte uppfattas som något negativt utan vara ett sätt för både arbetsgivare och arbetstagare att komma till ett bra avslut där det inte finns några tveksamheter om sådant som omfattas av rättsliga krav eller rör proprietära uppgifter för företaget.

9.3 ENTREPRENÖRER OCH ANNAN INHYRD PERSONAL ELLER FÖRETAG

Detta stycke syftar till att ge stöd för elföretag i samband med upphandlingar som innebär att entreprenörer eller annan inhyrd personal kan komma att komma i kontakt med skyddsvärd information, för verksamheten kritiska komponenter, anläggningar eller annan verksamhet,



information eller annat objekt som är av proprietär natur för det berörda företaget.

9.3.1 UTFORMNING AV KONTRAKT

OBS. Om verksamheten omfattas av SUA, se vidare 9.3.5 Registerkontroll och SUA.

Det är alltid rimligt att genomföra en riskanalys innan man påbörjar en upphandling av nämnda slag. Detta oavsett upphandlingens storlek, det är innehållet – arten – av det som ska göras som avgör behovet av att ha en god säkerhet i upphandlingen och den efterföljande entreprenaden. Storleken och utförandet på nämnda riskanalys kan, och bör, naturligtvis variera med storlek och betydelse på den specifika upphandlingen.

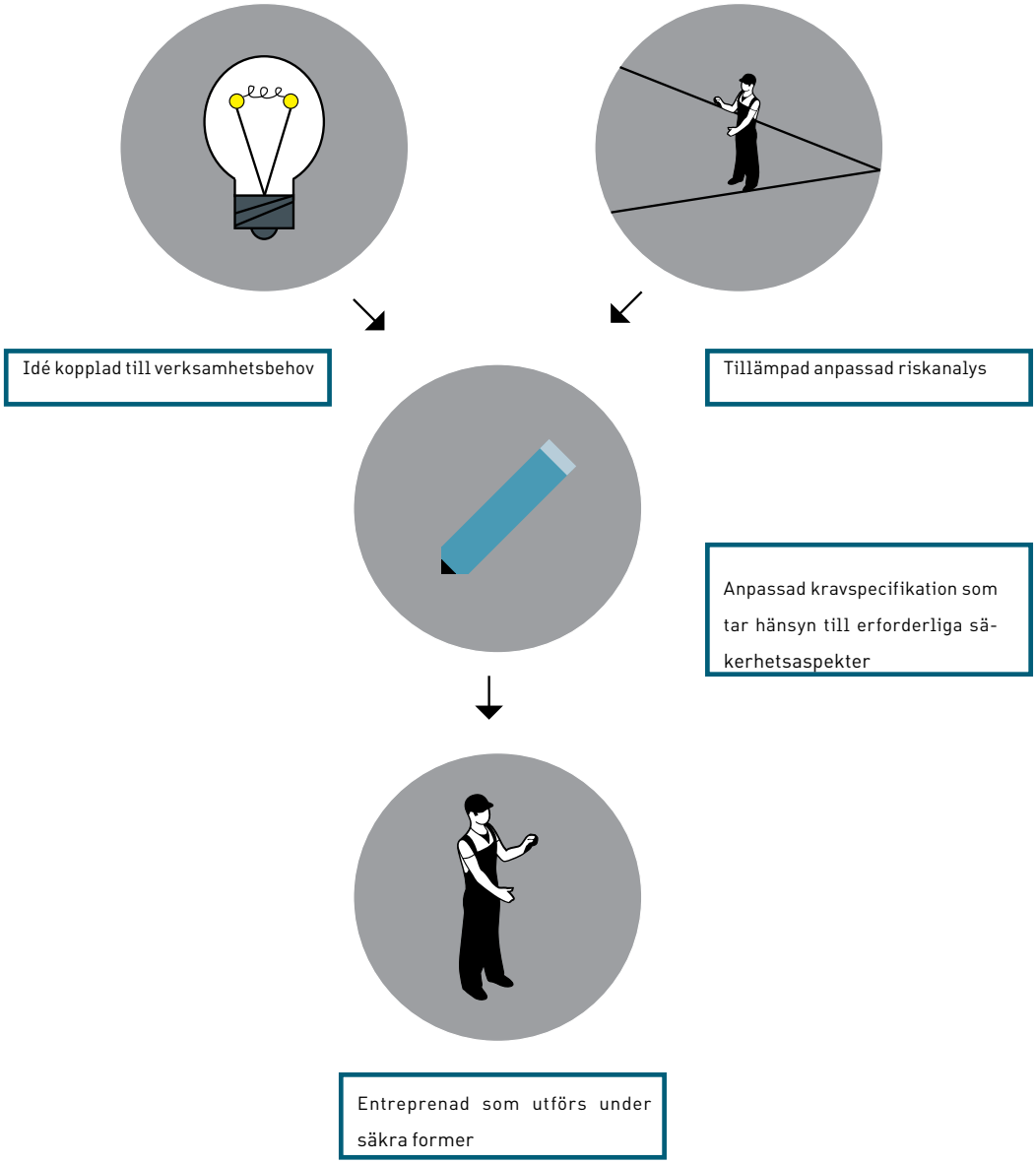
Några frågeställningar som bör beaktas inom ramen för riskanalys före upphandling enligt ovan.

- Kan entreprenören komma i kontakt med uppgifter som rör rikets säkerhet eller skyddet mot terrorism i samband med entreprenadarbetet? Går det att anlita en utländsk entreprenör?
- Kan entreprenören komma i kontakt med uppgifter som är av proprietär natur för företaget i samband med entreprenadarbetet?
- Behöver entreprenören, eller motsvarande, ta del av och själv hantera och förvara uppgifter enligt ovanstående punkter.
- Kommer entreprenören inom ramen för uppdraget att få tillgång till, och på något sätt ha möjlighet att påverka, företagets IT-miljö?
- Behöver entreprenören, eller motsvarande, få tillträde till områden och lokaler som företaget betraktar som skyddsvärda inom ramen för uppdraget?
- Har entreprenören, eller motsvarande, god vandel? Finns det historia av otillbörligheter i entreprenörens tidigare utförda arbeten?
- Har entreprenören tillräckligt gott säkerhetsmedvetande för att hantera sådana uppgifter som denne kan komma i kontakt med under uppdraget?

Ovanstående är att se som ett ledande exempel på vilka frågeställningar som måste redas ut innan en upphandling genomförs. Beroende på vad uppdraget innebär så måste ett mera dynamiskt angreppssätt användas i analysen.

Sett mot frågeställningar och resultatet av en riskanalys enligt ovan är det därefter enkelt att utforma vissa delar av kravspecifikationen för uppdraget. Nedan följer en uppräkning av några nyckelord/fraser som kan, och i tillämpliga fall bör, användas när utformning av kravspecifikation för uppdraget sker.

- Entreprenörens företag och tillämplig personal ska kontrakteras med avtal som reglerar säkerheten och berörd personal ska genomgå lämplighetsprövning.
- Entreprenörens företag och tillämplig personal ska underteckna sekretessavtal, se underkapitel nedan, innan uppdraget får påbörjas.
- Information och andra uppgifter som delges entreprenören ska hanteras enligt följande:
  - Kvittering, personlig uppsikt eller förvaring enl. SS3492. Återlämning mot kvittens. Destruktion av arbetskopior, berörda datamedia m.m.
  - Kvittering, personlig uppsikt, inlåsning i tunnplåtsskåp som inryms i låst kontorsutrymme.
  - Larm med väktarutryckning till arbetsplats, kontorsutrymme, etc.
  - Delgivning inom uppdraget noteras på delgivningslista.
- Arbetsplats som uppdraget berör ska om så är tillämpligt skyddas med tillfälligt områdesskydd (ev. larm, rondering med väktare etc.).



Figur 7. Säkerhet i samband med upphandling.

- Alla aktiviteter som entreprenör, eller personal hos entreprenören, genomför i företagets IT-system övervakas och granskas. Enskild kan ställas till ansvar för otillbörliga aktiviteter.
- Entreprenör får inte utan uttryckligt, i tillämpliga fall skriftligt, tillstånd från företaget engagera personal i andra led.
- I de fall entreprenör med tillstånd engagerat personal i andra led ska samma krav enligt specifikation gälla för personal i andra led. Entreprenören ansvarar för att personal i andra led uppfyller givna krav inom ramen för uppdraget.

Ovanstående uppräkning utgör ett exempel men täcker in några av de viktigaste aspekterna i samband med upphandling. Resultatet från en enkel riskanalys kan lätt omsättas enligt ovanstående till lämpliga krav i en kravspecifikation för en upphandling.

9.3.2 SEKRETESSAVTAL

Nedanstående är ett exempel på hur ett sekretessavtal mellan två parter kan vara utformad.

Ort/Datum
[uppgifter företag 1] [uppgifter företag 2]

Mot bakgrund att ovanstående företag, **namn på företag 1** och **namn på företag 2**, avser ingå samarbete tecknas nedan avtal om sekretess då uppgifter av konfidentiellt slag kan komma att lämnas.

1. Konfidentiell information
Konfidentiell information är information om företagen, oavsett slag, som kan komma att lämnas under parternas samarbete som berör kunskap, affärshemligheter eller annan information oavsett typ om vardera avtalsparten vars yppande kan komma att skada något av företagen.

2. Icke-konfidentiell information
Information som är allmänt veterlig, eller som avtalsparterna redan vet om varandra sedan innan samarbetets början, anses inte vara konfidentiell information.

3. Sekretessen gäller
Detta avtal om sekretess innebär att ingen utav avtalsparterna får lämna ut sådan konfidentiell information om varandra till någon utomstående, såsom personer, företag, myndigheter och organisationer.

4. Undantag från sekretess
Konfidentiell information kan dock ges ut om den ena avtalsparten tillåter den andra avtalsparten att göra detta, eller om myndighet beslutat att sådan information ska lämnas ut.

5. Återlämnande av konfidentiell information
Vid upphörandet av parternas samarbete ska konfidentiell information återlämnas. Återlämnande ska också ske om någon utav av avtalsparterna kräver detta.

6. Vite vid avtalsförbrytelse
Om någon utav av avtalsparterna bryter mot detta avtal om sekretess ska vite utgå med **belopp**.

7. Övrigt
Om något bör tilläggas till avtalet kan detta skrivas här.

Signatur företrädare företag 1 *Signatur företrädare företag 1*

9.3.3 UTBILDNING

Utbildning av entreprenörer och uppdragstagare ska normalt sett inte vara nödvändigt. Det skulle ju faktiskt ha en motsatt effekt gentemot den önskade, man upphandlar eller köper in något, en vara eller tjänst, för att man inte kan eller har resurser att lösa problemet själv. Det finns dock undantag. Ett sådant är när det handlar om uppgifter som rör rikets säkerhet eller skyddet mot terrorism, säkerhetsskydd. I sådana fall krävs inte sällan utbildning av entreprenör och/eller dennes personal.

Om ett elföretag finner behov av att utbilda entreprenörer eller personal hos entreprenörer vad avser säkerhetsskydd och därtill kopplat regelverk så kan med fördel tillämpligt material enligt bilaga 1, metodreferenser, till denna vägledning användas.

9.3.4 UPPFÖLJNING OCH KONTROLL

Även entreprenörer och annan inhyrd personal behöver kontrolleras. Sådan kontroll är nödvändig av samma skäl som den krävs för egen personal och motsvarande. Det är emellertid lätt att missa denna möjlighet då den i allt väsentligt kräver avtalsreglering för att fungera. Av detta följer att kontroll som man i egenskap av beställare vill utöva under ett uppdrag eller entreprenad måste specificeras i exempelvis upphandlingsunderlaget.

Det finns otaliga exempel på hur brister har upptäckts i pågående uppdrag. De kan upptäckas av en slump eller som följd av att någon informerar om dem. I värsta fall upptäcks bristerna som följd av en inträffad incident.

Många gånger kan en beställare ledas att tro att en ordalydelse i ett upphandlingsunderlag eller annan kravspecifikation betyder samma sak för utföraren som för beställaren. Om då kontrollfunktioner inte reglerats finns det i stort sett inga möjligheter att upptäcka att ett missförhållande råder.

Följande formuleringar är förenklade avidentifierade krav från en kravspecifikation som rör upphandling av extern datadrift och kan tjäna som inspiration eller exempel i samband med utformning av eget upphandlingsunderlag eller egen kravspecifikation.

- Krav_kontroll_nn: Beställaren får inom ramen för uppdragets utförande genomföra stickprovskontroller av uppdragstagarens förmåga och efterlevnad av de krav som anges under rubriken Krav_information_n_t.o.m._j, Krav_IT-säkerhet_n_t.o.m._j samt Krav_fysiskt_skydd_n_t.o.m._j i detta dokument.
- Oförmåga eller andra brister hos uppdragstagaren ska rättas inom 48 timmar från kontrolltillfälle. Om uppdragstagaren fallerar att uppfylla kraven på tillämpligt sätt inom den stipulerade tiden kan beställaren avsluta uppdraget.

9.3.5 REGISTERKONTROLL OCH SUA

BS! Detta stycke gäller företag eller del av företag som gör uppdrag åt myndighet som omfattas av SUA, vanligen service, underhåll och entreprenadarbeten. Stycket syftar särskilt till att belysa att SUA inte kan "ärvas" från en part till en annan.

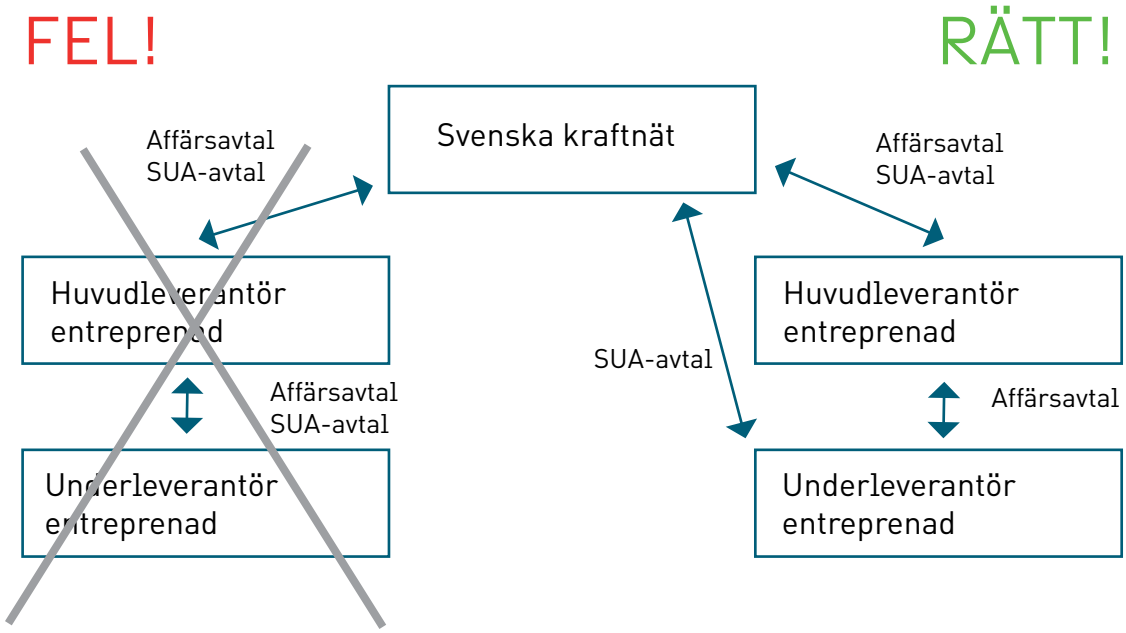
För uppgifter som rör rikets säkerhet eller skyddet mot terrorism så är Svenska kraftnäts förskrifter 2013:1 Affärsverket svenska kraftnäts föreskrifter och allmänna råd om säkerhetsskydd tvingande.

Ett SUA-avtal kan inte "ärvas" från en huvudsaklig leverantör till en underleverantör. Man måste skilja på de affärsmässiga avtalen och SUA, se figur 8.

En leverantör som har ett SUA-uppdrag kan således inte på något sätt "överlåta" dess egenskaper, skyldigheter eller andra drag på en underleverantör. Detta måste göras av Svenska kraftnät. Det är således viktigt att tidigt i en process där SUA identifierats som ett behov kontrollera om behov finns av att engagera underleverantörer och om dessa kan komma att få del av uppgifter som rör rikets säkerhet eller skyddet mot terrorism.

9.3.6 AVSLUTANDE AV UPPDRAG ELLER KONTRAKT

Ofta när uppdrag avslutas, endera för att uppdraget löpt ut eller av annan anledning, så glöms grundläggande säkerhetsaspekter bort. Det kan röra uppföljande säkerhetssamtal som rör kon-



Figur 8. Skillnaden på affärsmässiga avtal och SUA.

fidentialitet kring information eller genomgång av och insamling av utdelade resurser, exempelvis information, åtkomst i IT-system etc.

Det bör inför varje projekt som involverar externa uppdragstagare upprättas en plan som tydligt reglerar vad som ska göras i samband med ett uppdrags avslutande. En sådan plan kan, beroende på uppdragets utformning, vara omfattande. För många små och medelstora uppdrag torde det dock räcka med en kort ingress som beskriver problematiken inom uppdraget, vilka som berörs samt lämpligen en lista över resurser som ska ges särskild uppmärksamhet i samband med uppdragets avslutande.

9.3.7 TILLFÄLLIG PERSONAL MED KORT ELLER PERIODISK TJÄNSTGÖRING

I detta sammanhang omnämns tillfällig personal med kort eller periodisk tjänstgöring endast för att påminna om att de problem och därtill kopplade åtgärder och lösningar som redovisats tidigare i detta avsnitt även är tillämpliga för och bör tillämpas på personal med kort eller periodisk tjänstgöring. Sådan personal har erfarenhetsmässigt ofta hamnat "mellan stolarna" historiskt sett.

9.4 INTERAKTION OCH UTBYTE MED PERSONAL, FÖRETAG OCH MYNDIGHETER FRÅN ANDRA LÄNDER

9.4.1 SECURITY- OCH FACILITY-CLEARANCE

Begreppen (eng.)Personal security clearance och (eng.)Facility security clearance är befintliga och tillämpas i flera länder i Europa, dock inte i Sverige. Det bör här särskilt påpekas att Personal security clearance (PSC) inte är samma sak som registerkontroll i samband med säkerhetsskyddade uppdrag.

I Säkerhetspolisens vägledning för säkerhetsskyddad upphandling står bland annat följande:

> När det gäller civilt internationellt samarbetet finns för närvarande ingen författningsreglering. Uppkommer behov av säkerhetsklarering med mera vid sådant samarbete hänvisas till NSA (eng.)National Security Authority vid Utrikesdepartementets sekretariat för säkerhet, sekretess och beredskap.

Detta innebär i praktiken att sådana frågor alltid ska hänskjutas till Utrikesdepartementet. Vid tidpunkten för utgivande av denna vägledning

gäller dock en annan (eng.)De-Facto rutin enligt efterföljande två underrubriker.

9.4.2 PERSONAL SECURITY CLEARANCE

Svenska kraftnät har med stöd av berörda myndigheter etablerat en rutin för genomförande av personal security clearance (PSC) med stöd av UD NSA och FM MUST (Försvarsmakten - militära underrättelse- och säkerhetstjänsten).

Företag som har behov av att pröva PSC ska inkomma med hemställan härom till Svenska kraftnät, säkerhetsskydd. Svenska kraftnät handlägger därefter ärendet med stöd av MUST[7] eller NSA vid UD.

Det bör här särskilt påpekas i vilken omfattning Svenska kraftnät kan hjälpa företag vad avser PSC. Följande uppräknade situationer är sådana där Svenska kraftnät kan, och ska, hjälpa företag med PSC.

- Då en person som inte är Svensk Medborgare kommer, eller kan komma, i kontakt med uppgifter, exempelvis i IT-system, som rör rikets säkerhet eller skyddet mot terrorism i samband med besök eller värv på företag i Sverige.
- Då en person som inte är Svensk Medborgare kommer, eller kan komma, att behöva tillträde till och verka i anläggning som rör rikets säkerhet eller skyddet mot terrorism i samband med besök eller värv på företag i Sverige.
- Då en person vid ett svenskt företag behöver få ett PSC utfärdat för att ett företag eller myndighet i mottagande land kräver det i samband med värv för företaget i det mottagande landet.

Mall för hemställan finns på Svenska kraftnäts hemsida och energisäkerhetsportalen.

9.4.3 FACILITY SECURITY CLEARANCE

Vad gäller facility security clearance (FSC) så hänskjuts ansvaret på respektive företag. Företagen äger sina anläggningar och är således ansvariga för säkerheten i och kring dem. Svenska kraftnät ställer inga krav på att företag i Sverige ska inneha FSC för sina anläggningar i Sverige. Ett företag kan av andra skäl, exempelvis krav från utländskt företag eller företagets utländske huvudägare, behöva ta fram FSC för anläggningar. Om företaget då väljer att placera en samlad mängd säkerhetsrelaterad information i FSC så kan denna behöva granskas av Svenska kraftnät i samband med tillsyn i enlighet med SvKFS 2013:1. Se sista stycket nedan.

FSC har bäring på två områden. 1) Är anläggningen säkerhetsmässigt acceptabel för att husera och hantera sådan information som kan förekomma i den? Detta kan bland annat bygga på säkerhetsanalys. 2) Är besökande personal "klarerad" för att få tillträde till anläggningen? Här kommer bedömningarna an på bland annat PSC, om besökare/entreprenör/medarbetare från annan del av företaget etc. ska beledsagas inom anläggningen m.m.

Beslut om FSC ska alltid bygga på resultatet av analys, slutsatser därav samt uppställda kriterier, exempelvis om en person ska ha PSC för att kunna få FSC för en anläggning som företaget kontrollerar.

Det ska finnas ett dokumenterat och beslutat regelverk hos företag som har behov eller skyldighet av att tillämpa FSC. Regelverket ska vara tillgängligt för granskning av Svenska kraftnät i samband med tillsyn eller på anmodan. Härvid kontrollerar dock Svenska kraftnät endast de uppgifter som rör rikets säkerhet eller skyddet mot terrorism.

7. Militära underrättelse- och säkerhetstjänsten

10 FYSISKT SKYDD

10.1 ALLMÄNT

Begreppet säkerhetsskydd är definierat och vad som gäller för skydd och förvaring likaså, men vad som menas med högt skyddsvärde, skyddsvärt eller verksamhetskritiskt är sällan definierat så att det finns en homogen samsyn på vad som kvalificerar sig för dessa begrepp.

Det lättaste sättet att kontrollera om det finns information eller uppgifter som har ett skyddsvärde är att ställa sig frågor av typen.

- Kan den här uppgiften spridas fritt?
- Kan dessa handlingar ligga framme öppet eller finns det personer som är obehöriga att ta del av informationen?
- Kan våra tekniska lösningar visas upp fritt för alla?

Om svaret på denna typ av frågor är tveksamt eller nej så kan man sluta sig till att det föreligger ett skyddsvärde av något slag. Med detta skyddsvärde följer även ett behov av att tillföra ett fysiskt skydd.

I elbranschen finns begreppet betydelseklassning som kan hjälpa till att avgöra var ett ökat skyddsbehov föreligger. Svenska kraftnät och Svensk Energi har tagit fram en vägledning för fysiskt grundskydd.

Länk till vägledningen:

http://www.svk.se/Global/01_Om_oss/Pdf/Sakerhetsskydd/130410-Vagledning-Fysiskt-grundskydd.pdf

Vägledningen beskriver ingående hur ett fysiskt skydd kring exempelvis en anläggning ska vara beskaffat

Fysiskt skydd berörs även delvis i kap. 12 Informationssäkerhet samt i kap. 13 IT-säkerhet i denna vägledning.

11 ELBEREDSKAP

Elberedskap utgör ett eget säkerhetsområde med egna föreskrifter och egen vägledning som stöd.

Länk till elberedskapsföreskrifterna:
http://www.svk.se/Global/07_Tekniska_krav/Pdf/Foreskrifter/SvKFS-2013-2.pdf

För att hitta vägledningen, sök på Svenska kraftnäts webbplats www.svk.se eller kontakta Svenska kraftnät.

Postadress: Svenska kraftnät, Box 1200, 172 24 Sundbyberg. Tel: 010-475 80 00. E-mail: registrator@svk.se

12 INFORMATIONSSÄKERHET

12.1 BESKRIVNING AV KAPITLETS INDELNING

Denna vägledning syftar bland annat till att harmoniser med, och inte stå i motsats till ISO 27000 standarden. Anledningen till detta är att det inte är ovanligt att branschföretag använder sig av, åtminstone valda delar, av standarden.

Vägledningen gör inte anspråk på att vara uttömmande eller för den elen följa standarden slaviskt, dock ska det vara möjligt att känna igen sig i de områden som beskrivs.

12.2 DEFINITION AV INFORMATIONSSÄKERHET

SIS definierar begreppet Informationssäkerhet enligt följande; Säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet (även ansvarighet och oavvislighet).

Definitionen är som brukligt i akademiska sammanhang något krystad. I takt med att all verksamhet, styrning och alla objekt som kan kopplas till det berörs av information så är det svårt att se var informationssäkerhet inte har någon räckvidd.

I föreskriftssammanhang används ofta begrepp som "uppgift om". Det implicerar i stort sett all information som kan knytas till ett objekt och som i detta fall skulle kunna ha påverkan på säkerheten. Det finns tyvärr många exempel från verkligheten där exempelvis ritningar över anläggningar har hanterats på ett, ur säkerhetssynpunkt, otillfredsställande sätt, främst på grund av att ingen bedömning om deras relevans för säkerheten har genomförts.

En brasklapp i detta sammanhang blir, på grundval av ovanstående, att definitionen av informationssäkerhet måste tolkas bredare än vad den antyder.

12.3 RISKBEDÖMNING OCH RISKBEHANDLING

Riskbedömning och riskbehandling innefattar bland annat riskanalys, åtgärder, utvärdering och riskhantering.

Se vidare 4 Riskanalys och 3 Hot, hotbild och hotbeskrivning i denna vägledning.

12.4 SÄKERHETSPOLICY

En säkerhetspolicy är ett inriktningsdokument för informationssäkerheten som ingår i ISO 27000 standarden. Målet med en säkerhetspolicy är "Att ange ledningens viljeinriktning och stöd för informationssäkerhet i enlighet med verksamhetskrav och relevanta lagar och föreskrifter".

Mindre organisationer och andra som väljer att helt eller till del följa standarden ska således här ange vilken inriktning informationssäkerheten ska ges inom organisationen eller företaget. Titeln på dokumentet kan således upplevas som

lite missvisande eftersom den avser informationssäkerhet.

För sådana företag som inte har valt att implementera standarden men i övrigt väljer att hantera säkerheten utifrån grundval av verksamhetsbehov och utfall från tillämpliga analyser så kan dokumentet anses som överflödigt.

12.5 ORGANISATION AV INFORMATIONSSÄKERHETEN

Målet med att skapa organisation kring informationssäkerheten är enligt ISO 27000 standarden att den "Ska styra informationssäkerheten inom organisationen". Se vidare 7 Organisation i denna vägledning.

12.6 HANTERING AV TILLGÅNGAR (ENG.)ASSET MANAGEMENT

12.6.1 ALLMÄNT

Syftar enligt ISO 27000 standarden till att uppnå och upprätthålla lämpligt skydd av organisationens tillgångar.

Inom ramen för nämnda standard finns mycket information att hämta som rör hantering av tillgångar. I denna vägledning kommer fokus att ligga på två av de områden som omnämns i standarden och som, i allt väsentligt, får ses som en förutsättning för att kunna uppnå en god säkerhet oavsett vilket säkerhetsområde som avses. Dessa områden är följande.

1. Ägarskap av informationstillgångar.
2. Informationsklassificering.

Dessa omnämns i denna vägledning på en nivå som ska vara möjlig att implementera och vidmakthålla med små och enkla resurser.

12.6.2 ÄGARSKAP AV INFORMATIONSTILLGÅNGAR

Vad som avses framgår med all önskvärd tydlighet av rubriken. Om det finns en informationstillgång, oavsett vari den består, så måste det finnas någon som känner ansvaret för att hålla informationstillgången:

> BEFINTLIG
Den ska vara framtagen och färdigställd.

> KOMPLETT
Den ska omfatta alla relevanta aspekter av informationstillgången.

> KORREKT
Den ska inte innehålla fel och vara uppdaterad m.a.p. ändringar.

> TILLGÄNGLIG
Den ska finnas till hands för de som behöver den när de behöver den.

> KLASSIFICERAD
Se vidare 12.6.3 Informationsklassificering nedan.

Detta kan låta självklart men brister erfarenhetsmässigt ofta. Det finns således en säkerhetsmässig vinst i att utse "ägare" till olika informationstillgångar och uppdra åt dessa att se till att den berörda informationstillgången håller, eller strävar mot, ovan nämnda standard.

Det är, sett mot ovanstående lätt att se varför en ansvarig ägare för en informationstillgång bidrar till en ökad säkerhet och ökad effektivitet i företagets verksamhet. Som så många andra aktiviteter som rör informationssäkerhet så är det initialt sett en, icke ringa, arbetsinsats som behöver genomföras. Därefter torde arbetet med att hålla informationstillgången uppdaterad och i den kvalitet som anges ovan utgöra, och upplevas, som en integrerad del av den dagliga verksamheten. Som med allt annat som tas upp i denna vägledning så är skalbarhet och anpassning efter företagets storlek A och O.

Det är bättre att göra någonting än att inte göra någonting alls.

12.6.3 INFORMATIONSKLASSIFICERING

Det finns många modeller för att klassificera information. Inte sällan är dessa modeller komplexa och innefattar klassificering på flera attribut i många nivåer.

Informationsklassificering har historiskt skett i militära tillämpningar sedan urminne tider. Ett av de mer kända exemplen är romarna som identifierade skyddsvärd information

rörande sina militära förehavanden. Detta i sig var varken nytt eller unikt men de etablerade en välkänd skyddsmekanism som standardmässigt användes på sådan information, Caesarkryptot (se bild ovan).

Häri ligger också en av de viktigaste lärdomarna i hur informationsklassificering bör ske. För varje nivå av klassificering som man tillför på ett attribut så ökar komplexiteten, men framförallt. För att det ska vara meningsfullt med olika nivåer och klassificering på flera attribut så krävs det att det för varje möjlig kombination av attribut och nivå finns unika hanteringsregler. Om det inte gör det så finns det kombinationer av klassificeringar som har samma hanteringsregler, de tillför då ingenting i sammanhanget.

Vad som även är tänkvärt i detta sammanhang är, som tidigare nämnts komplexiteten i såväl klassificeringsmodell som i hanteringsregler. Om vi som ett exempel låter anta att vi har en befintlig klassificeringsmodell som klassificerar informationstillgångar på attributet konfidentialitet i tre olika nivåer; öppen, intern och konfidentiell. För var och en av dessa nivåer föreligger hanteringsregler, exempelvis enligt följande:

Öppen	Inga särskilda hanteringsregler.
Intern	Får inte delges personal utom företaget utan godkännande av informationsägaren. Informationsbärande media får inte lämnas framme i lokaler som är tillgängliga för andra än företagets personal.
Konfidentiell	Får inte delges personal utom företaget utan godkännande av VD eller säkerhetschef. Informationsbärande media ska alltid hållas under uppsikt eller inlåst i tunnplåtsskåp eller förvaring med högre skyddsnivå.

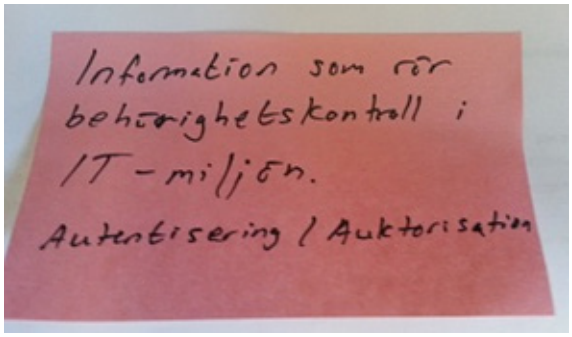
Det bör särskilt påpekas att strävan ska vara att hålla antalet nivåer så lågt som det är lämpligt och möjligt då ett ökat antal nivåer medför att det kan vara svårt att förstå skillnader mellan, och tillämpa hanteringsregler, för de olika nivåerna.

I denna vägledning kommer endast klassificering på ett attribut, konfidentialitet, att beskrivas. Detta för att delge en enkel modell som är tillämplig för de allra flesta företag som ingår i målgruppen för denna vägledning.
Själva essensen med att klassificera informationstillgångar är att man också tillför hanteringsregler som reglerar hur informationstillgångar i de olika nivåerna faktiskt får hanteras, användas, delges, försändas, förvaras och avvecklas.

Som vanligt gäller **det är bättre att göra någonting än ingenting.** Nedanstående modell ska ses som ett exempel som bygger på lång erfarenhet av informationshantering i olika sammanhang och tillämpningar. Modellen är beskriven i fyra steg men kan lätt kortas av genom att slå samman delar av två nivåer eller helt enkelt ta bort nivåer. Fördelen är att den redan är befintlig och enkel och därmed kan användas tämligen ograverat av företag som är målgrupp för denna vägledning.

Process för att klassificera information. Denna process kan liknas vid vilken modellering eller riskanalys som helst och genomförs med fördel av en för ändamålet lämplig grupp eller i tillämpliga fall person. Inventera vilka informationstillgångar som finns i företaget. Glöm inte att ”uppgift om” en anläggning också är en informationstillgång. Dokumentera dessa. Detta kan beroende på hur man går tillväga och vilken spridning man har på informationstillgångarna göras på olika sätt. Ett sätt som ofta

fungerar bra är att inventera och dokumentera informationstillgångarna på post-it lappar eller motsvarande. Även här är det viktigt att låta enkelhet råda utan att för den sakens skull lämna utrymme för misstolkningar. Ett klassiskt exempel är information som rör åtkomst i IT-system.

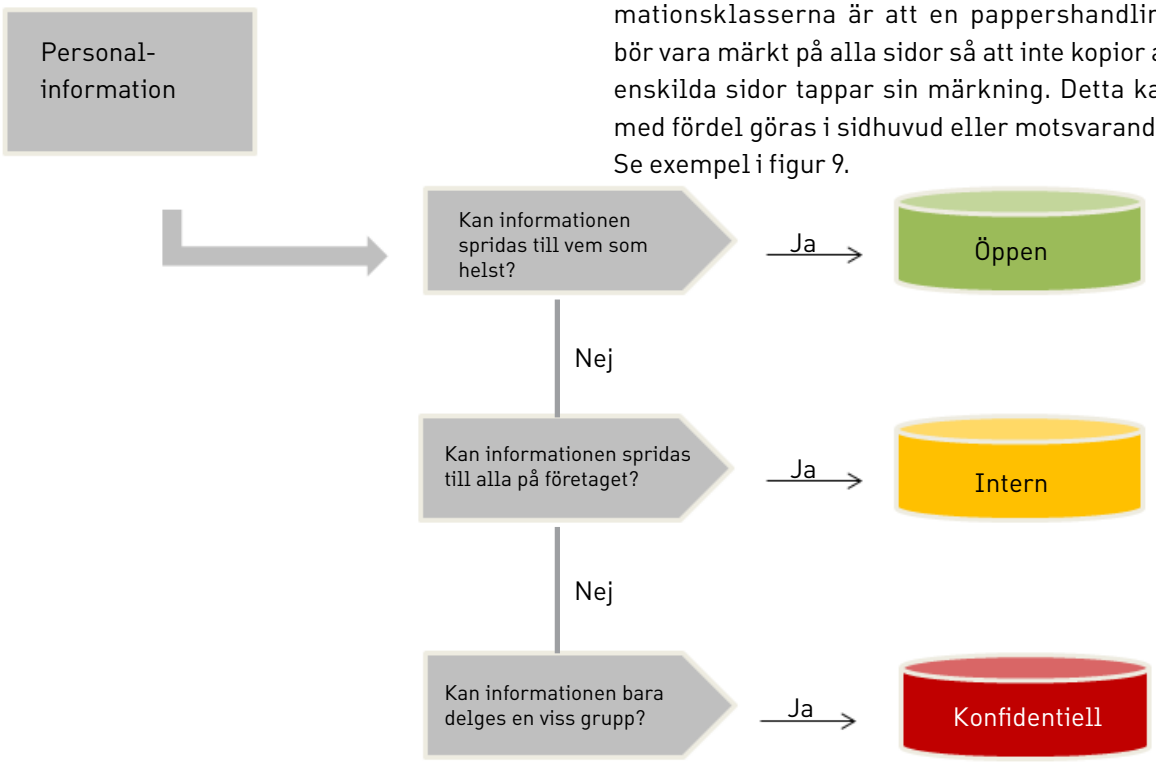


När inventeringen får anses vara komplett, eller så nära komplett man kan komma under rådande omständigheter så vidtar klassificeringsarbetet. Notera att vi ännu inte har talat om nivåer i klassificeringen.

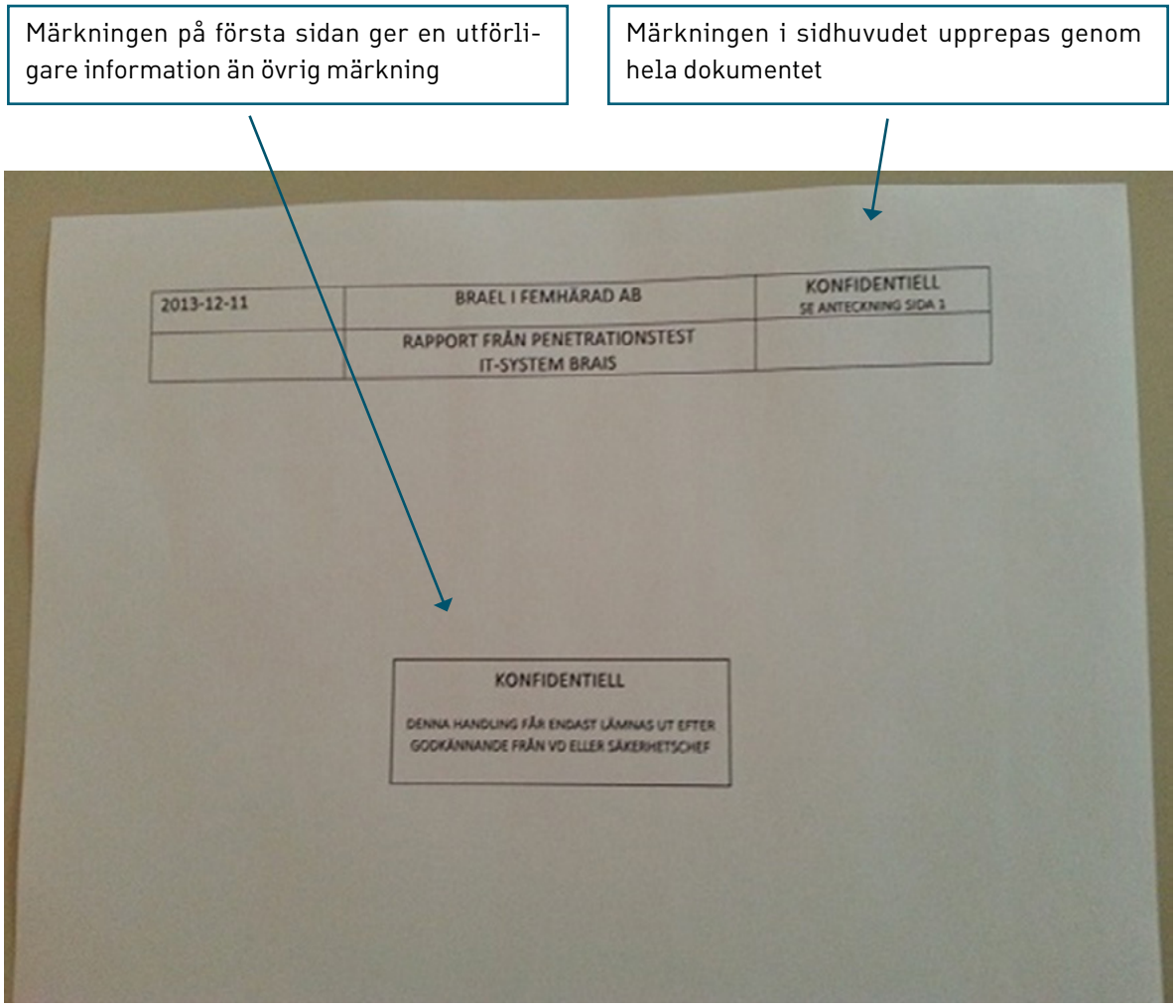
Det finns en enkel metod för att hitta rätt antal nivåer i samband med att klassificeringsarbetet pågår. För var och en av de inventerade informationstillgångarna ställs först frågan – **"Finns det personer överhuvudtaget som är obehöriga, alltså som inte ska få ta del av denna information?".** Om svaret på den frågan är nej så har vi nått vägs ände med den första klassificeringen, då är informationstillgången vad vi brukar kalla för **öppen**. Om svaret är ja så vidtar ett antal följdfrågor som beskrivs i nedanstående processbild. Antalet klassificeringsnivåer blir således så många som man får utfall i när man går igenom frågeställningarna. Observera att namnen på nivåerna är exempel och lika gärna kan ersättas med nummer, bokstäver eller andra namn. Man kan naturligtvis utöka antalet nivåer nedan med de kriterier som anses vara nödvändiga. Den redovisade modellen är dock enkel och tillämplig i de flesta fall.

Utöver klassificeringsprocessen så krävs att informationstillgången märks på ett adekvat sätt. Härvid måste hänsyn tas till att information hanteras på många olika sätt och i många olika former, alltså vilket medium information finns på. I denna vägledning ger vi exempel på hur märkning kan göras på pappersmedia, för olika typer av filer inklusive i filer där så är tillämpligt samt hur utrustning kan märkas, exempelvis servrar eller annan IT-utrustning.

Det lättaste att märka är, och har alltid varit, pappersmedia. En viktig sak att tänka på, särskilt när det gäller de mer skyddsvärda informationsklasserna är att en pappershandling bör vara märkt på alla sidor så att inte kopior av enskilda sidor tappar sin märkning. Detta kan med fördel göras i sidhuvud eller motsvarande. Se exempel i figur 9.



Figur 9. Process för informationsklassificering.



Exempel på märkning av pappersmedia.

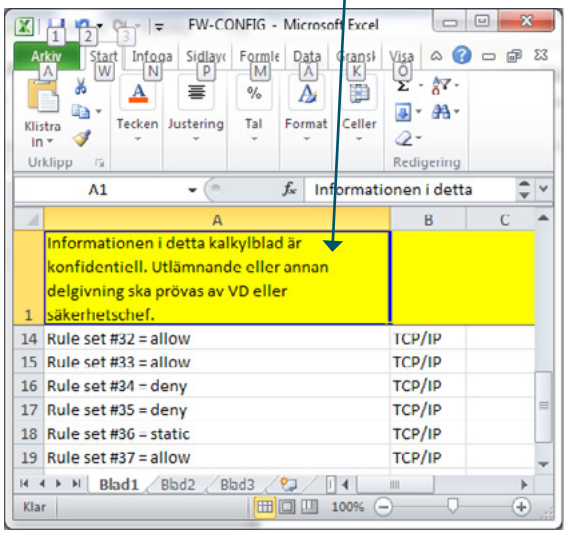
Filer, i stort sett oavsett vilken typ de är, kan märkas genom att tillföra en taxonomisk märkning i filnamnet. Detta innebär i klartext att man genom riktlinjer reglerar ett filnamnstillägg som anger vilken klassificering filen har se nedanstående exempel.

Filtyp	Informations-klass	Utförande på filnamn
Word [*.docx]	Öppen [_o]	Filnamn_o.docx
Excel [*.xlsx]	Intern [_i]	Filnamn_i.docx
Textfil [*.txt]	Konfidentiell [_k]	Filnamn_k.docx

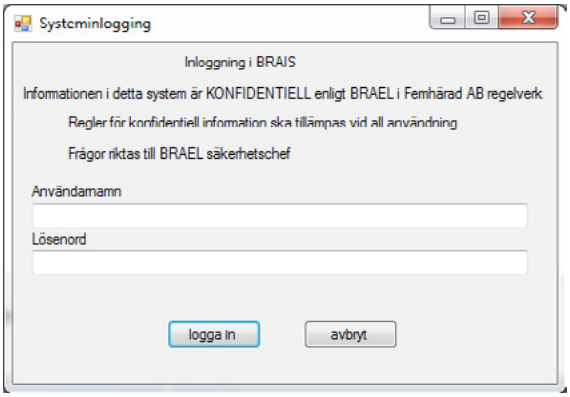
Generellt sett handlar det om att på ett informerande och tydligt sätt göra den som hanterar informationstillgången uppmärksam på att informationen som hanteras i förekommande fall ingår i en informationsklass och har ett skyddsvärde. Det förekommer att man väljer att inte märka öppen information. Det går naturligtvis att göra på det sättet men man bör bära med sig att detta ökar risken för oavsiktligt röjande eller felaktigt utlämnande om det brister i aktiviteten att klassificera informationen.

Nedan följer exempel på hur en användare kan uppmärksammas på att informationstillgången är klassificerad och har ett skyddsvärde i MS Excel och i ett godtyckligt IT-system via information i inloggningsrutan.

Märkning i ett låst fält i Excel



Märkning i en inloggningsruta till ett informationssystem



12.6.4 HANTERINGSREGLER KOPPLADE TILL INFORMATIONSKLASS

Informationsklassificeringen ska kopplas till hanteringsregler för att få verkan. Det innebär att för varje informationsklass ska det finnas tillämpliga regler för hur informationstillgångar får hanteras i varje given miljö. Detta är mycket en fråga som måste beslutas av varje företag utifrån behov, värderingar och bedömningar av tillämpliga hot och risker.

Det kan vara så enkelt som att konstatera att ”skyddsvärd information ska hållas inlåst eller under uppsikt” eller så komplext som en hel vägledning som bara reglerar hur hanteringen får och ska gå till.

Som vanligt gäller att det är bättre att göra något än att inte göra något alls.

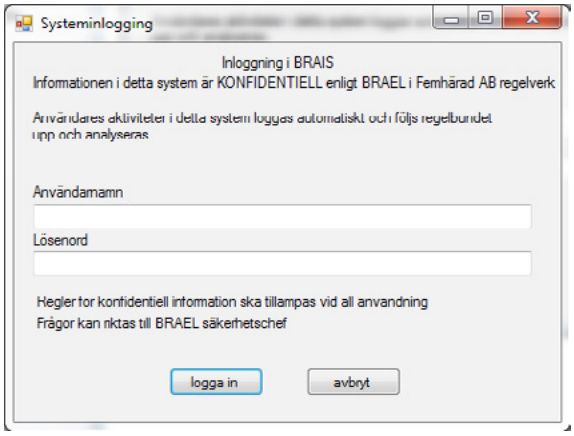
I denna vägledning ger vi ett enkelt exempel utifrån tidigare exempel på klassificering. Ökad grad, alltså mer skyddsvärd, av klassificering medför ett ökat behov av tydlighet och utförlighet i beskrivning av hur en informationstillgång får och ska hanteras, användas, delges, försändas, förvaras och avvecklas. I exemplet får antaganden göras om att den som beslutar om delgivning eller annan åtgärd kopplad till en informationstillgång är utsedd och känd av de som använder informationstillgången.

I exemplet på nästa sida ges endast korta fraser och ledord som ger en uppfattning om vad som behöver regleras i varje enskilt fall.

Vid delgivning av sådan information som för företaget är det mest skyddsvärda utifrån ett konfidentialitetsperspektiv så bör ett kvittensförfarande äga rum. Det innebär att man dokumenterar vem eller vilka som tagit del av informationstillgången, när och under vilka former. Om en händelse inträffar där det kan antas att sådan information utnyttjas otillbörligt så är delgivnings/kvittenslistor ett viktigt verktyg i utredningssyfte.

Analogt med ovanstående resonemang kring kvittering så bör aktiv säkerhetsloggning användas i motsvarande syfte och funktion i IT-system. En viktig sak i det sammanhanget är att informera om att sådan loggning sker, exempelvis i form av text i samband med inloggning i det aktuella systemet. Se exempel i figuren på nästa sida.

INFORMATIONS-KLASS	ANVÄNDNING HANTERING	DELGIVNING	FÖRSÄNDNING	FÖRVARING	AVVECKLING
Öppen	Inga restriktioner	Inga restriktioner	Inga restriktioner	Inga restriktioner	Informations-ägare beslutar
Intern	I alla företagets IT-system enligt arbetsordning	Till företagets personal. Annan personal efter delegat från VD eller säkerhetschef	Får sändas utanför företaget till godkända parter via e post och vanlig post	Inte öppet i utrymmen som är allmänt tillgängliga för personer som inte är anställda i företaget	Informations-ägare beslutar Metod: Papper: Tuggas IT-bundet: Överskrivning
Konfidentiell	Endast i BRAIS IT-system eller i pappersform	Endast utsedda eller beslutade av VD eller säkerhetschef Kvittenslista är krav	Till godkända parter krypterat med av säkerhetschef godkänt filkrypto eller till dito med rek post	I låst tunnplåtsskåp eller förvaring med högre skyddsnivå	VD eller säkerhetschef beslutar Metod: Papper: Tuggas IT-bundet: Destrueras



Bildtext: Exempel på information om loggning av användares aktiviteter i samband med inloggning i ett system.

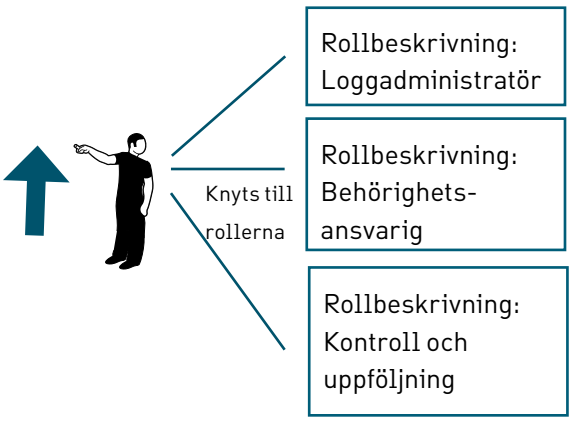
12.7 PERSONALRESURSER OCH SÄKERHET

Enligt ISO 27000 så är målet här att säkerställa att anställda, uppdragstagare och tredjepartsanvändare förstår sitt ansvar och är lämpliga för de roller de avses ha och för att minska risken för stöld, bedrägeri eller missbruk av resurser. Se även Kap. 9 Personal i denna vägledning.

12.7.1 BEFATTNINGAR, ROLLER OCH ROLLBESKRIVNINGAR

I samband med att ett företag etablerar en sund säkerhetsfunktion och säkerhetskultur så är det viktigt att ansvarsfördelning definieras. Denna ansvarsfördelning inbegriper vilka uppgifter den enskilde medarbetaren har inom ramen för säkerhetsarbetet. Detta är något som inte sällan endast finns i tankevärlden och dokumentation som reglerar vilka uppgifter en medarbetare har i säkerhetsarbetet är ofta bristfällig eller obefintlig.

Erfarenheten ger vid handen att det ofta är svårt att hålla befattningsbeskrivningar för medarbetare uppdaterade över tiden. Ett bättre sätt är då att bara övergripande dokumentera ansvarsområden i befattningsbeskrivningar och sedan knyta roller som beskrivs separat till respektive befattning. På detta sätt underlättas även dokumentativt och administrativt arbete i samband med att en medarbetare förändrar sina uppgifter. En befattning kan knytas till en eller flera roller föränderligt över tiden. Se figur på nästa sida.



Det finns två stora vinster för företaget med att tydligt dokumentera säkerhetrelaterade uppgifter i berörda befattningar och rollbeskrivningar.

1. Det blir mycket enklare att analysera säkerhetsfunktionen på företaget. Finns det utpekat ansvar för alla definierade säkerhetsrelaterade uppgifter? Om inte, varför? Hur kan dessa fördelas så att bästa effekt för verksamheten uppnås?

2. Effektivitetsvinster. Det blir sällan eller aldrig något problem med att uppgifter inom säkerhetsarbetet "faller mellan stolarna" eller utförs av flera parallellt.

Rollbeskrivningar behöver inte, och ska normalt sett inte vara omfattande eller komplexa. Roller och uppgifter bör beskrivas på en nivå som är lättbegriplig men ändå inte lämnar något utrymme för misstolkning. Ponera ett exempel där en person som arbetar i administrationen ges en säkerhetrelaterad roll som tillikauppgift för att separera kontrollfunktioner från utförarfunktioner, i detta exempel logghantering.

Exempel på utdrag ur rollbeskrivning:

> Rollen utgör loggadministratör för företagets IT-miljö.

> Som loggadministratör ansvarar medarbetaren för att på kvartalsbasis gå igenom kvartalsloggfil med stöd av verktyget LoggWizard och där enligt fördefinierade rutiner som återfinns i säkerhetsinstruktionen genomföra uppföljning och analys. En loggrapport ska upprättas vid varje analystillfälle och arkiveras i företagets loggsäkerhetspärm hos säkerhetschefen. Om loggadministratören upptäcker oegentligheter eller fel i samband med uppföljning och analys vidtas åtgärder enligt "rutin för utfall vid logganalys" som återfinns i säkerhetsinstruktionen.

Naturligtvis måste detaljerade rutiner för de uppgifter som åläggs finnas definierade. Vidare måste rollinnehavaren få eller inneha adekvat utbildning för de roller och uppgifter som denna åläggs.

12.7.2 KONTROLL AV PERSONAL FÖRE ANSTÄLLNING

Om en tillsättning/tilldelning av en befattning eller roll rör rikets säkerhet eller skyddet mot terrorism så gäller vad som anges i Kap. 8 Uppgifter som rör rikets säkerhet eller skyddet mot terrorism i denna vägledning.

I övriga fall finns ett flertal metoder och verktyg för att kontrollera en persons lämplighet inför anställning, tillsättning/tilldelning av en befattning eller roll. Exempel på detta är:

> Kontroll av personen via sociala medier.

> Tagande av referenser.

> Begära att personen frivilligt ska lämna uppgift ur belastningsregistret hos Polisen.

Observera att en sådan kontroll och eventuella beslut som grundas på utfall från sådan kontroll inte får ske på ett sätt som kan anses vara kränkande av den enskildes integritet, enskilda förehavanden, religiös övertygelse eller läggning.

12.7.3 UTBILDNING

Säkerhetshöjande (eng.)Security awareness program är ett bra sätt att generellt höja säkerhetsmedvetandet vid ett företag. Sådana program kan utformas på olika sätt, vara olika djupa och omfattande. Om ett företag har etablerat, eller ska etablera en förbättrad säkerhetsfunktion och säkerhetskultur så föreligger ett behov av att förmedla innehållet i denna. Att få medarbetare och andra tillämpliga samarbetspartners att ta

till sig och följa det säkerhetsrelaterade regelverk som etableras.

Det finns några saker som bör påpekas särskilt när det gäller att förmedla kunskap om regler, ansvar och uppgifter som rör säkerhet.

> Det finns sällan tid eller utrymme att täcka in hela området i en förmedlad utbildning såsom seminarier, interaktiva utbildningar etc. Prioritera vad som är viktigast och ta med det. Informera om resten och hänvisa till tillgänglig dokumentation.

> Utbildning är nödvändig. Oavsett om det sker i seminarieform, distribuerad dokumentation med kontrollfrågor/examination eller om det sker med stöd av interaktiva program.

> Regelbundenhet är den enskilt viktigaste punkten. Som med allting annat så faller saker man lär sig i glömska. Återkommande repetition, i förekommande fall med uppdaterat material, är bästa sättet att vidmakthålla en god säkerhetsnivå över tiden.

I frågan om val av metod för att utbilda och förmedla kunskap om säkerhetsrelaterat regelverk så måste det påpekas att det finns skillnader i framgångsfaktor beroende på val av metod. Nedan räknas tre generaliserade metoder upp med kommentarer kring genomförande och utsikter till framgång. Kostnader är abstrakt återgivna och ska ses jämförda mot varandra för respektive metod.

> Nr 1: Utbildning/Förmedling genom spridning av information/dokumentation [Framgångsfaktor: låg, arbetsbelastning/kostnad: låg]. Detta är den enklaste formen för att nå ut med information om exempelvis förändringar i regelverk. Typiskt så förmedlas information till berörda via e-post eller motsvarande. Några läser och förstår, några skummar innehållet på det viktigaste och ett antal lämnar det helt utan åtgärd. **Denna utbildningsmetod bör undvikas eller kompletteras med varianter av nummer 2 eller 3.**

> Nr2: Utbildning genom ett eller flera seminarier. I förekommande fall med prov/uppgifter för deltagare. [Framgångsfaktor: medel, arbetsbelastning/kostnad: medel]. Vanligtvis genomförs seminariebaserad utbildning i samband med större förändringar. Det är en traditionell och vedertagen metod men de flesta känner till dess brister. Seminarier blir aldrig bättre än utbildaren. Detta är ändå en mycket bättre metod än nummer 1 då det går att ställa frågor och aktivt delta under själva utbildningen/seminariet. **Denna utbildningsmetod är att föredra framför nummer 1.**

> Nr 3: Interaktiv utbildning genom exempelvis webbapplikation. [Framgångsfaktor: hög, arbetsbelastning/kostnad: medelhög]. Detta är en metod att utbilda i säkerhet som började användas under första halvan av 00-talet. Vinsterna med denna form av utbildning visade sig tämligen omgående och består bland annat av följande. Kontroll av att all berörd personal har genomgått utbildningen, kontroll på utfall, god förmåga till repetitionsutbildning och god förmåga att snabbt och enkelt uppdatera innehållet. **Denna utbildningsmetod rekommenderas om man vill nå framgång i sitt säkerhetsarbete.**

Oavsett vilket metodval man gör så är det viktigaste att utbildning och repetition genomförs. Utan utbildning kan man inte påstå att säkerheten har etablerats inom företaget. Vidare är en förutsättning för vidmakthållande att repetition sker över tiden och vid behov, exempelvis i samband med uppdateringar eller som följd av erfarenheter från incidenter.

12.8 FYSISK OCH MILJÖRELATERAD SÄKERHET

Här avses enligt ISO 27000 att förhindra obehörigt fysiskt tillträde, skador och störningar i organisationens lokaler och information.

Då elbranschen berörs av bland annat säkerhetsskyddslagstiftning påverkas kravbilden på fysiskt skydd i olika avseenden som ofta

går utanför vad som anges i ISO 27000 standarden. Fysiskt skydd har således ett eget kapitel i denna vägledning se vidare Kap. 10 Fysiskt skydd i denna vägledning.

12.9 STYRNING AV KOMMUNIKATION OCH DRIFT

Syftar enligt ISO 27000 till att säkerställa korrekt och säker drift av informationsbehandlingsresurser. Se vidare Kap. 13 IT-säkerhet i denna vägledning.

12.10 STYRNING AV ÅTKOMST

Syftar enligt ISO 27000 till att styra åtkomst till information.

Se även Kap. 13.18 Autentisering och auktorisation i denna vägledning.

I ovan nämnda kapitel beskrivs främst de tekniska aspekterna vad gäller styrning av åtkomst till informationstillgångar. I detta kapitel kommer främst de administrativa rutiner och funktioner som berör detta att avhandlas.

12.10.1 BEHOVSPRÖVNING OCH LÄMPLIGHET

All tilldelning av behörigheter till informationstillgångar bör bygga på ett behov sprunget ur den verksamhet som berörs. Ofta misstolkas konfidentialitet i det avseendet att **"ingen får ta del av den konfidentiella informationen".** Detta är en direkt felaktig tolkning av begreppet. Det betyder snarare **"det finns en definierad grupp som är behörig att ta del av och/eller på annat sätt hantera informationen".** En märkning som implicerar konfidentialitet av något slag innebär att det finns en uttalad tilldelning av behörighet.

Ett gammalt sätt att beskriva behörighet att ta del av informationstillgångar, som dock ännu håller, lyder i lite mer modern tappning; "Behörig till ett objekt är den som har rätt säkerhetsklarering och behöver objektet för att lösa sina arbetsuppgifter". För anställda vid myndigheter i Sverige betyder det att personen ska vara registerkontrollerad i rätt klass och ha behov av informationen för att sin tjänst.

För ett företag som strävar efter att ha en sund behörighetsprocess så finns således minst två möjliga attribut att göra bedömningar på; lämplighet och ett verksamhetsbehov. Båda dessa är lämpliga att beakta i samband med behovsprövning avseende tillgång till skyddsvärda informationstillgångar. I vissa fall, när det gäller information som rör rikets säkerhet eller skyddet mot terrorism, så gäller dessutom särskilda regler, se vidare Kap. 8 Uppgifter som rör rikets säkerhet eller skyddet mot terrorism.

För ett företag som utformar och tillämpar en process för behovsprövning vad gäller information **som inte** rör rikets säkerhet eller skyddet mot terrorism men som ändå av företagsmässiga skäl betraktas som skyddsvärd så finns ett antal alternativ på saker som kan ligga till grund för bedömning och prövning av en persons lämplighet.

- BEHOV
  Naturligtvis måste det föreligga ett verksamhetsbehov, det är grunden för att ett behov ska kunna sägas vara befintligt.
- VANDEL
  För ett företag finns ett antal olika sätt att kontrollera en persons vandel. Det kan exempelvis vara sökningar på Internet, i sociala medier m.m. Observera att det inte handlar om åsiktsregistrering utan om en allmän prövning av lämplighet.
- REFERENSER
  I samband med tilldelning av behörighet till skyddsvärda informationstillgångar bör alltid referenser kontrolleras. Detta gäller såväl uppgivna referenser som att höra efter med branschföreträdare i övrigt.

Ett företag är **inte skyldigt** att ge en person behörighet till informationstillgångar som, om de utnyttjas fel, kan skada företaget. De kan välja att göra det.

12.10.2 BEHÖRIGHETSADMINISTRATION

Med behörighetsadministration avses här de rutiner och processer som stödjer det administrativa arbetet med behörighetstilldelning. Det innebär i allt väsentligt att det ska finnas en dokumenterad rutin, journaler m.m. där behörigheter registreras och löpande följs upp.

Dokumentationen bör minst bestå av två

delar. En instruktion som reglerar arbetet för de som administrativt sköter behörighetsadministrationen samt en journal, tabell eller motsvarande som innehåller information om vilka behörigheter en enskild har tilldelats. Sådan journal eller tabell bör minst innehålla:

> Vem behörigheten tilldelats.
> Vilken behörighet som tilldelats.
> I vilket eller vilka system behörighet tilldelats.
> När behörigheten börjar gälla.
> När behörigheten slutar gälla.
> Vem som beslutat om behörighets tilldelning.
> Eventuellt särskilda villkor för (tillfälligt) upphävande av behörigheten såsom långtidssjukskrivning, tjänstledighet m.m.

Det är i detta sammanhang viktigt att berörd dokumentation hålls uppdaterad över tiden för att säkerställa att behörigheter hanteras på ett riktigt sätt.

12.10.3 REVOKERING AV BEHÖRIGHETER

En sak som ofta brister, såväl i myndighetsvärlden som i företagsvärlden, är revokering av behörigheter. Många IT-incidenter kan tillskrivas att det, länge, har legat kvar gamla, mer eller mindre kända, behörigheter i IT-system som sedan utnyttjas otillbörligt.

Det finns tre återkommande exempel där revokering av behörighet ofta brister:

> **(eng.)Defaultlösenord**
Många system och program har fabriksinställda konton och lösenord som är avsedda att användas i samband med förstagångsinstallation. Dessa kan lätt falla i glömska och bli kvar i systemet även efter driftsättning. Detta är ett allvarligt hot mot system då dessa behörigheter oftast är av typen (eng.)root, vilket innebär fullständiga administrativa rättigheter.
> Medarbetare som avslutat sin tjänst eller bytt roller eller befattning. Det är viktigt att åtgärder som rör ändringar i tjänst, befattning och roller uppmärksammas i behörighetsprocessen.
> Systemförändringar som innebär att tekniska användarkonton[8] inte längre behöver användas eller inte längre kräver lika långtgående behörigheter i systemsammanhang.

Ovanstående exempel utgör endast en del av problematiken men belyser ändå behovet av att reglera revokering i den dokumentation som styr behörighetsprocessen.

12.11 ANSKAFFNING, UTVECKLING OCH UNDERHÅLL AV INFORMATIONSSYSTEM

Målet här är enligt ISO 27000 att säkerställa att säkerheten är en integrerad del av informationssystem.

Utöver vad som i detta kapitel anges om utveckling, se även Kap. 13 IT-säkerhet och Kap. 9 Personal i denna vägledning.

Ofta har små organisationer och företag inte de resurser som erfordras för att, på ett säkerhetsmässigt godtagbart sätt, utveckla egna system av mer än ringa storlek. Säkerheten i egenutvecklade applikationer och motsvarande ligger ofta i det underliggande systemet, oftast operativsystemet. Detta ställer i sin tur krav på hur ett egenutvecklat system får användas, spridas, kommunicera etc. Effekten av detta blir ofta att utöver själva utvecklingen av applikation eller system så tillkommer bland annat:

> Analys av omständigheter kring avsedd användning, inkluderar lämpligen riskanalys.
> Framtagande av systemdokumentation, bland annat för att minimera nyckelpersonberoende.
> Framtagande av utbildningsmaterail och genomförande av utbildning för tilltänkta användare.

8. Avser användarkonton som används av system eller andra automatiska processer.

> Genomförande av testverksamhet i testmiljö.

> Framtagande av avbrotts- och återställningsplaner.

Exempel på riktlinjer för utveckling av egna applikationer och system finns exempelvis hos Open Web Application Security Project som ger ut öppna riktlinjer för en robust och säker programmering.

https://www.owasp.org/index.php/Main_Page

12.12 HANTERING AV INFORMATIONSSÄKERHETS INCIDENTER

Syftar enligt ISO 27000 till att säkerställa att informationssäkerhetshändelser och svagheter hos informationssystem kommuniceras på ett sådant sätt att korrigerande åtgärder kan vidtas i rätt tid.

Se vidare Kap. 14 Incidenthantering i denna vägledning.

12.13 KONTINUITETSPLANERING FÖR VERKSAMHETEN

Målet med kontinuitetsplanering är att motverka avbrott i organisationens verksamhet och att skydda kritiska verksamhetsprocesser från verkningarna av allvarliga fel i informationssystem eller katastrofer och att säkra återstart inom rimlig tid.

Se vidare Kap. 15 Avbrotts- och kontinuitetsplanering i denna vägledning.

13 IT-SÄKERHET

13.1 BESKRIVNING AV KAPITLETS INDELNING

Detta avsnitt i vägledningen syftar till att ge ett adekvat, lättarbetat och tillämpligt stöd i IT-säkerhetsarbetet, främst för små och medelstora elföretag. Innehållet är i allt väsentligt harmoniserat med ISO 27000 standarden men går inte in i alla detaljer. Innehållet tar upp sådant som av erfarenhet, och historiskt, bör ägnas uppmärksamhet i första led om IT-säkerhetsarbetet inte har getts tillräcklig uppmärksamhet tidigare.

13.2 DEFINITION AV IT-SÄKERHET

IT-säkerhet definieras av SIS enligt följande:

> Säkerhet beträffande IT-system med förmåga att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation.

Denna definition är bred och täcker väl in det som kan anses beröras av vad som benämns som IT-säkerhet. Det bör dock särskilt beaktas att inom elbranschen så utgör ofta industriella informations- och styrsystem en betydande del av IT för elföretagen. Dessa ska på intet sätt betraktas som undantagna från det som anges i avsnittet IT säkerhet. Tvärtom handlar en sund IT-säkerhet ofta om att harmonisera dessa olika grupperingar av IT så att säkerheten optimeras.

13.3 DOKUMENTERADE INSTRUKTIONER FÖR DRIFT, KONFIGURATION OCH ÄNDRINGSHANTERING

Det finns många exempel på när drift av IT-system, i synnerhet hos mindre organisationer och företag, sker (lat.)Ad-hoc, dvs. löpande i ett reaktivt beteende och ofta av en eller ett par enskilda personer. Inte sällan med olika ansvarsområden. Detta beteende leder ofelbart till nyckelpersonberoende och kommer över tiden att leda till störningar eller avbrott i IT-driften som kan vara allvarliga eller rent av omöjliga att återställa. De flesta som tillämpat eller perifert arbetat med IT i mindre organisationer eller företag vet att detta är ett befintligt, och allvarligt, problem som i slutändan inte sällan leder till merkostnader och/eller verksamhetsskador.

En enkel jämförelse med andra verksamheter ger vid handen att en sådan situation inte bara är ohållbar utan rentav absurd.

> Jämför ovan nämnda beteende med ett företag som tillverkar exempelvis en bil. Någon tar fram en prototyp som är bra på alla sätt. Vederbörande blir sedan opasslig eller på annat sätt indisponibel. Härvid framkommer att det inte finns några ritningar, felsökningsinstruktioner eller manualer på bilen. Således

måste företaget endera genomföra baklängeskonstruktion, (eng.)reverse engineering, på prototypen eller helt enkelt börja om från början igen.

Sett mot ovansagda exempel är det rent av skrämmande att många mindre och medelstora företag och organisationer tillåter sig själva att hamna i en situation där nyckelpersonberoende och avsaknad av dokumentation ytterst gör IT miljön till en tidsinställd bomb som bara väntar på rätt tillfälle att orsaka en störning eller ett avbrott som inte så lätt låter sig åtgärdas.

Sättet att adressera ovan nämnda problematik är att ha en dokumentation kring sina IT-miljöer som gör att nyckelpersonberoende minimeras och felsökning, återställning och reparation underlättas. Det finns några viktiga begrepp som måste beaktas när sådan dokumentation tas fram för att maximera nyttan med densamma. Dokumentationen måste vara:

> BEFINTLIG
Den ska vara framtagen och färdigställd.

> KOMPLETT
Den ska omfatta alla aspekter av IT-miljön.

> KORREKT
Den ska inte innehålla fel och vara uppdaterad m.a.p. ändringar i IT miljön.

> TILLGÄNGLIG
Den ska finnas till hands för de som behöver den när de behöver den.

Ovanstående påståenden om drift-, system- och förvaltningsdokumentation för IT kanske framstår som självklara men erfarenhet och historia talar tyvärr om att läget är ett annat.

Många gånger räds organisationer och företag framtagning av dokumentation i största allmänhet eller dokumentationsprojekt i synnerhet. Uppfattningen är ofta att det blir onödigt stora aktiviteter kopplade till dokumentation jämfört med själva IT-miljön eller rent av den verksamhet som ska stödjas. Inte sällan blir det så, men det behöver inte vara så. Ofta finns det erfarna tjänsteleverantörer på dokumentationsområdet att anlita. Fördelen med dessa är att de har genomfört sådana projekt och aktiviteter många gånger och oftast har en stor erfarenhetspool med tidigare framtagen dokumentation som medger återbruk i tillämpliga delar. Aktiviteter med att ta fram dokumentation för drift och förvaltning av IT bör dock alltid anpassas efter storlek och komplexitet på objektet, IT miljön, ifråga.

Ett exempel på ett bra sätt att hantera drift- och förvaltningsdokumentation är att skapa en s.k. wiki, jämför Wikipedia m.fl. Genom att göra detta får man ett dokumentationskoncept som medger enkelt underhåll, uppdateringar, återkopplingar m.m. Rätt tillämpat hjälper det också till att uppfylla de tidigare nämnda begreppen (befintlig, korrekt, komplett och tillgänglig) som en bra dokumentation bör präglas av.

I sådana fall man avser använda system eller programvara för att skapa en wiki eller motsvarande bör man om möjligt säkerställa att denna inte är Internetbaserad utan utgör en egen företagsbaserad instans av ett sådant system. Det innebär i klartext att programmet/systemet exekverar på företagets IT-resurser, inte på Internet.

Ett exempel på wiki som finns som färdigt koncept och är gratis att använda är mediawiki, se nedanstående länk.

http://www.mediawiki.org/wiki/MediaWiki

En sak som alltid bör beaktas med elektroniskt hanterad dokumentation för drift och förvaltning är att den kan göras tillgänglig även vid stora eller totala avbrott i IT miljön. Detta kan göras på två huvudsakliga sätt:

1. Skriva ut dokumentationen
Det är alltid bra att ha utskriven dokumentation men följande bör beaktas och göras uppmärksamt för brukaren av utskriven dokumentation. Version kan vara oklar m.a.p. uppdatering av IT-miljön. Detta följer av att drift- och förvaltningsdokumentation ofta är stor till volym och utskrifter är tungjobbade. Med detta sagt är det dock bra att ha en utskriven kopia i säkert förvar även om den inte är helt uppdaterad.

2. Ha en särskild elektronisk kopia, en egen instans, av wikin eller annan elektronisk

dokumentation. Det behöver inte vara en avancerad IT-miljö för att hantera wiki eller dokument utan det duger med vanliga COTS[9] . I de flesta fall torde det räcka med en bärbar PC för några tusenlappar. En sådan PC bör dock förvaras på ett sätt så att den skyddas mot sådana hot som kan påverka den övriga miljön, exempelvis strömspikar, oönskade vätskeutsläpp, geomagnetisk påverkan m.m. **Ett exempel** på lämpligt sätt kan vara att förvara den i ett jordat plåtskåp i ett brandskyddat område i egen byggnads inre beläget minst en våning ovan jord.

Drift- och förvaltningsdokumentation för IT-miljöer bör alltid omfatta minst fyra huvudsakliga dokument.

1. Systemdokumentation
(HIK Handbok Installation & Konfiguration)
Systemdokument för bland annat installation och konfiguration.

Utgörs ofta av en del förklarande text om systemsamband kompletterade med olika installationsanvisningar för produkter och system. En av de viktigaste sakerna med systemdokumentationen (HIK:en) är att den återspeglar vilka organisations- eller företagsspecifika konfigurationsändringar som måste göras efter exempelvis en standardinstallation av ett serveroperativsystem.

2. Drifthandbok
Ska beskriva vilka dagliga och övriga regelbundna, stickprovsbaserade och händelsestyrda aktiviteter som ska och bör vidtas i olika sammanahang i IT miljön. Några exempel kan vara tagande av särskilda säkerhetskopior, test av återställning av objekt från säkerhetskopia, uppgradering eller byte av disk eller hantering av loggar.

3. Driftjournal
En logg över sådana åtgärder som vidtas i IT-miljön. Syftet med journalen är att det ska vara möjligt att spåra, och eventuellt återskapa, händelseförlopp i IT-miljön samt att det ska vara möjligt att kontrollera att inga fel har begåtts.

4. Förvaltningshandbok
En instruktion som ska ta upp saker som inte direkt rör driften men som kommer att påverka den. Exempel kan vara omsättnings- och uppgraderingsplaner för hård- och mjukvara. Instruktioner för hur planering av system- och applikationsförändringar får och ska gå till. Här kan även drift- och förvaltningsorganisationen återges med roller och befattningar och i en bilaga kan dessa kläs med faktiska personer med kontaktuppgifter.

Ovanstående benämningar handbok, journal etc. kan ge sken av ett omfattande dokumentativt arbete. Då kan följande vara tänkvärt.

> Allting ska göras så enkelt som möjligt
> – men inte enklare
>
> Citat: Albert Einstein (1879 – 1955)

Dokument ska inte skapas för dokumentens skull utan för det syfte de avses. Ovanstående citat är således fullt tillämpligt i detta fall ty man måste ha en dokumentation som lever upp till de förväntningar som ställs på densamma annars kan den rent av bli kontraproduktiv.

Ovan nämnda fyra dokument ska ses som en vägledning i vad som behöver dokumenteras. Därmed inte sagt att detta måste göras i fyra volyminösa egna dokument. Anpassning till IT-miljön som ska dokumenteras, verksamheten som ska stödjas och andra faktorer spelar naturligtvis in. För många mindre organisationer och företag räcker det ofta att skapa ett dokument med ovanstående som innehållsrubriker och en del tillämpliga bilagor.

Anpassa dokumentationens omfattning till IT-miljön och verksamheten, inte tvärtom!

13.4 ROLLER I DRIFT- OCH FÖRVALTNINGSORGANISATION

Drift och förvaltning av IT handlar i allt väsentligt om att tillgodose verksamhetsbehov genom att tillhandahålla och upprätthålla tekniska lösningar som stödjer verksamheten.

9. (eng.)Commercials Off The Shelf.

I dessa sammanhang är det bra om det finns uttalade verksamhetsbehov som ska lösas med stöd av IT. Således finns här behov av roll/er som identifierar verksamhetsbehov och formulerar krav som kan omsättas till lösningar. Andra roller bör sedan ges uppgiften att realisera, ta fram, lösningar för att möta och uppfylla dessa krav. Fördelen med ett sådant förfarande är att det finns en tydlig roll som har formulerat kraven på lösningen och således kan godkänna en framtagen lösning medan en annan roll har uppgiften att ta fram lösningen. Detta skulle förfelas om det var samma roll (i detta fall person) som stod för både krav och lösning. Det är, oavsett vilken organisationsform det gäller, svårt att motivera att den som tagit fram en lösning också är den som godkänner lösningen.

Olika företag är olika stora och har således skilda förutsättningar att närma sig denna problematik. Generellt bör några roller särskilt beaktas i detta sammanhang:

> Rollen "verksamhetsbehov" anger vilken funktionalitet som söks
"Jag vill kunna göra följande från min arbetsstation..."

> Rollen "kravställare" formulerar funktionella krav på en sådan lösning, exempelvis krav på hur ett gränssnitt och bakomliggande funktionalitet ska fungera i olika sammanhang. Rollerna "verksamhetsbehov" och "kravställare" kan utan risk för konflikt vara samma person.

> Rollen "utförare" tar fram en teknisk lösning. Funktioner, applikationer, system, integration m.m.

> Rollen "granskare/godkännare" går igenom den färdiga lösningen och "mäter" denna mot de ställda kraven. Om kraven anses vara tillräckligt uppfyllda så kan lösningen godkännas. Rollen "granskare/godkännare" kan vara samma som "verksamhetsbehov/kravställare".

Några saker måste beaktas i varje del av en sådan här process är:

> Säkerhetsaspekter (hot- och risker med funktion/lösning).

> Behovsanalys (behöver verksamheten funktionen).

> Ekonomisk rimlighet (kostnad/nyttokalkyl.

> Teknisk genomförbarhet (finns det lämpliga tekniska lösningar).

> Livslängd (är det lämpligt m.a.p. lösningens förväntade livslängd).

> Användbarhet (kommer det att fungera på ett användbart sätt).

Genomgång av ovanstående punkter kan antyda att processen är krånglig och tungjobbad men den ska betraktas utifrån ett övergripande rådgivande perspektiv. Tillämpning och anpassning måste naturligtvis alltid ske till det aktuella företagets förmåga och storlek. **Det viktigaste att ta till sig i denna process är dock att skilja på vem som utformar verksamhetsbehov och krav från den som tar fram lösningen på dessa krav. Detta sker i syfte att inte hamna i en olämplig jäv-liknande situation där den som tagit fram en lösning är densamma som godkänner den.**

Vad gäller tillämpliga befattningar som rör IT-säkerhet så hänvisas till 7 Organisation i denna vägledning.

En sak som tål att påpekas särskilt är att oavsett vilka befattningar man väljer att ha i en IT-säkerhetsorganisation så ska det finnas övergripande beskrivningar som åskådliggör befattningens ansvarsområde samt detaljerade rollbeskrivningar som kan knytas, tilldelas, befattningar. Dessa är till stor hjälp för att klara ut avgränsningar, ansvarsområden samt för att analysera om det saknas resurser för ett ansvarsområde eller en viktig uppgift. Erfarenheten ger vid handen att det, främst i mindre företag brister i befintlighet och utformning av sådana beskrivningar.

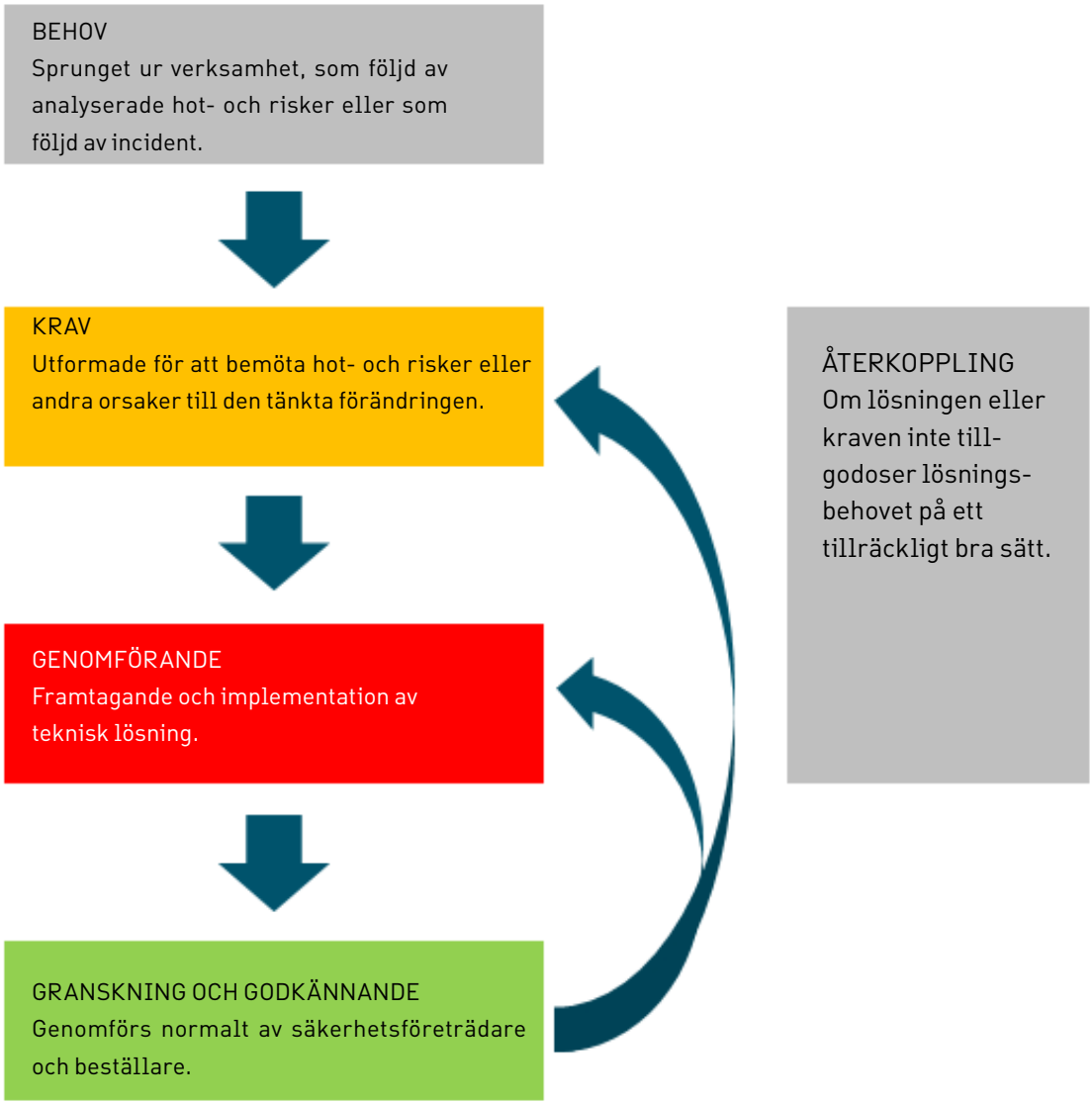
Analogt med resonemanget ovan om beställar- och utförarrollen så måste även förhållandet kravställare, utförare, granskare beaktas. När det gäller säkerhetskrav som ställs på IT så ska granskningen och godkännandet av kravuppfyllnaden, dvs. utförandet på den tekniska lösningen ske av någon annan. En kravställare kan också vara granskare men det synes olämp-

ligt att denne också är utförare. I de fall det finns någon IT-säkerhetsorganisation så bör arbetsgången i möjligaste mån följa gången behov – krav – genomförande – granskning och godkännande.

Även resonemanget i figur 10 kring förhållandet kravställare, utförare (genomförande), granskare kan framstå som komplext och omständigt. Härvid måste det påpekas att även denna process är skalbar och bör göras så enkel som situationen tillåter. En betydande framgångsfaktor är dock att, om än i en förenklad form, dokumentera vad som gäller i de olika stegen av denna process.

13.5 UTVECKLING OCH TEST SAMT TEST- OCH REFERENSMILJÖER

Många organisationer och företag, och här inte endast små och medelstora utan även stora företag och organisationer, har drabbats av problem kopplade till det faktum att man blandar exempelvis test eller utveckling med produktionsmiljön. Det är än idag inte ovanligt att förändringar som inte är testade sker direkt i produktionsmiljö och påverkar denna negativt.



Figur 10. Förhållandet kravställare, utförare (genomförande), granskare.

Exempel:
Ett E-handelsbolag där driftpersonal genomför otestad förändring av webbplats som leder till driftstörning eller avbrott med ekonomiska konsekvenser som följd.

För en organisation eller ett företag som har ett starkt beroende till IT så behövs i huvudsak tre olika typer av IT-miljöer som på olika sätt är separerade ifrån varandra.

> PRODUKTIONSMILJÖ(ER)
I produktionsmiljö får endast det som behövs för verksamhetens drivande förekomma. Produktionsmiljö kan vara ett samlingsnamn på flera logiskt eller fysiskt separerade miljöer. Det kan exempelvis vara kontorsinformationssystem med ekonomi och HR[10]-system eller egen miljö med industriella informations- och styrsystem.

> TESTMILJÖ(ER)
En testmiljö ska minst på logisk nivå likna den miljö som den avser utgöra testmiljö för. I vissa fall krävs även att denna miljö har samma typ av hårdvara. Själva essensen med en testmiljö är att där försöka framkalla fel, störningar eller avbrott genom att testa system och applikationer till extrema nivåer. Detta i syfte att hitta potentiella felkällor och åtgärda dessa innan något driftsätts i produktionsmiljö. Det bör särskilt påpekas att det kan behövas en särskild testmiljö för industriella informations- och styrsystem.

> REFERENSMILJÖER
Det finns ofta flera referensmiljöer. Det är i grunden en miljö som i allt väsentligt ska likna produktionsmiljön och användas exempelvis för test av återställning av hel eller partiell säkerhetskopia. Det finns dock många tillämpningar och i takt med att många system fungerar på standardmässig hårdvara så har kravet på att referensmiljöer ska vara helt produktionslika avtagit.

10. (eng.) Human resources

När det gäller hur man tekniskt går tillväga för att sätta upp exempelvis test eller referensmiljöer så har teknikutvecklingen ökat valmöjligheterna markant sedan millennieskiftet. Virtualisering, olika typer av kluster och annan teknik samt lägre priser på olika typer av hårdvara ökar valmöjligheterna.

Denna vägledning kommer inte att försöka dra några generellt gällande slutsatser kring hotbilder för de olika typer av teknisk plattform som finns tillgängliga. Inte minst då hotbilder av detta slag har en tendens att förändras över tiden. Det måste dock påpekas att en av de enskilt viktigaste sakerna att företa i samband med val av detta slag är att genomföra en riskanalys där olika aspekter kopplade till de plattforms- och teknikval man står inför belyses, och då särskilt med avseende på användningsområdet. En sådan riskanalys **behöver inte** vara omfattande eller komplex utan måste som allting annat anpassas till ändamålet.

> Det skulle exempelvis kunna vara så enkelt som att beslut behöver fattas om anskaffning av testmiljö för systemet xyz. Xyz löper på en virtuell server i den stora produktionsmiljön på företaget Elbolab. Det synes rimligen naturligt att ha även testmiljön i en virtuell miljö och frågeställningen som hot- och riskmässigt kommer i första rummet är då rimligen om man vågar ha den virtuella testmiljön i samma fysiska maskin som den virtuella produktionsmiljön.

Belys och dokumentera riskerna innan beslut fattas!

Referensmiljöer skiljer sig definitionsmässigt från testmiljöer främst i det avseendet att de inte är avsedda för kortsiktiga och potentiellt destruktiva tester. Exempel på användningsområden är:

> Långvariga driftsäkerhetstester.

> Test av återställning av säkerhetskopia.

> Utvärdering av säkerhetshändelser, exempelvis som utfall från logganalys.

> Parallellkörning av ersättningssystem innan produktionsdrift.

13.6 UTKONTRAKTERING (ENG.)OUTSOURCING

Utöver vad som står i detta avsnitt se även 9.3 Entreprenörer och annan inhyrd personal eller företag i denna vägledning.

Vad som ofta förbises eller försummas i samband med utkontraktering av IT-verksamhet är säkerhetskrav. I många fall har den kontrakterade parten färdiga mallar, paket och avtal med förmånlig ekonomi. Att för en verksamhet som överhuvudtaget har något som är att betrakta som skyddsvärt, oavsett det rör säkerhet eller på annat sätt är kritiskt för verksamheten, anta ett sådant standardpaket för en utkontraktering är inte lämpligt om inte egna analyser validerat tillämpligheten för egna system och verksamheter.

Säkerhetskrav måste vara en integrerad del i alla upphandlingar som rör utkontraktering av IT. Att säga att det inte finns något i ett godtyckligt IT-system som är skyddsvärt och på detta sätt motivera att inte ha med säkerhetskrav är numera direkt osant. I princip alla IT-system innehåller exempelvis personuppgifter och omfattas redan där utav reglerad styrning.

Anledningen till att säkerhetskrav ofta ”glöms bort” i sådana här sammanhang är att de är kostnadsdrivande. Det bör då beaktas att kostnaden för att inte ha med säkerhetskrav kan bli mångdubbel i händelse av att något oönskat inträffar.

Det finns över tiden många exempel där organisationer och företag drabbats av denna problematik. Nedan ges ett exempel från 2012.

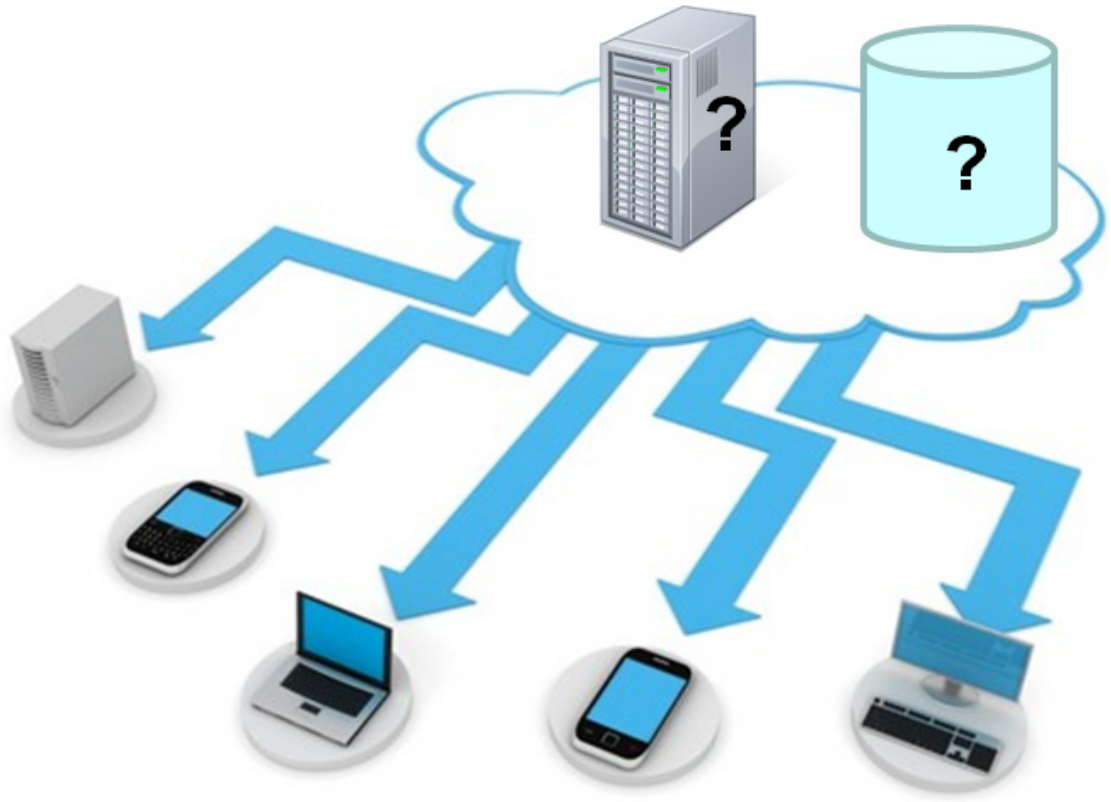
Källa: Computer Sweden

Utdrag:
...
Nyheter: Sedan Region Skåne outsourcat sin it flaggar it-chefen Niklas Sundler för att driftsäkerheten blivit sämre. "Det känns onekligen så, men vi väntar på en utomstående revision", säger han.
Region Skåne har i omgångar lagt ut delar av sin IT-verksamhet på utomstående leverantörer. Efter incidenter förra året, bland annat Tietos jättekrasch, menar nu Niklas Sundler som är tillförordnad IT-chef att driftsäkerheten troligtvis påverkats av outsourcingen.

– Vi måste fråga oss om vi inte har fått en sämre driftsäkerhet sedan outsourcingen. Det känns ju onekligen så, med tanke på de incidenter som inträffade förra året, men vi väntar på en utomstående revision, säger Niklas Sundler.

Efter Tietokraschen i november förra året tappade Region Skåne ett stort antal filer och i augusti förra året drabbades man av en annan störning som gjorde att man var nära att tappa ett stort antal patientjournaler.

– Den gången var det inte backup eller rutiner som räddade oss, utan ren tur, säger Niklas Sundler.
...



Figur 11. Molntjänster.

Denna vägledning ger inga råd om huruvida man bör utkontraktera IT-verksamhet eller inte utan fokuserar på vad som bör beaktas om detta övervägs.

Om utkontraktering av IT-verksamhet övervägs så bör minst följande steg vidtas:

- Riskanalys kopplad mot den IT-verksamhet som avses utkontrakteras. Lämplighet, vilka aspekter är viktiga, kan vi behålla insyn etc.
- Utformning av säkerhetskrav som ska ingå med god vägning i upphandlingsunderlag. Här bör särskilt nämnas att när det gäller rättsliga krav så finns inget utrymme för vägning eller förhandling. Sådana krav ska alltid vara uppfyllda.
- I samband med utvärdering bör personal med god säkerhetskunskap och erfarenheter från liknande aktiviteter delta.
- Rimlighetsvärdering och lämplighetsvärdering. Är det verkligen rimligt att anta att kontraktören kan uppfylla kraven till nämnda pris? Är det rimligt att flytta berörda uppgifter till exempelvis molntjänster som fysiskt kan lagra information i främmande land? Om något låter för bra för att vara sant så är det rimligen inte sant!

13.7 MOLNTJÄNSTER

Molntjänster, (eng.)Cloud services, även kallat molnet, är en teknik baserad på användning av datorer över Internet. Ofta kopplas stora resurser samman med stor, och för kunden, okänd geografisk spridning. Resurserna utgörs exempelvis processorkraft, lagringsresurser, applikationer och funktioner. Åtkomst sker oftast som tjänster på Internet. Ur säkerhetssynpunkt är det viktigt att påtala främst två saker.

- I molnet saknar kunden **kunskap om och kontroll** över infrastrukturen inklusive eventuella säkerhetsfunktioner.
- Av ovanstående punkt följer även att **uppföljning och granskning** inte kan ske.

> Information lagrad i molnet **omfattas av lagstiftningen i det land där den aktuella hårdvaran är geografiskt placerad.**

Sett mot ovanstående kan två viktiga slutsatser dras om molnet.

1. Molnet är inte lämpligt för hantering av okrypterad information som äger ett högt skyddsvärde och har krav på kontroll och möjlighet till uppföljning.

2. Om man ändå använder molntjänster till information som är skyddsvärd ankommer det på kunden att själv tillföra tekniskt skydd för informationen. Dvs. exempelvis att man krypterar informationen i sina egna system innan den placeras i molntjänster.

13.8 ACKREDITERING – SYSTEMGODKÄNNANDE

Ett bra sätt att hantera IT-system är att ha ett ackrediteringsförfarande. Det innebär att man beslutar på förhand vilka krav som ska vara uppfyllda för endera en viss typ av system eller för specifika system, allt beroende på hur stor eller komplex verksamheten och mognaden avseende exempelvis klassificering av information och system är.

Exempel på saker som bör ingå i beslutsgrunden för ett IT-system är:

> Skyddsvärdet

> Autentiseringsfunktioner

> Auktorisation/behörighetskontroll

Källa: SÄKERHET24 - Computer Sweden
publicerad 2013-09-24 av Jonas Ryberg
Utdrag (del av artikel):

...
Lätt lura myndighet med usb-minne
David Jacoby arbetar som säkerhetsexpert på antivirusföretaget Kaspersky. Precis som alla andra antivirusföretag säljer de mjukvara som ska skydda kunderna mot de senaste it-hoten och sårbarheterna.

Men i sin senaste rapport ifrågasätter David Jacoby hur effektiv den skyddstrategin egentligen är. Tillsammans med ett annat säkerhetsföretag, Outpost 24, valde han att undersöka hur duktiga företag är på att täppa igen de säkerhetshål de uppmärksammas på. Enligt den undersökningen tar det 80 dagar för ett svenskt företag att täppa igen ett nytt säkerhetshål. Det är något sämre än snittet för världen som samma undersökning sätter till 70 dagar.

- Många av företagen är sårbara också för sådant som är tio år gammalt. Vi är duktigare på att skydda oss mot sådant som är nytt och häftigt. Säkerhetsbranschen måste prata om det som är relevant och inte glömma bort gamla och triviala hot, säger David Jacoby.

Han kritiserar sin egen bransch för att bara vilja sälja på kunderna programvara - och inte lära ut säkerhetstänkande.

- Det är lätt att köpa ett program men svårt att lära hela personalen säkerhetstänkande, säger han.

...

> Funktioner för säkerhetskopiering
> Utfall från genomförda tester
> Logghantering

Exempel på formella saker som bör finnas med i beslutet:

> Systemägare eller systemansvarig
> Datum för beslut
> Eventuella avsteg från gällande krav
> Beslutets giltighet i tid
> Referenser till dokumentation som ligger till grund för beslutet

Ett ackrediteringsbeslut är att betrakta som ett formellt beslut om driftgodkännande. Således bör det finnas någon som är utsedd ägare till systemet, dvs. någon som inom organisationen äger ansvar för och hanterar ekonomi, säkerhet och användning av systemet.

Om förändringar i systemet genomförs så måste den som är ansvarig för systemet besluta om ett nytt ackrediteringsbeslut ska fattas på grundval av de nya ingångsvärdena. Det är alltså lämpligt att definiera vad som utgör betydande förändringar som medför behov av ny utvärdering och nytt beslut.

13.9 SKYDD MOT SKADLIG KOD

Många organisationer och företag anger ofta att de har ett fullgott skydd mot skadlig kod när de har installerat antivirusprogram och motsvarande på arbetsstationer och övriga tillämpliga datorer. Detta får dock endas anses utgöra en del av det totala skyddet mot skadlig kod vilket exemplet nedan visar på.

Anslutning av extern parts utrustning, oavsett det är en dator eller datamedia av något slag bör alltid vara reglerat. Den reglering man väljer bör också bygga på vad kommit fram till i sin riskanalys. Regleringen kan exempelvis ta sig uttryck i följande:

Man har gästterminaler tillgängliga som sitter på eget nät

Man har trådlöst nät för gäster som är segmenterat från det egna nätet

Det finns dokumenterade instruktioner om vilka datamedia som tillåts användas i de egna datorerna

För att de två första punkterna ska fungera så förutsätts att det på sådana terminaler eller nät finns tillgång till Internet och utskriftsmöjligheter.

Det har sagts att det bästa antivirusskyddet är det som man har i huvudet. Det är en sanning med modifikation. Gott säkerhetsmedvetande i kombination med väl uppsatta programsviter mot skadlig kod ger det bästa skyddet.

All personal bör under alla omständigheter utbildas i de säkerhetsregler som är beslutade inom företaget, på det viset minimeras risken för att exemplet i artikeln ovan upprepas.

Vad gäller antivirusprogram och program mot annan skadlig kod så bör sådan vara installerad på alla arbetsstationer och i övrigt där det inte är tekniskt olämpligt.

Historiskt finns ett glapp mellan konstors-informationssystem och industriella informations- och styrsystem. Härvid bör ovanstående formulering beaktas ” i övrigt där det inte är tekniskt olämpligt”. Strävan bör vara att skyddet är likvärdigt i företagets alla system där det är tillämpligt.

13.10 SÄKERHETSKOPIERING OCH ÅTERSTÄLLNING AV INFORMATION OCH DATA

Det enskilt vanligaste misstaget som görs vad avser säkerhetskopiering är att återställning, vare sig hel eller partiell, aldrig testas. När så den dagen kommer då ett fel, en incident med skadlig kod eller ett intrång föranleder en återställning så är osäkerheten stor.

Förr innebar säkerhetskopiering nästan alltid datamedia i form av band. I dagsläget sker mycket av de korta rotationerna direkt på disk och ibland saknas helt externa media som exempelvis band.

Oavsett hur rutiner och funktioner för säkerhetskopiering konfigureras så bör detta vara resultatet av ett behov som i sin tur är vägt mot analyserade hot och risker.

Olika typer av data och information kräver i sin tur olika nivåer och regelbundenhet vad gäller säkerhetskopiering. Oavsett teknisk lösning så

kan följande sägas om periodicitet i tagande av säkerhetskopior.

> Information som bearbetas dagligen inom ramen för verksamheten och som har påverkan på verksamheten bör säkerhetskopieras dygnsvis.

> Information som uppdateras sällan men är av betydelse för verksamheten bör säkerhetskopieras på ett sådant sätt att eventuell förlust är ringa. Om mängden inte är en påverkande faktor kan även denna typ av information säkerhetskopieras dygnsvis.

> Operativsystem behöver i sig inte säkerhetskopieras om inte beroendet till konfigurationer och tiden det tar att återskapa dessa i samband med en ominstallation uppväger fördelarna med att säkerhetskopiera.

> Applikationer och system bör alltid säkerhetskopieras i enlighet med tillverkarens rekommendationer. Om sådana saknas bör egen analys av data och information bestämma periodiciteten.

> Databaser i enlighet med tillverkarens rekommendationer. Ibland kan det vara motiverat att ta en fullständig diskavbildning som säkerhetskopia av en databas och i andra fall endast exportera databasfilen. Om rekommendationer saknas bör egen analys av data och information samt omvärldsundersökning rörande specifik databas bestämma periodiciteten.

> Övriga data eller information bör säkerhetskopieras i enlighet med tillgängliga rekommendationer, (lat.)De facto standarder eller i enlighet med resultat av egen analys.

I många IT-miljöer säkerhetskopieras information och data till ett SAN (eng.)Storage area network. Detta är ofta i ett kort perspektiv en acceptabel lösning. Om detta SAN:

> används enkom för att hantera säkerhetskopior,

> är logiskt beläget på ett eget nätsegment eller motsvarande,

> samt är försett med tekniska skyddsfunktioner för att motverka informationsförlust i samband med diskkrasch, exempelvis RAID5[11] med (eng.)Hot Swap.

Då kan detta SAN med fördel användas för säkerhetskopior på längre sikt. Vad som menas med längre sikt måste härledas genom lokal riskanalys. Det finns många faktorer som påverkar detta beslut, exempelvis:

> Det fysiska utförandet, skyddet, på datahallen där SAN:et är beläget (brandskydd, inbrottsskydd, skydd mot oönskat vätskeutsläpp m.m.).

> Att SAN:et är uppsatt med On-line UPS[12].

> A och B kraft till SAN:et.

> Reservkraftaggregat för datahall.

Oavsett hur hög säkerhetsnivå som omgärdar SAN:et måste man i slutändan ändå överväga det faktum att den fysiska maskinen kan råka ut för ett, än så osannolikt, totalhaveri med intern brand eller mjukvarufel som förstör innehållet på flera diskar oåterkalleligt. Det är således bra att ha en plan för vilken information som man vill ska finnas kvar efter en katastrof oavsett hur allvarlig den är. För denna information bör man sedan bestämma ett intervall, exempelvis halvår, år eller tvåårsbasis och växla ut bandkopior som förvaras i valv på annan geografisk ort. Exempelvis en bank i ett vidare geografiskt område.

När alla rutiner och funktioner är etablerade och dokumenterade, företrädesvis i drifthandbok eller motsvarande, återstår endast en sak. Att planera in och genomföra test av återställning i en referensmiljö. Planläggning av dessa test bör ske så att rutiner, funktioner och miljö som ska nyttjas för att genomföra test av återställning dokumenteras, företrädesvis i drifthandbok eller motsvarande. På motsvarande sätt bör testerna i förväg schemaläggas i driftjournalen. På detta sätt blir dessa tester en del av den dagliga driften, även om de sker sällan.

11. RAID (eng.)Redundant Array of Inexpensive Discs
12. UPS (eng.)Uninterrupted Power Supply

En bonuseffekt av detta är att man effektivt har minimerat ett av de vanligaste och allvarligaste hoten mot IT-driften.

13.11 KRYPTERING

13.11.1 ALLMÄNT

För att skydda egen information mot obehörig åtkomst eller förvanskning i samband med lagring transmission eller annan överföring så kan med fördel funktioner och teknisk utrustning för kryptering användas.

För de flesta operativsystem så finns idag möjlighet att använda redan befintliga funktioner för att kryptera lagrad information eller förbindelser. Exempel på sådana är MS BitLocker Drive Encryption för lagrad data, SSL för webbkommunikation och IP-sec för att kryptera informationsinnehållet i de paket som skickas över nätverk eller etablera en säker tunnel mellan två datorer i ett nätverk. Att använda dessa lösningar har fördelen att:

- om de implementeras rätt m.a.p. nyckel/certifikathantering är mycket säkra och
- att de är i stort sett kostnadsfria. Det kostar dock arbete att implementera och dokumentera dessa funktioner samt därtill kopplad nyckel/certifikathantering.
- Vid krypterad lagrad data när det gäller obehörig åtkomst till fysisk maskin (dator) så behöver detta inte per automatik innebära att data är röjt till obehörig utan denna kan fortfarande anses vara skyddad.

Ett annat sätt att skydda sin kommunikation mellan exempelvis ett huvudkontor och en anläggning är att använda hårdvara till uppkopplingen som redan är försedd med krypteringsfunktioner för att skapa en tunnel mellan respektive hårdvara, i vanligaste fall en kombinerad router/brandvägg. De flesta tillverkare av sådan utrustning har funktioner för detta inbyggt.

Man bör alltid analysera behovet av att kryptera enheter som kan medföras av medarbetare eller motsvarande utanför tillträdesbegränsat område. Detta gäller såväl lagrad data som kommunikation med system.

En sak som i alla tillämpningar av kryptering måste beaktas och omhändertas på ett säkert och dokumenterat sätt är hanteringen av nycklar och/eller certifikat. Det finns flera sätt att lösa detta på.

Där stöd för certifikat är befintligt så är det fördelaktigt att använda certifikat från en CA (eng.)Certificate Authority. Lagen (2000:832) om kvalificerade elektroniska signaturer gäller sådana certifikatutfärdare som är etablerade i Sverige och som utfärdar kvalificerade certifikat till allmänheten. En certifikatutfärdare som avser att utfärda kvalificerade certifikat till allmänheten är skyldig att anmäla detta hos Post- och telestyrelsen, som är tillsynsmyndighet.

Ett annat sätt som är tillämpligt exempelvis om man upprättar en tunnel mellan exempelvis två hårdvaruplattformar (router/brandvägg) är att man i egen regi dokumenterar och hanterar ett antal nycklar som samtidigt måste uppdateras i båda plattformarna. I detta fall är det viktigt att hanteringen av dessa nycklar omgärdas med tillbörlig säkerhet vad avser konfidentialitet då en röjd nyckel i allt väsentligt betyder att förbindelsen inte längre kan betraktas som skyddad. Man måste härvid även beakta att sättet att distribuera sådana nycklar står i paritet med det skydd man vill uppnå.

13.11.2 SÄRSKILDA BEAKTANDEN

OBS! Detta stycke gäller endast vis sådana tillfällen då företag erhåller uppdrag av Svenska kraftnät som omfattas av SUA.

Det bör här särskilt påpekas att hantering, här särskilt kryptering, av hemliga uppgifter, se vidare 8.2 Hemliga uppgifter och övriga uppgifter, alltid regleras i SUA avtal i samband med uppdrag som inbegriper hemliga uppgifter. Härvid regleras vid behov kryptering med stöd av utrustning som godkänts av TSA[13].

13. Totalförsvarets signalskyddssamordning.

OBS! Detta stycke gäller för uppgifter som rör rikets säkerhet eller skyddet mot terrorism och som konstaterats genom säkerhetsanalys enligt SvKFS 2013:1.

Vad som anges i 13.11 Kryptering, Allmänt är tillämpligt för uppgifter som rör rikets säkerhet eller skyddet mot terrorism och som konstaterats inom ramen för säkerhetsanalys, se vidare 8.2 Hemliga uppgifter och övriga uppgifter. Det bör här särskilt påpekas att uppgifterna till innehåll kan vara identiska med hemliga uppgifter hos myndighet. Detta beror på att lagstiftningen inte medger att uppgifter som upprättas och ägs av företag, definitionsmässigt, kan vara hemliga. Således ska företag som äger och hanterar uppgifter som rör rikets säkerhet eller skyddet mot terrorism sträva mot att hanteringen präglas av samma säkerhetsnivå som en myndighet omgärdar motsvarande uppgifter med. Tekniska lösningar såsom IT-system ska granskas avseende säkerheten i och kring systemet[14]. Detta gäller vid drifttagning av system som innehåller uppgifter som rör rikets säkerhet eller skyddet mot terrorism, förändring av system uppgifter som rör rikets säkerhet eller skyddet mot terrorism eller konstaterande att ett befintligt system innehåller uppgifter som rör rikets säkerhet eller skyddet mot terrorism. För att en sådan granskning ska vara trovärdig bör den vara oberoende. Validiteten av granskningar kontrolleras i samband med tillsyn eller när Svenska kraftnät begär in sådan uppgift.

13.12 ÅTKOMST FRÅN MOBILA ENHETER

De senaste tio åren har sett en explosionsartad ökning av mobila tillämpningar inom IT-området. Funktioner, applikationer och system kan styras med hjälp av mobila enheter som exempelvis surfplattor och telefoner.

I många fall innebär denna utveckling en förbättring i arbetssituation och –miljö för personal på fältet. Det finns dock flera aspekter på säkerhet som måste beaktas inom ramen för denna tillämpning. En sådan aspekt är att de mobila enheterna, av naturliga skäl, är små och lätt förkommer genom exempelvis slarv eller glömska. Detta kan vara svårt att ta till sig initialt då de flesta är rädda om sin surfplatta eller mobiltelefon. Statistiken talar dock ett tydligt språk och det finns en förklaring. I stort sett alla människor har idag en mobiltelefon. Många som jobbar i tekniska branscher har dessutom någon form av surfplatta eller en bärbar dator. Datorer, telefoner och/eller surfplattor som tillförs den enskilde för att lösa arbetsuppgifter är då inte den enskildes egendom och detta har en påverkan i hanteringen, omedveten eller inte.

I vissa fall kan det vara befogat att tillåta medarbetare att utföra kritiska handgrepp i verksamhetens system från egen utrustning, exempelvis som en del i beredskapsåtgärder. Sådana åtgärder bör dock vara förberedda med säkra, ackrediterade[15], lösningar för detta.

En annan aspekt på detta som måste beaktas är stöldrisken. Denna kopplad till erfarenheter av att arbetsutrustning ofta lämnas i exempelvis fordon i samband med lunch eller annat behovsuppehåll i arbetet medför en ökad säkerhetsrisk.

Man bör, med beaktande av föregående stycke, alltid överväga behovet av att låta kryptera data som lagras på mobila enheter.

Det synes onödigt att i denna vägledning ytterligare förklara det olämpliga i att tillåta att helt privat mobil enhet används för åtkomst till kritiska system i verksamheten.

Några saker som bör beaktas kopplat till användningen av mobila enheter i systemsammanhang är:

- Utbildning och dokumenterade instruktioner om hur mobila enheter får och ska hanteras. Detta bör regelbundet följas upp och kontrolleras.
- Utred behoven och identifiera risker kopplade till hur mobila enheter avses användas. Anpassa den tekniska åtkomsten efter resultatet.
- Välj tekniska lösningar som är säkerhetsmässigt beprövade i sammanhanget.

14. SvKFS 2013:1 17§
15. Av företaget godkänd teknisk lösning.

13.13 KOMMUNIKATIONS-INFRASTRUKTUR

Med kommunikationsinfrastruktur avses här nätverk, trådbundna eller trådlösa som används av det egna företaget för att förmedla data och information mellan personer och tekniska enheter som företaget förfogar över eller på annat sätt använder. Vidare avses tillämpliga korskopplingsutrymmen eller motsvarande.

13.13.1 NÄTVERK OCH TRÅDLÖSA NÄTVERK

I de flesta fall betraktas interna datanätverk som är förlagda i egna lokaler som säkra och i de flesta fall är detta ett korrekt antagande under vissa förutsättningar.

- Att kablage till trådbundet nät är förlagt på ett sätt så att den inte är åtkomlig för manipulation i utrymmen som kan beträdas av obehöriga.
- Att kablaget i sin merpart är möjligt att inspektera, dvs. synligt för behöriga och inte passerar genom utrymmen som man saknar kontroll över.
- Att utrustning som utgör del av korskoppling, routrar, hubar etc. huserar i låsta utrymmen som är otillgängliga för obehöriga.
- Att ingen del av nätverket går öppet förlagd mellan olika byggander även om det är inom tillträdesbegränsat område. Om kablage används för okrypterad förmedling av kommunikation mellan olika byggnader bör denna förläggas i larmad kanalisation.
- Om trådlösa nät används så måste detta vara krypterat. Många utrustningar som används för att förmedla trådlöst nätverk är dock behäftade med sådana säkerhetsbrister att de ändå kan forceras av s.k. hackare och användningen av dessa bör avgränsas från företagets kärnverksamhet och inte överhuvudtaget användas där skyddsvärd information förekommer.

En sund nätfilosofi inom ett företagsområde bör innefatta följande:

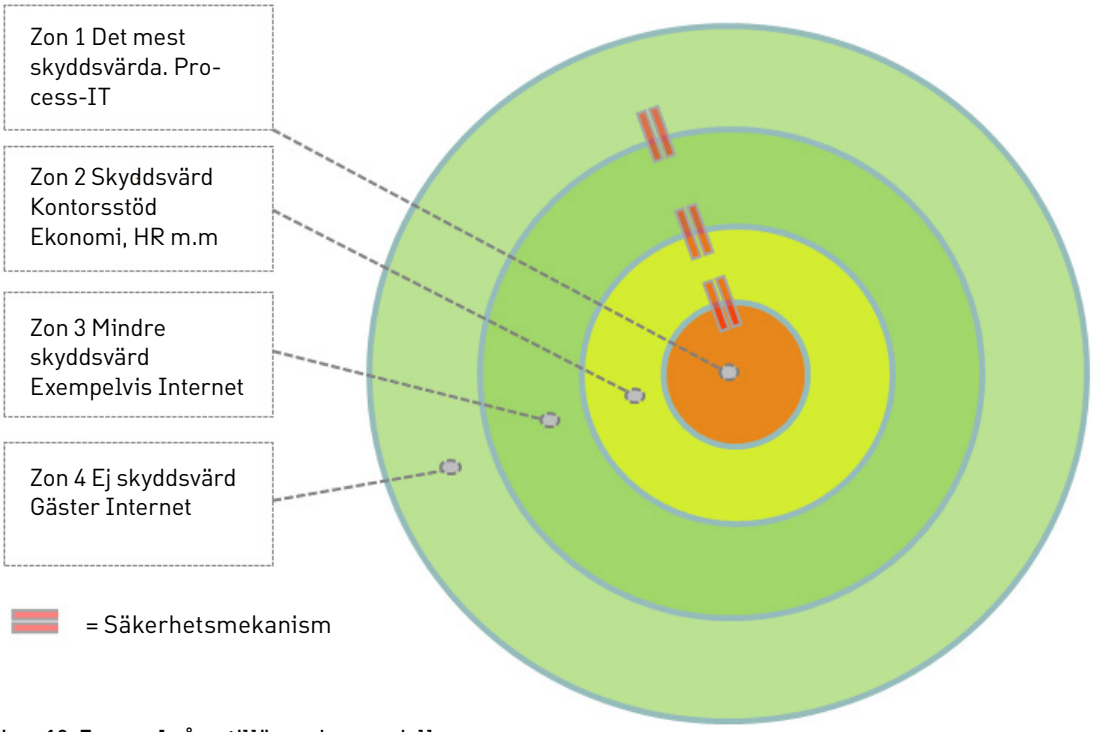
- Ett trådbundet nät som är förlagt enligt vad som anges ovan och används till personalens ordinarie arbetsstationer oavsett dessa är bärbara eller stationära.
- Ett dedicerat trådbundet nät för industriella informations- och styrsystem som företaget använder och som där det är möjligt är förlagt enligt vad som anges ovan. Om trådlösa anslutningspunkter används i sådant nät är det att betrakta som en förutsättning att de är krypterade och avståndsmässigt anpassade till det aktuella skalskyddets omfattning.
- Ett trådlöst krypterat nätverk som kan användas av personal för Internetåtkomst när man inte är på sin ordinarie arbetsplats. Här kan eventuellt även e-post tillåtas med ett extra säkerhetslager, exempelvis webbmail med SSL.
- Ett trådlöst krypterat nätverk som endast medger direkt åtkomst till Internet och är avsett för gäster. För att främja gästers e-post m.m. så bör denna anslutning ligga på DMZ eller helt utanför företagets ordinarie anslutningspunkt mot Internet.

13.13.2 SEPARATION OCH ISOLATION AV NÄTVERK (ZONER)

Den typ av separation som avses mellan, och i förekommande fall i, nätverk kan utgöras av olika typer av tekniska lösningar. Dessa kan bestå av mjukvara, hårdvara eller kombinationer av dessa.

Det lättaste sättet att visualisera en modell där separation sker mellan olika lager, zoner, är att föreställa sig en lök. Lökens yttersta skal utgör ytan mot omvärlden och varje lager längre in i löken motsvarar en nivå närmare det som är mest skyddsvärt.

Lager eller zoner kan som tidigare nämnts separeras på olika sätt. Beroende på vilket sätt man väljer så erhålls olika grader, eller nivåer, av säkerhet respektive teknisk funktionalitet vad avser själva kommunikationen mellan lagren. Separationen mellan zonerna definieras huvudsakligen av två saker:



Figur 12. Exempel på en tillämpad zonmodell.

ZON	INNEHÅLL	KOMMUNIKATION	EGET NÄT
1	Styrning av produktionsprocesser och manöver av ställverk m.m.	Tillåts endast utåt från zon 1 till zon 2 s.k. (eng.)reporting.	Ja
2	Ekonomisystem, HR-system, filareor och andra viktiga system.	Tillåts utåt från zon 2 till zon 3 och 4 samt delvis, exempelvis epost, inåt från överliggande zoner.	Kan ev. delas med zon 3 logiskt.
3	Internet, ev. intranät och e-post.	Tillåts utåt från zon 3 till zon 4 samt delvis, exempelvis epost, inåt från zon 4.	Kan ev. delas med zon 2 logiskt .
4	"Rått" Internet för gäster.	Tillåts endast ut mot Internet.	Ja

- Respektive zon utgörs av ett eget nät. Detta nät kan vara logiskt separerat men med ökat skyddsvärde ökar behovet av att zonen utgörs av ett eget fysiskt nät. Alltså ju längre "in i löken" desto större anledning att ha fysiskt egna nätverk.
- Mellan varje zon finns en säkerhetsmekanism av något slag som reglerar hur ett informationsutbyte mellan zonerna får ske. Detta kan, och bör, vara olika beroende på riktningen av informationen mellan lagren.

Om vi förutsätter att exemplet ovan representerar ett godtyckligt mindre till medelstort elföretag inom produktion så kan man använda följande för att exemplifiera och visualisera zonmodellen.

För att bibringa en säker kommunikation i de fall kommunikation sker över zongränser kan olika tekniker användas. Vanligast är olika varianter av brandväggar och datadioder. Brandväggar kan ofta konfigureras på olika sätt med regler för utåtgående och inkommande kommunikation. Datadioder tillåter i sin hårdaste form endast kommunikation i en riktning, därav namnet. Det finns dock varianter av datadioder som tillåter viss kommunikation i motsatt riktning men oftast kraftigt begränsad.

13.14 DATAMEDIA OCH DÄRTILL KOPPLAD HANTERING

Alla lösa, eller löstagbara, datamedia kan utgöra ett hot mot IT-miljön om de hanterats felaktigt. Det finns idag programkod som kan användas för att låta exempelvis ett USB-minne infektera en värddator bara genom att sättas in i densamma. Ett exempel på sådan programkod är Switchblade [läs mer: http://hak5.org/usb-switchblade]

Ett annat sätt på vilket lösa datamedia kan utgöra ett hot mot IT-miljön är helt enkelt genom att de förkommer och därmed riskerar att utnyttjas otillbörligt av någon obehörig. Detta i sin tur kan påverka konfidentialiteten, riktigheten eller tillgängligheten i den verksamhet som berörs om vederbörande utnyttjar informationen.

Ett väl genomtänkt och verksamhetsanpassat regelverk för hur lösa datamedia får och ska hanteras måste finnas, vara känd av personalen och tillgänglig för personalen. För mindre företag kan ett sådant regelverk utgöras av en enkel instruktion som i de flesta fall torde inrymmas på en A4-sida. Det viktiga med en sådan instruktion är att den passar för den verksamhet som bedrivs och att den bygger på vederlagda antagen kring hot och risker som kan påverka verksamheten. I slutet av detta avsnitt ges några exempel på formuleringar som kan användas i en sådan instruktion.

Några exempel på datamedia vars användning och avveckling bör regleras:

> USB-minnen, flash minnen och motsvarande.
> Löstagbara och externa hårddiskar.
> Mobiltelefoner – de är i dagsläget att betrakta som externa diskar.
> Säkerhetskopior – band, skivor m.m.
> Datorer som ska avvecklas. Mycket konfidentiell information har röjts genom bärgande av hårddiskar från skrotade datorer.
> CD och DVD skivor och alla motsvarande typer av skivor.

Några exempel på användning, förvaring och avveckling som bör regleras i en skriftlig instruktion:

> Användning av USB-minnen, flash minnen, motsvarande minneskort och externa hårddiskar. Vilka får användas och hur?
> Vad gäller för användning av CD, DVD och motsvarande skivmedia? Företagsmedia, media från större och mindre tillverkare av programvara etc.
> Hur mobiltelefoner får anslutas till företagets IT-miljö. Företagstelefoner, privata telefoner, gästers telefoner m.m.
> Förvaringsregler för alla uppräknade typer av datamedia. Låst skrivbordshurts, tunnplåtsskåp, säkerhetsskåp, valv etc.
> Hur avveckling av alla uppräknade typer av datamedia ska ske.

Destruktion, överskrivning eller annan åtgärd.

Exempel på formuleringar och utformning av instruktion för användning, förvaring och avveckling av **datamedia. Observera att listan på nästa sida endast utgörs av några utvalda exempel.**

13.15 REGLERING AV INFORMATIONSUTBYTE

Ett vanligt problem idag är att det i många organisationer och företag ofta inte är utrett, vare sig avseende hot och risker eller verksamhetsbehov, hur information ska få flöda mellan olika system, datamedia och nätverk. Vad gäller datamedia se 13.14 Datamedia och därtill kopplad hantering tidigare i detta kapitel.

För informationsutbyte mellan nätverk och IT-system sätts i många fall inga begränsningar upp vilket öppnar för onödiga hot och risker i IT-miljön. I myndighetsvärlden är problemet känt och många myndigheter har sedan länge vidtagit åtgärder för att motverka nämnda problematik. Det bör här nämnas att då är problemen som adresseras inte endast av teknisk natur utan avser motverka även mänskliga misstag i olika typer av försändning av information. I tillämpliga fall regleras vad som får utbytas, hur det får utbytas, mellan vilka system eller andra typer av anslutningspunkter det får utbytas och det är reglerat i tid.

Som med alla råd som ges i denna vägledning så ska enkelhet eftersträvas. Det bästa sättet att hitta den nivå som är acceptabel är att analysera vilka hot och risker man far genom olika typer av sammankoppling och exponering mot externa nät och system.

Några saker som torde vara tillämpliga även för små och medelstora företag är följande:

> ZONGRÄNSER
  Som tidigare nämnts i denna vägledning så definieras en zongräns av skillnaden mellan två nät och en därtill reglerande säkerhetsmekanism. Beroende på hur zongränsen ser ut i praktiken så är det lämpligt att på ett väl dokumenterat sätt reglera vilken information som får utbytas i vilken riktning, när och hur. Kryptering, autentisering och auktorisation bör regleras.

> INTRANÄT
  Ofta representerar intranät en logisk plats som utnyttjas för att utbyta eller tillgodogöra sig information som används i det dagliga arbetet. För att höja tillförlitligheten och tilltron till nämnda information så kan intranätet skydda med exempelvis SSL (eng.)Secure Socket Layer.

> E-POST
  En stor del av allt informationsutbyte sker i dag med e-post. Ofta glöms e-post bort när regleringar för olika system införs. Det är viktigt att både på teknisk nivå och administrativ nivå reglera vad e-post får användas till och hur den får användas. Många elektroniska hot och risker relaterar sig som bekant till bilagor och länkar i e-post.

Oavsett vilka regleringar som beslutas och införs vad avser informationsutbyte så behöver dessa dokumenteras, förmedlas till berörd personal samt följas upp och kontrolleras. Följande dokument bedöms minst påverkas:

> Drifthandbok för IT-system eller –miljö.

> Personalinstruktion/säkerhetsinstruktion.

> Utbildningsmaterial för företagets personal avseende säkerhet.

DATAMEDIA	ANVÄNDNING	FÖRVARING	AVVECKLING
Företags-USB	Får användas i företagets samtliga IT-system men inte i andra system, vare sig privata eller annan organisations.	Minst i låst skrivbordshurts, tunnplåtsskåp eller motsvarande.	Destruktion genom IT-avdelningens försorg.
Priv./Gäst-USB	Får ej användas	N/A	N/A
Företagsmobil	Får användas i företagets samtliga IT-system ansluten via exempelvis USB-kabel men inte i andra system, vare sig privata eller annan organisations.	Personlig uppsikt 24/7	Fabriksåterställning av telefon genom IT-avdelningens försorg. Destruktion av minneskort
Privat mobil	Får ej anslutas i företagets IT-system ansluten via exempelvis USB-kabel.	N/A	N/A
Företagsdator	Enligt arbetsordning	Enligt arbetsordning	Hårddiskar och andra ingående databärande media destrueras genom IT-avdelningens försorg.

13.16 ELEKTRONISK HANDEL

För information rörande elektronisk handel hänvisas till ISO 27002 avsnitt 10.9 Tjänster för elektronisk handel.

13.17 FÖRLÄGGNING AV SERVRAR - DATAHALL

Förläggning av, och utformning av, datahall är något som historiskt har orsakat mycket problem som kunde ha undvikits om bara sunt förnuft hade fått råda på ett tidigt stadium. Det finns exempel på datahallar:

> Som förlagts i samma utrymmen som stigarledningar till vattenförsörjning av hela fastigheter.

> Som förlagts i källarplan när organisationens simbassäng är belägen på våningen ovanför.

> I städskrubbar, som fortfarande används som städskrubbar.

> Delat med förråd.

> I olarmad container på gårdsplan utanför områdesskyddet.

Listan kan göras lång men har en gemensam nämnare; **avsaknad av eller grava brister i riskanalysen som bör föregå etablering av datahall.**

Det finns mycket tillgänglig dokumentation om hur man utformar en datahall. Det är inte denna vägledning ambition att förklara hur datagolv, rackstrukturer och kanalisationer mellan rackrader och korskoppling ska utformas. Det är snarare denna vägledning uppgift att informera om potentiella problem av mer föränderlig karaktär och sådant som ofta förbises när en datahall ska etableras.

Val av lokal för att etablera datahall. Det finns några saker att beakta när man väljer lokal som ska användas till datahall. Det enskilt viktigaste är lämpligheten utifrån ett hot- och riskperspektiv. Några frågeställningar som bör analyseras är:

> Finns det risk för oönskat vätskeutsläpp som kan påverka utrustningen? (vattenledningar, källarutrymme med tveksamt dränage, avloppsöversvämning etc.)

> Delas utrymmet av annan verksamhet som har utrustning i lokalen, och hur kan det i så fall påverka datahallen?

> Finns det separata utrymmen som ändå är i nära anslutning till den tänkta datahallen för förläggning av exempelvis UPS-system?

> Finns det möjlighet att etablera aggregat för reservkraftsförsörjning inom ett lämpligt avstånd med stöd av skyddad kanalisation för kablage?

> Finns det möjlighet till skyddade (mekaniskt skydd och brandskydd) kanalisationer för strömförsörjningskablage och annat transmissionskablage?

> Är lokalen belägen oroväckande nära högspänningsutrustning, järnväg, tunnelbana eller annan verksamhet som kan påverka elektrisk utrustning?

> Är för lokalen omkringliggande verksamheter acceptabla ur säkerhetssynpunkt?

> Är det fysiska skyddet av datahallen homogent eller finns det delar som har ett nedsatt skydd och kan utnyttjas otillbörligt?

> Finns det lämplig plats för förläggning av eventuell kylmaskin?

> Kan lokalen övervakas och larmas (inbrott och brand) på ett för verksamheten lämpligt sätt?

Som med allting kan man sällan uppnå ett fullgott resultat. Det är dock synnerligen viktigt att känna till vilka brister som finns så att detta ägnas tillbörlig uppmärksamhet inom ramen för framtida drift och daglig verksamhet.

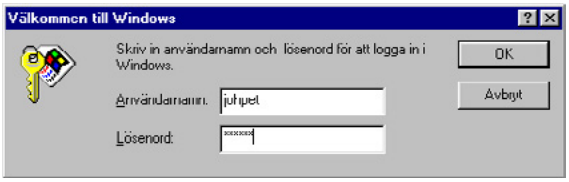
Om en datahall ska förändras eller nyetableras – genomför en riskanalys som minst tar upp ovanstående frågor.

13.18 AUTENTISERING OCH AUKTORISATION

13.18.1 AUTENTISERING

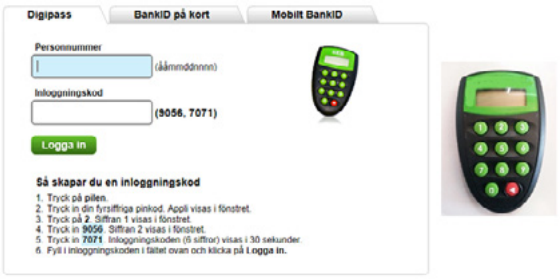
Med autentisering avses enligt SIS [teknisk] verifiering av uppgiven identitet eller av ett meddelandes riktighet.

När det gäller IT-system så är den vanligaste formen av autentisering användarnamn och lösenord. Se exempel i figur nedan.



Detta kallas ibland "vanlig" eller "svag" autentisering. Anledningen till detta är att det enda som krävs för att någon annan ska kunna utnyttja en persons konto i ett system är att dennes lösenord är känt. Detta är den enskilt vanligaste formen av autentisering och används bland annat av otaliga tjänster på Internet såsom webbaserad e-post, konton på tjänstesiter av olika slag m.m. Denna form av autentisering brukar också definieras på följande sätt – "Någon man är och något man vet". Där betyder det "man är" ett användarnamn. Dessa följer oftast någon form av standard och är allmänt kända, i exempelrutan ovan kan man exempelvis "baklänges" sluta sig till att användaren förmodligen heter någonting i stil med "Johan, Johnna, Johanna eller Johannes Pettersson". Således bygger denna form av autentisering endast på en enda hemlighet, lösenordet. Därav kallas denna typ av autentisering ofta för svag autentisering.

En bättre form av autentisering är den som benämns stark autentisering. Stark autentisering innebär att det finns ytterligare minst en hemlig faktor som måste tillföras autentiseringsprocessen. Ett exempel härvid är de flesta varianter av inloggning till olika Internetbanker. Se exempel i figuren.



I detta exempel består autentiseringen utöver det "man är", i detta fall ett personnummer, av en teknisk lösning som inbegriper ett kryptografiskt (eng.)Challenge response förfarande. Den lilla dosan som banken tillhandahållit innehåller då ytterligare en hemlighet som bidrar till ökad säkerhet i autentiseringsprocessen. Processen är nu inte längre bara "Någon man är och något man vet" utan har nu gått till att bli "Någon man är och något man vet och något man har". Det man har är då den lilla elektroniska dosan och det man vet är PIN[16]-koden till dosan. Denna typ av autentisering är enormt mycket bättre än den svaga typen men är mera omständlig och innebär dessutom att man personligen tillförs ett objekt (eng.)Token för att kunna fullfölja autentiseringen.

Den elektroniska dosan, digipass, är att se som ett exempel. Stark autentisering med objekt som består av aktiva kort eller andra typer av objekt förekommer också.

En annan typ av autentisering som också brukar betraktas som stark är autentisering med biometriskt komplement. "Någon man är och något man är" exempelvis fingeravtryck, handflatsavtryck eller näthinneavbildning. Det är dock en stor spridning av kvalitet och säkerhetsnivå på biometriska produkter och system för autentisering vilket inte minst påvisas av följande händelse.

16. PIN (eng.)Personal Identification Number

Källa: Svenska Dagbladet. Publicerad 23 september 2013. Utdrag:

...

Nya Iphones fingertrycksskydd hackat

Hackerkollektivet Germanys Chaos Computer Club har tagit sig runt det skydd som fingeravtryckläsaren på nya Iphone 5S är tänkt att ge.

Det rapporterar den brittiska tidningen the Guardian som hänvisar till filmer som hackarna har lagt ut på nätet.

Gruppen påstår sig ha fotograferat ett fingeravtryck på en glasskiva. Bilden har sedan applicerats på en tunn plastfilm vilken i sin tur har använts för att låsa upp den aktuella telefonen.

Nyheten kommer bara ett par dagar efter att Apple startat sin försäljning av den nya telefonmodellen.

”Detta visar - återigen - att fingeravtrycksbiometri är olämpligt som metod för tillträdeskontroll och bör undvikas”, skriver Germanys Chaos Computer Club.

...

Generellt kan sägas att om man avser implementera biometriska autentiseringslösningar så bör man välja sådan som är certifierade enligt någon tillämplig säkerhetsstandard.

Det finns ytterligare en typ av autentisering som kan sägas vara stark utan att för den sakens skull vara beroende av tekniska lösningar för att fungera, tvåhandsfattning. Tvåhandsfattning kallas ibland också för dualitets-autentisering och kan ta sig uttryck på många sätt. Gemensamt för dem är dock att de alla kräver att två personer samverkar med varsin del för att autentiseringen ska lyckas. Nedan följer några exempel på tillämpad tvåhandsfattning:

- Konsolåtkomst på server i datorhall som skyddas genom att två behöriga personer vet varsin del av lösenordet och således inte kan logga in utan att de båda anger sin del av lösenordet.
- Åtkomst till konsol i datahall där administratören har tillgång till konsolens lösenord men inte fysiskt kan komma in i datahallen utan måste åtföljas av annan person som fysiskt låser upp och närvarar.
- Åtkomst till skyddsvärt utrymme där två personer i förening måste använda sina objekt (eng.)Token för att låsa upp utrymmet. Alternativt att den ena låser upp och den andre larmar av.

Vad gäller tillämpning av autentiseringsmekanismer, rutiner och processer så bör dessa väljas utifrån skyddsvärdet på, och hotbilden mot, det objekt eller den IT-miljö som autentiseringen avser att skydda mot obehörig åtkomst.

En enskild typ av inloggning bör alltid ske med någon form av stark autentisering. Fjärråtkomst till sådant som är skyddsvärt. Om en medarbetare från exempelvis sin bärbara arbetsstation kan komma åt det mest skyddsvärda som företaget har så är det direkt orimligt att inloggning via sådan arbetsstation sker utan stark autentisering

13.18.2 AUKTORISATION

SIS definierar auktorisation enligt följande. Fastställande av åtkomsträttigheter för en användare till olika systemresurser. För att kunna förklara auktorisationsprocessen tittar vi även på hur SIS definierar begreppet behörighet. ”Rättighet för en användare att använda informationstillgångar på ett specificerat sätt”. SIS definierar även begreppet användare enligt ”person som utnyttjar informationstillgångar”. Man bör dock betänka att även automatiska processer, system- till systemkommunikation såsom exempelvis systemövervakningen också måste betraktas som användare på en teknisk nivå.

Med dessa begrepp kan vi nu titta närmare på vad som skiljer autentisering och auktorisation. Kortfattat kan man säga att autentisering är beviset på att du är du medan auktorisation är att du har givits tillåtelse att ta del av olika objekt. Samtidigt innebär auktorisationen att du inte får ta del av vissa andra objekt. Se exempel i figur.

AUTENTISERINGSPROCESS
Kontroll av att användaren är den som användaren uppger. Sker exempelvis med användarnamn och lösenord.

AUKTORISATIONSPROCESS
Kontroll av vilka objekt användaren äger rätt att ta del av. I detta fall den översta och nedersta "resursen i hurtsen" men inte den mellersta. Kontrollen sker mot regler som definierats för den specifika användaren.

I många fall används endast autentisering för att ge åtkomst till resurser i ett IT-system, i de flesta fall med administratörsrättigheterna undantagna. Det finns dock mycket att tjäna på att tillämpa auktorisation i någon form ur ett säkerhetsperspektiv.

För att auktorisation ska kunna tillämpas krävs det att det finns definierade objekt eller grupper av objekt till vilka behörighet kan ges eller nekas. Detta i sin tur implicerar att man måste klassificera sina informationstillgångar vilket även det leder till en ökad nivå av säkerhet.

Det finns olika modeller och kriterier för att designa en auktorisationsprocess. Det kan vara att få ta del av information som är placerad i en viss informationsklass eller enskilda objekt som getts ett särskilt skydd. Ett gammalt sätt att beskriva auktorisationsprocessen, som dock ännu håller lyder i lite mer modern tappning; "Behörig till ett objekt är den som har rätt säkerhetsklarering och behöver objektet för att lösa sina arbetsuppgifter". Härav följer att den svenska modellen för auktorisation, åtminstone i myndighetsvärlden, bygger på minst två kriterier. Det ger en tvådimensionell matris, vanligen kallad matrismodell när det gäller auktorisation inom ramen för behörighetskontrollsystem. En annan västerländsk modell bygger enbart på säkerhetsklareringen och ger således en endimensionell modell, vanligen kallad lökprincipen. Denna ger personen ifråga tillgång till alla informationsresurser som finns i det lager som personen är klarerad för.

Oavsett vilken metod för auktorisation man väljer bör behörigheter tilldelas efter någon typ av behovsprövning. Det är förmodligen inte rimligt att driftpersonal behöver ha full åtkomst till ekonomisystemet, eller omvänt att ekonomipersonal behöver ha åtkomst till styrsystem. Klart är att verksamheten tjänar säkerhetsmässigt på att ha en auktorisationsprocess som bygger på analys av behov och lämplighet.

13.19 ÖVERVAKNING, LOGGHANTERING OCH UPPFÖLJNING

13.19.1 ÖVERVAKNING

Med övervakning avses i detta fall systemövervakning. Denna vägledning gör inga ambitioner av att recensera produkter som används i detta syfte utan vill på enklaste sätt påpeka att de existerar och i många fall är dessutom gratisprodukter för detta syfte både kompetenta, lätthanterliga och i högsta grad tillämpliga för en säkerhetsmässigt adekvat systemövervakning.

Som med så många andra saker som tas upp i denna vägledning så bör införandet, konfigurationen och nyttjandet av en produkt för systemövervakning bygga på resultat från analys som beaktar behov samt hot och risker.

Generellt kan dock sägas att om ett företag har och använder industriella informations- och styrsystem i sin kärnverksamhet så är det en stark rekommendation att utreda ett eventuellt behov och eventuella vinster med att implementera ett övervakningssystem.

13.19.2 LOGGHANTERING OCH UPPFÖLJNING

De allra flesta IT-system loggar användarnas aktiviteter i någon omfattning. Loggningen är oftast möjlig att konfigurera i avseendet vad som loggas, hur och när.

Loggning i IT-system är en starkt bidragande faktor till god säkerhet.

I vissa handböcker utgivna av myndigheter kan man läsa "loggningen syftar till att avgränsa misstänkta och fria oskyldiga". Det kan låta melodramatiskt men är i själva verket essensen av vad loggningen innebär. Möjligheten att spåra och återskapa ett händelseförlopp vilket i sin tur sker på förekommen anledning.

Ett fel, en incident, en informationsförlust etc. Utöver att avgränsa misstänkta och fria oskyldiga kan loggningen också ge stöd till följande:

> Upptäcka händelser som utgör eller kan utgöra ett hot.
> Avvärja fortsatt hot genom att vidta korrekta åtgärder.
> Utreda inträffade händelser.
> Bedöma eventuella skadeverkningar i form av menbedömningar.
> Återställa otillbörliga förändringar.

Vad ska loggas?

Det första som behöver ske i samband med att en process för en sund logghantering implementeras är att utreda vad som ska loggas. Som allt annat bör detta bygga på en analys av behov samt hot och risker. Denna vägledning ger endast exempel på vad som kan vara intressant att logga ur en säkerhetssynpunkt. Det finns dock ofta behov av att logga andra parametrar som exempelvis sådana som rör hur program och system fungerar och uppför sig i olika sammanhang. Gemensamt för säkerhetsrelaterade loggar är att de i alla avseenden behöver ge svar på minst följande i sin enklaste tappning; Vem, Varifrån, På/Till vad, När, Lyckad/Nekad, Hur, Resurs. I tabellen nedan följer ett exempel på innehåll i en logg utformad enligt detta. I verkligheten kan loggen se mera komplex ut och innehålla mer information, detta är ett **konceptuellt exempel.**

DEL AV LOGGPOST	TYP	EXEMPEL
Vem	Autentiserat ID	470932-1234
Varifrån	IP-adress	192.168.120.13
På/Till vad	IP-adress	192.168.120.101
När	Tidsnummer/ Tidsstämpel	201312241500:0001
Lyckad/Nekad	Booleskt värde	Lyckad
Hur	Metod	Ändrad
Resurs	Informations-resurs	G:\HR\payroll\individlön.res

Nedan följer en uppräkning av saker som är exempel på vad som kan anses vara värt att logga ur en säkerhetssynpunkt:

> in/utloggningar på tider som skiljer sig markant från den enskildes normala arbetstider.
> Upprepade försök att ge sig tillgång till resurs för vilken behörighet saknas.
> Åtkomst till informationsresurs.
> Ändring av informationsresurs.
> Permanent borttagande av informationsresurs.
> Införande/Ändring/Borttagning av program eller annan exekverbar kod.
> Start och stopp av operativsystemet.
> Start och stopp av loggningen.
> Förändring av vad som loggas.
> Förändring av systemklockan.
> Förändring av annan kritisk information.

För att säkerställa loggarnas integritet, vilket ofta är ett stort problem i utredningssammanhang, så bör säkerhetsloggning uppfylla följande krav:

> Åtkomst till loggsystem bör ske med stark autentisering.
> Logghantering och logganalys bör vara lätt att genomföra och administrera.
> Loggarna ska vara skyddade mot manipulering.

Dessa krav implicerar ett antal saker. Säkerhetsloggar bör exporteras till en egen logisk/fysisk area som är skild från andra system och säkerhetskopior.

Det bör finnas ett system av något slag för att följa upp och analysera loggar. Vidare måste det också finnas en person som kan använda detta system och analysera loggar. Denna person ska

vara skild från ordinarie drift vad avser arbetsuppgifter.

Om det är möjligt bör loggar skyddas exempelvis genom digital signering för att säkerställa integriteten i materialet.

Hela processen för logghanteringen bör vara väl dokumenterad.

14 INCIDENTHANTERING

De flesta organisationer som i sin verksamhet nyttjar IT på ett eller annat sätt kommer att utsättas för olika typer av oförutsedda händelser, alltifrån stöld av utrustning till datorer som smittas av skadlig kod. De flesta sådana händelser går att hantera med enkla rutiner som en del av den löpande verksamheten. Ibland inträffar det dock större och mer svårhanterbara händelser som får hanteras mer utifrån situationens allvar och utan att det finns möjlighet att hantera händelsen med ordinarie drift- eller verksamhetsrutiner.

En fungerande incidenthantering förutsätter att det finns någon typ av incidentberedskap och planering i form av sådant som kontaktlistor, vissa typer av rutiner för reservdrift eller manuell hantering, beslutsmässighet och förståelse för att kunna hantera incidenten utifrån de särskilda omständigheter som följer, med mera.

Traditionella incidenter och **säkerhetspåverkande händelser** inom elsektorn kan vara sådant som att någon obehörig stjäl kablage, att ledningsstolpar skadas eller att någon saboterar utrustning i en anläggning. **IT-säkerhetsrelaterade incidenter** är relativt nya händelser som kan påverka de fysiska industriprocesserna för elproduktion och eldistribution, vilket i sin tur kan leda till andra konsekvenser för verksamheten, miljö eller människors hälsa. Företag i elsektorn måste ha en incidentberedskap och en incidenthantering som klarar av att hantera bägge typerna av incidenter inom sitt ansvarsområde.

En vanligt förekommande utmaning i IT-säkerhetsrelaterad incidenthantering är att beslutsfattare ställs mellan två val: återställning eller vidare utredning. Det naturliga alternativet är oftast att vilja återuppta normal driftstatus och återställa allt till hur det var innan incidenten inträffade. Detta kan ibland komma på konflikt med behovet av insamling av elektroniska bevis, att kunna fortsätta att leta efter ursprungsproblemet eller liknande utredningssteg. Detta är särskilt viktigt när incidenten beror på mänskliga fel, obehörigt användande eller uppsåtliga angrepp. Det är därför viktigt i IT-incidenter att den eller de som leder incidenthanteringen är väl införstådda med att de ska kunna ta beslut som är långsiktigt bra, men som i själva incidentsituationen kan kännas felaktiga.

Viktiga steg att tänka på när det gäller IT-säkerhetsrelaterade incidenter är

- att IT-säkerhetsrelaterade incidenter är annorlunda än ordinarie IT-incidenter, inte minst med tanke på prioriteringar, behov av specialverktyg och specialkompetens, sekretess runt själva utredningen och liknande,
- att tidigt börja samla in underlag, loggar, filer och elektroniska spår,
- att säkra att den information man tror sig ha verkligen finns kvar och inte försvinner under fötterna på en, exempelvis att

datamedia för säkerhetskopior inte återanvänds eller att äldre loggar raderas automatiskt av systemets bakgrundsjobb,

- att man planerar för det värsta men hoppas på det bästa. Detta gäller såväl vad det gäller menbedömningar, men också vad det gäller att uppskatta eller planera arbetsinsatser. Inte sällan utvecklar sig incidenthantering till dygnetruntarbete som kan pågå i flera veckor.

En naturlig del inom en organisation är att ha händelserapportering som en del i IT-incidenthanteringen, dvs. att det rapporteras att en händelse inträffat. Rapportering av IT-incidenter görs av många anledningar, bland annat:

- Kunna informera ansvariga om att händelsen inträffat.
- Kunna utgöra underlag i en lägesbild.
- Fungera som underlag för senare ändringar i lednings-, kvalitets- och andra system.
- Indata och underlag för statistik.

Som en del av incidenthanteringen kan det behövas tas externa kontakter, i vissa fall frivilliga såsom att kontakter med incidenthanteringsorganisationer, exempelvis CERT.SE i Sverige eller ICS-CERT i USA som har hand om incidenter som involverar industriella kontrollsystem. Andra externa kontakter kan vara med rättsvårdande myndigheter om brott har begåtts eller misstänks, samt sektors- och tillsynsmyndigheter. Inom elsektorn finns det i Svenska kraftnäts föreskrifter (SvKFS 2013:1) bestämmelser om att elbolag ska rapportera in vissa typer av händelser till sektorsmyndigheten. Närmare information om hur denna inrapportering ska ske beskrivs på Svenska kraftnäts webbplats.

Vid såväl interna som externa kontakter och informationsutbyte finns det ett behov av att hålla god sekretess och skydda informationen. Därför kan ibland särskilda behov uppkomma av att kunna skicka krypterad e-post, att kunna förmedla dokument säkert eller att inte använda vissa existerande kommunikationslösningar såsom exempelvis en IP-telefonitjänst som nyttjar ett nätverk i vilket det pågår en IT-säkerhetsincident.

Mer information om IT-incidenthantering finns i ISO/IEC 27002 Kap 13. Riktlinjer för identifiering, insamling, sammanställning och bevarande av digitala bevis finns närmare beskrivet i standarden ISO/IEC 27037:2012.

15 AVBROTTS- OCH KONTINUITETSPLANERING

Begreppen avbrottsplanering och kontinuitetsplanering betyder i att planera för vilka åtgärder som ska vidtas i samband med olika avbrott och för att verksamheten ska återfå sin ordinarie förmåga och kapacitet. Orden används ofta slarvigt men generellt kan sägas att avbrottsplanering utgör en enklare, mera jordnära, planering medan kontinuitetsplanering både som aktivitet och produkt ofta är omfattande.

En mera utförlig beskrivning av kontinuitetsplanering finns i ISO/IEC 27002 Kap 14.

I denna vägledning kommer avbrottplanering att beskrivas.

Alla verksamheter drabbas någon gång av avbrott eller störningar som påverkar förmågan att verka på avsett sätt negativt. Vilken effekt detta får på verksamheten i form av kostnader merarbete och andra förluster beror naturligtvis på om man förberett sig för att hantera sådana störningar eller avbrott. Man brukar skämtsamt säga planera för det bästa och förbered dig på det värsta. Med förberedelser avses här att planera för hur man ska agera vid olika typer av störningar och avbrott.

Vad ska man då planera för? Återigen vänder vi oss till riskanalys som verktyg för att identifiera potentiella problem som kan leda till störningar eller avbrott av sådan karaktär som måste bemötas med åtgärder. Vilka urvalskriterier som ligger till grund för att identifiera problem som ska bemötas och sådana som ska väljas bort måste beslutas av varje enskilt företag utifrån egna värderingar. Det finns dock ett antal frågeställningar som man bör beakta inom ramen för urvalsprocessen. Dessa frågeställningar förutsätter att man har gjort någon form av analys av vilka risker som kan påverka verksamheten på ett sådant sätt som avses. Det är viktigt att inte fastna helt i IT-spåret när man gör en sådan riskanalys utan se till verksamheten som helhet och vilka delprocesser och system som är avgörande för den. Det är naturligtvis normalt att en sådan analys får en tyngdpunkt på IT men den bör inte enbart handla om det.

Frågeställningar för att underlätta urvalsprocessen.

- Risker bygger oftast på att man har bedömt sannolikheten för att något ska inträffa och skadan/konsekvensen givet att det har inträffat. Det är viktigt att ställa sig frågan; **ska vi ta hänsyn till sannolikheten eller är skadan oacceptabel om den inträffar? I så fall spelar förmodligen inte sannolikheten någon roll och åtgärder bör vidtas i vilket fall.**
- Kan ett identifierat problem motverkas kostnadseffektivt? Framstår det som att den kostnad det bär att motverka problemet väl understiger effekten av att slippa problemet eller minimera effekterna av det?
- Kan problemet motverkas genom logistiska insatser eller förberedelser. Om

erforderlig utrustning finns och problemet kan motverkas genom att placera utrustning på ett bra sätt så är det förmodligen en mycket kostnadseffektiv insats.

> När det gäller IT-system. Hur ser supportavtal ut med leverantörer? Många leverantörer har mycket förmånliga avtal vad gäller inställelse, felsökning och reparation. Detta måste alltid beaktas i dessa sammanhang.

> Vidare för IT-system så bör man beakta att IT-system i dag är i stort sett oersättliga för verksamheten de stödjer. Att tillämpa reservrutiner med "papper och penna samt telefon och telefax!" är oftast en utopi som inte låter sig göras till någon rimlig nivå i verkligheten.

> Vidare för IT-system bör också särskild uppmärksamhet ägnas hårdvara. Är det standardmässiga komponenter som används? Hyllvaror? Om inte så kan leveranstider vara ett stort problem som kan driva oacceptabla kostnader.

> Hur ser företagets kommunikationsmöjligheter ut? I dagens IT-dominerade miljöer så är det inte alls säkert att telefoni fungerar i samband med ett IT avbrott. Man bör alltid beakta vilken förmåga man har att kommunicera inom och utom företaget i samband med olika typer av händelser och planera utifrån detta.

Att planera för att kunna hantera avbrott av olika typ kräver att man dokumenterar detta. Med tanke på dokumentationens art och dess vikt för verksamheten så är det aldrig fel att ha sådan dokumentation på papper. Att betänka i detta sammanhang är dock att dokumentationen måste vara tillgänglig där den behövs, ofta på plats i lokala anläggningar och motsvarande.

Ett sätt att hantera dokumentationen är att

IT-SYSTEM

Kontorsinformationssystem innehåller ofta personalsystem, e-post, Internet, löne- och ekonomisystem m.m. De är sällan tidskritiska för verksamheten i mer än så omfattning att ett avbrott på ett par timmar är acceptabelt.

IT-system som styr eller på annat sätt hanterar industriella informations- och styrsystem kan vara mycket tidskritiska beroende på problemets art. Alltså vilken typ av störning eller avbrott det handlar om.

IT-system som hanterar lås, larm olika sorts inpassering såsom elektriskt manövrerade grindar kan vara mycket tidskritiska. Särskilt om det inte går att kringgå systemet eller om man inte känner till hur man kringgår ett sådant system.

TELEFONI

Få saker är så frustrerande som att inte kunna kommunicera telefonledes i dagens samhälle. Detta vet alla som någon gång har glömt sin mobiltelefon hemma och sedan åkt till jobbet. Analys bör avgöra om företaget ska anskaffa system för redundant talkommunikation.

AVBROTT I FÖRSÖRJNINGSKEDJA

Förseningar i eller utebliven försörjning av utrustning eller förbrukningsvaror som krävs i det dagliga arbetet kan ge upphov till störningar eller avbrott i verksamheten. Detta kan exempelvis vara drivmedel eller förbrukningsvaror och reservdelar.

AVBROTT ELLER STÖRNING I BEROENDE VERKSAMHETER

Verksamheten kan påverkas av förseningar eller avbrott i kommunala och övriga transportsystem för pendlare. Det finns exempel där inte ens en tiondel av ordinarie arbetsstyrka kunde ta sig till arbetsplatsen som följd av utebliven transport.

SMITTSPRIDNING

I exempelvis förkylnings- och influensatider kan verksamheten påverkas på ett sätt som kräver extraordinära åtgärder för att kunna verka.

ha den digitalt men i sin helhet tillgänglig på ett antal mobila enheter som förvaras på ett tillämpligt säkert sätt. Enskilda medarbetare kan exempelvis ständigt ha en kopia av avbrottsplaneringen tillgänglig i en mobil enhet som medförs vid allt arbete. Här kan särskilt nämnas surfplattor, läsplattor och motsvarande vilka är ett mycket bra sätt att kostnadseffektivt kunna ha god tillgänglighet till kritisk information oavsett när och hur en störning eller ett avbrott inträffar.

Några områden som man bör fokusera på när man genomför sin analys och avbrottsplanering syns i listan på sidan 124. Listan är inte komplett utan beror naturligtvis på lokala förutsättningar och företagsspecifika inriktningar men den ger ett bra exempel att utgå ifrån.

Att dokumentera avbrottsplaner är i sig inte särskilt svårt när man har beaktat risker och gjort sina urval. Det handlar i allt väsentligt om att skapa en instruktion som anger ett antal väl definierade steg för att återta en förmåga. Stegen bör vara uppdelade så att det är lätt att läsa in sig på ett steg, vidta den åtgärden, kontrollera utfallet och gå vidare med nästa steg i instruktionen till dess förmåga är återtagen. Det går att utforma instruktionerna som exempelvis listor, tabeller eller flödesscheman. Ett flödesschema har den fördelen att man lätt kan få en överblick om en åtgärd kan få flera utfall. I tabellen nedan följer några enkla exempel på utformning.

De exempel som redovisats gör inte anspråk på att återspegla en exakt verklighet utan syftar till att utgöra inspiration i arbetet med att utforma tillämplig planering och dokumentation för att motverka störningar och avbrott.

Slutligen måste sägas att avbrottsplanering inte kan bli effektiv man inte övar på att genomföra den. Detta är en mycket viktig del av en effektiv och verkningsfull avbrottsplanering.

Det finns flera sätt att öva inför avbrott, gemensamt är dock att det måste inbegripa moment som ingår i avbrottsplaneringen.

Nedan följer några exempel på hur man kan öva inför avbrott.

- Ett enkelt sätt att öva är att med hela eller delar av personalen gå igenom olika delar av avbrottsplanerna, kontroller och visa var de finns samt kontrollera att de är läsbara, aktuella och begripliga.
- Ett lite mer utförligt sätt att öva är att göra en så kallad kaderövning. Då kan en del av personalen, en kader, genomföra eller

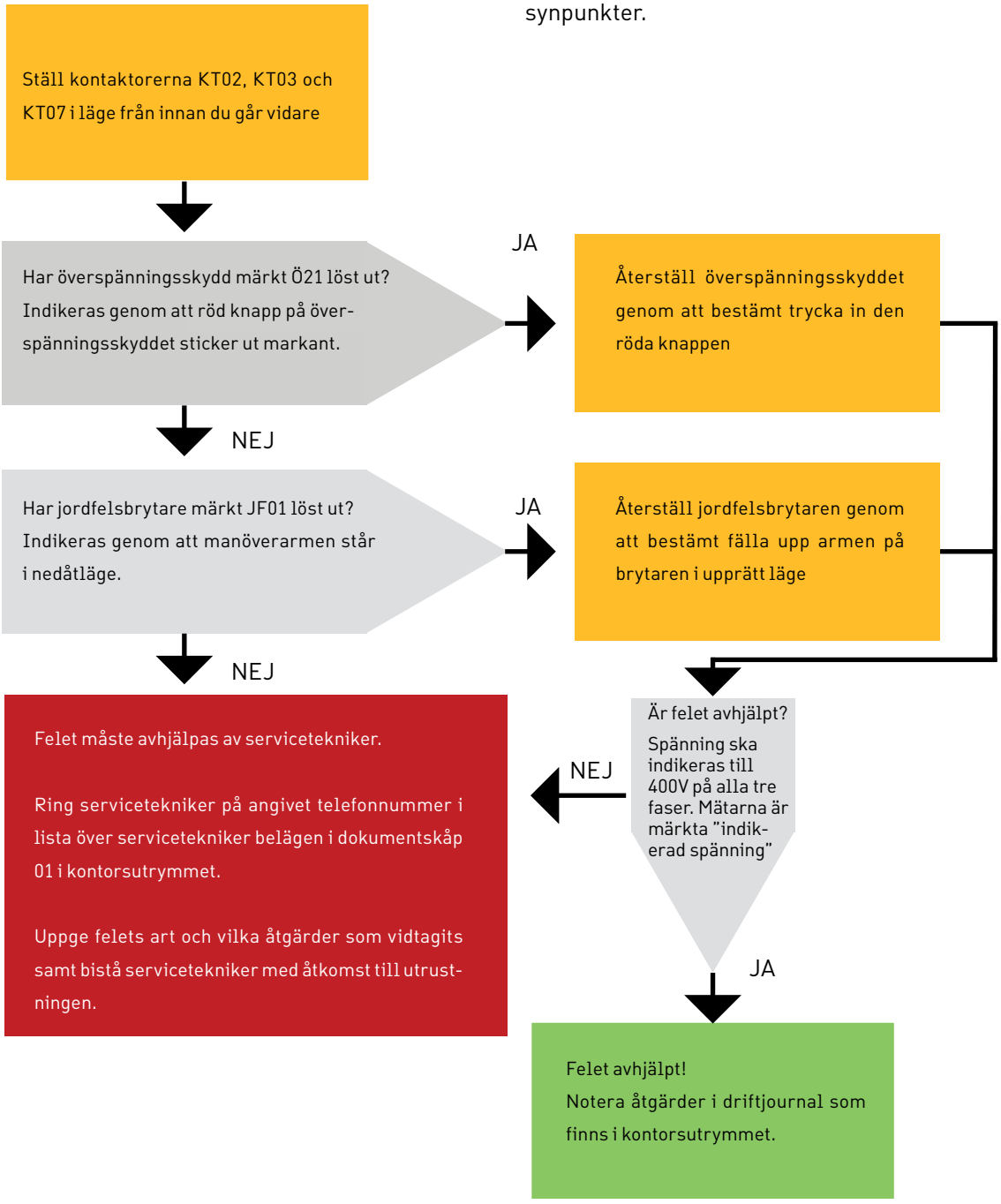
ÅTERSTÄLLNING AV FILSERVER. (FÖRUTSÄTTNING: ÅTERSTÄLLNINGEN ÄR EN ÅTGÄRD EFTER ETT MJUKVARUFEL. VID HÅRDVARUFEL SE TABELL XXX)

STEG	AKTIVITET
1	Installera serveroperativsystem från dvd-media IDOSSERV001 (finns i tunnplåtsskåp i datarum och i redundant förvaring i företagsvalvet) som standardinstallation genom att sätta i datamedia, starta om servern och välja [starta från cd/dvd]
2	När installationen av operativsystem är klar, starta om servern och låt den göra alla tillämpliga automatiska uppdateringar. Starta därefter om servern igen.
3	Installera filserversystemet FSSYSX från dvd-media FS002 (finns i tunnplåtsskåp i datarum och i redundant förvaring i företagsvalvet) som standardinstallation och låt eventuella automatiska uppdateringar ske.
4	Editera filen FSCONFIG belägen i rootkatalogen så att raderna 1 till 3 har följande utseende. 1%SERVER_ALLOW_EXPLICIT_ONLY% 2%FS_ALLOW_ANY_DOMAIN="BRAELISJUHARAD.COM"% 3%FS_ALLOW_ADMIN_CONSOLE%
5	Återställ senaste uppsättning filer från säkerhetskopia via bandstation. Instruktion för detta finns på bandstationen. OBS kontrollera katalogstruktur i enlighet med nämnda instruktion. (säkerhetskopior finns i tunnplåtsskåp i datarum och i redundant förvaring i företagsvalvet och är datummärkta).
6	Verifiera att åtkomst till filer kan ske från arbetsstation.

simulera genomförande av handgrepp som innebär återställning efter avbrott i olika verksamheter och system.

> Vid något tillfälle bör övning genomföras där åtgärder vidtas på riktigt. Det kan exempelvis vara att man inducerar och simulerar ett haveri, exempelvis att ett blixtnedslag löser ut överspänningsskydd och jordfelsbrytare eller att ett IT-system behöver ominstalleras. I fallet med IT-system bör detta lämpligen ske i referensmiljö, se vidare kap. 13 IT-säkerhet i denna vägledning.

Oavsett hur man väljer att testa och öva inför avbrott så är det viktigt att man tar tillvara erfarenheter från sådan övning och genomför förbättringar om behov av sådana identifierats. Det är härvid viktigt att alla som deltagit i övning ges tillfälle att dela med sig av erfarenheter och synpunkter.



Figur 13. Exempel flödesschema. Återställning av reservkraftaggregat efter spänningsbortfall. (Förutsättning: inget mekaniskt haveri har inträffat)

16 SÄKERHETSARKITEKTURER

Se även Kap. 13 IT-säkerhet i denna vägledning.

En säkerhetsarkitektur är ett antal principer som utgör grunden för de skydds- och kontrollmekanismer, hur dessa är beskaffade och utformade, hur de möter krav från systemägare och användare, och hur skydden är anpassade mot gällande hotbild. Att ha en väl utformad säkerhetsarkitektur innebär att man kan arbeta strukturerat och systematiskt med att få in säkerhet när nya system införs, när IT-landskapet förändras eller när nya tekniska lösningar ska integreras.

Bland de byggklossar som formar organisationens säkerhetsarkitektur finns, bland annat:

- Behörighetsmodeller och behörighetssystem.
- Klassningsmodeller av system och information.
- Skydd på nätverksnivå, nättopologi, segmentering och zonmodeller.
- Systemsäkerhet i form av processer för uppdateringar, härdning, formella säkerhetsmodeller, med mera.
- Applikationssäkerhet i form av anpassade utvecklingsprocesser som även inkluderar säker programutveckling och säkerhetstestning.

Dessa byggklossar består i praktiken ofta av säkerhetsprodukter eller olika tekniska arrangemang och lösningar.

Mer konkret är säkerhetsarkitekturens byggklossar utformade från många enkla och raka säkerhetsprinciper sådant som:

- Försvar i djupled (eng. defense in depth).
- Varierat skydd (eng. diversity of protection).
- Lägsta privilegienivå (eng. least privilege).
- Skydd vid källan (eng. protection at source).
- Begränsningspunkter (eng. choke points).
- Säkert tillstånd vid fel (eng. fail-safe).
- Spårbarhet i varje steg av hanteringen.

Genom att skapa en övergripande säkerhetsarkitektur som utifrån dessa typer av enkla principer bygger tekniska skydd, utformar driftsrutiner eller processer, så går det att skapa en systematiskt och strukturerat säkerhet i IT-landskapet, dess olika komponenter och användningsområden.

17 SÄKERHET I INDUSTRIELLA INFORMATIONS- OCH STYRSYSTEM

Produktion och distribution av el är idag helt beroende av datorbaserade system för styrning, reglering samt övervakning av de processer som är styr produktionen eller distributionen. Sett ur ett historiskt perspektiv så har fysiska industriprocesser kontrollerats av mekaniska eller elektromekaniska maskiner, vilka i sin tur styrdes och övervakades av mänskliga operatörer. Modernisering och tekniska landvinningar har gjort att IT kommit in och möjliggjort automatisering av själva processtyrningen samt att mänskliga operatörer får en minskad roll. Olika delar av anläggningsutrustning, automationssystem och industriella informations- och styrsystem består till allt större del på digitalteknik och datorer.

Den långsiktiga trenden för de produkter och lösningar som finns har varit att gå ifrån de tidigare leverantörsspecifika lösningar mot öppna standarder likväl som tekniklösningar som används inom vardaglig IT-hantering. Kontrollsystem, och tillhörande datorsystem, nyttjar därmed i större utsträckning befintliga allmänna standarder och standardlösningar för komponenter, mjukvara, hårdvara samt kommunikationsprotokoll. Av detta följer att de säkerhetsproblem som finns för standardlösningar även kommer att påverka kontrollsystem och de system som finns i elproduktion och eldistribution. Den allmänna tekniska utvecklingen tillsammans med kund- och verksamhetskrav på informationsutbyte med administrativa IT-lösningar har drivit fram dessa standardlösningar. Effekten av detta blir att vissa principer och rutiner som gäller för administrativ IT även måste överföras att gälla på den utrustning som används i anläggningar och för att styra fysiska processer. De speciella krav och förutsättningar som gäller i anläggningar och för styrsystem innebär dock att vissa nya krav och regler måste hanteras samt att några av de överförda principerna och rutinerna måste anpassas.

Fokus för säkerhet inom industriella styrsystem ligger som regel på tillgänglighet och snabba svarstider (så kallad realtidskontroll), till skillnad mot det fokus som finns inom kontorsautomation där man har istället ofta prioriterar konfidentialitet (sekretess) för att skydda affärshemligheter och dokument med känsligt innehåll.

När IT används som en del av styrning av fysiska processer som vi tidigare nämnt så kan felaktigheter, missbruk eller aktiva angrepp leda till direkta fel i elproduktion, eldistributionen, elhandel, kan leda till skador på anläggning och utrustning samt i svåra fall även medföra person- eller miljöskador. IT och digitala komponenter används också i skyddsutrustning för skydda anläggningar och utrustning på ett säkert sätt. När IT används för skyddsfunktioner är det extra viktigt att IT-säkerheten är god, vilket bland annat kan innebära att skyddsfunktionerna hålls logiskt eller fysiskt separerade från andra IT-komponenter. Annars kan det hända att

fel i IT-komponenterna, eller IT-säkerhetsincidenter som involverar dessa IT-funktioner eller komponenter, även kan påverka skyddsfunktioner, vilka kan blockeras, avaktiveras eller på annat sätt störas ut.

IT i industriella sammanhang innebär ofta speciella förutsättningar, framförallt på grund av att system, komponenter och applikationer ska användas på ett tillämpat sätt i en miljö som ställer hårda krav, exempelvis på svarstider och tillgänglighet. En viktig aspekt är att system eller komponenter nyttjas under lång tid. Detta påverkar behovet att få in skydd och säkerhetsfrågor i IT-lösningarna rätt ifrån början. Arkitekturella fel eller grundläggande designmissar kan sällan ändras efter drifttagning eftersom särskilda omständigheter gäller vid underhåll av IT-baserade komponent i driftsatta anläggningar.

För att nå ökad effektivitet kopplas industriella informations- och styrsystem allt oftare upp mot andra system, inte minst mot interna affärssystem, som håller kundinformation och/eller anläggningsinformation. Dessutom förekommer allt oftare kopplingar mot externa publika nätverk såsom Internet, inte minst för att externa leverantörer ofta erbjuder olika tjänster med allt ifrån fjärrdiagnostik och service till optimering av processens olika processteg. Dessa integrationer kan leda till att känslig utrustning och komponenter kan utsättas för exponering och i förlängningen för angrepp och säkerhetsrelaterade händelser.

Säkerhet i industriella informations- och styrsystem påverkas till stor del av vad leverantörerna av system och service har för inställning till säkerhet, och därmed hur de utformar sina produkter och systemlösningar. Traditionellt sett har förståelsen för säkerhet i allmänhet och IT- och informationssäkerhet i synnerhet varit låg hos dessa. Detta beror bland annat på att industriella informations- och styrsystem har varit fysiskt separerad från övrig IT, att ansvar och löpande drift av dessa system inte skötts av IT-avdelningar eller organisationens IT-personal samt att kravställningen på produkter och leverantörer ofta inte nämnt IT-säkerhet. Det är därför viktigt med att säkerhetskrav tas med i kravställning och de olika anbudsförfrågningarna.

Säkerhet i det löpande arbetet påverkas av det ledningssystem för säkerhet som finns i organisationen, den säkerhetskultur och säkerhetsmognad som organisationen har utvecklat, samt kompetens och engagemang hos den egna personalen. För processingenjörer, servicepersonal och driftspersonal i anläggningar eller drifts- och anläggningschefer är IT-säkerhetsfrågorna ofta nya och ovana problem att förstå och hantera. Därför är grundutbildning, vidareutbildning samt övningar viktiga steg för att nå ökad förståelse samt bygga upp erfarenhet runt dessa frågor.

Svenska kraftnät har gett ut föreskrifter inom säkerhetsskydd och elberedskap som bland annat omfattar krav på säkerhetsskydd och IT- och informationssäkerhet i form av:

- förebyggande skyddsåtgärder för styr- och reglersystemets kritiska IT-processer (SvKFS 2013:2 § 2),
- komplettering och förstärkning av styr- och reglersystem inklusive kommunikationsförbindelser (SvKFS 2013:2 § 2),
- robusthetshöjande teknisk installation i styrsystem och tillhörande kommunikationsförbindelser (SvKFS 2013:2 § 2).

Svenska kraftnät har dessutom gett ut **Tekniska Riktlinjer 04 "IT-säkerhet"** som kan användas som förlaga vid kravställning på säkerhetsfrågorna vid upphandling och projektering av industriella informations- och styrsystem.

Myndigheten för samhällsskydd och beredskap har givit ut olika dokument och olika typer av media som ger kunskapshöjning, vägledningar och råd inom områdena kritisk samhällsinfrastruktur och industriella informations- och styrsystem. En resurs som förtjänar att lyftas fram är deras **Vägledning till industriella informations- och styrsystem**, vilket ger handgripliga råd, har inbyggda kontrollfrågar för att utvärdera organisationens mognad inom området säkerhet i industriella informations- och styrsystem, pekar på användbara referenser, med mera.

Förutom de allmänna vägledningar och råd så finns det en internationell standard för

området IEC 62443, ”Industrial communication networks – Network and system security” som består av flera delar. Denna standard introducerar bland annat ett ”ledningssystem för cybersäkerhet”, analogt med standarden ISO/IEC 27000 som introducerar ett ”ledningssystem för informationssäkerhet”. Cybersäkerhet är deras benämning för säkerhet inom industriella informations- och styrsystem.

18 REFERENSER

Offentlighets- och sekretesslag (2009:400)

Offentlighets- och sekretessförordning (2009:641)

Elberedskapslag (1997:288)

Förordning (1997:294) om elberedskap

Lag (1993:1742) om skydd för landskapsinformation

Förordning (1993:1745) om skydd för landskapsinformation

Personuppgiftslag (1998:204)

Personuppgiftsförordning (1998:1191)

Skyddslag (2010:305)

Skyddsförordning (2010:523)

Säkerhetsskyddslag (1996:627)

Säkerhetsskyddsförordningen (1996:633)

Svenska kraftnäts Föreskrifter, SvKFS 2013:1 "Affärsverket svenska kraftnäts föreskrifter och allmänna råd om säkerhetsskydd"
http://www.svk.se/Global/07_Tekniska_krav/Pdf/Foreskrifter/SvKFS-2013-1-webb.pdf

Svenska kraftnäts Föreskrifter, SvKFS 2013:2 "Affärsverket svenska kraftnäts föreskrifter och allmänna råd om elberedskap"
http://www.svk.se/Global/07_Tekniska_krav/Pdf/Foreskrifter/SvKFS-2013-2.pdf

BSI Threat catalogue
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf?__blob=publicationFile

Reference source for threats, vulnerabilities, impacts and controls in IT risk assessment and risk management, version 1.0
http://www.enisa.europa.eu/activities/risk-management/files/deliverables/reference-source-for-threats-vulnerabilities-impacts-and-controls-in-it-risk-assessment-and-risk-management/at_download/fullReport

SIS HB 550 "Terminologi för informationssäkerhet, utgåva 3" ISBN 978-91-7162-705-6

SS-ISO/IEC 27000:2009 "Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Översikt och terminologi"

SS-ISO/IEC 27001:2006 “Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav”

SS-ISO/IEC 27002:2005 ”Informationsteknik – Säkerhetstekniker – Riktlinjer för styrning av informationssäkerhet”

SS-ISO/IEC 27003:2010 ”Informationsteknik – Säkerhetstekniker – Vägledning för införande av ledningssystem för informationssäkerhet ”

SS-ISO/IEC 27005:2008 “ Informationsteknik – Säkerhetstekniker – Riskhantering för informationssäkerhet”

ISO/IEC 31000:2009 “Risk management – Principles and guidelines”

IEC 62443-1-1/TS “Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models” Edition 1.0 2009-07

IEC 62443-2-1 “Industrial communication networks – Network and system security –
Part 2-1: Establishing an industrial automation and control system security program” Edition 1.0 2010-11

IEC/TR 62443-3-1 “Industrial communication networks – Network and system security –
Part 3 1: Security technologies for industrial automation and control systems”

IEC 62443-3-3 “Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels” Edition 1.0 2013-08

Svenska kraftnät Tekniska Riktlinjer 04 IT-säkerhet
http://www.svk.se/PageFiles/41244/TR%204-02-B.pdf

BILAGA 1 - FÖRTECKNING AV METODER

1. Beskrivning av dokumentet

Detta dokument utgör en förteckning, ett index, över de metoder som exempelmässigt beskrivs för att stödja aktiviteter och åtgärder som anges i vägledning för IS/IT-säkerhet och säkerhetsskydd. De metoder som är beskrivna utgör i allt väsentligt återgivna de-facto metoder som används i säkerhetssfären nationellt och internationellt.

Varje metod som refereras i denna förteckning anges med en kort beskrivning för att ge läsaren förståelse för innehållet i metoden.

Det bör dock särskilt påpekas att referenserna utgör exempel på metoder för hur vissa uppgifter och problem kan lösas. Resultatet och tillämpligheten är alltid beroende på utförandet och tillgängliga ingångsvärden.

De metodbeskrivningar som anges i detta dokument återges i respektive fall med länkar till nämnd metod. I vissa fall kan länken vara av övergripande karaktär och fördjupad sökning på mål-webbplats kan vara nödvändig. Detta främst på grund av att vissa metodbeskrivningar som refereras till vid tiden för skapandet av detta dokument ännu ej publicerats.

2. Förteckning av metoder

Nedanstående förteckning hänvisar med länkar till respektive metodstöd. Kolumnen kategori refererar i tillämpliga fall till motsvarande avsnitt i ISO/IEC 27002 standarden.

Förteckning

METOD	KATEGORI	ALLMÄN BESKRIVNING	UNDERBILAGA
Metoder för ledning och styrning av informationssäkerhetsarbetet	27k Kap 5 & 6	Olika sätt att införa ledningssystem för informationssäkerhet i de ledningssystem som existerar i organisationen.	Nr 1.1 MSB har tagit fram ett heltäckande paket med metoder och verktyg för införande av LIS: https://www.informationssakerhet.se Nr 1.2 Svensk Energi, EBITS: Att införa LIS: Förberedelser inför anpassning till ISO/IEC 17799 http://www.svenskenergi.se/Vi-arbetar-med/Fragor-A-F/EBITSInformationssakerhet/Att-infora-LIS-Ledningssystem-for-InformationsSakerhet/ 1.3 Svensk Energi, EBITS Nulägesanalys, ett arbetsverktyg vid genomförandet av LIS http://www.svenskenergi.se/Global/Dokument/EBITS/nulagesanalys.pdf
Riskanalys	27k Kap 4	Enkla metoder för att definiera och genomföra hot-, risk- och sårbarhetsanalys på ett godtyckligt objekt (anläggning, IT-system etc.).	Nr 2.1 Svenska kraftnäts vägledning för riskanalys. http://www.svk.se. Nr 2.2 I MSBs paket för införande av LIS finns i block 2-Analysera ett en metod för riskanalys. https://www.informationssakerhet.se/Global/Metodst%C3%B6d%20f%C3%B6r%20LIS/Riskanalys.pdf
Säkerhetsanalys	SäkF	Nr 1: En bransch-anpassad metod för att genomföra säkerhetsanalys enligt 5§ säkerhetsskydds-förordningen (1996:633). Nr 2: SÄPO vägledning säkerhetsskydd inklusive säkerhetsanalys.	Nr 1. Svenska Kraftnät: Vägledning Säkerhetsanalys: http://www.svk.se/Global/01_Om_oss/Pdf/Sakerhetsskydd/Sakerhetsanalys.pdf Nr 2. Säkerhetspolisen: Säkerhetsskydd en vägledning: http://www.sakerhetspolisen.se/download/18.34ffc68f1235b740c0680004426/Sakerhetsskyddenvagledning1007.pdf
Inventering av informationsresurser	27k Kap 7	Metoder och kriterier för att inventera och bedöma informationsresurser	Nr 4. I MSBs paket för införande av LIS finns i block 2-Analysera ett en metod för Verksamhetsanalys vilken innefattar inventering och bedömning. https://www.informationssakerhet.se/Banners/Verksamhetsanalys.pdf
Informationsklassificering	27k Kap 7	Metoder för att klassificera information som kan förekomma hos bland annat elföretag.	Nr 5.1 I MSB:s paket för införande av LIS finns i block 2-Analysera ett en metod för Verksamhetsanalys vilken innefattar Informations-klassificering: https://www.informationssakerhet.se/Banners/Verksamhetsanalys.pdf Nr 5.2 Svensk Energi, EBITS Informationsklassning: https://www.informationssakerhet.se/Dokumentbanken/Modell-for-klassificering-av-information-/

METOD	KATEGORI	ALLMÄN BESKRIVNING	UNDERBILAGA
Metod för att granska/utvärdera tekniskt skydd i IT-system	27k Kap (10, 11) & 15	Olika metoder för att på ett övergripande och enkelt sätt göra en egenbedömning av vilken skyddsnivå IT-system har och bedöma om den är tillämplig för det systemet sett emot vilken information som hanteras i systemet.	Nr 6.1 I MSBs paket för införande av LIS finns i block 2 Analysera en metod för GAP-analys samt en checklista för detta. https://www.informationssakerhet.se/Banners/Gapanalys.pdf https://www.informationssakerhet.se/Global/Metodst%C3%B6d%20f%C3%B6r%20LIS/Gapanalys%20checklista.pdf Nr 6.2 Svensk Energi, EBITS: Checklista för IT-säkerhet för mindre företag http://www.svenskenergi.se/Vi-arbetar-med/Fragor-A-F/EBITSInformationssakerhet/Checklista-for-IT-sakerhet-for-mindre-foretag/
Metod för att granska/utvärdera skydd av anläggning	27k Kap 9 & 15	Olika metoder för att på ett övergripande och enkelt sätt göra en egenbedömning av vilken skyddsnivå en anläggning har och bedöma om den är tillämplig för den verksamhet som bedrivs och vikten av det som anläggningen försörjer.	Nr 7.1 Svenska Kraftnät: Handbok Säkerhet vid energiföretag http://www.svk.se/PageFiles/41623/100621_Handbok_Sakerhet_vid_energiforetag_Svart-vit.pdf Nr 7.2 Svenska Kraftnät: Vägledning Fysiskt grundskydd http://www.svk.se/Global/01_Om_oss/Pdf/Sakerhetsskydd/130410-Vagledning-Fysiskt-grundskydd.pdf Nr 7.3 Svenska Kraftnät: Riktlinjer för riktade beredskapsåtgärder http://www.svk.se/Global/07_Tekniska_krav/Pdf/TR9-130218/TR9-03-utgava-3.pdf Nr 7.4 Svenska Kraftnät: Vägledning fysiskt Områdesskydd http://www.svk.se/Global/02_Press_Info/Pdf/Broschyrer/Vagladning_fysiskt_Omradesskydd_090108_tryckt.pdf Nr 7.5 Svensk Energi, EBITS: Checklista för IT-säkerhet för mindre företag http://www.svenskenergi.se/Vi-arbetar-med/Fragor-A-F/EBITSInformationssakerhet/Checklista-for-IT-sakerhet-for-mindre-foretag/
Metoder för att utvärdera säkerhetsarbetets kvalitet och effekt	27k Kap 10 & 15	Utvärderingsexempel och metoder att utföra effektmätningar på informationssäkerhetsarbetet	Nr 8.1 I MSBs paket för införande av LIS finns i block 6-Förbättra en metod: Utveckla LIS och skyddet. https://www.informationssakerhet.se/Global/Metodst%C3%B6d%20f%C3%B6r%20LIS/Utveckla%20LIS%20och%20skyddet.pdf

METOD	KATEGORI	ALLMÄN BESKRIVNING	UNDERBILAGA
Metoder för att hantera IT-incidenter i industriella processystem	27k Kap 13	Incidenthanterings-metoder att använda i samband med hantering av IT-incidenter i industriella processystem	Nr 9.1 MSB Vägledning till ökad säkerhet i industriella kontrollsystem https://www.msb.se/RibData/Filer/pdf/25548.pdf Nr 9.2 CERT-SE:s incidenthanteringsprocess (CIHSP) https://www.cert.se/incidenthantering/ Detta stöd riktar sig inte specifikt mot industriella processystem utan är ett generellt stöd. Dock är det omfattande, genomarbetat och strukturerat. Rätt använt och i tillämpliga delar är det ett stöd för hantering av IT-incidenter i industriella processystem.
Metoder för kompetensutveckling av informations-säkerhetskompetens	27k Kap 8	Olika metoder, inklusive utbildning och övningar, för att öka kompetensen hos den egna personalen inom områdena IT- och informationssäkerhet, särskilt för industriella styr- och reglerprocesser inom energisektorn	Nr 10.1 MSB: Informations-säkerhetsutbildningar. Här förtecknas lämpliga utbildningar. Dock saknas särskilt anpassade utbildningar för industriella styr- och reglerprocesser inom energisektorn https://www.informationssakerhet.se/Global/Kompetensutveckling/Informationssakerhetsutbildningar.pdf
Metoder för kravställning i samband med upphandling och projektering	27k Kap 12	Beskrivning av olika krav-hanteringsmetoder för att kunna fånga krav, beskriva krav, och följa upp krav i samband med olika aktiviteter såsom upphandlingar och projekt.	Nr 11.1 Svensk Energi, EBITS Bättre beställare: http://www.svenskenergi.se/Global/Dokument/EBITS/B%c3%a4ttre%20best%c3%a4llare%20v%201.0.pdf Detta kortfattade PM beskriver i fem steg en process för upphandling med säkerhet i åtanke. Texten avser i första hand upphandling av IT-system inom energibranschen, anpassat för små och medelstora energiföretag. Nr 11.2 Svenskt Näringsliv Ett forskningsprojekt i samverkan mellan Svenskt Näringsliv/Näringslivets Säkerhetsdelegation/Försvarets Materielverk/Försvarsmakten och Center for Service, Science and Innovation vid Stockholms Universitet har under 2011 tagit fram ett dokument med namn: ”Säkerhet vid anskaffning och utveckling av system.” Dokumentet, som är baserat på ISO 27000, är att betrakta som en vägledning och den är främst avsedd för Försvarsmakten och dess leverantörer, men kan användas även av andra. http://www.svensktnaringsliv.se/material/rapporter/vagledning-for-informationssakerhets-deklarationen_148920.html

METOD	KATEGORI	ALLMÄN BESKRIVNING	UNDERBILAGA
Metoder för kontinuitetsplanering	27k Kap 14	Beskrivningar och metoder för avbrotts- och kontinuitets-planering	Nr 12.1 I MSBs paket för införande av LIS finns i block 2 Analysera en metod för GAP-analys samt en checklista för detta. https://www.informationssakerhet.se/Banners/Gapanalys.pdf https://www.informationssakerhet.se/Global/Metodst%C3%B6d%20f%C3%B6r%20LIS/Gapanalys%20checklista.pdf Nr 12.2 Svensk Energi, EBITS Kontinuitetsplanering: http://www.svenskenergi.se/Global/Dokument/EBITS/ex-kontinuitetsplanering.pdf http://www.svenskenergi.se/Global/Dokument/EBITS/Kontinuitetsplanering-bilagor.pdf

BILAGA 2 - ÅTGÄRDSPLAN

5 FEMHÄRADS EL AB

Säkerhetsavdelningen

VD: Lillian Ström
Säkerhetschef: Svante Stensäker

2014-02-30

Åtgärdsplan efter säkerhetsanalys

OBSERVERA
Detta är ett fiktivt och begränsat exempel på en åtgärdsplan efter genomförd säkerhetsanalys enligt 5§ säkerhetsskyddsförordningen (1996:633)

Åtgärdsplan efter genomförd säkerhetsanalys enligt 5§ säkerhetsskyddsförordningen (1996:633)

Bakgrund

Som en följd av Svenska kraftnäts föreskrifter 2013:1 om säkerhetsskydd genomförde Femhärads EL under Jan och Feb 2014 en säkerhetsanalys med stöd av tillgängliga vägledningar från Svenska kraftnät. Inom ramen för genomförandet av denna analys konstaterades bland annat att Femhärads EL anläggning K9 behöver skyddas mot terrorism. I och med detta ska tillämpligt regelverk för säkerhetsskydd tillämpas och adekvata åtgärder snarast vidtas.

Åtgärder mot utfall av analys

Åtgärd/Aktivitet
En säkerhetsskyddschef måste utses. VD har beslutat att säkerhetschefen, Svante Stensäker, tillika utses till säkerhetsskyddschef vid Femhärads EL AB med omedelbar verkan.

Tidplan
Redan genomfört, se vidare VD Beslut Dok-ID 5H2014-0047.

Åtgärd/Aktivitet
Femhärads EL anläggning K9 ska förses med ett adekvat skydd mot terrorism i enlighet med gällande regelverk om säkerhetsskydd och i enlighet med riktlinjer/vägledningar m.m. som anges av Svenska kraftnät. Skyddet ska omfatta fysiskt skydd, tekniskt/logiskt skydd samt genomgång

och revidering av administrativa rutiner och organisation kopplad mot aktiviteter och verksamhet som rör Femhärads EL anläggning K9.

Entreprenörer som behöver engageras för att genomföra arbete vid Femhärads EL anläggning K9 ska upphandlas i enlighet med regelverk för säkerhetsskyddad upphandling enligt Svenska kraftnäts regelverk.

Säkerhetsskyddschef ska ta fram säkerhetsplan som ska gälla vid arbetet med säkerhetshöjande åtgärder som rör Femhärads EL anläggning K9.

Tidplan
Säkerhetsplan ska vara framtagen 2014-03-23
Säkerhetshöjande åtgärder, inklusive alla entreprenadarbeten, ska vara klara 2014-10-20.

Åtgärd/Aktivitet
Då olika typer av arbete och entreprenader tidigare genomförts vid Femhärads EL anläggning K9 innebär att uppgifter om anläggningen kommit ett flertal personer till känna finns ett behov av att kartlägga spridningen av denna information. När kartläggningen är genomförd ska en menbbedömning göras avseende vilken information som fortfarande kan vara aktuell och känd av obehöriga efter det att säkerhetshöjande åtgärder genomförts. En rapport som återspeglar detta ska upprättas och insändas till Svenska kraftnät som en incidentrapport med begäran om yttrande/rådgivning i ärendet.

Tidplan
Kartläggning ska vara klar 2014-04-15
Rapportering till Svenska kraftnät ska ha skett 2014-04-28

Åtgärd/Aktivitet
Samtlig personal vid femhärads EL AB ska genomgå utbildning i säkerhetsskydd. Deltagandet är obligatoriskt. Utbildningen kommer att äga rum vid totalt tre tillfällen. Måndag den 12e Maj, förmiddagspass och eftermiddagspass samt för eftersläntrare Tisdag den 27e Maj kl. 09:00-11:00.

Utbildningen sker med stöd av extern föreläsare. Personalen indelas på utbildningspass enligt följande.

Måndag den 12e Maj: förmiddag (08:30-11:00)

Albert, Britta, Cissi, David, Erik, Filip, Gustav, Hannah och Ivar.

Måndag den 12e Maj: eftermiddag (13:00-15:30)

Johan, Kalle, Lillian, Mona, Nisse, Olle, Pia, Rut och Svante.

Tidplan
Tanken är att samtliga ska delta Måndag den 12e Maj. Om någon är sjuk eller av andra skäl inte kan delta så ska hen delta Tisdag den 27e Maj kl. 09:00-11:00.

Åtgärd/Aktivitet
IT-chefen Cissi ska inventera uppgifter i Femhärads EL AB IT-system och kontrollera vilken information som rör Femhärads EL anläggning K9. En förteckning ska upprättas där det framgår i vilka system informationen finns. Cissi ska sedan tillsammans med Svante upprätta en åtgärdsplan för att hantera påträffade uppgifter på ett sätt så att regelverket kan uppfyllas.

Tidplan
Inventering ska vara klar 2014-04-01.
Åtgärdsplan ska vara klar 2014-04-20.
Åtgärder ska därefter påbörjas omgående och färdigställas snarast.

Åtgärd/Aktivitet
Envar vid Femhärads EL AB ska vara uppmärksam på uppgifter som rör Femhärads EL anläggning K9. Om nya uppgifter eller uppgifter som av någon anledning inte redan omhändertagits i denna åtgärdsplan upptäcks så ska detta utan dröjsmål rapporteras till säkerhetschefen Svante.

Tidplan
Sker löpande.

Utbildningen sker med stöd av extern föreläsare. Personalen indelas på utbildningspass enligt följande.

Måndag den 12e Maj: förmiddag (08:30-11:00)

Albert, Britta, Cissi, David, Erik, Filip, Gustav, Hannah och Ivar.

Måndag den 12e Maj: eftermiddag (13:00-15:30)

Johan, Kalle, Lillian, Mona, Nisse, Olle, Pia, Rut och Svante.

Tidplan
Tanken är att samtliga ska delta Måndag den 12e Maj. Om någon är sjuk eller av andra skäl inte kan delta så ska hen delta Tisdag den 27e Maj kl. 09:00-11:00.

Åtgärd/Aktivitet
IT-chefen Cissi ska inventera uppgifter i Femhärads EL AB IT-system och kontrollera vilken information som rör Femhärads EL anläggning K9. En förteckning ska upprättas där det framgår i vilka system informationen finns. Cissi ska sedan tillsammans med Svante upprätta en åtgärdsplan för att hantera påträffade uppgifter på ett sätt så att regelverket kan uppfyllas.

Tidplan
Inventering ska vara klar 2014-04-01.
Åtgärdsplan ska vara klar 2014-04-20.
Åtgärder ska därefter påbörjas omgående och färdigställas snarast.

Åtgärd/Aktivitet
Envar vid Femhärads EL AB ska vara uppmärksam på uppgifter som rör Femhärads EL anläggning K9. Om nya uppgifter eller uppgifter som av någon anledning inte redan omhändertagits i denna åtgärdsplan upptäcks så ska detta utan dröjsmål rapporteras till säkerhetschefen Svante.

Tidplan
Sker löpande.

SVENSKA KRAFTNÄT
BOX 1200
172 24 SUNDBYBERG
STUREGATAN 1

TEL 010 475 80 00
FAX 010 475 89 50

WWW.SVK.SE