Bundesamt
für Sicherheit in der
Informationstechnik

BSI-standard:100-2

IT-grundskydd-tillvägagångssätt

Version 1.0

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189, 53175 Bonn • Postfach 200363, 53133 Bonn
Tel.: +49 (0) 1888 9582-0 • Fax: +49 (0) 1888 9582-400 • Internet: www.bsi.bund.de

---

Innehållsförteckning

---

1 Inledning

1.1 Versionshistorik

Utgåva	Version	Författare
December 2005	1.0	BSI

1.2 Målsättning

BSI har med tillvägagångssättet enligt IT-grundskydd utvecklat en metodik för ett effektivt ledningssystem för informationssäkerhet som enkelt kan anpassas till förhållandena inom en konkret institution.

Metodiken, som beskrivs i de följande kapitlen, bygger på BSI-standard 100-1 Ledningssystem för informationssäkerhet (LIS) (se [BSI1]) och förklarar det där presenterade IT-grundskydd-tillvägagångssättet. Ett ledningssystem för informationssäkerhet (LIS) är det planerade och organiserade tillvägagångssättet för att erhålla och behålla en lämplig säkerhetsnivå för informationssäkerheten. För detta ändamål visas explicit för varje enskild fas, som beskrivs i BSI-Standard 100-1, det av IT-grundskydd föreslagna genomförandet.

IT-grundskydd är en standard för att etablera och bibehålla en lämplig IT-säkerhetsnivå inom en institution. Denna av BSI 1994 införda metoden, som därefter har vidareutvecklats, är såväl ett tillvägagångssätt för att bygga upp ett ledningssystem för informationssäkerhet som en omfattande grund för riskbedömning, kontroll av den befintliga IT-säkerhetsnivån samt implementering av den lämpliga IT-säkerheten.

Ett av de viktigaste målen med IT-grundskydd är att minska insatserna inom IT-säkerhetsprocessen. Det uppnås genom att kända tillvägagångssätt för förbättring av informationssäkerheten har samlats och presenteras för användning på nytt. Därför innehåller IT-grundskydd-katalogerna standardrisker och standardsäkerhetsåtgärder för typiska IT-system som efter behov kan användas i det egna ledningssystemet (LIS). Genom att på lämpligt sätt använda de av IT-grundskydd rekommenderade organisatoriska, personella, infrastrukturella och tekniska standardsäkerhetsåtgärderna uppnås en IT-säkerhetsnivå för den betraktade affärsprocessen. Nivån är lämplig och tillräcklig för det normala skyddsbehovet och kan utgöra en bas för affärsprocesser med stort skyddsbehov.

1.3 Målgrupp

Detta dokument riktar sig i första hand till dem som ansvarar för IT-säkerhet, IT-säkerhetschefer, IT-experter och alla intresserade IT-rådgivare som har ledningsansvar avseende informationssäkerhet. Det är även en ändamålsenlig bas för IT-ansvariga, chefer och projektledare som ansvarar för att IT-säkerhetsaspekter beaktas i tillräcklig grad inom deras institution respektive projekt.

Tillvägagångssättet i IT-grundskydd riktar sig till institutioner av alla storlekar och slag som behöver en kostnadseffektiv och målinriktad metod för att bygga upp och genomföra den för dem lämpliga säkerheten vad gäller informationssäkerhet. Begreppet institution används i detta sammanhang för företag,

myndigheter och andra offentliga eller privata organisationer. IT-grundskydd kan användas både av små och stora institutioner. Man ska i samband med detta tänka på att alla rekommendationer ska betraktas och i lämplig omfattning genomföras utifrån aktuell institutions förhållanden.

1.4 Tillämpning

I BSI-standard 100-1 ”Ledningssystem för informationssäkerhet” beskrivs med vilka metoder som informationssäkerhet kan initieras och styras inom en institution. Tillvägagångssättet enligt IT-grundskydd ger konkret hjälp hur ett ledningssystem för informationssäkerhet kan införas steg för steg. De enskilda faserna i denna process behandlas och det presenteras föredömliga lösningar från praktisk verksamhet så kallade ”kända framgångsrika arbetssätt” för att klara uppgifterna.

Detta tillvägagångssätt erbjuder en omfattande stomme för en LIS och måste endast anpassas till en institutions individuella förutsättningar. På så sätt kan ett lämpligt ledningssystem för informationssäkerhet byggas upp. För att med framgång etablera en kontinuerlig och effektiv IT-säkerhetsprocess måste en hel rad åtgärder genomföras. I det sammanhanget erbjuder IT-grundskydd-tillvägagångssättet och IT-grundskydd-katalogerna anvisningar om metoder och ger praktiska råd för genomförandet.

Dessutom erbjuder IT-grundskydd-tillvägagångssättet en standard enligt vilken institutionen kan offentliggöra sin egen LIS:s kvalitet med hjälp av ett certifikat samt ett kriterium för att man ska kunna få kännedom om mognadsgraden hos andra institutioners ledningssystem för informationssäkerhet.

En certifiering enligt IT-grundskydd kan även användas som säkerhetskrav för möjliga samarbetspartners för att definiera erforderlig nivå för IT-säkerheten hos partnern. Även om en annan metodik används som bas för ett LIS är det trots det möjligt att dra nytta av IT-grundskydd-tillvägagångssättet. På så sätt ger IT-grundskydd även lösningsansatser för olika arbetsuppgifter som berör IT-säkerheten, till exempel utarbetande av IT-säkerhetskonceptet, revision och certifiering. Beroende på de aktuella arbetsuppgifterna är det ändamålsenligt att tillämpa IT-grundskydd på olika sätt genom att exempelvis utnyttja olika aspekter av det. Allt efter användningsområde utgör enskilda komponenter, hot- och åtgärdskatalogerna samt andra hjälpmedel, som IT-grundskydd ställer till förfogande, en hjälp vid arbetet med ledningssystemet.

Kapitel 2 ger en översikt över de viktigaste stegen vid införandet av ett LIS och tillvägagångssättet för att ta fram ett IT-säkerhetskoncept.

I Kapitel 3 beskrivs hur de grundläggande faserna i starten av IT-säkerhetsprocessen kan se ut och vilka organisationsstrukturer som där är ändamålsenliga. Dessutom presenteras en systematisk väg för hur en fungerande ledningen av IT-säkerheten kan utformas och vidareutvecklas under arbetets gång.

Kapitel 4 beskriver IT-grundskydd-tillvägagångssättet för framtagning av ett IT-säkerhetskoncept. Där visas hur grundinformationen först samlas in via ett IT-nätverk och hur den kan minskas genom gruppbildning. Utgående från affärsprocesserna måste därefter skyddsbehovet för IT-tillämpningar, IT-system, kommunikationssystem och lokaler fastställas. Utifrån IT-grundskydd-katalogernas rekommendationer måste de för aktuellt IT-nätverk passande komponenterna och åtgärderna därefter väljas ut, dvs. modelleringen enligt IT-grundskydd genomföras. Innan IT-säkerhetsåtgärder genomförs måste befintliga och extra säkerhetsåtgärder integreras i IT-grundskydd-tillvägagångssättet.

Den viktigaste uppgiften för ett LIS är att garantera att IT-säkerheten upprätthålls. Detta tema behandlas i kapitel 5 där visas även möjligheten att offentliggöra den uppnådda IT-säkerhetsnivån i form av en certifiering.

IT-grundskydd-tillvägagångssättet men framförallt IT-grundskydd-katalogerna kompletteras regelbundet och anpassas till aktuell utveckling. Ett ständigt erfarenhetsutbyte med användare av IT-grundskydd gör

en behovsanpassad vidareutveckling möjlig. Dessa ansträngningar har som slutligt mål att kunna ange aktuella rekommendationer för typiska IT-säkerhetsproblem.

1.5 Litteraturförteckning

[BSI1] Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 100-1, Version 1.0, Dezember 2005, www.bsi.bund.de

[BSI2] IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 1.0, Dezember 2005, www.bsi.bund.de

[BSI3] Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 100-3, Version 1.0, Februar 2004, www.bsi.bund.de

[GSHB] IT-Grundschutzhandbuch - Standard-Sicherheitsmaßnahmen, BSI, jährlich neu, http://www.bsi.bund.de/gshb

[SHB] IT-Sicherheitshandbuch - Handbuch für die sichere Anwendung der Informationstechnik, BSI, Version 1.0 - März 1992, Bundesdruckerei

[OECD] Organisation for Economic Co-operation and Development (OECD), Guidelines for the Security of Information Systems and Networks, 2002, www.oecd.org/sti/security-privacy

[ZERT] Allgemeine Informationen zum IT-Grundschutz-Zertifikat, zum Lizenzierungsschema für Auditoren und zum Zertifizierungsschema für IT-Grundschutz unter www.bsi.bund.de/gshb/zert

[13335] ISO/IEC 13335 ”Management of information and communications technology security”, ISO/IEC JTC1/SC27

[17799] ISO/IEC 17799:2005 ”Information technology - Code of practice for information security management”, ISO/IEC JTC1/SC27

[27001] ISO/IEC 27001:2005 ”Information technology - Security techniques - Information security management systems requirements specification”, ISO/IEC JTC1/SC27

2 Ledningssystem för informationssäkerhet med IT-grundskydd

Moderna affärsprocesser inom näringsliv och myndigheter är i dag inte alls tänkbara utan IT-stöd. En tillförlitlig fungerande informationsteknik är absolut nödvändig för att upprätthålla verksamheten. Därför utgör en bristfälligt skyddad informationsteknik en ofta underskattad riskfaktor som kan vara ett hot mot många institutioners existens. Därvid går det att få en grundsäkerhet av institutionens IT med förhållandevis små medel.

För att erhålla en behovsanpassad IT-säkerhetsnivå behövs det visserligen mer än att enbart skaffa antivirusprogram, brandväggar eller system för säkerhetskopiering. Ett helhetskoncept är viktigt. Till det hör fram för allt ett fungerande och i institutionen integrerat ledningssystem för informationssäkerhet. Ledningssystem för informationssäkerhet är den delen av den allmänna riskhanteringen som ska garantera konfidentialitet, riktighet och tillgänglighet hos information, tillämpningar och IT-system. Här handlar det om en kontinuerlig process vars strategier och koncept ständigt ska kontrolleras beträffande dess effektivitet och verkan samt vid behov uppdateras.

IT-säkerhet är inte enbart en fråga om teknik utan beror i hög grad av de organisatoriska och personella förutsättningarna. Tillvägagångssättet enligt BSI:s IT-grundskydd och IT-grundskydd-katalogerna tar sedan länge hänsyn till detta, eftersom BSI rekommenderar såväl tekniska som icketekniska standardsäkerhetsåtgärder för typiska IT-tillämpningar och IT-system. Framträdande är där praktiska och aktivitetsorienterade anvisningar med målet att hålla starttröskeln i IT-säkerhetsprocessen så låg som möjligt och att undvika mycket komplexa tillvägagångssätt.

I IT-grundskydd-tillvägagångssättet visas hur ett effektivt ledningssystem för informationssäkerhet kan vara uppbyggt och hur IT-grundskydd-katalogerna kan användas inom ramen för denna uppgift. Tillvägagångssättet enligt IT-grundskydd i kombination med IT-grundskydd-katalogerna erbjuder en systematisk metodik för att ta fram IT-säkerhetskoncept och beprövade standardsäkerhetsåtgärder som redan används inom talrika myndigheter och företag.

IT-grundskydd-katalogerna som publicerades redan 1994 och i dag omfattar mer än 3 000 sidor beskriver möjliga risker samt skyddsåtgärder. IT-grundskydd-katalogerna vidareutvecklas ständigt och kompletteras behovsanpassat med aktuella facktermer. All information runt IT-grundskydd kan hämtas på BSI:s webbplats utan kostnad. För att stödja det internationella samarbetet hos myndigheter och företag ställs alla dokument som rör IT-grundskydd till förfogande på engelska och i elektronisk form.

Allt fler affärsprocesser kopplas samman via informations- och kommunikationsteknik. Detta är förknippat med en ökande komplexitet hos de tekniska systemen och med ett växande beroende av att tekniken fungerar korrekt. Därför är nödvändigt att alla inblandade agerar planerat och organiserat för att driva igenom en lämplig IT-säkerhetsnivå och upprätthålla denna. En förankring av denna process inom alla affärsområden är endast garanterad om denna uppgift ligger hos den översta ledningsnivån. Den översta ledningsnivån ansvarar för att en organisation fungerar målinriktat och korrekt och därmed även för att IT-säkerheten är garanterad internt och externt. Ledningen måste därför initiera, styra och övervaka IT-säkerhetsprocessen. Hit hör strategiska riktlinjer för IT-säkerhet, begripliga föreskrifter och även organisatoriska förhållanden för att IT-säkerhet ska kunna uppnås i alla affärsprocesser.

Ansvaret för IT-säkerheten ligger kvar på denna nivå, uppgiften ”IT-säkerhet” delegeras visserligen till en IT-säkerhetsansvarig.

Om dessa förhållanden inte föreligger i en konkret situation så bör man först försöka genomföra att de saknade IT-säkerhetsåtgärderna införs på arbetsnivå. I varje fall bör man emellertid påverka att ledningsnivån får ökat medvetande om vikten av IT-säkerhet så att den framöver tar ansvar för denna fråga. Den IT-säkerhetsprocess som man ofta kan se starta på arbetsnivå leder visserligen till en förbättring av

säkerhetssituationen men garanterar däremot inte att IT-säkerhetsnivån varaktigt vidareutvecklas.

Tillvägagångssättet enligt IT-grundskydd beskriver en väg hur ett ledningssystem för informationssäkerhet kan byggas upp och integreras inom en institution. När en institution har ett effektivt och i affärsprocessen integrerat ledningssystem för informationssäkerhet kan man utgå från att detta såväl kan uppnå den eftersträvade säkerhetsnivån och om nödvändigt förbättra den men även att klara av nya utmaningar.

Ett välunderbyggt och väl fungerande ledningssystem för informationssäkerhet är den absolut nödvändiga grunden för att kontinuerligt och tillförlitligt genomföra säkerhetsåtgärder inom en institution. Förutom den utförliga behandlingen i detta dokument finns det därför i IT-grundskydd-katalogerna en komponent för lednings av informationssäkerhet. Denna är såväl avsedd för att uppnå en enhetlig metodik vid tillämpning av IT-grundskydd samt för att kunna inkludera ledningssystemet, i enlighet med dess betydelse, i certifieringen enligt IT-grundskydd.

Som komplement till tillvägagångssättet enligt IT-grundskydd finns det i IT-grundskydd-katalogerna implementeringshjälpmedel för IT-säkerhetsprocessen att tillgå i form av standardsäkerhetsåtgärder. Målet med dessa IT-grundskydd-rekommendationer är att genom användning av organisatoriska, personella, infrastrukturella och tekniska standardsäkerhetsåtgärder uppnå en säkerhetsnivå för IT-system som är lämplig och tillräcklig för det normala skyddsbehovet och kan utgöra grund för IT-system och tillämpningar med mycket stort skyddsbehov.

I IT-grundskydd-katalogerna beskrivs hur IT-säkerhetskoncept utarbetas och kontrolleras utifrån standardsäkerhetsåtgärder. För typiska processer, tillämpningar och komponenter inom informationstekniken finns dessutom lämpliga paket (”komponenter”) av standardsäkerhetsåtgärder. Dessa komponenter är utifrån respektive fokus uppdelade i fem skikt:

- Skikt 1 omfattar samtliga övergripande IT-säkerhetsaspekter. Exempel är komponenterna personal, säkerhetskopiering och lämna ut på entreprenad.
- Skikt 2 behandlar infrastrukturen. Exempel är komponenterna byggnader, serverrum och hemarbetsplatser.
- Skikt 3 behandlar de enskilda IT-systemen. Exempel är komponenterna telekommunikationssystem, bärbar dator och mobiltelefon.
- Skikt 4 behandlar frågor beträffande hur IT-systemen är sammankopplade. Exempel är komponenterna heterogena nät, remote access samt nät- och systemhantering.
- Skikt 5 slutligen behandlar de egentliga IT-tillämpningarna. Exempel är komponenterna e-post, webbserver och databaser.

Varje komponent innehåller en kort beskrivning över ämnet, en lista med hänvisning till i respektive fall relevanta hot och en lista med hänvisning till motsvarande relevanta säkerhetsåtgärder. Hoten och åtgärderna är däremot ordnade var för sig i kataloger.

2.1 Begreppsförklaring

Målet med informationssäkerhet är att skydda information. Det kan vara fråga om information som är sparad på papper, i datorer eller i personers huvuden. IT-säkerhet avser i första hand skyddet av elektroniskt lagrad information och bearbetningen av denna. Begreppet informationssäkerhet i stället för IT-säkerhet är därför mer omfattande och används därför i större utsträckning. Eftersom begreppet IT-säkerhet ännu används i stor utsträckning i litteraturen används det fortsatt även i denna samt andra IT-grundskydd publikationer.

Planerings- och ledningsuppgiften som är nödvändig för att bygga upp och kontinuerligt genomföra en genomtänkt och verksam process för att skapa informationssäkerhet betecknas informationssäkerhets-management. Av samma skäl som ovan angetts för begreppen informationssäkerhet och IT-säkerhet används nedan oftast det kortare begreppet IT-säkerhetsmanagement.

2.2 Översikt över IT-säkerhetsprocessen

Tillvägagångssättet enligt IT-grundskydd är en hjälp vid uppbyggnad och upprätthållande av IT-säkerhets-processen inom en institution genom att vägar och metoder för det generella förfarandet men även lösningen av specifika problem anges.

För utformning av IT-säkerhetsprocessen krävs ett systematiskt förfarande så att en lämplig IT-säker-hetsnivå kan uppnås. Inom ramen för IT-grundskydd består IT-säkerhetsprocessen av följande faser:

- Initiering av IT-säkerhetsprocessen:
    - Ledningsnivåns ansvar
    - Utformning och planering av IT-säkerhetsprocessen
    - Val och etablering av en lämplig organisationsstruktur för gruppen för IT-säkerhet
- Utarbetande av ett IT-säkerhetskoncept
- Genomförande av IT-säkerhetskonceptet
    - Genomförande av IT-säkerhetsåtgärderna
    - Utbildning och ökat medvetande
- Upprätthållande av IT-säkerheten under arbetets gång

Figur: Initiering av IT-säkerhetsprocessen

Några av dessa faser kan även genomföras parallellt. T.ex. kan utformning och planering av IT-säkerhets-processen ske samtidigt med etableringen av IT-säkerhetsorganisationen eller så kan utbildningen och medvetandegörandet planeras under hela processen. I detta fall måste de tidigarelagda faserna uppdateras

med de nya resultat som kommer fram.

2.3 Utarbetande av ett IT-säkerhetskoncept

Att utarbeta ett IT-säkerhetskoncept är en av de centrala uppgifterna för IT-säkerhetsgruppen. Utifrån resultaten i den tidigare fasen identifieras här de erforderliga IT-säkerhetsåtgärderna och dokumenteras i IT-säkerhetskonceptet.

För att bättre kunna strukturera och bearbeta det mycket heterogena IT-området inklusive användningsmiljön tillämpar IT-grundskydd modulprincipen. De enskilda komponenterna som beskrivs i IT-grundskydd-katalogerna återspeglar typiska områden för IT-användningen. De sträcker sig från överordnade ämnen som ledningssystemet för informationssäkerhet, förebyggande av nödsituationer eller koncept för säkerhetskopiering till speciella komponenter i en IT-miljö. IT-grundskydd-katalogerna omfattar hotbilden och åtgärdsrekommendationer för olika komponenter och IT-system som kan sammanfattas i en komponent. BSI reviderar och uppdaterar regelbundet de befintliga komponenterna för att hålla rekommendationerna på en nivå motsvarande senaste tekniska rön. Dessutom kompletteras det befintliga verket regelbundet med ytterligare komponenter.

I kapitel 3 i detta dokument (samt komponent 1.0 i IT-grundskydd-katalogen) visas IT-säkerhetsprocessen översiktligt. Kapitel 4 innehåller en detaljerad förklaring av de av IT-grundskydd rekommenderade stegen för att ta fram IT-säkerhetskonceptet:

- IT-strukturanalys
- Fastställande av skyddsbehov
- Val av åtgärder: modellering enligt IT-grundskydd
- Grundläggande säkerhetskontroll
- Kompletterande säkerhetsanalys

De som ansvarar för IT-säkerheten kan utifrån olika anledningar och målsättningar använda tillvägagångssättet enligt IT-grundskydd och IT-grundskydd-katalogerna. I enlighet därmed beror även ordningsföljden för genomförandet av och intensiteten hos de enskilda föreslagna stegen på den befintliga IT-säkerhetsmiljön och respektive användares perspektiv.

2.4 Ledningsnivåns övertagande av ansvar

Varje myndighets eller företags högsta ledning ansvarar för att hela verksamheten fungerar målstyrt och organiserat och därigenom garanterar man IT-säkerheten internt och utåt. Det kan även vara reglerat i olika lagar allt efter verksamhetsområde och organisationsform. Ledningen måste initiera, styra och övervaka IT-säkerhetsprocessen. Ansvaret för IT-säkerheten ligger kvar på denna nivå, uppgiften ”IT-säkerhet” delegeras visserligen till en IT-säkerhetsansvarig. Dessutom krävs att ledningsnivån intensivt deltar i ledningsprocessen IT-säkerhet. Endast så kan ledningen för IT-säkerhet säkerställa att inga ohållbara risker finns och att resurser satsas på rätt ställe. Den högsta ledningsnivån är den instans som tar beslut om riskhantering och som måste ställa motsvarande resurser till förfogande.

Det faktum att ledningsnivån bär ansvaret när det gäller förebyggande och hantering av IT-säkerhetsrisker tänker företagsledningarna ofta ännu inte på i tid. I enlighet därmed är behörigheter och ansvar som gäller IT-säkerhetsfrågor ofta inte fastlagda. Information i rätt tid över möjliga IT-risker kan efter en IT-säkerhetsincident ses av ledningen för företaget eller myndigheten som en skyldighet för de IT-ansvariga. Av detta skäl är det att rekommendera att de IT-ansvariga upplyser företagets respektive myndighetens

ledning om möjliga risker och konsekvenser till följd av bristande IT-säkerhet. I varje fall ansvarar emellertid ledningsnivån för att säkerställa att den i rätt tid och i erforderlig omfattning erhåller informationen. Till de säkerhetsrelevanta ämnena hör exempelvis:

- säkerhetsriskerna för institutionen och dess information och de därmed förbundna verkningarna och kostnaderna ska redovisas
- verkningarna av IT-säkerhetsincidenter på de kritiska affärsprocesserna bör visas
- säkerhetskrav som finns till följd av lagstadgade och avtalade föreskrifter måste beskrivas
- de för branschen typiska standardtillvägagångssätten som rör IT-säkerhet bör presenteras
- fördelarna med en certifiering, för att gentemot kunder, affärspartners och tillsynsenheter kunna visa vilken nivå som har uppnåtts beträffande informationssäkerhet, bör kommenteras.

Eftersom uttalande från utomstående tredje part ofta tillmäts större vikt än vad egna medarbetare säger kan det vara förnuftigt att engagera externa konsulter när det gäller att öka företagsledningens respektive myndighetens lednings medvetande om IT-säkerheten.

Ledningsnivån bär emellertid ansvaret för att säkerhetsmålen uppnås. All personal i en organisation måste emellertid vara engagerade i säkerhetsprocessen. Idealiskt är att följande principer följs:

- initiativet för IT-säkerhet utgår från myndighetens respektive företagets ledning
- totalansvaret för IT-säkerhet ligger kvar där
- uppgiften ”IT-säkerhet” har ett aktivt stöd från myndighetens respektive företagets ledning
- myndighetens respektive företagets ledning utser de medarbetare som ansvarar för IT-säkerhet och förser dem med erforderliga befogenheter och resurser

Ledningsnivån måste även utgöra en förebild inom området IT-säkerhet. Det innebär bland annat att ledningsnivån beaktar alla föreskrivna säkerhetsregler.

Ledningsnivån måste fram för allt satsa på att IT-säkerhet integreras i alla relevanta affärsprocesser, metoder och projekt. Erfarenhet visar att den IT-säkerhetsansvarige härvid behöver ledningens fulla stöd för att av alla fackansvariga involveras i alla viktiga aktiviteter trots rådande situation med generellt höga resultatkrav.

Ledningsnivån måste, för såväl ledningen för IT-säkerhet som för alla andra områden, sätta målen så att den eftersträvade IT-säkerhetsnivån kan uppnås inom alla områden med de resurser som har ställts till förfogande (personal, tid, pengar).

3 Initiering av IT-säkerhetsprocessen

För att uppnå en lämplig och tillräcklig IT-säkerhetsnivå respektive att upprätthålla denna krävs å ena sidan ett planerat och organiserat tillvägagångssätt och å andra sidan en adekvat organisationsstruktur. Dessutom är det nödvändigt att definiera IT-säkerhetsmål och en strategi för att nå målen samt att etablera en kontinuerlig IT-säkerhetsprocess. På grund av betydelsen, de långtgående konsekvenserna av de beslut som ska fattas och av ansvaret måste detta tema alltid initieras av den högsta ledningsnivån.

3.1 Utformning och planering av IT-säkerhetsprocessen

För att kunna uppnå och upprätthålla en lämplig IT-säkerhetsnivå är det nödvändigt att etablera en kontinuerlig IT-säkerhetsprocess och att fastställa en lämplig IT-säkerhetsstrategi. En IT-säkerhetsstrategi är till hjälp för planeringen av det fortsatta förfarandet för att uppnå det uppsatta IT-säkerhetsmålet. Den anges av ledningen och baseras på ett företags affärsmål respektive en myndighets uppdrag. Ledningen anger grundläggande IT-säkerhetsmål och bestämmer vilken IT-säkerhetsnivå som är lämplig med hänsyn till affärsmålen och fackuppgifterna. De därför erforderliga medlen måste likaså ställas till förfogande av ledningsnivån.

3.1.1 Fastställande av förutsättningar

Ett företags eller en myndighets principiella mål och uppgifter utgör grunden för alla affärsprocesser respektive fackmetoder och aktiviteter. För att lägga fast en lämplig IT-säkerhetsstrategi bör varje institution därför fastställa sina viktigaste affärsprocesser och fackuppgifter. Vid det här laget finns det knappast områden inom vilka viktiga affärsprocesser fungerar utan IT-stöd. Sambanden mellan affärsprocesser och den använda informationstekniken utgör grunden för beslutet om vilken säkerhetsnivå som är lämplig i varje fall. Nedan förklaras denna beslutsprocess närmare.

För varje affärsprocess och varje facktillämpning måste en kontaktperson utses. Denne så kallade informationsägare ansvarar för alla frågor rörande informationsbearbetning inom ramen för denna affärsprocess. De fackansvariga eller informationsägarna är exempelvis ansvariga för delegering av uppgifter och hantering av information inom ramen för den affärsprocess som de har hand om. För varje affärsprocess och fackuppgift måste det fastställas hur kritisk, dvs. vilket skydd som behövs, den bearbetade informationen är. Företagsledningen respektive myndighetens ledning måste slutligen bifalla skyddsbehovet för varje affärsprocess eftersom säkerhetskrav uppkommer och resurser måste kopplas till dessa.

Via analysen av affärsprocesserna går det att härleda uppgifter om verkan av IT-säkerhetsincidenter på affärsverksamheten. I många fall räcker det att arbeta med en mycket grov beskrivning av affärsprocesserna.

Följande frågor ska gå att besvara:

- Vilka affärsprocesser är beroende av en fungerande, alltså en korrekt och kravanpassat arbetande informationsteknik?
- Vilken information bearbetas för dessa affärsprocesser?
- Vilken information är särskilt viktig och därmed skyddsvärd vad beträffar konfidentialitet, riktighet och tillgänglighet (t.ex. personrelaterade data, kunddata, strategisk information, hemlig information som utvecklingsdata, patent, metodbeskrivningar)?

Många interna förutsättningar kan påverka IT-säkerheten och måste fastställas. I detta tidiga skede handlar det inte om att detaljerat beskriva informationstekniken. Det bör emellertid finnas en grov översikt, vilken information för en affärsprocess som bearbetas med vilka IT-tillämpningar och IT-system.

Dessutom måste likaså alla externa förutsättningar som påverkar IT-säkerheten fastställas. Det är exempelvis lagstadgade förutsättningar, miljöpåverkan, krav från kunder och affärspartners eller branschspecifika IT-säkerhetsstandarder.

För att för varje viktig affärsprocess så snabbt som möjligt och omfattande fastställa alla relevanta förutsättningar rekommenderas att ett kort säkerhetssamtal (brainstorming) hålls för varje affärsprocess. Dessa säkerhetssamtal bör genomföras under ledning av den IT-säkerhetsansvarige med vederbörande informationsägare respektive fackansvariga samt motsvarande IT-ansvariga. Resultaten bör dokumenteras enligt ett i förväg fastlagt schema.

Punkter att utföra:

• utse kontaktperson för alla affärsprocesser och facktillämpningar

• utföra en grov uppskattning av värdet av information, affärsprocesser och facktillämpningar

• fastställa förutsättningar.

3.1.2 Formulering av allmänna IT-säkerhetsmål

Vid starten av varje säkerhetsprocess bör IT-säkerhetsmålen bestämmas noggrant. I annat fall finns risken att IT-säkerhetsstrategier och –koncept utarbetas och dessa inte uppfyller myndighetens respektive företagets verkliga krav. Det kan betyda att oönskade risker tas men även att för mycket resurser investeras i olämpliga eller för påkostade IT-säkerhetsåtgärder.

Därför bör först allmänna IT-säkerhetsmål härledas ur institutionens principiella mål och de allmänna förutsättningarna. Från dessa härleds senare konkreta IT-säkerhetskrav på IT-verksamheten när IT-säkerhetskonceptet tas fram och vid utformningen av IT-säkerhetsorganisationen. Möjliga allmänna IT-säkerhetsmål för en institution kan t.ex. vara:

• hög tillförlitlighet vid utförande, även vad beträffar hantering av information (tillgänglighet, riktighet, konfidentialitet)

• att garantera institutionens goda rykte utåt

• bibehålla de värden som investerats i teknik, information, arbetsprocesser och kunskap

• säkra de stora möjligen oersättliga värden hos den bearbetade informationen

• säkra informationens kvalitet, t.ex. när den utgör grund för vittgående beslut

• garantera de krav som är ett resultat av lagar och förordningar

• minskning av de kostnader som uppstår vid skada (såväl genom att undvika sakskador som att förebygga skador) och

• att säkerställa arbetsförloppens kontinuitet inom institutionen.

För att kunna definiera IT-säkerhetsmål bör man först göra en uppskattning av vilka affärsprocesser respektive metoder och information som är nödvändiga för att utföra uppgiften och vilken vikt som ska läggas vid dessa. I samband med detta är det viktigt att klarlägga i vilken grad som lösandet av uppgiften inom institutionen beror på den IT som används och att den fungerar säkert. För definitionen av IT-

säkerhetsmålen är det lämpligt att klart ange de grundvärden som ska skyddas tillgänglighet, riktighet och konfidentialitet och eventuellt att prioritera. Dessa uppgifter kommer att spela en viktig roll under IT-säkerhetsprocessen vid val av IT-säkerhetsåtgärderna och -strategierna.

Att bestämma IT-säkerhetsmålen och den eftersträvade IT-säkerhetsnivån är däremot endast starten av IT-säkerhetsprocessen. Konkreta beslut avseende resurser och investeringar som uppkommer under IT-säkerhetsprocessen måste godkännas av den högsta ledningsnivån i ett senare skede. Det betyder att här måste det inte utföras någon detaljerad analys av IT-strukturerna och de möjliga kostnaderna för IT-säkerhetsåtgärder utan enbart ett uttalande om vad som är av särskild vikt för institutionen och varför.

För att bättre förstå IT-säkerhetsmålen kan den eftersträvade IT-säkerhetsnivån visas för enskilda, särskilt viktiga affärsprocesser respektive områden inom institutionen beträffande IT-säkerhetens grundvärden (konfidentialitet, riktighet, tillgänglighet). Detta är till hjälp för den senare formuleringen av det detaljerade IT-säkerhetskonceptet.

Nedan anges några exemplariska kriterier för bestämning av en lämplig IT-säkerhetsnivå. Med hjälp av de uppgifter som snarast gäller kan IT-säkerhetsnivån (normal, hög eller mycket hög) bestämmas. Under denna fas av IT-säkerhetsprocessen handlar det om att formulera de första vägvisande uttalandena som i de senare faserna kommer att användas som grund och inte om att detaljerat fastlägga skyddsbehov.

Mycket hög:

- Skyddet av konfidentiell information måste ovillkorligen vara garanterat och i säkerhetskritiska områden uppfylla stänga krav på konfidentialitet.
- Informationen måste i högsta grad vara korrekt.
- Institutionens centrala uppgifter går inte att utföra utan användning av IT. Begränsade reaktionstider för kritiska beslut kräver att aktuell information alltid är tillgänglig, avbrottstider kan inte accepteras.

Sammantaget gäller: Bortfall av IT leder till ett totalt sammanbrott av institutionens verksamhet eller har allvarliga följder för offentlig eller privat verksamhet.

Hög:

- Skyddet av konfidentiell information måste uppfylla höga krav och vara mer uttalat inom säkerhetskritiska områden.
- Bearbetad information måste vara korrekt, fel som uppträder måste kunna registreras och undvikas.
- Inom institutions kärnverksamhet pågår tidskritiska förlopp eller det utförs uppgifter med mycket stor volym vilka inte kan utföras utan hjälp av IT. Endast korta avbrottstider är acceptabla.

Sammantaget gäller: Vid skada kan centrala områden av institutionen inte utföra sina uppgifter, skador medför att institutionen som sådan eller tredje part påverkas negativt i hög grad.

Normal:

- Skyddet av information som endast är avsedd för intern användning måste vara garanterat.
- Mindre fel kan accepteras. Fel som i hög grad negativt påverkar utförandet av uppgifter måste däremot kunna registreras och undvikas.
- Längre avbrottstider som medför att tidsgränser överskrids kan inte accepteras.

Sammantaget gäller: Skador medför att institutionen påverkas negativt.

Det är ovillkorligen nödvändigt att ledningsnivån medverkar när IT-säkerhetsmålen formuleras. För detta i

IT-säkerhetsprocessen grundläggande steget kan det även vara förnuftigt att koppla in en extern IT-säkerhetsexpert. För att bestämma den eftersträvade IT-säkerhetsnivån måste institutionens mål ses i förhållande till dess IT-säkerhetskrav. Man bör däremot ta hänsyn till det faktum att i regel är tillgängliga resurser för implementeringen av IT-säkerhetsåtgärder begränsade. Av denna anledning är det särskilt viktigt att identifiera det verkliga behovet av tillgänglighet, riktighet och konfidentialitet eftersom en hög IT-säkerhetsnivå i regel även är förbunden en stor implementeringsinsats. Här kan också rekommenderas att prioritera de formulerade kraven när det är möjligt. Det kommer vid resursplaneringen i senare faser av IT-säkerhetsprocessen att utgöra ett beslutsunderlag.

Tips om beskrivningarnas omfattning

I denna tidiga fas av IT-säkerhetsprocessen handlar det inte om att i detalj se på alla IT-system och tillämpningar eller en komplex riskanalys. Det är viktigt att ha en översikt över vilka säkerhetskrav som ställs på informationstekniken utifrån affärsprocesser eller metoder. När den eftersträvade IT-säkerhetsnivån har bestämts bör till exempel följande frågor besvaras:

- Vilka kritiska uppgifter hos myndigheten respektive företaget kan inte, endast otillräckligt eller med avsevärda extrainsatser utföras utan stöd av IT?
- Vilka viktiga beslut hos myndigheten respektive företaget är baserade på konfidentialitet, riktighet och tillgänglighet?
- Vilken verkan kan avsiktliga eller oönskade IT-säkerhetsincidenter ha?
- Bearbetas med den använda informationstekniken information vars konfidentialitet ska skyddas speciellt?
- Beror viktiga beslut på att informationen, som bearbetas med IT, är korrekt, aktuell och tillgänglig?

Beskrivningarna av den eftersträvade IT-säkerhetsnivån bör vara anpassade till respektive miljö. Korta motiveringar är till hjälp för motivationen som bygger därpå. Det kunde exempelvis för ett sjukhus heta: ”På röntgenavdelningen krävs en mycket hög IT-säkerhetsnivå eftersom människors liv hänger på att IT-systemen fungerar korrekt.”

Punkter att utföra:

- värdera affärsprocessernas, metodernas och informationens betydelse
- bestämma allmänna IT-säkerhetsmål
- få ledningsnivåns samtycke.

3.1.3 Utarbetande av en IT-säkerhetspolicy

IT-säkerhetspolicyn beskriver lättbegripligt för vilka ändamål, med vilka medel och med vilka strukturer som informationssäkerhet bör byggas upp inom en institution. Den innehåller de av institutionen eftersträvade IT-säkerhetsmålen samt den tillämpade IT-säkerhetsstrategin. IT-säkerhetspolicyn beskriver därmed även via IT-säkerhetsmålen den eftersträvade IT-säkerhetsnivån inom en myndighet eller ett företag. Den är därmed samtidigt ett krav och ett uttalande att denna IT-säkerhetsnivå bör uppnås på institutionens alla nivåer.

IT-säkerhetspolicyn bör tas fram i följande steg:

- **Ansvaret hos myndighetens respektive företagets ledning för IT-säkerhetspolicyn**

Med IT-säkerhetspolicyn dokumenteras vilken strategisk position som institutionsledningen intar för att uppnå IT-säkerhetsmålen på organisationens alla nivåer.

Eftersom IT-säkerhetspolicyn utgör det centrala strategidokumentet för en institutions IT-säkerhet måste den vara så utformad att alla organisationsenheter kan identifiera sig med dess innehåll. När policyn tas fram bör därför så många områden som möjligt delta. Varje institution måste slutligen emellertid besluta vilka avdelningar och nivåer som ska medverka vid formuleringen av IT-säkerhetspolicyn.

När IT-säkerhetspolicyn tas fram är det lämpligt att utnyttja följande organisationsenheters fackkunskaper: IT-användning, IT-drift, säkerhet (IT och infrastruktur), personalavdelning, företagsnämnd, revision, ekonomi och juridik.

• Fastställa giltighetsområde

Av IT-säkerhetspolicyn ska det framgå för vilka områden den gäller. Giltighetsområdet kan vara hela institutionen eller delar av den. Det är däremot viktigt att de betraktade affärsuppgifterna och -processerna ingår i giltighetsområdet. Speciellt för större organisationer är det inte alltid en enkel uppgift att fastställa giltighetsområdet. En orientering efter ansvar kan därvid vara till hjälp.

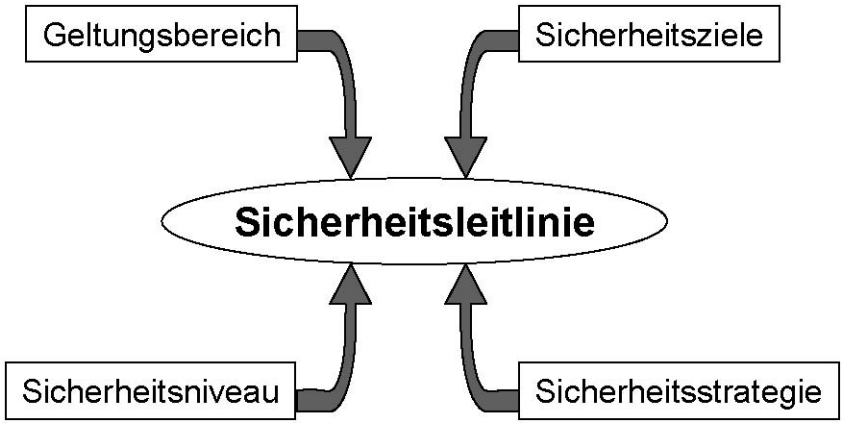
• IT-säkerhetspolicyns innehåll

IT-säkerhetspolicyn bör vara kort och koncist formulerad eftersom mer än 20 sidor inte har fungerat i praktiken. Den bör innehålla minst följande information:

- IT-säkerhetens vikt och betydelsen av IT för att lösa uppgifterna
- IT-säkerhetsmålens relation till affärsmålen och institutionens uppgifter
- säkerhetsmål och säkerhetsstrategins kärnpunkter för den använda informationstekniken
- försäkran att IT-säkerhetspolicyn genomförs av institutionsledningen och direktiv för resultatkontrollen och
- beskrivning av den för genomförande av IT-säkerhetsprocessen etablerade organisationsstrukturen (jämför M 2.193 *Uppbyggnad av en lämplig organisationsstruktur för IT-säkerhet*).

Dessutom kan följande uttalanden läggas till:

- för motivationen kan några för affärsprocessen viktiga hot markeras och de viktigaste lagarna och föreskrifterna och andra viktiga förutsättningar (som avtal) anges
- de viktiga uppgifterna och ansvarsområdena inom IT-säkerhetsprocessen bör presenteras (speciellt för gruppen för IT-säkerhet, den IT-säkerhetsansvarige, IT-användarna och IT-administratörerna). Dessutom bör kontaktpersoner för säkerhetsfrågor utses
- program för främjande av IT-säkerheten genom utbildning och åtgärder för ökat medvetande kan tillkännages.



Figur: IT-säkerhetspolicyns innehåll

• Sammankallande av en utvecklingsgrupp för IT-säkerhetspolicyn

Om det inom myndigheten eller företaget redan finns en grupp för IT-säkerhet så bör denna utveckla respektive kontrollera och revidera IT-säkerhetspolicyn. Därefter presenteras detta förslag för myndighetens respektive företagets ledning för godkännande.

Om gruppen för IT-säkerhet håller på att byggas upp så bör en arbetsgrupp för utarbetande av IT-säkerhetspolicyn etableras. Denna grupp kan under IT-säkerhetsprocessen överta funktionen för gruppen för IT-säkerhet. Det är lämpligt om följande personer ingår i arbetsgruppen företrädare för IT-användarna, företrädare för IT-driften och en eller flera medarbetare med tillräckliga kunskaper i ämnet IT-säkerhet. Idealiskt är om det även ingår en medlem av ledningsnivån som kan bedöma betydelsen av informationstekniken för myndigheten eller företaget.

• Tillkännagivande av IT-säkerhetspolicyn

Det är viktigt att myndighetens respektive företagets ledning markerar sin målsättning och förväntningar genom att tillkännage IT-säkerhetspolicyn och inom hela organisationen förtydligar vikten samt betydelsen av IT-säkerhet. Alla medarbetare bör därför känna till IT-säkerhetspolicyns innehåll och kunna förstå det. IT-säkerhetspolicyn bör förklaras för nya medarbetare innan de får tillgång till informationsbearbetning.

Eftersom institutionsledningens ansvar med referens till IT-säkerhetspolicyn är avgörande bör policyn vara skriftlig. Myndighetens respektive företagets ledning bör formellt ha godkänt den. IT-säkerhetspolicyns innehåll bör alltså inom institutionen inte endast vara känd utan även vara enkelt åtkomlig t.ex. i intranätet. Om den innehåller konfidentiella uttalanden bör dessa placeras i en bilaga till policyn som är märkt konfidentiell.

Slutligen bör alla medarbetare göras uppmärksamma på att från varje medarbetare förväntas ett engagerat, samarbetsinriktat samt ansvarsmedvetet handlande inte bara vid utförande av uppgifter i allmänhet utan även vid utförande av uppgiften ”IT-säkerhet”.

• **Uppdatering av IT-säkerhetspolicyn**

IT-säkerhetspolicyn bör regelbundet kontrolleras huruvida den är aktuell och vid behov anpassas. Härvid bör exempelvis beaktas huruvida affärsmål eller uppgifter har förändrats, huruvida nya organisationsstrukturer har skapats eller om nya IT-system har införts. Vid den ofta snabba utvecklingen inom IT-

området å ena sidan och säkerhetsläget å andra sidan rekommenderas att man tänker över IT-säkerhetspolicyn minst vartannat år.

Punkter att utföra:

• erhålla ledningsnivåns uppdrag att utarbeta en IT-säkerhetspolicy

• fastställa giltighetsområde

• sammankalla arbetsgrupp för IT-säkerhetpolicyn

• genom ledningsnivån se till att IT-säkerhetspolicyn träder i kraft

• tillkännage IT-säkerhetspolicyn

• regelbundet kontrollera IT-säkerhetspolicyn och vid behov uppdatera.

3.2 Uppbyggnad av en IT-säkerhetsorganisation

Den eftersträvade IT-säkerhetsnivån kan endast uppnås om IT-säkerhetsprocessen genomförs inom hela verksamheten. Denna övergripande karaktär hos IT-säkerhetsprocessen gör det nödvändigt att lägga fast roller inom institutionen och tillordna rollerna motsvarande uppgifter. Dessa roller ska besättas med kvalificerade medarbetare och utföras av dessa. Endast på det sättet kan det garanteras att alla viktiga aspekter beaktas och att samtliga uppgifter som uppkommer utförs effektivt.

Organisationen som krävs för främja och genomföra IT-säkerhetsprocessen kallas IT-säkerhets-organisation.

Hur många personer som i någon organisationsstruktur och med vissa resurser är sysselsatta med IT-säkerhet beror på aktuell institutions storlek, sammansättning och struktur. I alla fall bör en IT-säkerhetsansvarig utses som ansvarig för IT-säkerhet. I större organisationer bör dessutom en grupp för IT-säkerhet etableras. Denna grupp styr alla övergripande uppgifter med betydelse för IT-säkerheten och utarbetar föreskrifter och riktlinjer.

För att säkerställa en direkt väg till institutionens ledning bör dessa roller ligga som stabsfunktioner. På ledningsnivån bör uppgiften IT-säkerhet entydigt ligga hos en medlem av företagets eller myndighetens ledning. Den IT-säkerhetsansvarige rapporterar till vederbörande.

Grundregel:

Det viktigaste när rollerna inom ledningen av IT-säkerhet definieras är att:

• totalansvaret för korrekt och säker lösning av uppgifterna (och därmed för IT-säkerheten) ligger kvar hos ledningsnivån

• att minst utse en person (normalt sett den IT-säkerhetsansvarige) som främjar och koordinerar IT-säkerhetsprocessen

• varje medarbetare ansvarar lika mycket för sina ordinarie arbetsuppgifter som för att IT-säkerheten upprätthålls på dennes arbetsplats och i omgivningen.

Integration av IT-säkerhet i organisationsövergripande förlopp och processer

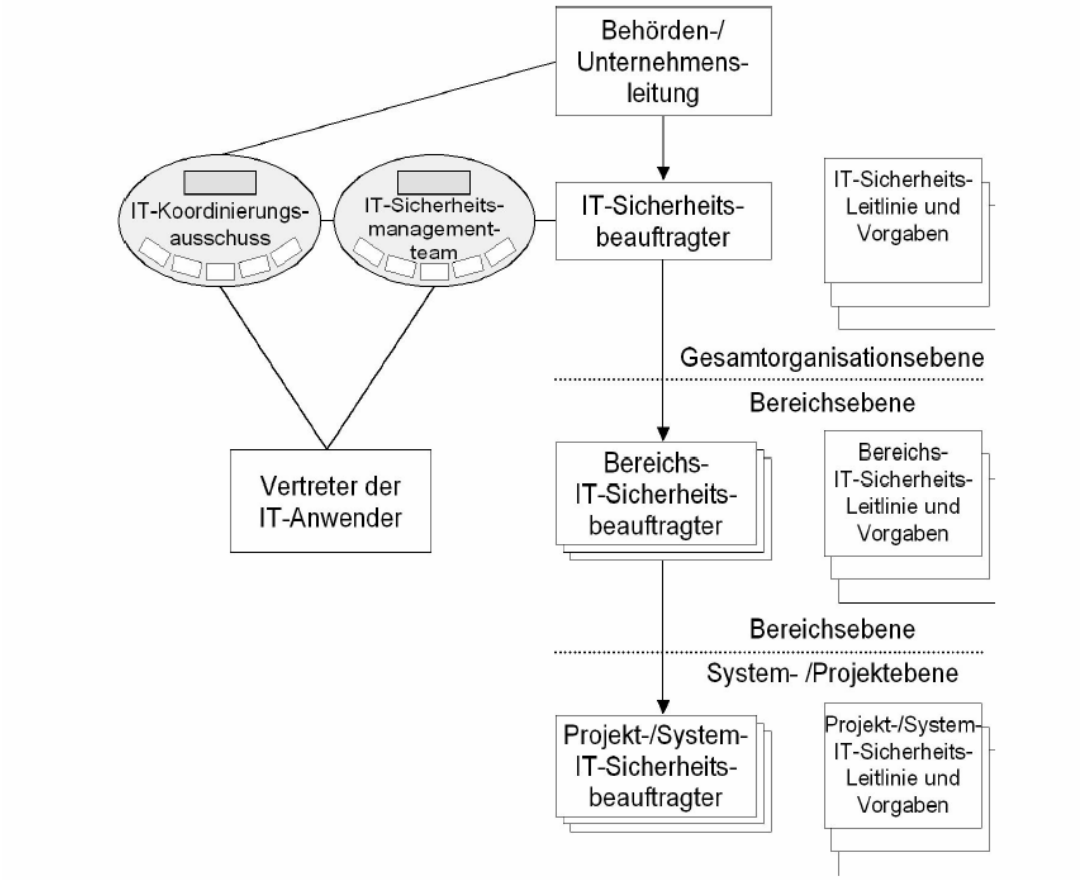
Ledning av IT-säkerhet är bara en av många ledningsuppgifter men har däremot inflytande på nästan alla områden inom en institution. Därför måste ledningen för IT-säkerhet integreras på ett förnuftigt sätt i befintliga organisationsstrukturer och kontaktpersoner utses. Uppgifter och befogenheter måste vara klart

avgränsade från varandra. I samband med detta måste garanteras att nödvändiga IT-säkerhetsaspekter inte endast beaktas vid enskilda åtgärder utan vid alla strategiska beslut (till exempel när verksamhet läggs ut på entreprenad eller när elektroniska distributionskanaler används). För att säkerställa detta är det viktigt att IT-säkerhetsorganisationen i rätt tid blir inkopplad i alla projekt som kan påverka informations-säkerheten.

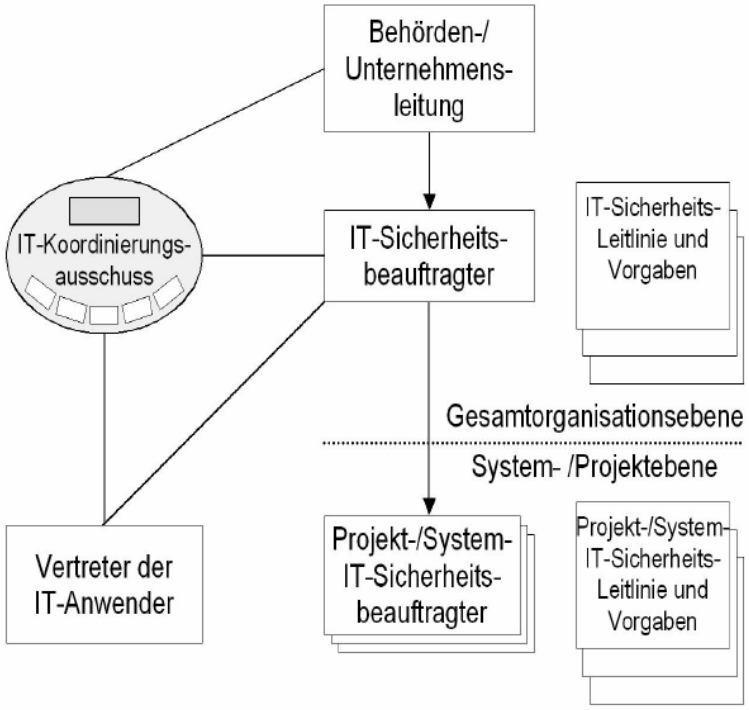
Fram för allt i större organisationer finns det ofta redan ett övergripande riskhanteringssystem. Eftersom IT-risker tillhör de viktigaste operationella riskerna bör metoderna för IT-riskhantering avstämmas med de redan etablerade metoderna.

Uppbyggnad av IT-säkerhetsorganisationen

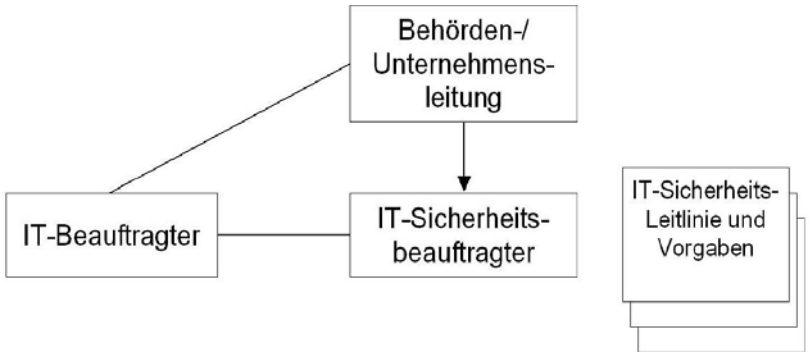
Beroende på institutionens storlek finns olika möjligheter för hur IT-säkerhetsorganisationen kan vara uppbyggd. I figurerna nedan visas tre olika uppbyggnader. Den första figuren visar strukturen för IT-säkerhetsorganisationen i en stor institution. Den andra figuren visar uppbyggnaden i en medelstor institution i vilken gruppen för IT-säkerhet och den IT-säkerhetsansvarige har lagts samman. Den tredje figuren visar en struktur för IT-säkerhetsorganisationen i en liten institution där alla uppgifter hanteras av den IT-säkerhetsansvarige.



Figur: Uppbyggnad av IT-säkerhetsorganisationen i en stor institution



Figur: Uppbyggnad av IT-säkerhetsorganisationen i en medelstor institution



Figur: Uppbyggnad av IT-säkerhetsorganisationen i en liten institution

Här kan klart påpekas att de i figurerna visade centrala rollerna inte ovillkorligen måste innehas av olika personer. Den personella besättningen riktar sig efter aktuell institutions storlek, tillgängliga resurser och den eftersträvade IT-säkerhetsnivån. Resursplaneringen för att stödja IT-säkerheten måste ske så att den beslutade IT-säkerhetsnivån även faktiskt kan uppnås.

Uppgifter, ansvar och befogenheter i IT-säkerhetsorganisationen

IT-säkerhetsansvarig och gruppen för IT-säkerhet måste ha klart definierade uppgifter, ansvar och befogenheter vilka ska fastställas av ledningsnivån. För att kunna utföra sin uppgift bör de vara delaktiga i

alla relevanta metoder och beslut. Rollerna ska integreras i organisationsstrukturen på sådant sätt alla inblandade kan kommunicera med varandra. För uppgiften som IT-säkerhetsansvarig respektive som medlem i gruppen för IT-säkerhet bör kvalificerade personer utses. Vid behov kan uppgifter delegeras till områdes-IT-säkerhetsansvarig, IT-projektledare, IT-system-säkerhetsansvarig.

Den IT-säkerhetsansvarige

IT-säkerhet försummas ofta så att den får stå tillbaka för de dagliga arbetsuppgifterna. Därigenom finns vid oklar ansvarsfördelning risken att IT-säkerhet i princip blir ”någon annans problem”. Därmed skjuts ansvaret för IT-säkerhet fram och tillbaka tills ingen längre tror sig ha ansvaret. För att undvika detta bör en huvudkontaktperson för IT-säkerhetsfrågor, en IT-säkerhetsansvarig utses. Denne koordinerar uppgiften IT-säkerhet inom myndigheten respektive företaget och driver frågan. Om det förutom denne finns fler personer med säkerhetsuppgifter och hur IT-säkerheten är organiserad beror på institutionens storlek.

För att framgångsrikt kunna planera, genomföra och upprätthålla en IT-säkerhetsprocess måste ansvaret vara klart definierat. Det måste alltså finnas roller definierade vilka svarar för olika frågor för att IT-säkerhetsmålen ska uppnås. Dessutom måste det ha utsetts personer som är kvalificerade och som har tillgång till tillräckliga resurser för att klara dessa roller.

Den IT-säkerhetsansvarige är ansvarig för att ta hänsyn till allt som har betydelse för IT-säkerheten inom institutionen. Den IT-säkerhetsansvariges huvuduppgift består i att ge råd till institutionens ledning när de ska utföra sina uppgifter som rör IT-säkerheten och att ge stöd när den ska genomföras. Dennes uppgifter omfattar bland annat:

- att leda IT-säkerhetsprocessen och medverka i alla därmed sammanhängande uppgifter
- att ge stöd åt ledningsnivån när IT-säkerhetspolicyn tas fram
- att koordinera framtagandet av IT-säkerhetskonceptet, konceptet för hantering av nödsituationer och andra delkoncept och att koordinera systemsäkerhetsriktlinjer samt utfärda ytterligare riktlinjer och regler för IT-säkerheten
- att initiera och kontrollera genomförandet av IT-säkerhetsåtgärder
- att lämna rapporter till ledningsnivån och gruppen för IT-säkerhet över tillståndet för IT-säkerheten
- att koordinera säkerhetsrelevanta projekt
- att undersöka IT-säkerhetsincidenter
- att initiera och koordinera åtgärder för ökat medvetande samt utbildning.

Den IT-säkerhetsansvarige ska dessutom knytas till alla nya projekt med anknytning till IT samt introduktionen av nya IT-tillämpningar och IT-system för att garantera att IT-säkerhetsaspekter beaktas i de olika projektfaserna.

Kravprofil

För att kunna utföra dessa uppgifter är det önskvärt att den IT-säkerhetsansvarige har kunskap och erfarenhet inom områdena IT-säkerhet och IT. Eftersom denna uppgift kräver förmåga inom flera områden bör man vid valet dessutom tänka på att följande kvalifikationer finns:

- identifiering med målen för IT-säkerheten, överblick över institutionens uppgifter och mål och insikt i nödvändigheten av IT-säkerhet
- samarbets- och teamförmåga men även förmåga att hävda sig (få andra uppgifter kräver så stor kompetens och skicklighet i umgänget med andra personer: ledningsnivån måste i IT-säkerhetsprocessens centrala frågor om och om igen involveras, beslut måste krävas in och IT-

användarna måste, eventuellt med hjälp av den IT-säkerhetsansvarige, involveras i IT-säkerhetsprocessen)

- erfarenhet av projektledning helst från området systemanalys och kunskap om metoder för riskbedömning.

En IT-säkerhetsansvarig måste dessutom vara beredd att sätta sig in i nya områden och att följa utvecklingen inom informationstekniken. Denne bör utbilda och vidareutbilda sig så att han har de erforderliga fackkunskaperna för att utföra sina uppgifter.

Samarbete och kommunikation

Samarbetet med IT-användaren kräver mycket skicklighet eftersom dessa först måste övertygas om nödvändigheten av, de för dem ofta något besvärliga, IT-säkerhetsåtgärderna. Ett likaså känsligt ämne är att fråga IT-användare om säkerhetskritiska händelser och sårbarhet. För att garantera resultatet från dessa utfrågningar måste IT-användarna övertygas om att ärliga svar inte leder till problem för dem själva.

Den IT-säkerhetsansvariges förmåga att kommunicera krävs inte enbart gentemot IT-användarna. Lika viktigt är att den IT-säkerhetsansvarige kan hävda sin mening beträffande sakfrågor gentemot myndighetens eller företagets ledning. Han måste ha självförtroende och kunna kommunicera för att vid tillfälle även protestera mot ett beslut som inte ligger i linje med målet en säker IT-drift.

Oberoende

Det rekommenderas att funktionen som IT-säkerhetsansvarig organisatoriskt är placerad som en stabsuppgift. Det är t.ex. problematiskt om en person som ansvarar för IT-driften dessutom ska ha denna funktion eftersom det med stor sannolikhet leder till intressekonflikter. De dubbla rollerna kan leda till att han som IT-säkerhetsansvarig kan protestera mot beslut som i hög grad skulle underlätta hans uppgift som driftansvarig eller som rentav kraftigt favoriseras av hans chef.

Datasekretessombud

En ofta ställd fråga är om funktionen som IT-säkerhetsansvarig samtidigt kan innehas av datasekretess-ombudet. De båda rollerna utesluter principiellt inte varandra men några aspekter måste förvisso först klaras ut:

- Gränssnitten mellan de båda rollerna bör klart definieras och dokumenteras. Dessutom bör det för båda rollerna finnas direkta rapporteringsvägar uppåt. Vidare bör man tänka igenom huruvida konfliktladdade frågor dessutom bör rapporteras till revisionen för kännedom.
- Det måste säkerställas att den IT-säkerhetsansvarige har tillräckliga resurser för att tillvarata båda rollerna. Vid behov måste denne erhålla personellt stöd.

Man får inte glömma att även den IT-säkerhetsansvarige behöver en kvalificerad ställföreträdare.

IT-säkerhetsgruppen

IT-säkerhetsgruppen utgör ett stöd för den IT-säkerhetsansvarige genom att den koordinerar övergripande åtgärder i hela organisationen, samlar in information och genomför kontrolluppgifter. Den exakta inriktningen beror på den aktuella institutionens storlek, tillgängliga resurser och den eftersträvade IT-säkerhetsnivån. I extremfall består gruppen endast av en person, den IT-säkerhetsansvarige som då har hand om alla uppgifter inom IT-säkerhetsprocessen.

Uppgifter för gruppen för IT-säkerhet är speciellt:

- att bestämma IT-säkerhetsmål och -strategier samt att ta fram IT-säkerhetskonceptet

---

- att kontrollera genomförandet av IT-säkerhetspolicyn
- att initiera, styra och kontrollera IT-säkerhetsprocessen
- att medverka vid framtagandet av IT-säkerhetskonceptet
- att kontrollera huruvida de i IT-säkerhetskonceptet planerade IT-säkerhetsåtgärderna fungerar som avsett samt att de är lämpliga och verksamma
- att planera program för utbildning och ökat medvetande vad gäller IT-säkerhet samt
- att ge råd i IT-säkerhetsfrågor till IT-koordineringsgruppen och ledningsnivån.

Gruppens sammansättning

För att kunna klara sina uppgifter bör gruppen bestå av personer som har kunskap om IT-säkerhet, IT-system samt erfarenhet av organisation och förvaltning. Där utöver bör gruppen för IT-säkerhet återspegla en organisations olika områden. I gruppen för IT-säkerhet bör minst följande roller finnas representerade: en IT-ansvarig, den IT-säkerhetsansvarige och en företrädare för IT-användarna. Om det i organisationen redan finns en liknade kommitté skulle dess uppgifter utvidgas med de säkerhetsrelaterade. För att understryka betydelsen av IT-säkerhet är det däremot tillrådligt att etablera en grupp för IT-säkerhet och förse denna med lämpliga resurser.

Endast få antingen mycket stora organisationer eller sådana med ett stort behov av IT-säkerhet kommer att ha möjligheten att kunna ha personer som på heltid permanent arbetar i gruppen. I allmänhet sköts dessa uppgifter som en bisyssla till de ordinarie uppgifterna. Ett undantag är däremot när IT-säkerhetsprocessen tas fram första gången. Om möjligt bör medlemmarna i gruppen för IT-säkerhet under detta skede i hög grad befrias från sina övriga uppgifter. Beslutet om och i vilken omfattning denna befrielse är lämplig även därefter beror på fördelningen av uppgifter mellan gruppen för IT-säkerhet och den IT-säkerhetsansvarige. Det slutliga beslutet i denna fråga ligger hos institutionens ledning. I varje fall bör ledningen för IT-säkerhet sammanträda regelbundet för att garantera en kontinuerlig styrning av IT-säkerhetsprocessen.

Områdes-IT-säkerhetsansvarig, IT-projekt- respektive IT-system-säkerhetsansvarig

I stora organisationer kan det vara nödvändigt att sätta in särskilda IT-säkerhetsansvariga för de olika områdena. Den områdes-IT-säkerhetsansvarige ansvarar inom sitt område (t.ex. avdelning eller filial) för alla säkerhetsbehov med avseende på IT-system och -tillämpningar. Allt efter storleken på det område som hanteras kan den områdes-IT-säkerhetsansvariges uppgift skötas av en person som redan har anförtrotts liknande uppgifter t.ex. den områdes-IT-ansvarige). Tänk vid valet av områdes-IT-säkerhetsansvarig på att denne har god kännedom om uppgifter, förhållanden och arbetsförlopp inom området som denne svarar för.

En institutions olika IT-system och -tillämpningar har ofta olika IT-säkerhetskrav som eventuellt är sammanfattade i en IT-system-säkerhetspolicy och som kräver olika IT-säkerhetsåtgärder. Analogt gäller för den IT-projekt-säkerhetsansvarige med den skillnad att uppgifterna är IT-projektspecifika i stället för IT-systemspecifika.

Uppgifterna för den IT-projekt-, IT-system- respektive områdes-säkerhetsansvarige omfattar:

- att genomföra den IT-säkerhetsansvariges anvisningar
- att genomföra IT-säkerhetsåtgärderna enligt IT-system-säkerhetspolicyn
- att sammanställa IT-systemspecifik information och lämna över till den IT-säkerhetsansvarige

---

- att vara kontaktperson på plats för IT-användarna
- att medverka vid val av IT-säkerhetsåtgärder för genomförande av IT-system-säkerhetspolicyn
- sammanställa information om behov av utbildning av och ökat medvetande hos IT-användare åt den IT-säkerhetsansvarige
- att regelbundet kontrollera och utvärdera loggfiler samt
- att till den IT-säkerhetsansvarige meddela säkerhetsrelevanta incidenter som eventuellt uppträder.

Följande *kvalifikationer* bör finnas:

- detaljerade IT-kunskaper eftersom dessa underlättar samtalen med IT-användarna och är till nytta vid sökning efter IT-säkerhetsåtgärder för de speciella IT-systemen samt
- kunskap om projektledning som kan vara till hjälp vid organisation av IT-användarintervjuer och vid upprättande av planer för genomförandet av IT-säkerhetsåtgärder samt vid kontroll av dessa.

IT-koordineringsgrupp

IT-koordineringsgruppen är i regel inte en permanent funktion inom en institution utan sammankallas vid behov (t.ex. vid planering av större IT-projekt). Gruppens uppgift är att koordinera samspelet mellan gruppen för IT-säkerhet, företrädaren för IT-användarna, den IT-säkerhetsansvarige och institutionens ledning.

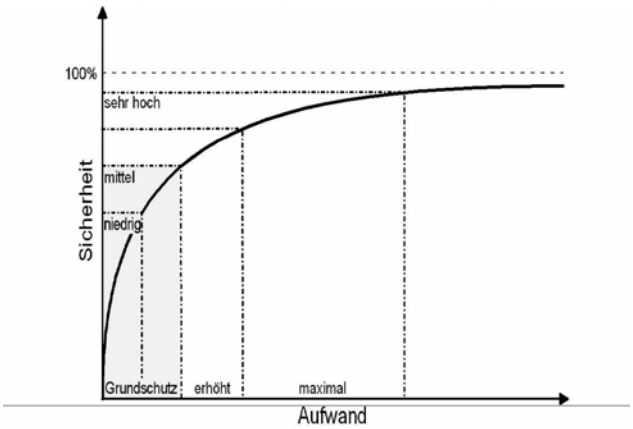
Punkter att utföra:

- fastställa roller för utformning av IT-säkerhetsprocessen
- tilldela rollerna uppgifter och ansvarsområden
- fastställa besättningen av rollerna
- dokumentera IT-säkerhetsorganisationen
- integrera ledningen för IT-säkerhet i organisationsövergripande förlopp och processer.

3.3 Ställa resurser till förfogande för IT-säkerheten

Hot kan orsaka skador och därmed kostnader. Att förebygga risker kräver även resurser – en effektiv riskhantering är ett hjälpmedel för att styra dessa kostnader. En lämplig omfattning av IT-säkerhet kan alltid endast uppnås och upprätthållas med motsvarande insats. Därför ska man när IT-säkerhetsnivån fastställs och konkreta IT-säkerhetskrav formuleras för varje institution tänka på att den eftersträvade IT-säkerhetsnivån även är ekonomiskt meningsfull. Om det visar sig att de ställda säkerhetskraven inte kan finansieras måste säkerhetskraven men även affärsprocesserna och IT-driftens utformning principiellt tänkas igenom.

Erfarenhet visar att förhållandet mellan insatsen, som krävs för att öka IT-säkerhetsnivån, och den därigenom uppnådda säkerhetsvinsten blir allt mer ogynnsamt ju högre den eftersträvade IT-säkerhetsnivån är. Absolut perfekt IT-säkerhet kan inte uppnås. Diagrammet nedan ska förtydliga hur stor insats som måste göras i förhållande till eftersträvad IT-säkerhetsnivå. Denna insats ger en orientering om de personella, tidsmässiga och ekonomiska resurser som är nödvändiga för att uppnå denna IT-säkerhetsnivå.



’Figur: Förhållande insats/nytta för IT-säkerhet

Vid val av de enskilda stegen i IT-säkerhetsprocessen är det ovillkorligen nödvändigt att för varje åtgärd noga se på aspekten kostnad/nytta. Till en avsevärd förbättring av IT-säkerhetsnivån bidrar ofta enkla organisatoriska regler som kan implementeras utan stora insatser eller extra teknisk utrustning. Först när dessa elementära IT-säkerhetsåtgärder har införts är det meningsfullt att investera i tekniska och dyrbara säkerhetsinfrastrukturer.

IT-säkerhet kräver ekonomiska, personella och tidsmässiga resurser som ledningen måste ställa till förfogande i den omfattning som motsvarar de formulerade kraven. Ofta förknippas enbart tekniska lösningar med begreppet IT-säkerhet. Därför är det nödvändigt att påpeka att investeringar i personella resurser och organisatoriska regler ofta är effektivare än investeringar i säkerhetsteknik. Enbart teknik löser inga problem. Den måste alltid vara integrerad i en lämplig organisatorisk ram.

Ställa resurser till förfogande för IT-driften

Grundförutsättning för en säker IT-drift är att denna fungerar friktionsfritt, dvs. den är klokt planerad och organiserad. Därför måste tillräckliga resurser ställas till förfogande för IT-driften. Typiska problem för IT-driften (knappa resurser, överbelastade förvaltare eller en ostrukturerad och dåligt underhållen IT-miljö) måste i regel lösas så att de egentliga IT-säkerhetsåtgärderna kan genomföras verksamt och effektivt.

Utnyttjande av externa resurser

I praktiken saknar de interna IT-säkerhetsexperterna ofta tid för att analysera alla säkerhetsrelevanta påverkansfaktorer och förutsättningar (t.ex. lagstadgade krav eller tekniska frågor). Delvis saknar de även motsvarande underlag. I dessa fall är det förnuftigt att ta hjälp av externa experter. Det måste dokumenteras av de interna IT-säkerhetsexperterna så att ledningsnivån ställer nödvändiga resurser till förfogande.

Att lägga ut delar av IT-driften eller speciella tjänster som exempelvis driften av brandväggen kan öka IT-säkerheten om det innebär att man kan utnyttja specialister som inte finns internt. Komponenten Lägga ut på entreprenad ger rekommendationer vad som härvid ska beaktas med hänsyn till säkerhet.

Resurser för gruppen för IT-säkerhet respektive den IT-säkerhetsansvarige

Enkäter rörande IT-säkerhet visar att den effektivaste IT-säkerhetsåtgärden ofta är att utse en IT-säkerhetsansvarig. När en IT-säkerhetsansvarig har tillsatts minskar antalet IT-säkerhetsincidenter signifikant i de flesta organisationer. För att den IT-säkerhetsansvarige ska kunna fullgöra sina uppgifter måste denne fram för allt beviljas tillräckligt med tid för arbetet. I mindre organisationer är det möjligt att

en medarbetare sköter den IT-säkerhetsansvariges uppgifter parallellt med sin egentliga verksamhet.

Endast få antingen mycket stora organisationer eller sådana med ett stort behov av IT-säkerhet kommer att ha möjligheten att kunna ha personer som på heltid permanent arbetar i en grupp för IT-säkerhet. I allmänhet sköts dessa uppgifter av medarbetarna som en bisyssla till de ordinarie uppgifterna. Ett undantag är däremot när IT-säkerhetsprocessen tas fram första gången. Om möjligt bör medlemmarna i gruppen för IT-säkerhet under detta skede i hög grad befrias från sina övriga uppgifter.

Etableringen av en grupp för IT-säkerhet har fördelen att olika organisationsenheter involveras i säkerhetsprocessen och kompetenser blandas. Därigenom kan IT-säkerhet snabbare införas inom alla organisationsenheter och det uppstår mindre friktionsförluster. Exempelvis skulle följande organisationsenheter kunna delta och koordinera säkerhetsaktiviteterna: IT-säkerhet, revision, IT-administration, IT-ledning, dataskydd, företagsnämnd, fackavdelningar, installationsteknik, juridik.

Hänsyn till lönsamhet vid utarbetande av IT-säkerhetsstrategin

Vid utformningen av IT-säkerhetsstrategin ska lönsamhetsaspekter beaktas från början. Om det visar sig att de nödvändiga IT-säkerhetsåtgärderna inte kan genomföras med de resurser som står till bud måste strategin ändras. När anspråk och de ekonomiska ramarna divergerar för mycket måste affärsprocesser eller sättet hur IT-verksamheten bedrivs principiellt tänkas igenom.

Resurser för kontroll av IT-säkerheten

Kontrollen av effektivitet och lämplighet hos IT-säkerhetsåtgärder måste säkerställas genom tillräckliga resurser. Om möjligt bör det även kontrolleras huruvida de använda resurserna står i ett rimligt förhållande till säkerhetsnyttan. Om det till exempel visar sig att säkringen av bestämda IT-system orsakar mycket höga kostnader ska man fundera över alternativa åtgärder. Det kan exempelvis vara förnuftigt att inte ansluta vissa IT-system till osäkra nät när insatsen för att säkra nät är för hög.

Punkter att utföra:

• i hela IT-säkerhetsprocessen ta hänsyn till lämplighet och lönsamhet

• säkerställa balans mellan organisatorisk och teknisk IT-säkerhet

• begära lämpliga resurser för IT-driften, ledning av IT-säkerheten och kontrollen av IT-säkerheten

• vid behov ta hjälp av externa resurser.

3.4 Involvera alla medarbetare i IT-säkerhetsprocessen

IT-säkerhet berör alla medarbetare utan undantag. Varje enskild medarbetare kan genom ett ansvars- och säkerhetsmedvetet handlande hjälpa till att undvika skador och bidra till framgången. Att öka medvetandet om IT-säkerhet och motsvarande utbildning av medarbetarna är därför en grundförutsättning för IT-säkerhet. IT-säkerheten påverkas i avgörande grad även av arbetsklimat, gemensamma ideal och medarbetarnas engagemang.

För alla medarbetare, interna som externa, måste aspekter som rör informationssäkerhet beaktas från rekryteringen till dess de slutar.

Utbildning och ökat medvetande

Alla medarbetare måste utbildas och få ökat medvetande om betydelsen av säkerhetsåtgärder och deras användning. Därför måste utbildningskoncept tas fram för olika målgrupper (t.ex. administratörer, chefer,

användare, bevakningspersonal). Utbildningarna avseende IT-säkerhet måste därvid integreras i existerande utbildningskoncept.

I princip måste alla medarbetare, som anställs eller som får nya uppgifter, få en grundlig introduktion och utbildning. Vid utformning respektive val av utbildningsaktiviteter bör alla relevanta säkerhetsaspekter integreras. Även erfarna IT-användare bör regelbundet fräscha upp och komplettera sina kunskaper.

Medarbetare måste regelbundet göras medvetna om IT-säkerhetsaspekter för att blir medvetna om riskerna i samband med den dagliga hanteringen av information. För att uppnå en verksam ökning av medvetandet är det exempelvis lämpligt att skapa ett säkerhetsforum på intranätet. Där publiceras tips om IT-säkerhetsåtgärder och aktuella skadefall, medarbetarna erbjuds workshops och föredrag om IT-säkerhet eller så görs facktidskrifter tillgängliga.

Kontaktperson för IT-säkerhetsfrågor och rapporteringsvägar

För att medarbetare ska hålla kontakten med IT-säkerhetsämnena även efter utbildningsåtgärderna är det viktigt att utse kontaktpersoner för IT-säkerhetsfrågor och tillkännage vem som har denna funktion. Endast så kan medarbetare aktivt stödjas och varaktigt tillämpa säkerhetspolicies och -koncept i praktiken. Till det hör även definitionen av rapporteringsvägar och informationsvägar uppåt för IT-säkerhets-incidenter. Varje medarbetare ska veta hur han ska agera vid misstanke om en säkerhetsincident och veta vem som är ansvarig kontaktperson eller det ska vara möjligt att snabbt och i alla lägen att få reda på denna information.

Medarbetarnas delaktighet

Medarbetare ska informeras om meningen med säkerhetsåtgärder. Det är speciellt viktigt när de medför försämrad komfort och funktion. I enskilda fall kan säkerhetsåtgärder vara en fråga för medbestämmande så att personalen ska deltaga.

Om medarbetarna i god tid deltar i planeringen av säkerhetsåtgärder eller utformningen av organisatoriska regler innebär det flera fördelar:

- idéer och kunskap inom den egna institutionen utnyttjas bättre
- den praktiska nyttan av säkerhetsåtgärder eller organisatoriska regler ökas. Detsamma gäller åtgärdernas effektivitet
- viljan att faktiskt följa föreskrifter och åtgärder ökar
- arbetsklimatet påverkas positivt när medarbetarna känner sig delaktiga i ledningens beslut.

När medarbetare byter uppgift eller slutar sin anställning

När medarbetare slutar eller får andra uppgifter eller förlorar behörigheter måste det följas av lämpliga säkerhetsåtgärder (t.ex. att rättigheter upphör, nycklar lämnas tillbaka) samt dokumenteras.

Punkter att utföra:

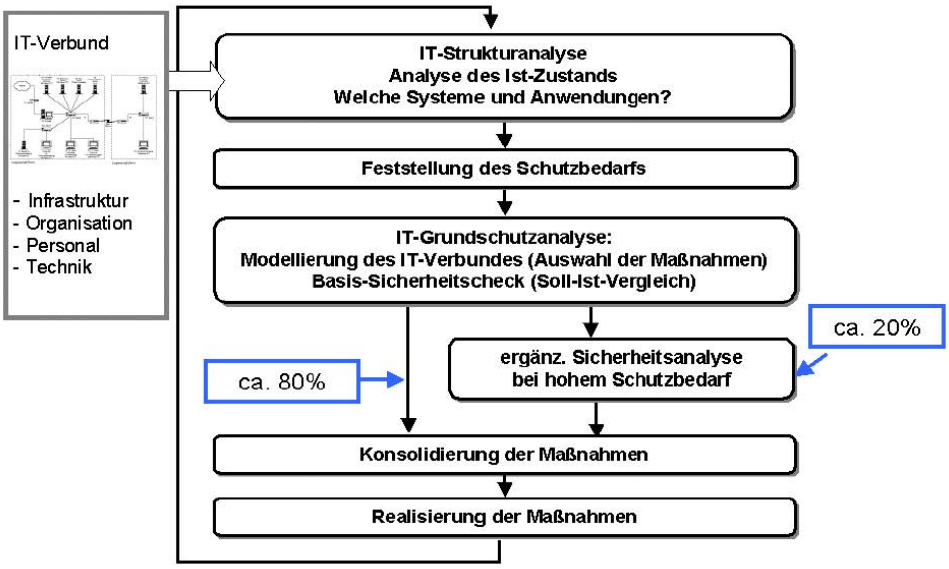
- involvera i god tid medarbetarna och företagsnämnden vid planering och utformning av IT-säkerhetsåtgärder och regler
- regelbundet utbilda och öka medvetandet hos alla medarbetare beträffande de aspekter av IT-säkerheten som berör dem
- informera alla medarbetare om meningen med IT-säkerhetsåtgärderna
- utse kontaktperson för IT-säkerhetsfrågor och tillkänna befogenheter

- fastställa och tillkännage rapporteringsvägar och informationsvägar uppåt för IT-säkerhetsincidenter
- säkerställa att erforderliga säkerhetsåtgärder efterlevs när medarbetare slutar eller byter arbetsuppgift.

4 Utarbetande av ett IT-säkerhetskoncept enligt IT-grundskydd

Ett av IT-grundskydds mål är att erbjuda ett pragmatiskt och effektivt tillvägagångssätt för att uppnå en normal IT-säkerhetssäkerhetsnivå som även kan vara en grund för en högre säkerhetsnivå. När en IT-säkerhetsprocess har startats och IT-säkerhetspolicien och IT-säkerhetsorganisationen har definierats upprättas IT-säkerhetskonceptet för institutionen. För detta ändamål rekommenderas i IT-grundskydd-katalogerna för IT-system organisatoriska, infrastrukturella och tekniska standardsäkerhetsåtgärder. Dessa är strukturerade i komponenter så att de kan sättas samman som moduler.

Komponenterna spelar en central roll i IT-grundskydds metodik. De är enhetligt uppbyggda för att användningen av dem ska vara enkel. Varje komponent börjar med en kort beskrivning av aktuell komponent, tillvägagångssättet respektive IT-systemet. I anslutning där till visas hotbilden. Hoten är där uppdelade i områdena force majeure, organisatoriska brister, mänskliga faktorn, tekniska fel och uppsåtliga handlingar.



Figur: Utarbetande av IT-säkerhetskonceptet i ledningssystemet för informationssäkerhet

IT-grundskydds metodik

Vid den traditionella riskanalysen bestäms först hoten och bedöms med sannolikheter för inträffande och därefter väljs lämpliga IT-säkerhetsåtgärder ut för att kunna bedöma den kvarvarande restrisken. Denna uppgift har i IT-grundskydd redan utförts för varje komponent och de för en typisk kontorsmiljö passande IT-säkerhetsåtgärderna har valts ut. Vid användning av IT-grundskydd reduceras denna uppgift till en bör-är-jämförelse mellan de i IT-grundskydd-katalogerna rekommenderade och de redan genomförda åtgärderna. I samband med detta konstaterade, saknade eller endast otillräckligt genomförda åtgärder visar säkerhetsbristerna som det gäller att åtgärda genom de rekommenderade åtgärderna. Endast vid ett signifikant större skyddsbehov måste dessutom en kompletterande säkerhetsanalys genomföras med beaktande av kostnads- och nyttoaspekter. Härvid räcker det däremot i regel att komplettera de rekommenderade åtgärderna enligt IT-grundskydd-katalogerna med motsvarande individuella, kvalitativt mer högvärdiga åtgärder. Ett enkelt tillvägagångssätt härför finns beskrivet i BSI-dokumentet ”Riskanalys baserat på IT-grundskydd ”.

De i IT-grundskydd-katalogerna upptagna åtgärderna utgörs av standardsäkerhetsåtgärder alltså de åtgärder vilka ska användas för aktuella komponenter enligt senaste rön för att uppnå en lämplig bassäkerhet. I samband med detta utgör åtgärderna som krävs för IT-grundskydd-certifieringen minimum för vad som i varje fall är förnuftigt att genomföra vad gäller förebyggande säkerhetsåtgärder. De som ”extra” markerade åtgärderna har i praktiken likaså visat sig vara beprövade. De riktar sig däremot till tillämpningsfall med förhöjda säkerhetskrav.

Säkerhetskoncept, som tas fram med hjälp av IT-grundskydd, är kompakta eftersom man inom konceptet endast behöver referera till motsvarande åtgärder i IT-grundskydd-katalogerna. Detta förbättrar möjligheterna att begripa och översiktligheten. För att utforma rekommendationerna av åtgärder så att de är lättare att genomföra så beskrivs säkerhetsåtgärderna detaljerat i katalogerna. Vid användning av fackterminologi tas hänsyn till att beskrivningarna ska kunna förstås av de personer som ska genomföra åtgärderna.

För att förenkla genomförandet av åtgärderna finns IT-grundskydd-katalogernas texter även i elektronisk form. Därutöver underlättas genomförandet av åtgärderna även genom hjälpmedel och mönsterlösningar som ställs till förfogande av BSI och delvis även av användare av IT-grundskydd.

Tillvägagångssättet enligt IT-grundskydd är grovt indelat i följande områden:

Definition av IT-nätverket

Att genomföra IT-grundskydd i ett stort steg är ofta ett alltför ambitiöst mål. Många små steg och en långfristig, kontinuerlig förbättringsprocess utan stora investeringar i början kan ofta vara mer framgångsrikt. Det kan på så sätt vara bättre att först införa den erforderliga säkerhetsnivån endast inom utvalda områden. Utifrån dessa embryon bör därefter säkerheten kontinuerligt förbättras i den totala organisationen.

Först måste därför IT-nätverket fastställas för vilket IT-säkerhetskonceptet ska gälla. Med ett IT-nätverk avses helheten av infrastrukturella, organisatoriska, personella och tekniska komponenter som finns för att lösa uppgiften inom ett bestämt tillämpningsområde av informationsbearbetningen. Ett IT-nätverk kan därvid omfatta en institutions hela IT eller även enskilda områden som är indelade genom organisatoriska strukturer (t.ex. avdelningsnät) eller gemensamma affärsprocesser respektive IT-tillämpningar (t.ex. personalinformationssystem).

IT-strukturanalys

För att ta fram ett IT-säkerhetskoncept och speciellt för användningen av IT-grundskydd-katalogerna är det nödvändigt att analysera och dokumentera den föreliggande informationsteknikens struktur. På grund av den i dag mycket vanliga sammankopplingen av IT-system kan en nättopologiplan användas när en analys påbörjas. Det är viktigt att beakta följande aspekter:

• den befintliga infrastrukturen

• de organisatoriska och personella förutsättningarna för IT-nätverket

• de sammankopplade och inte sammankopplade IT-system som används i IT-nätverket

• kommunikationsförbindelserna mellan IT-systemen och mot omvärlden

• i IT-nätverket använda IT-tillämpningar.

IT-strukturanalysen enskilda steg beskrivs, i form av en anvisning, detaljerat i kapitel 4.1 i detta dokument.

Fastställande av skyddsbehov

Syftet med att fastställa skyddsbehovet är att ta reda på vilket skydd som är tillräckligt och lämpligt för affärsprocesserna, den därvid bearbetade informationen och den använda informationstekniken. För detta ändamål betraktas för varje tillämpning och den bearbetade informationen de förväntade skadorna som kan uppstå vid en negativ påverkan av konfidentialitet, riktighet eller tillgänglighet. Det är där även viktigt att realistiskt bedöma de möjliga följdskadorna. En indelning i de tre skyddsbehovskategorierna ”normalt”, ”stort” och ”mycket stort” har visat sig fungera väl.

De enskilda stegen för att fastställa skyddsbehovet förklaras i detalj i kapitel 4.2 i detta dokument.

IT-säkerhetskoncept

Informationstekniken inom myndigheter och företag präglas i dag vanligen av IT-system som i hög grad är sammankopplade. I regel är det därför lämpligt att inom ramen för en IT-säkerhetsanalys respektive ett IT-säkerhetskoncept att se på ett större IT-nätverk och inte se på enskilda IT-system. Förutsättning för att använda IT-grundskydd-kataloger på ett IT-nätverk är detaljerade uppgifter om dess struktur. Dessa kan exempelvis erhållas via den ovan beskrivna IT-strukturanlysen. Därefter måste IT-grundskyddets komponenter i ett modelleringssteg avbildas på det aktuella IT-nätverkets komponenter.

I kapitel 4.3 i detta dokument beskrivs hur modelleringen av ett IT-nätverk bör utföras genom att IT-grundskydd-komponenter används. Hur den efterföljande bör-är-jämförelsen bör utföras med ledning av en grundläggande säkerhetskontroll beskrivs i kapitel 4.4.

Grundläggande säkerhetskontroll

Den grundläggande säkerhetskontrollen är ett instrument som erbjuder en snabb överblick över den befintliga IT-säkerhetsnivån. Med hjälp av intervjuer bestäms statusen hos ett befintligt (enligt IT-grundskydd modellerat) IT-nätverk vad beträffar genomförandegraden av IT-grundskydds säkerhets-åtgärder. Som resultat finns en katalog i vilken genomförandestatusen ”umbärlig”, ”ja”, ”delvis” eller ”nej” är registrerad för varje relevant åtgärd. Genom identifieringen av ännu inte eller endast delvis genomförda åtgärder visas förbättringsmöjligheter för den betraktade informationsteknikens säkerhet. Kapitel 4.4 beskriver en handlingsplan för genomförande av en grundläggande säkerhetskontroll. I samband med detta tas hänsyn till såväl de organisatoriska aspekterna som till de krav som ställs vid projektgenomförandet.

IT-säkerhetsrevision

De säkerhetsåtgärder som ingår i IT-grundskydd kan även användas för IT-säkerhetsrevisionen. Här rekommenderas samma tillvägagångssätt som vid den grundläggande säkerhetskontrollen. För varje komponent är det arbetsbesparande och till hjälp att med ledning av åtgärdstexterna ta fram en checklista som är speciellt anpassad till den egna institutionen. Detta underlättar revisionen och förbättrar ofta resultatens repeterbarhet.

Mer omfattande IT-säkerhetsåtgärder

Standardsäkerhetsåtgärderna enligt IT-grundskydd ger i normalfallet ett lämpligt och tillräckligt skydd. Vid ett stort eller ett mycket stort skyddsbehov kan det dock vara förnuftigt att kontrollera om det behövs extra eller som ersättning bättre IT-säkerhetsåtgärder. Lämpliga åtgärder för områden med större skyddsbehov bör väljas via kompletterande säkerhetsanalyser.

En metod som kan användas är tillvägagångssätt som finns beskrivet i BSI-dokumentet ”Riskanalys baserat på IT-grundskydd”. I kapitel 4.5 visas denna metod översiktligt. Att en kompletterande säkerhetsanalys genomförs framgångsrikt beror i hög grad av projektgruppens fackkunskaper. Därför är det ofta förnuftigt att anlita extern personal med ämneskunskaper.

Genomförande av IT-säkerhetskoncept

En tillräcklig IT-säkerhetsnivå kan endast uppnås när: befintliga svaga punkter hittas i en säkerhetsanalys, det oförändrade tillståndet anges i ett säkerhetskoncept, erforderliga åtgärder identifieras och när speciellt dessa åtgärder konsekvent genomförs. I kapitel 4.6 beskrivs vad som måste beaktas vid genomförandeplaneringen av IT-säkerhetsåtgärder.

Certifiering enligt IT-grundskydd

Tillvägagångssättet enligt IT-grundskydd och IT-grundskydd-katalogerna används inte endast för IT-säkerhetskonceptet utan i allt högre grad som referens för en säkerhetsstandard. Genom en IT-grundskydd-certifiering respektive –kvalificering kan en institution internt och utåt dokumentera att den i erforderlig omfattning har genomfört IT-grundskydd.

4.1 IT-strukturanalys

I IT-grundskydd-katalogerna rekommenderas standardiserade IT-säkerhetsåtgärder för typiska kontorsmiljöer. Eftersom varje kontorsmiljö emellertid har sina speciella förhållanden måste IT-säkerhetsåtgärderna anpassas till dessa. De måste anpassas till de affärsprocesser som ska skyddas, till den informations som bearbetas i dessa processer samt till de IT-system och IT-tillämpningar som används. Det är därför nödvändigt att ha en översikt tillgänglig över de använda IT-tillämpningarna och IT-systemen.

4.1.1 Inventering av IT-nätverket

I praktiken bestäms ur analysen av affärsprocesserna i regel först den informationen och de IT-tillämpningar som är affärskritiska och därefter de berörda IT-systemen. Beroende på situation kan det även vara klokt att först bestämma IT-systemen och därefter betrakta de IT-tillämpningar som används i dessa.

Även om tillvägagångssättet enligt ovan har använts är det mycket bra att betrakta den omvända ordningsföljden: Å ena sidan medför det en kontroll huruvida alla IT-system verkligen har tagits med. Ofta går det att finna IT-system, som tidigare inte har tilldelats någon IT-tillämpning, eftersom deras betydelse kanske inte var känd för de tillfrågade informationsägarna. Å andra sidan kontrolleras verkligen vilka IT-tillämpningar som faktiskt är installerade i IT-systemen. I samband med detta visar det sig om säkerhetskritiska tillämpningar har missats.
IT-strukturanalysen tjänar till att lyfta fram information som behövs för det fortsatta tillvägagångssättet för att ta fram ett IT-säkerhetskoncept enligt IT-grundskydd. Analysen är uppdelad i följande deluppgifter:

- nätplansundersökning
- undersökning av IT-systemen
- inventering av IT-tillämpningarna och den tillhörande informationen
- inventering av IT-lokalerna
- komplexitetsminskning genom gruppbildning.

Dessa deluppgifter beskrivs nedan och förklaras genom ett exempel. En utförlig version av exemplet finns i hjälpmedlen till IT-grundskydd.

4.1.2 Nätplansundersökning

Utvärdering av en nätplan

En lämplig utgångspunkt för IT-strukturanalysen utgör en nätplan (exempelvis i form av en

nättopologiplan). En nätplan är en grafisk översikt över de komponenter som används inom det betraktade området samt hur dessa är sammankopplade. I detalj bör planen visa följande objekt:

- IT-system, dvs. klienter och servrar, aktiva nätkomponenter (som hubbar, växlar, routrar, WLAN anslutningspunkter), nätskrivare, etc.
- nätförbindelser mellan dessa system, dvs. LAN-förbindelser (som Ethernet, Token Ring), WLAN, Backbone-tekniker (som FDDI, ATM), etc.
- det betraktade områdets anslutningar till omvärlden, dvs. kommunikationsvägar via ISDN eller modem, Internetanslutningar via analoga tekniker eller routrar, radioförbindelser eller hyrda ledningar till avlägsna byggnader etc.

Till varje visat objekt hör vidare en minimimängd information som kan hämtas ur en tillordnad katalog. För varje IT-system bör minst följande finnas noterat:

- en entydig beteckning (exempelvis det fullständiga värddatornamnet eller ett identifikationsnummer)
- typ och funktion (exempelvis databasserver för tillämpning X)
- använd plattform (dvs. hårdvaruplattform och operativsystem)
- placering (exempelvis byggnads- och rumsnummer)
- den ansvarige administratören
- de befintliga kommunikationsgränssnitten (t.ex. Internetanslutning, Bluetooth, WLAN-adapter) samt
- typ av nätanslutning och nätadressen.

Inte enbart för IT-systemen själva utan även för nätförbindelserna mellan systemen och förbindelserna externt krävs bestämd information nämligen:

- kabeltyp respektive kommunikationsanslutning (t.ex. optokabel eller WLAN baserat på IEEE 802.11)
- den maximala dataöverföringshastigheten (t. ex. 10 Mbit/s)
- de för de undre skikten använda nätprotokollen (t.ex. Ethernet, TCP/IP)
- vid externa anslutningar: detaljer om det externa nätet (t.ex. Internet, Internetleverantör).

Det rekommenderas att områden med olika skyddsbehov markeras.

Nätplanen måste inte nödvändigtvis finnas på papper. Om informationstekniken inom företaget respektive myndigheten har överskridit en viss omfattning finns möjligheten att använda hjälpprogram för att upprätta och underhålla nätplanen eftersom dokumentationen kan vara mycket komplex och ständigt förändras.

Uppdatering av nätplanen

Institutionens nätplan är inte alltid uppdaterad eftersom IT-strukturen i regel ständigt anpassas till institutionens krav och underhållet av nätplanen binder resurser. I praktiken är det endast större förändringar av IT-strukturen som föranleder att planen uppdateras.

Med hänsyn till användningen av nätplanen för IT-strukturanalysen utgör alltså nästa steg att jämföra den föreliggande nätplanen (respektive delplanerna om den totala planen har delats upp för att ge en bättre överblick) med den faktiska IT-strukturen och vid behov att uppdatera planen. I detta ärende ska de IT-ansvariga och administratörerna av de enskilda tillämpningarna och näten konsulteras. Om program för en centraliserad nät- och systemstyrning används bör man i vart fall kontrollera huruvida dessa program kan vara till hjälp när en nätplan tas fram. Man ska tänka på att funktioner för automatisk eller halvautomatisk

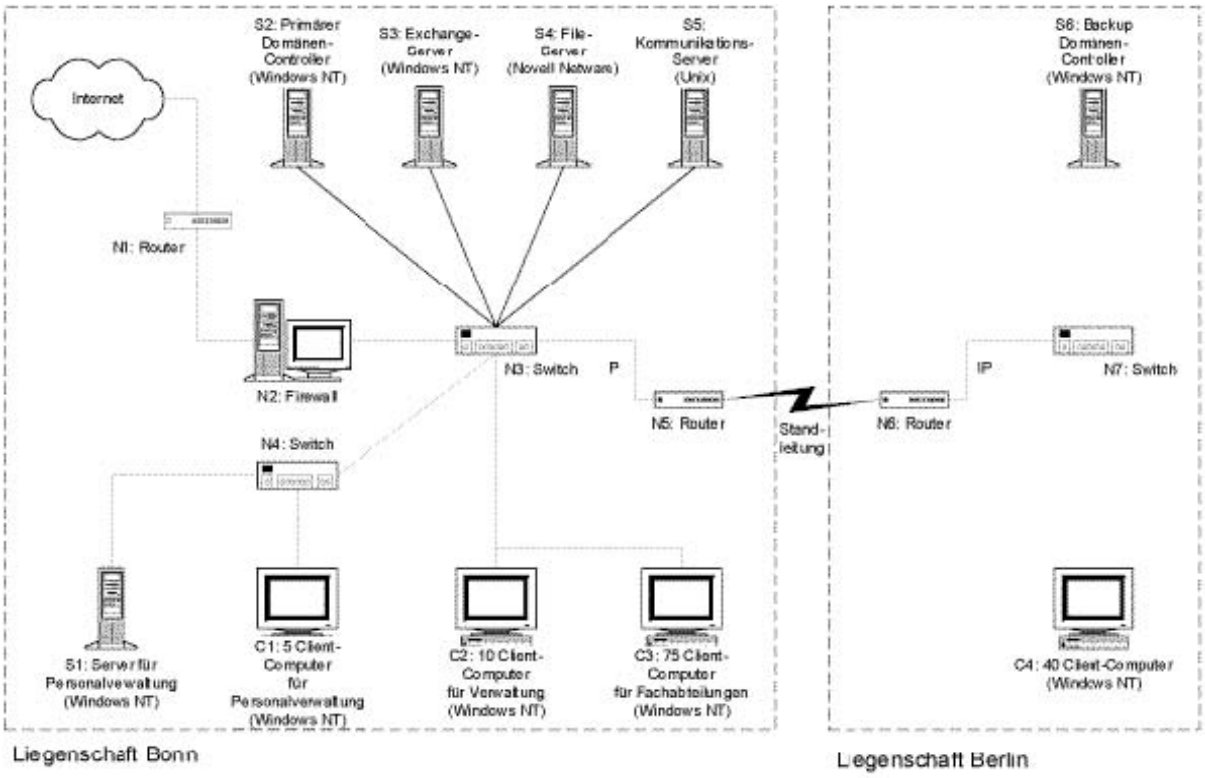
inventering av komponenter temporärt ger upphov till extra nättrafik. Det måste klarläggas att denna nättrafik inte negativt påverkar IT-driften.

Exempel: Organisations- och förvaltningsverket (OFV) - del 1

Nedan visas utifrån en fiktiv myndighet, OFV, förebildligt hur en uppdaterad nätplan kan se ut. Observera att OFV:s IT-struktur inte på något sätt är optimal med hänsyn till IT-säkerhet. Den används enbart för att illustrera tillvägagångssättet tid användning av IT-grundskydd. Här ges endast en överblick, det kompletta exemplet finns i hjälpmedlen till IT-grundskydd.

OFV är en fiktiv myndighet med 150 medarbetare av vilka 130 arbetar vid bildskärmsarbetsplatser. Myndigheten är uppdelad på ett huvudkontor i Bonn och en filial i Berlin där bland annat deluppgifterna policy, normering och koordinering hanteras. Av de 130 bildskärmsarbetsplatserna finns 90 på huvudkontoret och de övriga på filialen.

För att myndigheten ska kunna sköta sitt uppdrag är alla arbetsplatser sammankopplade i ett nät. Filialen är ansluten via en hyrd fast linje. Alla riktlinjer och föreskrifter samt formulär och standardtexter kan alltid tas fram av alla medarbetare. Alla relevanta arbetsresultat sparas i en central databank. Handlingar produceras, vidarebefordras och undertecknas uteslutande elektroniskt. För genomförande och support av alla funktioner har en IT-avdelning skapats vid huvudkontoret.



Figur: Exempel på en schematisk nätplan

I den visade nätplanen är IT-systemen markerade med ett nummer (servrar, klienter och aktiva nätkomponenter i formen S*n*, C*n* respektive N*n*), samt funktionerna och vid behov operativsystemet (inom parantes).

På båda platserna har klienterna placerats i lämpliga grupper. Förvisso är alla 130 klienter nästan identiskt konfigurerade men de skiljer sig åt med hänsyn till vad de används för, integreringen i nätet och de

infrastrukturella förutsättningarna. Grupp C1 representerar de fem klienterna på personalavdelningen. Dessa är kopplade till personalavdelningens server S1 på huvudkontoret. C2 och C3 omfattar de tio klienterna på administrationsavdelningen respektive 75 klienterna på fackavdelningarna på huvudkontoret. De skiljer sig åt uteslutande med hänsyn till de använda tillämpningsprogrammen. Grupp C4 slutligen utgörs av klienterna på filialen. Den gruppen skiljer sig från C1 till C3 genom den omgivande infrastrukturen och den avvikande kopplingen till det totala nätet.

Punkter att utföra:

- gå igenom befintliga grafiska presentationer av nätet exempelvis nättopologiplaner
- vid behov uppdatera nätplaner eller upprätta nya
- gå igenom befintlig tilläggsinformation om de ingående IT-systemen och uppdatera och komplettera vid behov
- gå igenom befintlig tilläggsinformation om de ingående kommunikationsförbindelserna och uppdatera och komplettera vid behov.

4.1.3 Inventering av IT-systemen

Med hänsyn till att skyddsbehovet senare ska fastställas och att en modellering av IT-nätverket ska utföras bör en tabell över de befintliga och planerade IT-systemen upprättas. Begrepper IT-system omfattar därvid inte endast datorer som sådana utan även aktiva nätkomponenter, nätskrivare, telekommunikationssystem etc. Det tekniska genomförandet av ett IT-system står i förgrunden, exempelvis arbetsplats-pc, Windows NT-server, klienter under Windows XP, Unix-servrar, telekommunikationssystem. Här bör endast systemet som sådant registreras (t.ex. Unix-server), inte de enskilda beståndsdelarna av vilka IT-systemet sätts samman (alltså dator, tangentbord, bildskärm, etc.).

Den fullständiga och korrekta inventeringen av de befintliga och planerade IT-systemen är inte bara avsedd för att ta fram ett IT-säkerhetskoncept. Den är även nödvändig för kontroll, underhåll, felsökning och reparation av IT-system.

Såväl de IT-system som är inkopplade i ett nät som de som inte är det ska inventeras. Det gäller alltså speciellt sådana som inte finns registrerade i tidigare upprättade nätplaner. IT-system som har lagts i en grupp när nätplanen har reviderats kan fortsatt behandlas som ett objekt. För de IT-system som inte finns med i nätplanen ska en kontroll göras om de kan sammanfattas på ett förnuftigt sätt. Detta är exempelvis möjligt om det finns ett större antal arbetsplats-pc som uppfyller de villkor för en gruppering som anges i kapitlet ”komplexitetsminskning genom gruppbildning”.

Vid denna inventering bör följande information som är till nytta för det följande arbetet noteras:

- en entydig beteckning av IT-systemet
- beskrivning (typ och funktion)
- plattform (t.ex. hårdvaruarkitektur/operativsystem)
- vid grupper: antalet sammanfattade IT-system
- IT-systemets placering
- IT-systemets status (i drift, testfas, under planering) och
- IT-systemets användare/administratör.

Exempel: Organisations- och förvaltningsverket (OFV) - del 2

Som exempel finns i följande tabell ett utdrag ur listan över IT-system hos OFV. Den fullständiga listan finns som bilaga till hjälpmedlen på cd-rom.

Nr	Beskrivning	Plattform	Antal	Placering	Status	Användare/Admin.
S1	Server för personalavdelning	Windows NT-server	1	Bonn, R 1.01	i drift	Personalavdelning
S2	Primär domänkontroller	Windows NT-server	1	Bonn, R 3.10	i drift	Alla IT-användare
C1	Grupp best. av klienter på personalavd.	Windows NT-workstation	5	Bonn, R 1.02 - R 1.06	i drift	Personalavdelning
C2	Grupp best. av klienter på admin.avd	Windows NT-workstation	10	Bonn, R 1.07 - R 1.16	i drift	Administrations-avdelning
C6	Grupp med de bärbara datorerna på filialen i Berlin	Laptop under Windows 95	2	Berlin, R 2.01	i drift	Alla IT-användare på filialen i Berlin
N1	Router för åtkomst av Internet	Router	1	Bonn, R 3.09	i drift	alla IT-användare
N2	Brandvägg	Application Gateway på Unix	1	Bonn, R 3.09	i drift	alla IT-användare
N3	Växel	Växel	1	Bonn, R 3.09	i drift	alla IT-användare
T1	Telekommunikations-system för Bonn	ISDN-system	1	Bonn, B.02	i drift	alla medarbetare på huvudkontoret i Bonn

IT-systemen respektive grupperna S1, S2, C1, C2, N1, N2 och N3 har hämtats direkt från nätplanen. Utöver nätplanen har de icke nätanslutna bärbara datorerna C6 (Laptop) och T1 lagts till (telekommunikationssystem).

Punkter att utföra:

- kontrollera huruvida existerande databanker eller översikter över de befintliga eller planerade IT-systemen är lämpliga för det vidare tillvägagångssättet
- göra lista över IT-systemen som finns i nätet respektive inte finns i nätet respektive uppdatera och komplettera
- märka IT-system respektive IT-systemgrupper med entydiga nummer eller förkortningar.

4.1.4 Inventering av IT-tillämpningarna och den tillhörande informationen

För att minska arbetsinsatsen inventeras de viktigaste IT-tillämpningarna som är i drift eller planeras på de betraktade IT-systemen. För att effektivt genomföra denna uppgift kan man låta bli att fullständigt inventera alla tillämpningar om det är säkert att för respektive IT-system anges de IT-tillämpningar:

- vars data respektive information och program har högsta behov av att hållas hemliga (konfidentialitet)
- vars data respektive information och program har högsta behov av att vara korrekta och oförändrade

(riktighet)

• som har de kortast tolererbara avbrottstiderna (största behov av tillgänglighet).

För att garantera detta, bör användarna respektive de som ansvarar för IT-tillämpningen vid inventering tillfrågas beträffande deras bedömning.

Det är enklare att definiera och inventera IT-tillämpningarna om dessa grupperas orienteras efter IT-systemen. Man bör börja med servrarna på grund av deras stora betydelse. För att bilden ska bli så balanserad som möjligt kan inventeringen därefter kompletteras med klienterna och system på enskilda arbetsplatser. Till slut bör det fastställas vilka anordningar för koppling i nätet som stöder vilka IT-tillämpningar.

Lämpligen bör tillämpningarna för referensändamål numreras. Eftersom många IT-säkerhetsansvariga samtidigt ansvarar för skydd av personrelaterade data är det lämpligt att här redan notera huruvida de beskrivna IT-tillämpningarna sparar och/eller bearbetar personrelaterade data. Eftersom en tillämpnings skyddsbehov i regel beror på skyddsbehovet för den informations som den bearbetar så bör den informationens typ även dokumenteras i tabellen.

Därefter tillordnas tillämpningarna de IT-system som behövs för att de ska utföras. Det kan vara IT-systemen på vilka IT-tillämpningarna bearbetas eller även de system som överför denna tillämpnings data.

Resultatet är en översikt, vilka viktiga IT-tillämpningar som bearbetas på vilka IT-system eller som används eller överförs av vilka IT-system.

En rekommendation är att för IT-tillämpningarna notera vilka affärsprocesser de stöder och vilken information som bearbetas. Varje affärsprocess har en ägare respektive ansvarig, Tillhörande IT-tillämpningar har användare. Denna information ska likaledes inventeras för att kontaktpersoner för IT-säkerhetsfrågor lättare ska kunna identifieras respektive för att snabbt kunna nå berörda användargrupper.

Resultatet kan lämpligen visas i en tabell.

Exempel: Organisations- och förvaltningsverket (OFV) - del 3

Nedan visas för det fiktiva exemplet OFV ett utdrag ur inventeringen av IT-tillämpningarna och tillordningen till de berörda IT-systemen:

Beskrivning av IT-tillämpningarna			IT-system						
Till.nr	IT-tillämpning/information	Personrel. data	S1	S2	S3	S4	S5	S6	S7
A1	Bearbetning av personaldata	X	X						
A2	Bidragshantering	X	X						
A3	Reskostnadsredovisning	X	X						
A4	Användarautenticering	X		X				X	
A5	Systemstyrning			X					
A6	Exchange (e-post, kalender)	X			X				
A7	Central dokumentförvaltning					X			

Förklaring: A_i X S_j = Exekveringen av IT-tillämpningen A_i beror på IT-systemet S_j .

Inventering av beroenden mellan IT-tillämpningar

För att få en bättre översikt kan man valfritt visa hur IT-tillämpningarna beror av varandra (t.ex. hur en IT-tillämpning är beroende av en bestämd databas).

Punkter att utföra:

- om inte alla IT-tillämpningar inventeras, fråga tillämpningsansvariga beträffande deras bedömning av vilka IT-tillämpningar per IT-system som har det största skyddsbehovet
- upprätta översikt över IT-tillämpningarna och märk med entydiga nummer eller förkortningar
- tillordna IT-tillämpningarna till IT-systemen (servrar, klienter, anordningar för koppling i nätet etc.) som behövs för att de ska exekveras
- notera för varje IT-tillämpningarna motsvarande affärsprocesser, bearbetad information, ägare och vid behov användare
- notera för varje IT-tillämpning i vilken utsträckning personrelaterade data bearbetas med den.

4.1.5 Inventering av lokalerna

Affärsprocesserna och tillämpningarna hanteras inte endast på definierade IT-system utan även i institutionens lokaler. Institutionen kan vara lokaliserad i en egen byggnad eller enbart på ett våningsplan beroende på institutionens storlek och många andra faktorer. Många institutioner utnyttjat lokaler som ligger i olika byggnader eller delar lokaler med andra institutioner. I ett säkerhetskoncept måste alla fastigheter, i vilka de studerade affärsprocesserna och tillämpningarna hanteras, beaktas. Här ingår fabriksområde, byggnader, våningsplan, rum samt vägen mellan dessa. Alla kommunikationsförbindelser som går över område som är tillgängligt för utomstående måste behandlas som externa förbindelser.

För det fortsatta tillvägagångssättet med modelleringen enligt IT-grundskydd och för planeringen av bör-är-jämförelsen är det till hjälp att göra en översikt över fastigheterna, fram för allt rummen, i vilka IT-system placeras eller vilka som används för IT-driften. Hit hör rum, som enbart är avsedda för IT-driften (som serverrum, arkiv för datamedium), samt sådana rum i vilka bland annat IT-system används (som kontorsrum) men även de sträckor över vilka kommunikationsförbindelserna löper. När IT-system finns i ett skyddsskåp, istället för i ett teknikrum ska skyddsskåpet registreras som ett rum.

Tips: Vid inventeringen av IT-systemen har deras placering redan tagits med.

Därutöver måste man undersöka om information som behöver skyddas förvaras i fler rum. Dessa rum måste då också inventeras. Den bearbetade informationens typ måste kunna härledas ur denna dokumentation.

Följande tabell visar hur en översikt över rummen skulle kunna se ut. Här finns redan kolumner för skyddsbehov men dessa fylls i först i ett senare skede.

Rum			IT/information	Skyddsbehov		
Be-teckning	Typ	Placering	IT-system/datamedium	Konfiden-tialitet	Riktig-het	Tillgäng-lighet
R U.02	Arkiv datamedium	Byggnad Bonn	Backup-datamedium (Säkerhetskopiering en gång per vecka server S1 till S5)			
R B.02	Teknikrum	Byggnad Bonn	Telekommunikationssystem			
R 1.01	Serverrum	Byggnad Bonn	S1, N4			
R 1.02 - R 1.06	Kontorsrum	Byggnad Bonn	C1			
R 3.11	Skyddsskåp i rum R 3.11	Byggnad Bonn	Backup-datamedium (Säkerhetskopiering en gång per dag server S1 till S5)			
R E.03	Serverrum	Byggnad Berlin	S6, N6, N7			
R 2.01 - R 2.40	Kontorsrum	Byggnad Berlin	C4, några med faxar			

Punkter att utföra:

- upprätta lista över alla fastigheter, byggnader och rum som har noterats vid inventeringen av IT-systemen
- lägga till ytterligare rum i vilka information med skyddsbehov förvaras eller på annat sätt bearbetas.

4.1.6 Komplexitetsminskning genom gruppbildning

Nästa steg består i att rensa nätplanen på information som inte behövs för de följande uppgifterna för att därigenom få planen mer översiktlig. Likartade komponenter bör sammanfattas i en grupp som i nätplanen visas som ett objekt.

Om det endast finns få grundkonfigurationer har en konsekvent gruppbildning dessutom fördelen att administrationen förenklas avsevärt. Genom en så hög grad av standardisering som möjligt i en IT-miljö minskas dessutom antalet potentiella säkerhetsluckor och säkerhetsåtgärderna för detta område kan utan urskiljning av de mest skilda svaga punkter realiseras. Det är inte bara till nytta för IT-säkerheten utan sänker även kostnaderna.

Komponenter kan tillordnas en grupp om komponenterna alla:

- är av samma typ
- är konfigurerade på samma eller nästan samma sätt
- är anslutna i nätet på samma eller nästan samma sätt (t.ex. till samma växel)

• är underkastade samma administrativa och infrastrukturella förutsättningar

• betjänar samma tillämpningar

• uppvisar samma skyddsbehov.

På grund av de nämnda förutsättningarna för gruppbildningen kan man beträffande IT-säkerhet utgå från att ett stickprov ur en grupp representerar gruppens IT-säkerhetsnivå.

Det viktigaste exemplet på gruppering av komponenter i nätplanen är säkert sammanfattning av klienter. Inom en institution finns det i regel ett stort antal klienter som enligt ovanstående schema kan delas upp i överskådligt antal grupper. I stora IT-nätverk där många servrar, på grund av redundans och genomströmning, har samma uppgift kan servrar även sammanfattas till grupper.

När en väl utförd gruppering är klar visas de sammanfattade komponenterna i nätplanen som ett objekt. I samband med detta ska man notera antalet komponenter som representeras genom gruppen. Vilken typ av komponenter det är ska också anges.

Punkter att utföra:

• sammanfatta likartade komponenter till grupper

• upprätta rensad nätplan i vilken varje grupp visas som ett objekt

• notera typ och antal för de sammanfattade komponenterna.

4.2 Bestämma skyddsbehov

När skyddsbehovet för den inventerade IT-strukturen bestäms sker det i fyra steg. Efter definitionen av skyddsbehovskategorierna bestäms utifrån typiska skadescenarior först skyddsbehovet för affärsprocesserna och de IT-tillämpningar som stöder dessa. Därefter bestäms skyddsbehovet för de enskilda IT-systemen med ledning av föregående steg. Med hjälp av dessa resultat bestäms slutligen skyddsbehovet för överföringssträckorna och rummen som används för IT-verksamheten.

4.2.1 Bestämma skyddsbehov för IT-tillämpningar

Mål när skyddsbehov bestäms är att utifrån affärsprocesserna att för varje registrerad IT-tillämpning inklusive dess data besluta vilket skyddsbehov den har beträffande konfidentialitet, riktighet och tillgänglighet. Detta skyddsbehov är relaterat till de möjliga skador som är kopplade till en negativ inverkan på den berörda IT-tillämpningen och därmed aktuell affärsprocess.

Eftersom skyddsbehovet oftast inte kan kvantifieras innehåller IT-grundskydd i fortsättningen endast en kvalitativ bedömning i vilken skyddsbehov delas in i tre kategorier:

Kategorier för skyddsbehov	
”normalt”	Följderna av skador är begränsade och kan överblickas.
”stort”	Följderna av skador kan vara betydande.
”mycket stort”	Följderna av skador kan uppnå en katastrofal omfattning som kan hota verksamhetens existens.

Följande steg förklarar hur adekvat kategori för skyddsbehov kan bestämmas för affärsprocesser och bakomliggande IT-tillämpningar.

Steg 1: Definition av kategorierna för skyddsbehov

Skadorna som kan uppstå för en affärsprocess respektive en IT-tillämpning inklusive dess data i samband med förlusten av konfidentialitet, riktighet och tillgänglighet kan tillordnas följande skadescenarior:

• brott mot lagar, föreskrifter eller avtal

• negativ påverkan av rätten till egna uppgifter

• påverkan av den personliga integriteten

• negativ inverkan på utförande av uppgiften

• negativ intern eller extern inverkan och

• ekonomiska följder.

Ofta tillhör en skada flera skadekategorier. Så kan exempelvis bortfallet av en IT-tillämpning negativ påverka hur en uppgift löses vilket medför direkta ekonomiska förluster samtidigt som det ger en imageförlust.

För att kunna avgränsa kategorierna för skyddsbehov ”normalt”, ”stort” och ”mycket stort” från varandra är det lämpligt att bestämma gränserna för de enskilda skadescenarierna. Följande tabell ger en orientering om vilket skyddsbehov som en potentiell skada och dess följer ger upphov till. Tabellerna ska av respektive institution anpassas till dess egna förhållanden.

Kategori för skyddsbehov ”normalt”	
1. • Brott mot lagar, föreskrifter eller avtal	- Brott mot lagar och föreskrifter med små konsekvenser - Ringa avtalsbrott med maximalt små avtalsviten
2. Negativ påverkan av rätten till egna uppgifter	- En negativ påverkan av rätten till egna uppgifter skulle av den enskilde bedömas som tolerabel. - Ett möjligt missbruk av personrelaterade data har endast liten inverkan på den berördes offentliga ställning eller ekonomiska förhållanden.
3. Påverkan av den personliga integriteten	- En påverkan förefaller inte möjlig.
4. Negativ inverkan på utförande av uppgiften	- Den negativa påverkan torde av den berörde bedömas som acceptabel. - Den maximala bortfallstid som kan accepteras är längre än 24 timmar.
5. Negativ intern eller extern inverkan	- En ringa respektive endast intern påverkan av anseende och förtroende kan förväntas.
6. Ekonomiska följder	- Den ekonomiska skadan kan accepteras av institutionen.

Kategori för skyddsbehov ”stort”	
1. • Brott mot lagar, föreskrifter eller avtal	- Brott mot lagar och föreskrifter med avsevärda konsekvenser - Avtalsbrott med stora avtalsviten
2. Negativ påverkan av rätten till egna uppgifter	- En avsevärd negativ påverkan av den enskildes rätt till egna uppgifter förefaller möjlig. - Ett möjligt missbruk av personrelaterade data har avsevärd inverkan på den berördes offentliga ställning eller ekonomiska förhållanden.
3. Påverkan av den personliga integriteten	- En påverkan av den personliga integriteten kan inte ovillkorligen uteslutas.
4. Negativ inverkan på utförande av uppgiften	- Den negativa påverkan torde av den berörde bedömas som ej acceptabel. - Den maximala bortfallstid som kan accepteras ligger mellan 1 och 24 timmar.
5. Negativ intern eller extern inverkan	- En kraftig påverkan av anseende och förtroende kan förväntas.
6. Ekonomiska följder	- Skadan medför avsevärd ekonomiska förluster men hotar inte verksamhetens existens.

Kategori för skyddsbehov ”mycket stort”	
1. • Brott mot lagar, föreskrifter eller avtal	- Fundamentalt brott mot lagar och föreskrifter - Avtalsbrott vars avtalsskador har mycket allvarliga följder
2. Negativ påverkan av rätten till egna uppgifter	- En mycket stor negativ påverkan av den enskildes till egna uppgifter förefaller möjlig. - Ett möjligt missbruk av personrelaterade data skulle helt förstöra den berördes offentliga ställning eller medföra ekonomisk ruin.
3. Påverkan av den personliga integriteten	- Allvarlig påverkan av den personliga integriteten är möjlig. - Fara för liv och lem.
4. Negativ inverkan på utförande av uppgiften	- Den negativa påverkan torde av alla berörda bedömas som ej acceptabel. - Den maximala bortfallstid som kan accepteras är kortare än 1 timme.
5. Negativ intern eller extern inverkan	- En påverkan av anseende eller förtroende över hela landet, eventuellt av en omfattning som hotar existensen, är tänkbar.
6. Ekonomiska följder	- Den ekonomiska skadan kan hota institutionens existens.

Individualisering av tillordningstabellen

Eftersom det inte går att utesluta att det i vissa fall kan förekomma fler skadescenarior bör dessa kompletteras i motsvarande grad. För alla skador som inte går att inordna under dessa scenarier måste ett yttrande göras över var gränsen ska dras mellan ”normalt”, ”stort” och ”mycket stort”.

Därutöver bör hänsyn tas till institutionens individuella förhållande: Om en skada på 200 000 euro i ett storföretag betyder en liten skada i förhållande till omsättningen och IT-budgeten kan en skada på 10 000 euro hota ett litet företags existens. Därför kan det vara förnuftigt att definiera ett procenttal som gränsvärde vilket är relaterat till totala omsättningen, vinsten eller IT-budgeten.

Liknande överväganden kan göras beträffande kraven på tillgänglighet. Så kan exempelvis ett bortfall på 24 timmar klassas som ännu acceptabelt. Om det sker en ökning av dessa bortfall, t.ex. fler än ett per vecka, så kan det inte accepteras.

När gränsen fastställs mellan ”normalt” och ”stort” bör man beakta att IT-grundskydds standardsäkerhetsåtgärder bör räcka för det normala skyddsbehovet. Det som fastställs bör på lämpligt sätt dokumenteras i säkerhetskonceptet eftersom valet av IT-säkerhetsåtgärder och därmed följdkostnader beror på det.

Steg 2: Genomgång av skadescenarier

De maximala skadorna och följdskadorna som kan uppstå ur en sådan situation betraktas utifrån möjligheten att en IT-tillämpnings eller den tillhörande informationens konfidentialitet, riktighet och tillgänglighet går förlorad. Med frågeställningen ”Vad skulle hända om ... ?” utvecklas *utifrån användarens perspektiv* realistiska skadescenarier och de förväntade materiella och ideella skadorna beskrivs. Storleken på dessa möjliga skador bestämmer slutligen IT-tillämpningens skyddsbehov. I samband med detta är det absolut nödvändigt att tillfråga de som ansvarar för den betraktade IT-tillämpningen samt användarna beträffande deras personliga bedömningar. De har i allmänhet en bra föreställning om vilka skador som kan uppstå och kan lämna värdefull information för inventeringen.

För att förenkla inventeringen av möjliga skador presenteras efter de nämnda skadescenarierna frågeställningar som undersöker de möjliga följderna. Dessa förslag gör inte anspråk på att vara fullständiga det är enbart en orienteringshjälp. I varje fall måste hänsyn tas till den individuella uppgiften och institutionens situation och dessa frågor kompletteras motsvarande.

I det följande tillvägagångssättet är det lämpligt att för de inventerade IT-tillämpningarna arbeta igenom de följande skadescenarierna inklusive frågeställningarna. Därefter bör, utifrån de ovan definierade tabellerna, skyddsbehovet fastställas med avseende på konfidentialitet, riktighet och tillgänglighet genom tillordning till en kategori för skyddsbehov.

Skadescenario ”Brott mot lagar, föreskrifter eller avtal”

Den typen av brott kan vara ett resultat av såväl förlusten av konfidentialitet som av riktigheten och likaledes av tillgängligheten. Skadans allvar beror därvid ofta på vilka juridiska konsekvenser som kan uppkomma för institutionen.

Exempel på relevanta lagar:

grundlag, civilrättslig lagstiftning, brottsbalk, datalagstiftning, sociallagar, handelsbalken, medbestämmandelag, upphovsrättslag, patentlag, aktiebolagslagen.

Exempel på relevanta föreskrifter:

förvaltningsföreskrifter, förordningar och reglementen.

Exempel på avtal:

serviceavtal inom området databearbetning, avtal som rör skydd av företagshemligheter.

Frågor:

Förlust av konfidentialitet

Finns det lagstadgade krav på att data ska vara konfidentiella?

Kan man räkna med åtal eller skadeståndskrav om information publiceras?

Ska avtal, vilka omfattar skydd av konfidentiella data, följas?

Förlust av riktighet

Finns det lagstadgade krav på att data är riktiga?

I vilken omfattning sker brott mot lagar respektive föreskrifter genom förlust av riktighet?

Förlust av tillgänglighet

Innebär bortfall av IT-tillämpningen brott mot förordningar eller rent av lagar? Om ja, i vilken omfattning?

Föreskriver lagar att bestämd information permanent är tillgänglig?

Finns det tidsfrister som tvingande ska innehållas vid användning av IT-tillämpningen?

Finns det avtal beträffande tidsfrister som ska innehållas?

Skadescenario ”negativ påverkan av rätten till egna uppgifter”

Vid införande och drift av IT-system och IT-tillämpningar finns risk att rätten till egna uppgifter skadas eller att personrelaterade data missbrukas.

Exempel på negativ påverkan av rätten till egna uppgifter:

• otillåten insamling av personrelaterade data utan stöd av lag eller samtycke

• obehörig åtkomst av personrelaterade data vid bearbetning och överföring av dessa

• obehörigt överlämnande av personrelaterade data

• användande av personrelaterade data för annat ändamål än det vid insamlandet tillåtna och

• förvanskning av personrelaterade data i IT-system eller vid överföringen.

Följande frågor kan användas för bedömning av möjliga följder och skador:

Frågor:

Förlust av konfidentialitet

Vilka skador kan uppstå för de berörda om personrelaterade data inte behandlas konfidentiellt?

Bearbetas personrelaterade data för otillåtna ändamål?

Är det vid en tillåten bearbetning av personrelaterade data möjligt att få reda på en persons hälsotillstånd eller dennes ekonomiska förhållanden?

Vilka skador kan uppstå genom missbruk av personrelaterade data?

Förlust av riktighet

Vilka skador skulle uppstå för de berörda om deras personrelaterade data oavsiktligt förvanskas eller avsiktligt manipuleras?

När skulle förlusten av personrelaterade datas riktighet tidigast märkas?

Förlust av tillgänglighet

Kan vid bortfall av IT-tillämpningen eller vid störning av dataöverföringen personrelaterade data försvinna eller förvanskas så att den berörde kan påverkas negativt vad gäller dennes offentliga ställning eller till och med befara personliga eller ekonomiska nackdelar?

Skadescenario: ”Påverkan av den personliga integriteten”

Ett IT-system eller en IT-tillämpning som fungerar felaktigt kan direkt medföra personskador, invaliditet eller dödsfall. Hur allvarlig skadan är kan mätas direkt utifrån den personliga skadan.

Exempel på sådana IT-tillämpningar och -system är:

• medicinska övervakningsdatorer

• medicinska diagnossystem

• datorer för flygtrafikledning och

• trafikinformationssystem.

Frågor:

Förlust av konfidentialitet

Kan en person skadas fysiskt eller psykiskt genom att personrelaterade data blir kända?

Förlust av riktighet

Kan personers hälsa skadas genom manipulerade programförlopp eller data?

Förlust av tillgänglighet

Hotas personers personliga integritet direkt genom bortfall av IT-tillämpningen eller IT-systemet?

Skadescenario ”Negativ inverkan på utförande av uppgiften”

Särskilt förlusten av en IT-tillämpnings tillgänglighet eller datas riktighet kan i hög grad negativt påverka hur en institution kan utföra sina uppgifter. Skadans allvar beror i detta fall på hur länge den negativa påverkan har pågått och i vilken omfattning de erbjudna tjänsterna har varit begränsade.

Exempel är:

• tidsfrister har dragits över på grund av fördröjd bearbetning av arbetsprocesser

• försenad leverans på grund av fördröjd bearbetning av beställning

• bristfällig produktion på grund av felaktiga styrdata

• otillräcklig kvalitetssäkring genom bortfall av ett testsystem.

Frågor:

Förlust av konfidentialitet

Finns det data vars konfidentialitet är grunden för att uppgiften kan utföras (t.ex. åtalsinformation, utredningsresultat)?

Förlust av riktighet

Kan förändring av data inskränka utförandet av uppgiften på sådant sätt att institutionen blir handlingsförlamad?

Uppstår stora skador om uppgifterna genomförs trots förvanskade data? När upptäcks otillåten ändring av data tidigast?

Kan förvanskade data i den betraktade IT-tillämpningen medföra fel i andra IT-tillämpningar?

Vilka följder uppkommer om data felaktigt tillordnas en person som i verkligheten inte är upphov till dessa data?

Förlust av tillgänglighet

Kan en institutions möjligheter att utföra sina uppgifter påverkas av bortfallet av IT-tillämpningen så mycket att väntetiderna för de berörda inte längre kan accepteras?

Berörs andra IT-tillämpningar av bortfallet av denna IT-tillämpning?

Är det viktigt för institutionen att ständigt vara garanterad åtkomst av IT-tillämpningar jämte program och data?

Skadescenario ”Negativ intern eller extern inverkan”

Olika slag av intern och extern påverkan kan uppkomma genom förlust av grundvärdena konfidentialitet, riktighet och tillgänglighet till exempel:

• minskat anseende för en myndighet respektive ett företag

• minskat förtroende för en myndighet respektive ett företag

• medarbetarnas moral försämras

• de ekonomiska relationerna till samarbetande företag påverkas negativt

• förlorat förtroende för en myndighets respektive ett företags arbetskvalitet och

• minskad konkurrensförmåga.

Skadans omfattning påverkas av hur mycket förtroendet har minskat eller storleken av den interna och externa inverkan.

Orsakerna till dessa skador kan vara av många slag:

• en institution blir handlingsförlamad genom IT-bortfall

• felaktiga publiceringar genom manipulerade data

• felbeställningar genom felaktiga lagerhållningsprogram

• tystnadsplikt beaktas ej

• fel person anklagas

• en avdelning förhindras att utföra sina uppgifter på grund av fel inom andra områden

• spaningsdata överlämnas till intresserad tredje person och

• konfidentiell information överlämnas till pressen.

Frågor:

Förlust av konfidentialitet

Vilka konsekvenser uppstår för institutionen till följd av otillåten publicering av de för IT-tillämpningen sparade data med skyddsbehov?

Kan förlusten av konfidentialiteten för de sparade uppgifterna leda till en försämrad konkurrensposition?

Uppkommer det tvivel på tystnadsplikten när konfidentiella, sparade uppgifter publiceras?

Kan publicering av data leda till politisk eller samhällelig osäkerhet?

Kan medarbetare förlora förtroende inom deras institution genom otillåten publicering av data?

Förlust av riktighet

Vilka skador kan uppkomma genom bearbetning, spridning eller överföring av felaktiga eller ofullständiga data?

Blir förvanskningen av data allmänt känd?

Skadas anseendet vid en publicering av förvanskade data?

Kan publicering av förvanskade data leda till politisk eller samhällelig osäkerhet?

Kan förvanskade data leda till lägre produktkvalitet och därmed förlorat anseende?

Förlust av tillgänglighet

Inskränker bortfallet av IT-tillämpningarna informationstjänsterna för externa?

Förhindrar bortfallet av IT-tillämpningar att affärsmål uppnås?

När märks bortfallet av IT-tillämpningen externt?

Skadescenario ”Ekonomiska följder”

Direkta eller indirekta ekonomiska skador kan uppkomma genom förlusten av konfidentialiteten för data med skyddsbehov, förändringen av data eller bortfallet av en IT-tillämpning. Exempel är:

• otillåtet överlämnande av forsknings- och utvecklingsresultat

• manipulering av ekonomiska data i ett redovisningssystem

• bortfall av ett IT-styrt produktionssystem och till följd därav minskad omsättning

• insyn i dokument rörande marknadsstrategi eller omsättningssiffror

• bortfall av ett reseföretags bokningssystem

• bortfall av en e-handelsserver

• sammanbrott i en banks transaktioner

• stöld eller ödeläggelse av hårdvara.

Totalskadans storlek sätts samman av de direkta och indirekta kostnaderna som uppstår som t.ex. genom sakskador, skadestånd och kostnader för extra insatser (t.ex. räddningsprocedurer).

Frågor:

Förlust av konfidentialitet

Kan publiceringen av konfidentiell information medföra skadeståndskrav?

Finns det i IT-tillämpningen data som utomstående (t.ex. konkurrerande företag) kan dra nytta av om de har kännedom därom?

Har forskningsdata, med avsevärt värde sparats med IT-tillämpningen? Vad händer om de otillåtet kopieras och lämnas vidare?

Kan finansiella skador uppkomma genom att data med skyddsbehov publiceras för tidigt?

Förlust av riktighet

Kan ekonomiska data manipuleras så att ekonomiska skador uppstår?

Kan publiceringen av konfidentiell information medföra skadeståndskrav?

Kan ekonomiska skador uppkomma genom förvanskade beställningsdata (t.ex. vid produktion just-in-time)?

Kan förvanskade data leda till felaktiga affärsbeslut?

Förlust av tillgänglighet

Påverkas produktionen, lagerhållningen eller försäljningen genom att IT-tillämpningen inte fungerar?

Uppstår ekonomiska förluster på grund av försenade betalningar respektive ränteförluster till följd av att IT-tillämpningen inte fungerar?

Hur stora är kostnaderna för reparations- och räddningsprocedur när följande har drabbat IT-systemet: det inte fungerar, fel, ödeläggelse eller stöld?

Kan en icke fungerande IT-tillämpning leda till bristande betalningsförmåga eller till avtalsviten?

Hur många viktiga kunder skulle drabbas om IT-tillämpningen inte fungerar?

Steg 3: Dokumentation av resultaten

Det är lämpligt att i en tabell dokumentera det ovan bestämda skyddsbehovet för de enskilda IT-tillämpningarna. Denna centrala dokumentation har fördelen att den kan användas som referens vid den följande bestämningen av skyddsbehov för IT-system.

Se därvid till att inte endast fastställandet av skyddsbehovet dokumenteras utan även de motsvarande motiveringarna. Dessa motiveringar tillåter senare att fastställandena kan spåras och återanvändas.

Exempel: Organisations- och förvaltningsverket (OFV) - del 4

I den följande tabellen finns de viktigaste IT-tillämpningarna, deras skyddsbehov och de motsvarande motiveringarna.

IT-tillämpning			Fastställande av skyddsbehov		
Nr	Beteckning	Pers. data	Grundvärde	Skyddsbehov	Motivering
A1	Bearbetning av personuppgifter	X	Konfidentialitet	stort	Personuppgifter är personrelaterade data med särskilt skyddsbehov, om de tillkännages kan det i hög grad påverka de berörda negativt.
			Riktighet	normalt	Skyddsbehovet är normalt eftersom fel snabbt uppmärksammas och data i efterhand kan rättas.
			Tillgänglighet	normalt	Avbrott upp till en vecka kan överbryggas med manuell metod.
A2	Bidragshantering	X	Konfidentialitet	stort	Bidragsdata är personrelaterade data med särskilt skyddsbehov. De innehåller delvis information om sjukdomar och läkarutlåtanden. Ett tillkännagivande kan påverka den berörde mycket negativt.
			Riktighet	normalt	Skyddsbehovet är normalt eftersom fel snabbt uppmärksammas och data i efterhand kan rättas.
			Tillgänglighet	normalt	Avbrott upp till en vecka kan överbryggas med manuell metod.

Här kan det vara förnuftigt att utöver denna information även att utifrån affärsprocesserna och fackuppgifterna se på skyddsbehovet utifrån ett helhetsperspektiv. Ett lämpligt sätt är att beskriva syftet med en IT-tillämpning i en affärsprocess eller i en fackuppgift och att ur resultatet härleda deras betydelse. Denna betydelse kan klassificeras på följande sätt:

IT-tillämpningens betydelse är för affärsprocessen respektive fackuppgiften:

• **normal:** Affärsprocessen respektive fackuppgiften kan med acceptabel merinsats utföras på annat sätt (t.ex. manuellt).

• **stor**: Affärsprocessen respektive fackuppgiften kan endast med betydlig merinsats utföras på annat sätt.

• **mycket stor**: Affärsprocessen respektive fackuppgiften kan överhuvudtaget inte utföras utan IT-tillämpningen.

Fördelen med att utföra en sådan integrerad tillordning ligger i synnerhet i att när skyddsbehovet fastställs kan ledningsnivån verka styrande för skyddsbehovet för de enskilda IT-tillämpningarna. Därför kan det vara så att en ansvarig för en IT-tillämpning klassar dess skyddsbehov som ”normalt” utifrån sina utgångspunkter medan ledningsnivån utifrån affärsprocessen respektive fackuppgiften däremot korrigerar denna bedömning uppåt.

Dessa valfria uppgifter bör likaledes dokumenteras i en tabell.

Punkter att utföra:

- definiera kategorier för skyddsbehov ”normalt”, ”stort ” och ”mycket stort ” respektive anpassa till den egna institutionen
- bestämma skyddsbehov för de inventerade IT-tillämpningarna utifrån skadescenarior och frågekataloger
- dokumentera IT-tillämpningarnas skyddsbehov och tillhörande motiveringar.

4.2.2 Bestämma skyddsbehov för IT-system

För att fastställa ett IT-systems skyddsbehov måste man först se på IT-tillämpningarna som har ett direkt samband med IT-systemen. En översikt över vilka IT-tillämpningar som är relevanta bestämdes i steget ”Inventering av IT-tillämpningarna och den tillhörande informationen”.

För att bestämma IT-systemets skyddsbehov måste nu de relevanta IT-tillämpningarnas möjliga skador betraktas fullt ut. Skyddsbehovet för ett IT-system bestäms i huvudsak av skadan respektive summan av skadorna med de allvarligaste följderna (maximumprincip).

När de möjliga skadorna och deras följder betraktas måste man även beakta att IT-tillämpningar som input eventuellt använder andra IT-tillämpningarnas arbetsresultat. En – för sig betraktad – mindre viktig IT-tillämpning A kan vinna i betydelse om en annan viktig IT-tillämpning B är hänvisad till dess resultat. I detta fall måste det skyddsbehov som har bestämts för IT-tillämpningen B överföras till IT-tillämpning A. Om det är fråga om IT-tillämpningar från olika IT-system så måste det ena IT-systemets krav på skyddsbehov även överföras till det andra (**beaktande av beroenden**).

Om flera IT-tillämpningar respektive olika information bearbetas i ett IT-system ska man tänka över huruvida en totalt större totalskada kan uppkomma genom kumulering av flera (t.ex. mindre) skador på ett IT-system. Då ökar IT-systemets skyddsbehov motsvarande (**kumuleringseffekt**).

Exempel: På en nätserver finns en institutions samtliga IT-tillämpningar som behövs för registrering av kunddata. Om en av dessa IT-tillämpningar inte fungerar skulle skadan bedömas som liten eftersom det finns tillräckligt med alternativa möjligheter. Om servern däremot inte fungerar (och därmed alla IT-tillämpningar) så ska den skada som uppstår bedömas som betydligt större. Uppgifterna kan eventuellt inte utföras under den nödvändiga tiden. Därför ska skyddsbehovet för dessa ”centrala” komponenter bedömas motsvarande högre.

Motsatt effekt kan också inträffa. Det är möjligt att en IT-tillämpning har ett stort skyddsbehov men man överför det inte på ett betraktat IT-system eftersom på detta IT-system körs endast oviktiga delområden av IT-tillämpningen. Här ska skyddsbehovet sättas in i sitt sammanhang (**fördelningseffekt**).

Exempel: Fördelningseffekten uppträder huvudsakligen beträffande grundvärdet tillgänglighet. På så sätt kan vid redundant utformning av IT-system de enskilda komponenternas skyddsbehov vara mindre än totaltillämpningens skyddsbehov. Även inom området konfidentialitet går det att föreställa sig fördelningseffekter: Om det har säkerställts att en klient endast kan hämta okritiska data från en väl skyddad databastillämpning så har klienten i motsats till databasservern ett litet skyddsbehov.

Visning av resultaten

Resultaten från fastställandet av IT-systemens skyddsbehov bör däremot noteras i en tabell. I den bör man anteckna vilket skyddsbehov varje IT-system har med avseende på konfidentialitet, riktighet och tillgänglighet. Ett IT-systems totala skyddsbehov härleds däremot ur skyddsbehovets maximum beträffande de tre grundvärdena konfidentialitet, riktighet och tillgänglighet. Ett IT-system har alltså ett stort skyddsbehov när det har skyddsbehovet ”stort” med avseende på ett av grundvärdena. I allmänhet är det klokt att dokumentera ett IT-systems skyddsbehov för alla tre grundvärdena eftersom det resulterar i olika typer av

---

säkerhetsåtgärder.

För ett IT-system kan det totala skyddsbehovet exempelvis härledas från att skyddsbehovet vad gäller konfidentialitet är stort. med avseende på riktighet och tillgänglighet visserligen normalt. Då kan det totala skyddsbehovet förvisso anges som stort det medför emellertid inte att skyddsbehovet avseende riktighet och tillgänglighet därigenom måste ökas. Det krävs alltså inga extra säkerhetsåtgärder för skyddet av riktighet eller tillgänglighet.

Särskilt vikt ska läggas på motiveringarna för bedömningarna så att dessa också är begripliga för utomstående. Här kan man referera tillbaka till fastställandet av IT-tillämpningens skyddsbehov.

Exempel: Organisations- och förvaltningsverket (OFV) - del 5

En sådan tabell kan exempelvis se ut enligt följande:

IT-system			Fastställande av skyddsbehov	
Nr	Beskrivning	Grundvärde	Skyddsbehov	Motivering
S1	Server för personalavdelning	Konfidentialitet	stort	Maximumprincip
		Riktighet	normalt	Maximumprincip
		Tillgänglighet	normalt	Maximumprincip
S2	Primär domänkontroller	Konfidentialitet	normalt	Maximumprincip
		Riktighet	stort	Maximumprincip
		Tillgänglighet	normalt	Enligt fastställandet av skyddsbehovet för tillämpning A4 ska man utgå från ett stort skyddsbehov för detta grundvärde. Man ska däremot tänka på att denna tillämpning är fördelad på två datorsystem. En autenticering via backup-domänkontrollern i Berlin är likaledes möjlig för medarbetarna i Bonn. Ett avbrott i den primära domänkontrollern kan accepteras i upp till 72 timmar. På grund av denna fördelningseffekt är skyddsbehovet därför ”normalt”.

Information: Om de flesta IT-tillämpningarna i ett IT-system endast har ett normalt skyddsbehov och det endast finns en eller ett par med stort skyddsbehov så bör man överväga att lägga dessa få i ett isolerat IT-system. Det systemet kan säkras mycket enklare och mer målinriktat varigenom det blir billigare. Ett sådant alternativ kan presenteras för ledningen för beslut.

Hjälpmedel:

För att fastställa skyddsbehov har hjälpmedel i form av formulär tagits fram. Dessa finns bland hjälp-medlen till IT-grundskydd.

Punkter att utföra:

- bestämma IT-systemens skyddsbehov med ledning av IT-tillämpningarnas skyddsbehov
- ta hänsyn till beroenden, maximumprincipen och vid behov kumulerings- respektive fördelningseffekten
- per IT-system dokumentera resultaten för konfidentialitet, riktighet och tillgänglighet samt motiveringarna

4.2.3 Fastställande av skyddsbehov för kommunikationsförbindelser

Efter att skyddsbehovet för de betraktade IT-systemen har fastställts i det föregående kapitlet ska skyddsbehovet för nätstrukturen nu tas fram. Bas för de fortsatta övervägandena är återigen den i kapitel 2.1 framtagna nätplanen för det IT-nätverk som ska undersökas.

För att förbereda besluten, på vilka kommunikationsvägar som kryptografiska säkerhetsåtgärder bör sättas in, vilka vägar som bör vara redundant utförda och via vilka förbindelser angrepp kan förväntas av interna och externa förövare, måste efter IT-systemen kommunikationsförbindelserna studeras. I det sammanhanget bedöms följande kommunikationsförbindelser som kritiska:

- Kommunikationsförbindelser, som är externa, dvs. som går in i eller över okontrollerade områden (t.ex. in i Internet eller över allmän mark). Dit kan även WLAN-anslutningar höra eftersom det är svårt att förhindra att angrepp sker på dessa utifrån allmänt område. Vid externa förbindelser finns risken att externa angripare utför penetrationsförsök på systemet som ska skyddas eller att datorvirus respektive trojaner överförs. Vidare kan en intern förövare överföra konfidentiell information via en sådan förbindelse.
- Kommunikationsförbindelser via vilka information med stort skyddsbehov överförs varvid det kan vara såväl information med höga krav på konfidentialitet som på riktighet eller tillgänglighet. Dessa förbindelser kan vara målet för avlyssning eller manipulering. Därutöver kan ett avbrott i en sådan förbindelse negativt påverka funktionen i viktiga delar av IT-nätverket.
- Kommunikationsförbindelser via vilka viss information med stort skyddsbehov inte får överföras. Detta gäller speciellt för konfidentiell information. Om anordningar för koppling i nätet har konfigurerats olämpligt eller felaktigt kan det hända att information som inte bör överföras trots allt överförs via en sådan förbindelse och kan angripas.

Inventering av kritiska kommunikationsförbindelser kan göras enligt följande. Först identifieras och registreras samtliga ”externa förbindelser” som kritiska förbindelser. Därefter undersöks samtliga förbindelser som går ut från ett IT-system med stort eller mycket stort skyddsbehov. I samband med detta identifieras de förbindelser via vilka information med stort skyddsbehov överförs. Därefter undersöks förbindelserna via vilka dessa data med stort skyddsbehov överförs vidare. Slutligen ska de kommunikationsförbindelser identifieras via vilka sådan information inte får överföras. Inventeringen ska omfatta:

- förbindelsen
- om det är fråga om en extern förbindelse
- om information med stort skyddsbehov överförs och om skyddsbehovet beror på konfidentialitet, riktighet eller tillgänglighet och
- om information med stort skyddsbehov inte får överföras.

Det kan vara lämpligt att dokumentera de inventerade uppgifterna i en tabell eller att det visas grafiskt i en nätplan.

Exempel: Organisations- och förvaltningsverket (OFV) - del 6

För det fiktiva exemplet OFV erhålls följande kritiska förbindelser:

I den grafiska redovisningen är de kritiska förbindelserna markerade med ”feta” linjer. Siffrorna bredvid linjerna markerar anledningen (respektive anledningarna) varför förbindelsen är kritisk och förklaras i kolumnhuvudena i tabellen nedan.

	Kritisk på grund av				
Förbindelse	K 1 Extern förbindelse	K 2 Hög konfidentialitet	K 3 Hög riktighet	K 4 Hög tillgänglighet	K 5 Ingen överföring
N1 - Internet	X				
N5 - N6	X				
S1 - N4		X			
S3 - N3				X	
S4 - N3				X	
S5 - N3				X	
C1 - N4		X			
N1 - N2				X	X
N2 - N3				X	
N4 - N3					X

Vid denna undersökning ska speciell vikt läggas vid att den framtagna översikten är komplett. Endast en missad, kritisk förbindelse kan förstöra den totala säkerheten. Så bör till exempel alla använda modem tas med eftersom potentiellt kritiska externa förbindelser kan utgå från dessa. Ofta betraktas däremot dessa externa modemförbindelser som prestigeobjekt vars existens förnekas för att man ska få personliga fördelar. Eller modem anskaffas och klassas som förbrukningsmaterial utan att IT-ansvariga informeras om vad de används till. För att uppnå en fullständig IT-säkerhet får sådana kritiska apparater och förbindelser dock inte missas.

Punkter att utföra:

- inventera externa förbindelser
- identifiera förbindelser via vilka kritisk information överförs
- registrera förbindelser via vilka viss information inte får överföras
- dokumentera alla kritiska kommunikationsförbindelser i tabell eller i grafisk form.

4.2.4 Fastställande av skyddsbehov för lokaler

Ur resultaten från fastställande av IT-systemens skyddsbehov bör man härleda skyddsbehovet för aktuella fastigheter och lokaler. Detta skyddsbehov beror på skyddsbehovet för i aktuellt rum installerade IT-system bearbetad information eller förvarade datamedium enligt maximumprincipen. I samband med detta bör dessutom en möjlig kumuleringseffekt beaktas om ett större antal IT-system befinner sig i en lokal vilket är vanligt i serverrum. Dessutom bör motivering av bedömningen av skyddsbehov dokumenteras.

Även här är det till hjälp att redovisa den nödvändiga informationen i en tabell som bygger på den redan

---

tidigare gjorda översikten över de inventerade lokalerna.

Exempel: Organisations- och förvaltningsverket (OFV) - del 7

Följande tabell visar ett utdrag av resultatet för OFV:

Rum		IT/information		Skyddsbehov		
Be-teckning	Typ	Pla-cering	IT-system/datamedium	Konfiden-tialitet	Riktig-het	Tillgäng-lighet
R U.02	Arkiv datamedium	Bygg-nad Bonn	Backup-datamedium (säkerhets-kopiering en gång per vecka server S1 till S5)	stort	stort	normalt
R B.02	Teknikrum	Bygg-nad Bonn	Telekommunikationssystem	normalt	nor-malt:	stort
R 1.01	Serverrum	Bygg-nad Bonn	S1, N4	stort	stort	normalt
R 1.02 - R 1.06	Kontorsrum	Bygg-nad Bonn	C1	stort	nor-malt:	normalt
R 3.11	Skyddsskåp i rum R 3.11	Bygg-nad Bonn	Backup-datamedium (säkerhetskopiering en gång per dag server S1 till S5)	stort	stort	normalt
R E.03	Serverrum	Bygg-nad Berlin	S6, N6, N7	normalt	stort	stort
R 2.01 - R 2.40	Kontorsrum	Bygg-nad Berlin	C4, några med faxar	normalt	normalt	normalt

Punkter att utföra:

- härleda lokalernas skyddsbehov utifrån IT-systemens och IT-tillämpningarnas skyddsbehov
- ta hänsyn till beroenden, maximumprincipen och vid behov kumulerings- respektive fördelningseffekten
- dokumentera resultat och motiveringar så att de är begripliga.

4.2.5 Tolkning av resultaten från fastställande av skyddsbehov

Resultaten från fastställandet av skyddsbehov erbjuder ett stöd för IT-säkerhetskonceptets fortsatta tillvägagångssätt. För skyddet som bygger på de i IT-grundskydd rekommenderade standardsäkerhetsåtgärderna antas följande beträffande kategorierna för skyddsbehov:

Skyddsverkan av standardsäkerhetsåtgärder enligt IT-grundskydd	
Kategori för skyddsbehov ”normalt”	Standardsäkerhetsåtgärder enligt IT-grundskydd är i allmänhet tillräckliga och lämpliga.
Kategori för skyddsbehov ”stort”	Standardsäkerhetsåtgärder enligt IT-grundskydd utgör ett grundskydd och är i vissa fall ensamma inte tillräckliga. Mer omfattande åtgärder kan bestämmas utifrån en kompletterande säkerhetsanalys.
Kategori för skyddsbehov ”mycket stort”	Standardsäkerhetsåtgärder enligt IT-grundskydd utgör ett grundskydd och är i allmänhet inte tillräckliga. De erforderliga extra säkerhetsåtgärderna måste bestämmas individuellt utifrån en kompletterande säkerhetsanalys.

Om skyddsbehovet för ett IT-system definieras som ”normalt” så räcker att schablonmässigt genomföra säkerhetsåtgärderna enligt IT-grundskydd. För IT-system, nätförbindelser och lokaler med IT-verksamhet med ”stort” och speciellt med ”mycket stort” skyddsbehov bör en kompletterande säkerhetsanalys planeras. Likaså bör man vid dessa komponenter i bör-är-jämförelsen beakta det stora skyddsbehovet vid bearbetningen av som ”extra” markerade åtgärder. Så kan exempelvis M 1.10 *Användning av säkerhetsdörrar* inte vara nödvändig i ett serverrum med normalt skyddsbehov men vara absolut nödvändigt vid stort skyddsbehov beroende på konfidentialitet.

Områden med olika skyddsbehov

När skyddsbehov fastställs visar det sig delvis att det inom det betraktade IT-nätverket finns områden i vilka det bearbetas information som har ett stort eller mycket stort skyddsbehov. Ett högre skyddsbehov i ett område överförs enligt maximumprincipen till andra områden. Även om endast få utvalda data har ett särskilt skyddsbehov medför det omfattande nätet och sammankopplingen av IT-system och tillämpningar snabbt att det stora skyddsbehovet överförs till andra områden enligt maximumprincipen.

För att minska risker och kostnader bör säkerhetszoner därför inrättas. Sådana säkerhetszoner kan omfatta lokaler men kan även ha en teknisk eller personell prägel.

Exempel:

- Säkerhetszoner i lokalen: För att varje kontorsrum inte permanent ska behöva vara låst eller övervakat bör zoner där många personer rör sig vara skilda från områden med stort skyddsbehov. Därför bör konferens- utbildnings- eller visningsrum liksom matsal med externa gäster vara placerade i närheten av byggnadens entré. Inpassering till byggnadsdelar med kontor kan då enkelt övervakas av en receptionist. Särskilt känsliga områden som en utvecklingsavdelning bör vara försedda med extra inpasseringskontroller t.ex. med kort.
- Tekniska säkerhetszoner: För att begränsa konfidentiella data till bestämda områden i ett LAN och för att förhindra att störningar i vissa komponenter eller angrepp negativt påverkar funktionen är det bra att dela upp det lokala datanätet (LAN) i flera delnät (se även M 5.77 *Bildning av delnät*).
- Personella säkerhetszoner: I princip bör varje person alltid endast tilldelas de behörigheter som behövs för att denne ska kunna utföra sina uppgifter. Därutöver finns det även olika roller som en person inte kan inneha samtidigt. Så bör en revisor samtidigt inte arbeta med bokföringen och med IT-administrationen eftersom denne inte kan och får kontrollera sig själv. För att förenkla tilldelning av behörigheter för inpassering och åtkomst bör persongrupper som har hand om funktioner som inte är förenliga med varandra arbeta i olika grupper eller på olika avdelningar.

Om områden med likartade säkerhetskrav redan omstruktureras på lämpligt sätt under planeringsfasen

sparar det mycket arbete i alla följande faser ända fram till revisionen.

Punkter att utföra:

• kontrollera om objekt med ökade säkerhetskrav kan koncentreras i säkerhetszoner

• notera objekt med ökade säkerhetskrav för en kompletterande säkerhetsanalys.

4.3 Val av åtgärder: Modellering enligt IT-grundskydd

När den nödvändiga informationen från IT-strukturanalysen och från fastställandet av skyddsbehov föreligger består nästa uppgift i att avbilda det betraktade IT-nätverket med hjälp av de befintliga komponenterna i IT-grundskydd-katalogerna. Resultatet utgörs av en IT-grundskyddsmodell av IT-nätverket vilken består av olika komponenter som vid behov även har använts flera gånger och innehåller en avbildning mellan komponenterna och IT-nätverket.

4.3.1 IT-grundskydd-katalogerna

Komponenter

IT-grundskydd-katalogerna omfattar hotbilden och åtgärdsrekommendationer för olika komponenter och IT-system som kan sammanfattas i en komponent.

I varje komponent beskrivs först den förväntade hotbilden varvid såväl de typiska hoten som de schablonmässiga sannolikheterna för inträffande beaktades. Denna hotbild är del av en förenklad riskanalys för typiska IT-miljöer och utgör grunden på vilken BSI har tagit fram ett specifikt åtgärdspaket från områdena infrastruktur, personal, organisation, hård- och programvara, kommunikation och förebyggande av nödsituationer. Fördelen i samband med detta är att användaren inte behöver några dyrbara analyser för att uppnå den nödvändiga skyddsnivån för ett genomsnittligt skyddsbehov. Desto mer räcker det i detta fall att identifiera de för de betraktade IT-systemen eller affärsprocesserna relevanta komponenterna och konsekvent och fullständigt genomföra de däri rekommenderade åtgärderna. Även om speciella komponenter eller användningsmiljöer föreligger vilka inte är tillräckligt behandlade i IT-grundskydd så erbjuder denna däremot en värdefull hjälp i arbetet. De då nödvändiga, kompletterande säkerhetsanalyserna kan då koncentreras till dessa komponenters eller förutsättningars specifika hot.

För att kunna hantera de innovationer och versionsbyten som kommer inom IT-området är IT-grundskydd-katalogerna uppbyggda i moduler med hjälp av komponentstrukturen. Därigenom kan katalogerna enkelt utökas och uppdateras.

Komponenterna är grupperade i följande kapitel:

B 1: Överordnade aspekter på IT-säkerheten

B 2: Infrastrukturens säkerhet

B 3:IT-systemens säkerhet

B 4: Säkerhet i nätet

B 5: Säkerhet i tillämpningar

Hotkataloger

Detta område innehåller de utförliga beskrivningarna av hoten som i de enskilda komponenterna benämns hotbild. Hoten är grupperade i fem kataloger:

G 1: Force majeure

G 2: Organisatoriska brister

G 3: Mänskliga felhandlingar

G 4: Tekniska fel

G 5: Uppsåtliga handlingar

Åtgärdskataloger

Denna del beskriver utförligt de i IT-grundskydd-katalogerna citerade IT-säkerhetsåtgärderna. Åtgärderna är grupperade i sex åtgärdskataloger:

M 1: Infrastruktur

M 2: Organisation

M 3: Personal

M 4: Hårdvara och programvara

M 5: Kommunikation

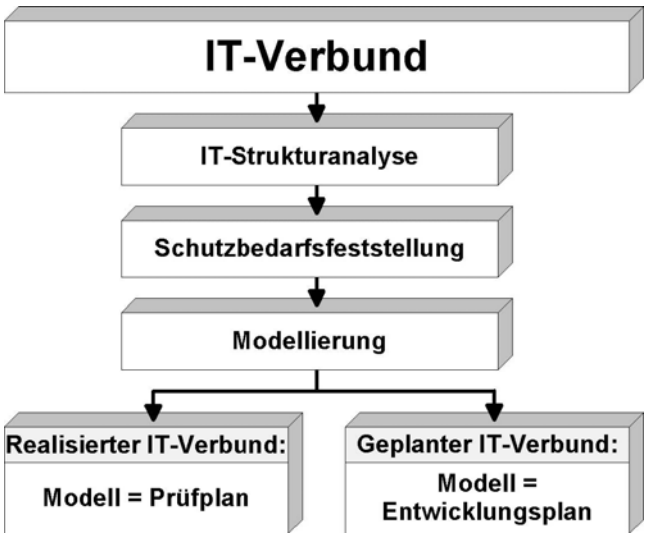
M 6: Förebyggande av nödsituationer

4.3.2 Modellering av ett IT-nätverk

Den framtagna IT-grundskyddsmodellen är oberoende av huruvida IT-nätverket består av IT-system som redan används eller huruvida det är fråga om ett IT-nätverk som ännu är i planeringsfasen. Modellen kan däremot användas på olika sätt:

- Ett redan infört IT-nätverks IT-grundskyddsmodell identifierar de relevanta standardsäkerhetsåtgärderna via de använda komponenterna. Den kan användas i form av en **kontrollplan** för att utföra en bör-är-jämförelse.
- Ett planerat IT-nätverks IT-grundskyddsmodell utgör däremot ett **utvecklingskoncept**. Den beskriver via de utvalda komponenterna vilka standardsäkerhetsåtgärder som måste införas när IT-nätverket ska genomföras.

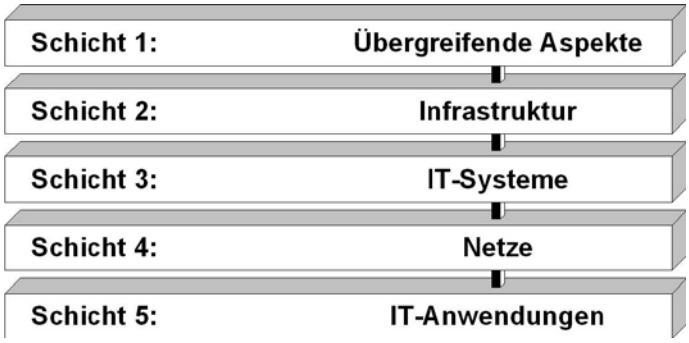
Figuren nedan förtydligar modelleringens placering och de möjliga resultaten:



Figur: Resultat av modellering enligt IT-grundskydd

Normalt kommer ett IT-nätverk som används att innehålla såväl genomförda delar som planerade delar. IT-grundskyddsmodellen innehåller då såväl en kontrollplan som andelar av ett utvecklingskoncept. Alla IT-säkerhetsåtgärder som är förutsedda i kontrollplanen respektive i utvecklingskonceptet utgör en gemensam bas för framtagning av IT-säkerhetskonceptet. Dit hör förutom de redan genomförda säkerhetsåtgärderna de som vid genomförandet av bör-är-jämförelsen identifierades som otillräckliga eller saknade samt de som är ett resultat av de delar av IT-nätverket som planeras.

För att i en figur visa ett allmänt komplext IT-nätverk på IT-grundskydds komponenter är det lämpligt att betrakta IT-säkerhetsaspekterna grupperade efter bestämda teman.



Figur: IT-grundskyddsmodellens skikt

Ett IT-nätverks IT-säkerhetsaspekter tillordnas de enskilda skikten enligt nedan:

- Skikt 1 omfattar de övergripande IT-säkerhetsaspekterna vilka gäller lika mycket för samtliga eller stora delar av IT-nätverket. Det gäller speciellt övergripande koncept och de därur härledda reglerna. Typiska komponenter i skikt 1 är bland annat ledning av IT-säkerhet, organisation, backup-koncept och datorviruskoncept.
- Skikt 2 behandlar byggnadsförhållanden med hänsyn till den infrastrukturella säkerheten. Det gäller speciellt komponenterna byggnad, serverrum, skyddsskåp och hemarbetsplatser.

- Skikt 3 gäller de IT-nätverkets enskilda IT-system som vid behov har sammanfattats i grupper. Här behandlas säkerhetsaspekterna såväl för klienter som för servrar men även för system på enarbetsplatser. I detta skikt finns exempelvis komponenterna telekommunikationssystem, bärbar dator samt klient under Windows 2000.
- Skikt 4 ser på nätaspekter hos IT-systemen som inte refererar till bestämda IT-system utan till nätförbindelserna och kommunikationen. Dit hör till exempel komponenterna heterogena nät, modem samt remote access.
- Skikt 5 slutligen behandlar de egentliga IT-tillämpningarna som används i IT-nätverket. I detta skikt kan bland annat komponenterna e-post, webbserver, faxserver och databaser användas för modellering.

Indelningen i dessa skikt har följande fördelar:

- IT-säkerhetens komplexitet minskas genom att en förnuftig uppdelning av de enskilda aspekterna görs.
- Eftersom överordnade aspekter och gemensamma infrastrukturella frågeställningar betraktas skilt från IT-systemen undviks redundanser eftersom dessa aspekter endast måste bearbetas en gång och inte upprepat för varje IT-system.
- De enskilda skikten har valts så att ansvaret för de betraktade aspekterna har lagts samman. Skikt 1 gäller IT-användningens principfrågor, skikt 2 området installationsteknik, skikt 3 administratörernas och IT-användarnas nivå, skikt 4 nät- och systemadministratörerna och skikt 5 slutligen de personer som ansvarar för och sköter IT-tillämpningarna.
- På grund av uppdelningen av säkerhetsaspekterna i skikt kan enskilda aspekter i resulterande IT-säkerhetskoncept enklare uppdateras och kompletteras utan att andra skikt berörs i större omfattning.

Modelleringen enligt IT-grundskydd består nu av att för varje skikts komponenter besluta om och hur de kan användas för avbildningen av IT-nätverket. Allt efter betraktad komponent kan denna avbildnings målobjekt vara av olika typ: enstaka affärsprocesser eller komponenter, grupper av komponenter, byggnad, fastigheter, organisationsenheter, osv.

IT-grundskyddsmodellen alltså tillordningen av komponenter till målobjekten bör dokumenteras i form av en tabell med följande kolumner:

- Komponentens nummer och rubrik
- Målobjekt eller målgrupp: Det kan t.ex. vara en komponents eller en grupps identifikationsnummer respektive namnet på en byggnad eller en organisationsenhet.
- Kontaktperson: Denna kolumn är först avsedd som platshållare. Kontaktpersonen bestäms inte inom ramen för modelleringen utan först vid planeringen av den egentliga bör-är-jämförelsen i den grundläggande säkerhetskontrollen.

Information: I denna kolumn kan sidoinformation och motiveringar för modelleringen dokumenteras.

Exempel: Organisations- och förvaltningsverket (OFV) - del 8

Följande tabell är ett utdrag ur modelleringen för den fiktiva myndigheten OFV:

Nr	Komponentens rubrik	Målobjekt/målgrupp	Kontakt-person	Information
1.1	Organisation	Etablering Bonn		Komponenten organisation måste behandlas separat för etableringarna Bonn och Berlin, eftersom i Berlin gäller egna organisatoriska bestämmelser.
1.1	Organisation	Etablering Berlin		
1.2	Personal	Hela OFV		OFV:s personaladministration sker centralt i Bonn.
2.5	Arkiv datamedium	R U.02 (Bonn)		I detta rum förvaras backup-datamedierna
3.203	Bärbar dator	C5		De bärbara datorerna i Bonn respektive Berlin sammanfattas i vardera en grupp.
3.203	Bärbar dator	C6		
5.4	Webbserver	S5		S5 fungerar som server för intranätet.
5.7	Databaser	S5		På server S5 ligger en databas

En detaljerad beskrivning av tillvägagångssättet för modelleringen av ett IT-nätverk finns i IT-grundskydd-katalogerna i kapitlet ”Skiktmodell och modellering”. Aktuell utgåva av IT-grundskydd-katalogerna [GSHB] kan laddas ned från BSI-webbservern. I samband med detta läggs särskild vikt vid förutsättningarna när en enskild komponent ska användas ändamålsenligt och för vilka målobjekt den ska användas.

Punkter att utföra:

- systematiskt gå igenom kapitlet ”Skiktmodell och modellering” i IT-grundskydd-katalogerna
- bestäm för varje komponent i IT-grundskydd-katalogerna för vilka målobjekt i det betraktade IT-nätverket den ska användas
- dokumentera tillordning av komponenter till målobjekt (”IT-grundskydd-modell”) samt motsvarande kontaktperson
- notera för en kompletterande säkerhetsanalys målobjekt som inte kan modelleras på lämpligt sätt.

4.4 Grundläggande säkerhetskontroll

För de följande övervägandena förutsätts det att för ett utvalt IT-nätverk följande delar av IT-säkerhetskonceptet enligt IT-grundskydd har upprättats. Med hjälp av IT-nätverkets IT-strukturanalys har

---

en översikt upprättats över befintlig IT, var den används och IT-tillämpningar som stöds. Med detta som grund har därefter fastställandet av skyddsbehov genomförts vars resultat är en översikt över IT-systemens IT-tillämpningar, lokalerna som används för IT och kommunikationsförbindelserna. Med hjälp av denna information har modelleringen av IT-nätverket enligt IT-grundskydd utförts. Resultatet var en avbildning av det betraktade IT-nätverket på IT-grundskydds komponenter.

Denna modellering enligt IT-grundskydd används nu som kontrollplan för att med hjälp av en bör-är-jämförelse ta reda på vilka standardsäkerhetsåtgärder som är genomförda tillräckligt eller endast otillräckligt genomförda.

Detta kapitel beskriver hur man ska gå tillväga vid genomförandet av grundläggande säkerhetskontroll, den centrala uppgiften för att ta fram ett IT-säkerhetskoncept. Denna grundläggande säkerhetskontroll består av tre olika steg. I det första steget görs de organisatoriska förberedelserna, särskilt väljs de relevanta kontaktpersonerna ut för bör-är-jämförelsen. I det andra steget genomförs den egentliga bör-är-jämförelsen med hjälp av intervjuer och stickprovskontroller. I det sista steget dokumenteras bör-är-jämförelsens resultat inklusive de insamlade motiveringarna.

Därefter beskrivs detaljerat dessa steg i den grundläggande säkerhetskontrollen.

4.4.1 Organisatoriska förarbeten

För att kunna genomföra bör-är-jämförelsen friktionsfritt behövs några förarbeten. Först bör alla interna dokument gås igenom, t.ex. organisationsregler, arbetsanvisningar, säkerhetsanvisningar, handböcker och ”informella” tillvägagångssätt som styr de IT-säkerhetsrelevanta förloppen. Dessa dokument kan vara till hjälp när genomförandegraden bestäms speciellt vid frågor om befintliga organisatoriska regler. Vidare ska det klarläggas vem som för tillfället ansvarar för innehållet för att rätt kontaktpersoner vid behov ska kunna utses.

Därefter bör fastställas om och i vilken omfattning externa institutioner måste delta när genomförande-statusen bestäms. Det kan exempelvis vara nödvändigt vid externa datorcentraler, överordnade myndigheter, företag som sköter IT-verksamheten på entreprenad eller byggmyndigheter som har ansvar för infrastrukturella åtgärder.

Ett viktigt steg innan den egentliga bör-är-jämförelsen genomförs är att ta reda på lämpliga intervjupartners. I detta ärende bör man, för varje enskild komponent som används för modelleringen av det aktuella IT-nätverket, fastställa en huvudkontaktperson.

- För komponenterna i skikt 1 ”Överordnade aspekter” framgår en lämplig kontaktperson i regel direkt av det i komponenten behandlade ämnet. För komponenten B 1.2 Personal bör exempelvis en medarbetare på den ansvariga personalavdelningen väljas som kontaktperson. För konceptkomponenterna, t.ex. komponent B 1.4 Backupkoncept finns i bästa fall den medarbetare tillgänglig som är ansvarig för utformningen av aktuellt dokument. I annat fall bör den medarbetare tillfrågas vars arbetsuppgifter omfattar utformning av regler för aktuellt område.
- I området för skikt 2 ”Infrastruktur” bör valet av lämpliga kontaktpersoner ske i samråd med avdelningen kontorsservice/installationsteknik. Allt efter den betraktade institutionens storlek kan exempelvis olika kontaktpersoner finnas för infrastrukturområdena kabelnät och skyddsskåp. På små institutioner kan kontorsansvarig ofta lämna information. Beträffande området infrastruktur bör man i vissa fall tänka på att involvera externa enheter. Det gäller speciellt större företag och myndigheter.
- I komponenterna i skikt 3 ”IT-system” och skikt 4 ”Nät” behandlas mer utförligt tekniska aspekter för de säkerhetsåtgärder som ska kontrolleras. I regel kommer därför administratören, av den komponent respektive grupp av komponenter som har tillordnats respektive komponent vid modelleringen, i fråga som huvudkontaktperson.

• För komponenterna i skikt 5 ”IT-tillämpningar” bör de som handhar respektive de som ansvarar för de enskilda IT-tillämpningarna väljas som huvudkontaktpersoner.

I många fall kan huvudkontaktpersonen inte lämna omfattande information rörande alla frågor beträffande aktuell komponent. Då är det en fördel att intervjua ytterligare en eller flera personer. Anvisningar om vilka medarbetare som bör väljas finns i avsnitten ”Ansvarig för initiering” och ”Ansvarig för genomförande” vilka finns i början av varje åtgärdsbeskrivning.

En tidplan bör upprättas för de intervjuer som ska hållas med de systemansvariga, administratörerna och andra kontaktpersoner. Här gäller det att man är uppmärksam på att koordinera tider med personer från andra organisationsenheter eller andra institutioner. Dessutom är det klokt att bestämma alternativa tider.

Allt efter projektgruppens storlek bör grupper med olika uppgifter bildas för genomförandet av intervjuerna. Det har visat sig lämpligt att arbeta i grupper om två personer. I samband med detta noterar en person de svar som erhålls och den andra personen ställer de nödvändiga frågorna.

Punkter att utföra:

• gå igenom interna dokument med bestämmelser och regler och klarlägga ansvaret för dessa dokument

• fastställa i vilken omfattning externa enheter måste involveras

• bestämma huvudkontaktperson för varje komponent som används i modelleringen

• stämma av tidplan för intervjuerna

• sammanställa grupp för intervjuer.

4.4.2 Genomförande av bör-är-jämförelsen

Om alla erforderliga förarbeten har utförts kan det egentliga insamlandet starta vid de tidigare fastställda tidpunkterna. För detta ändamål gås respektive komponents åtgärder, för vilka respektive intervjupartner är ansvarig, igenom i tur och ordning.

Som svar beträffande genomförandestatusen för de enskilda åtgärderna finns följande uttalanden:

”umbärlig”	-	Genomförandet av åtgärdsrekommendationerna av den föreslagna typen är inte nödvändiga, eftersom de motsvarande hoten motverkas genom andra adekvata åtgärder (t.ex. genom åtgärder som inte är upptagna i IT-grundskydd men som har samma verkan), eller åtgärdsrekommendationerna inte är relevanta (t.ex. eftersom tjänster inte har aktiverats).
”ja”	-	Alla rekommendationer i åtgärden har genomförts fullständigt och verksamt.
”delvis”	-	Några av rekommendationerna har genomförts, andra ännu inte eller endast delvis.
”nej”	-	Åtgärdernas rekommendationer har till största delen ännu inte genomförts.

Vid intervjuerna är det inte lämpligt att läsa åtgärdsrekommendationens text eftersom den inte är utformad för en dialog. Därför är det nödvändigt att den som intervjuar har kunskap om komponentens innehåll och som komplement bör hanterliga checklistor med stickord upprättas innan intervjuerna genomförs. För att i tveksamma fall kunna reda ut diskrepanser är det däremot klokt att ha hela åtgärdstexten tillgänglig. Under intervjun är det inte lämpligt att direkt mata in svaren i en pc eftersom det distraherar alla delta-

---

garna och ger oönskade avbrott i kommunikationen.

Intervjun kan genomföras i en avslappnad och produktiv arbetsatmosfär om den inleds med några inledande ord och syftet med den grundläggande säkerhetskontrollen presenteras. Det är bra att fortsätta med åtgärdsrubriken och kortfattat förklara åtgärden. I stället för att föra en monolog är det bättre att ge motparten möjligheten att gå in på de redan genomförda åtgärdsdelarna och därefter gemensamt diskutera kvarvarande punkter.

Intervjuns omfattning bestäms först av nivån på standardsäkerhetsåtgärderna och vidare aspekter beträffande tillämpningar med stort skyddsbehov bör först beaktas efter att den grundläggande säkerhetskontrollen är genomförd. Om det finns behov att verifiera de uttalanden som har gjorts under intervjuerna är det lämpligt att: stickprovsmässigt se på de motsvarande reglerna och koncepten, inom området infrastruktur gemensamt med kontaktpersonen på plats besiktiga de projekt som ska kontrolleras samt att kontrollera klient- respektive serverinställningar på utvalda IT-system.

Som avslutning på varje åtgärd bör de tillfrågade meddelas hur resultatet har utfallit (genomförandestatus för åtgärden: umbärlig/ja/delvis/nej) och detta beslut förklaras.

Punkter att utföra:

- beroende på ämnesområde i förväg upprätta checklistor
- förklara den grundläggande säkerhetskontrollens målsättning för dem som intervjuas
- ta reda på genomförandestatusen för de enskilda åtgärderna
- verifiera svar utifrån stickprov på objektet
- meddela resultat till dem som har intervjuats.

4.4.3 Dokumentation av resultaten

Resultaten av den grundläggande säkerhetskontrollen bör dokumenteras så att de kan uppfattas av alla deltagare och att de kan användas för planering av genomförandet av de åtgärder som saknas. För att underlätta dokumentationen av den grundläggande säkerhetskontrollens resultat erbjuder BSI två hjälpmedel.

Det är dels BSI-verktyget till IT-grundskydd (GSTOOL). Detta är ett stöd för hela tillvägagångssättet enligt IT-grundskydd och börjar med inventeringen av huvuddata och går vidare via fastställandet av skyddsbehovet, bör-är-jämförelsen (grundläggande säkerhetskontroll) samt genomförandet av åtgärderna och vidare till den avlutande säkerhetsrevisionen. Härigenom erhålls goda möjligheter för utvärdering och revision av resultaten, t.ex. sökning av bestämda noteringar, generering av rapporter, kostnadsutvärderingar samt statistikfunktioner.

Dessutom finns formulär tillgängliga som hjälpmedel till IT-grundskyddet. Till varje komponent i IT-grundskydd finns det en fil i wordformat i vilken resultaten av bör-är-jämförelsen kan registreras i tabellform för komponentens alla åtgärder.

Först bör följande noteras i de därför avsedda fälten i GSTOOL eller i formulären

- numret eller beteckningen på komponenterna eller gruppen av komponenter som tillordnades komponenten vid modelleringen
- platsen för de tillordnade komponenterna respektive gruppen av komponenter
- inventeringsdatum och namnet på den som utfört inventeringen samt

---

• de intervjuade kontaktpersonerna.

De egentliga resultaten av bör-är-jämförelsen läggs in tabellen som är förberedd på formuläret. I samband med detta bör, för varje åtgärd hos respektive komponent, fälten fyllas i enligt nedan:

• Genomförandegrad (umbärlig/ja/delvis/nej)

Här registreras den vid intervjun fastställda genomförandestatusen hos respektive åtgärd.

• Genomförande till

Detta fält fylls i allmänhet inte i under den grundläggande säkerhetskontrollen. Den reserverar plats för att i genomförandefasen på denna plats dokumentera till vilken tidpunkt åtgärden bör vara helt genomförd.

• Ansvarig person

Om det vid genomförandet av bör-är-jämförelsen är entydigt vilken medarbetare som kommer att ha ansvar för det fullständiga genomförandet av en saknad åtgärd så kan det dokumenteras i detta fält. Om ansvaret inte kan fastställas entydigt bör fältet förbli tomt. Senare under genomförandefasen noteras i fältet namnet på den person som har utsetts som ansvarig.

• Anmärkningar/motivering för icke-genomförande

För åtgärder vars genomförande visar sig umbärligt ska motiveringen respektive reservåtgärden anges. För åtgärder som ännu inte eller endast delvis har genomförts bör det i detta fält dokumenteras vilka rekommenderade åtgärder som ännu måste genomföras. I detta fält bör även noteras alla andra anmärkningar som är till hjälp för åtgärdande av saknade åtgärder eller som ska beaktas i samband med åtgärden.

• Kostnadsbedömning

För åtgärder som ännu inte eller endast delvis har genomförts kan en uppskattning noteras i detta fält beträffande ekonomiska och personella insatser som krävs för att åtgärda det som saknas.

Punkter att utföra:

• notera huvudinformation avseende verktyg, databas eller formulär

• notera information som rör den grundläggande säkerhetskontrollen och genomförandestatusen

• förutse fält respektive platshållare för genomförandeplaneringen.

4.5 Integrering av den kompletterande säkerhetsanalysen i IT-grundskydd-tillvägagångssättet

IT-grundskydds standardsäkerhetsåtgärder är i regel anpassade till och tillräckliga för typiska IT-tillämpningar och IT-system med normalt skyddsbehov. I bestämda fall måste dessa IT-grundskydd-åtgärder kompletteras med speciella IT-säkerhetsåtgärder med hjälp av en kompletterande riskanalys.

Dessutom ska det avgöras huruvida detta krävs ytterligare riskbedömningar för IT-nätverkets alla målobjekt som:

• har ett stort eller mycket stort skyddsbehov beträffande ett av de tre grundvärdena konfidentialitet, riktighet och tillgänglighet eller som

• med IT-grundskydds existerande komponenter inte kan avbildas (modelleras) i tillräcklig omfattning eller som

• används i användningsscenarier (miljö, tillämpning) som inte är förutsedda inom ramen för IT-

---

grundskydd.

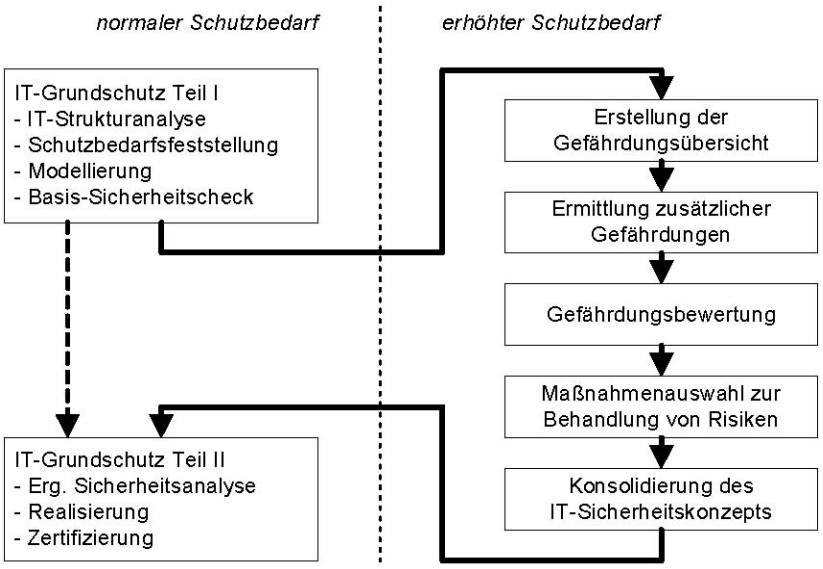
Exempel på tillämpningar eller IT-system, för vilka en kompletterande säkerhetsanalys rekommenderas, är Internetbanker och IT-system med speciella realtidsoperativsystem.

I en ledningsrapport ska det för varje målobjekt, som har en eller flera av ovanstående egenskaper, välgrundat motiveras huruvida det krävs en ytterligare riskbedömning. Målobjekten som gör en ytterligare riskbedömning nödvändig sammanfattas till riskområden. Det bör därvid vara tydligt för vilka områden en ytterligare riskbedömning är nödvändig.

Ledningsrapporten kommuniceras med institutionens ledning och måste godkännas av denna. Ledningen övertar därmed ansvaret.

BSI rekommenderar här att en *riskanalys som bygger på IT-grundskydd* används. Tillvägagångssättet finns publicerat som pdf-fil på BSI:s webbserver samt på BSI:s cd.

Den där beskrivna metodiken går att integrera i IT-grundskydd-processen enligt följande:



En framträdande fråga är: Vilka hot för IT-nätverket har genom IT-grundskydds standardsäkerhetsåtgärder ännu inte beaktats tillräckligt eller till och med inte alls?

För att få svar på denna fråga rekommenderar *riskanalysen som bygger på IT-grundskydd* följande extra arbetssteg som här anges kortfattat:

• Upprättande av översikten över hot

I detta första arbetssteg sammanställs för varje målobjekt som ska analyseras en lista på de respektive relevanta IT-grundskydd-hoten.

• Inventering av ytterligare hot

Hoten som har hämtats från IT-grundskydd kompletteras i detta steg genom extra hot som erhålls från det specifika användningsscenariet. Detta sker inom ramen för en gemensam brainstorming.

• Hotbedömning

För varje målobjekt och för varje hot kontrolleras huruvida de hittills förutsedda IT-säkerhetsåtgärderna ger ett tillräckligt skydd. Kontrollkriterierna är där fullständighet, mekanismstyrka och tillförlitlighet.

• Val av åtgärder för hantering av risker

Ledningsnivån måste ange hur de registrerade riskerna bör behandlas. I regel utarbetas för detta ändamål förslag och alternativ av IT-säkerhetsledningen. Det finns följande alternativ för hantering av risker:

- risker kan minskas genom motsvarande säkerhetsåtgärder
- risker kan undvikas (t.ex. genom omstrukturering av affärsprocesser eller IT-nätverket)
- risker kan föras över (t.ex. genom att verksamheter läggs ut på entreprenad eller genom försäkringar)
- risker kan accepteras.

Besluten hur de olika IT-säkerhetsriskerna ska hanteras ska dokumenteras i IT-säkerhetskonceptet. I samband med detta måste även restrisken bedömas och tydligt kommenteras.

• Konsolidering av IT-säkerhetskonceptet

Innan den ursprungliga IT-grundskydd-processen kan fortsättas måste det utvidgade IT-säkerhetskonceptet konsolideras. I samband med detta sker en total kontroll av IT-säkerhetsåtgärdernas lämplighet, samverkan, användarvänlighet och rimlighet.

Dessutom förklaras i *riskanalysen som bygger på IT-grundskydd* hur metodiken ska användas när IT-nätverket innehåller målobjekt för vilka det så långt inte finns någon lämplig komponent i IT-grundskydd.

En detaljerad redovisning av metodiken finns i originaldokumentet.

Viktigt: *Riskanalysen som bygger på IT-grundskydd* är ett tillvägagångssätt för att vid behov bestämma IT-säkerhetsåtgärder som går längre än de åtgärder som anges i IT-grundskydd-katalogerna. Fastän denna metodik har förenklats i jämförelse med andra liknande metoder kräver den ofta avsevärda insatser. För att så fort som möjligt åtgärda de viktigaste IT-säkerhetsproblemen är det ofta ändamålsenligt att *först* genomföra IT-grundskydd helt och först *därefter* genomföra en kompletterande säkerhetsanalys (avvikande från schemat ovan). Därigenom måste visserligen några steg totalt genomlöpas fler gånger, IT-grundskydd-åtgärderna genomförs dock tidigare. Denna alternativa ordningsföljd är särskilt lämplig när

1. det betraktade IT-nätverket redan är genomfört och i drift och
2. och de föreliggande målobjekten kan modelleras tillräckligt med IT-grundskydds existerande komponenter.

För planerade IT-nätverk eller för sådana med atypiska tekniker respektive användningsscenarier rekommenderas däremot den ovan avbildade ursprungliga ordningsföljden. Följande tabell sammanfattar respektive för- och nackdelar hos de båda alternativa ordningsföljderna:

Riskanalys direkt enligt den grundläggande säkerhetskontrollen	Riskanalys efter fullständigt genomförande av IT-grundskydd-åtgärderna
Möjliga fördelar: - Merkostnader undviks eftersom inga åtgärder genomförs vilka inom ramen för riskanalysen eventuellt ersätts genom kraftfullare åtgärder. - Eventuellt erforderliga åtgärder för hög säkerhet identifieras och genomförs tidigare.	Möjliga fördelar: - IT-grundskydd-åtgärder genomförs tidigare eftersom riskanalysen ofta är dyrbar. - Elementära säkerhetsluckor behandlas med hög prioritet innan avancerade hot analyseras.
Möjliga nackdelar: - IT-grundskydd-åtgärder genomförs senare eftersom riskanalysen ofta är dyrbar. - Eventuellt negligeras elementära säkerhetsluckor medan avancerade hot analyseras.	Möjliga nackdelar: - Merkostnader kan uppstå eftersom några IT-grundskydd-åtgärder genomförs vilka inom ramen för riskanalysen senare ersätts genom kraftfullare åtgärder. - Eventuellt erforderliga åtgärder för hög säkerhet identifieras och genomförs först senare.

Viktigt är dessutom att en r*iskanalys på grundval av IT-grundskydd* ofta är lättare att genomföra när den används i en följd för små delar av IT-nätverket. I ett första steg kan analysen exempelvis begränsas till den fysiska infrastrukturen dvs. till skyddet mot brand, vatten och obehörigt tillträde samt till korrekt el- och klimatförsörjning.

Punkter att utföra:

• fastställa för vilka målobjekt en riskanalys ska genomföras och dokumentera motivering

• ta beslut huruvida riskanalyserna genomförs före eller efter genomförandet av IT-grundskydd-åtgärderna

• systematiskt arbeta igenom BSI-dokumentet ”Riskanalys på grundval av IT-grundskydd” eller bestämma tid för senare genomgång

• integrera riskanalysernas resultat i IT-säkerhetskonceptet.

4.6 Genomförande av IT-säkerhetsåtgärderna

I detta kapitel presenteras olika aspekter som måste beaktas när IT-säkerhetsåtgärder genomförs. Det beskrivs hur genomförandet av IT-säkerhetsåtgärder som har konstaterats ej vara beaktade kan planeras, genomföras, följas och kontrolleras.

Innan genomförandet av IT-säkerhetsåtgärder kan påbörjas måste IT-strukturanalysen, fastställande av skyddsbehov och modelleringen ha utförts för det undersökta IT-systemet eller det undersökta IT-nätverket. Likaså måste den grundläggande säkerhetskontrollens resultat, alltså den därtill anslutande bör-är-jämförelsen, föreligga. Skulle en kompletterande säkerhetsanalys ha utförts för utvalda områden på grund av ett större skyddsbehov så bör de därvid utarbetade åtgärdsförslagen likaså föreligga och därefter beaktas.

Ska ett stort antal åtgärder genomföras och finns det eventuellt endast begränsade resurser tillgängliga i

form av pengar och personal så kan genomförandet av IT-säkerhetsåtgärderna utföras på det sätt som beskrivs i stegen nedan. Ett exempel som förklarar tillvägagångssättet finns i slutet av detta kapitel.

Om endast få saknade åtgärder, vars genomförande endast kräver små ekonomiska eller personella resurser, har identifierats kan ofta ett ad hoc-beslut tas om vem som ska genomföra dessa åtgärder och till vilken tidpunkt. Detta kan enkelt och okomplicerat dokumenteras i bör-är-jämförelsens tabeller. I detta fall kan de följande stegen 1, 3 och 4 slopas.

Steg 1: Urval av undersökningsresultaten

Vid en total genomgång bör först de saknade eller endast delvis genomförda IT-grundskydd-åtgärderna bedömas. För att göra det är det lämpligt att ur den grundläggande säkerhetskontrollens resultat extrahera alla inte genomförda respektive endast delvis genomförda åtgärder inklusive deras prioriteter och sammanfatta i en tabell.

Genom kompletterande säkerhetsanalyser kan eventuellt ytterligare åtgärder, som ska genomföras, ha identifierats. Dessa bör likaså noteras i en tabell. Dessa extra åtgärder bör efter ämne tillordnas modelleringens tidigare betraktade målobjekt och de motsvarande IT-grundskydd-komponenterna.

Steg 2: Konsolidering av åtgärderna

I detta steg konsolideras först de IT-säkerhetsåtgärder som ännu ska genomföras. Om extra säkerhets-analyser har genomförts kan IT-säkerhetsåtgärder härigenom ha tillkommit. Dessa kompletterar eller ersätter åtgärder från IT-grundskydd-katalogerna. Härvid kontrolleras för vilka IT-grundskydd-åtgärder genomförandet kan slopas eftersom mer värdefulla IT-säkerhetsåtgärder ersätter dem.

Eftersom IT-grundskydd ger rekommendationer för ett stort antal olika organisationsformer och tekniska utföranden måste de valda åtgärderna eventuellt konkretiseras respektive anpassas till de organisatoriska och tekniska förhållandena som råder inom institutionen. Dessutom bör alla IT-säkerhetsåtgärder en gång till kontrolleras beträffande deras lämplighet. De måste verksamt skydda mot de möjliga hoten men även vara praktiskt användbara. De får alltså t.ex. inte hindra metoder och procedurer eller eliminera andra säkerhetsåtgärder. I sådana fall kan det bli nödvändigt att ersätta vissa IT-grundskydd-åtgärder med andra adekvata IT-säkerhetsåtgärder.

För att även senare kunna förstå hur den konkreta åtgärdslistan upprättades och förfinades ska detta dokumenteras på lämpligt sätt.

Exempel:

- I en kompletterande säkerhetsanalys har fastställts att det som ett komplement till IT-grundskyddsåtgärderna även är nödvändigt med en autenticering med aktivt kort och lokal kodning av hårddiskar på NT-klienter för bearbetning av personaldata. Denna extra åtgärd skulle ersätta åtgärden M 4.48 *Lösenordsskydd under Windows NT*.

- I den grundläggande säkerhetskontrollen har fastställts att åtgärden M 1.24 *Undvikande av vattenförande ledningar* inte har genomförts och inte kan genomföras ekonomiskt till följd av de byggnadstekniska förutsättningarna. I stället bör som ersättningsåtgärd avledande plåtar installeras under de vattenförande ledningarna och plåtarna samtidigt övervakas med en vattenvarnare. Varnaren ger en signal så att den vattenskada som uppstår vid en skada snabbt upptäcks och då kan begränsas.

Steg 3: Uppskattning av kostnader och insatser

Eftersom budgeten för genomförande av IT-säkerhetsåtgärder i praktiken alltid är begränsad bör det för varje åtgärd som ska genomföras noteras vilka investeringar och personella insatser som behövs. Här bör

man skilja mellan investeringar respektive personella insatser som förekommer en gång eller som återkommer. I detta sammanhang visar det sig ofta att besparingar när det gäller teknik orsakar en fortlöpande hög personell insats.

I detta sammanhang ska man ta reda på huruvida alla identifierade åtgärder är ekonomiskt genomförbara. Om det finns åtgärder som inte kan finansieras bör det övervägas genom vilka reservåtgärder de kan ersättas eller om restrisken som uppstår genom den saknade åtgärden är acceptabel. Detta beslut ska likaså dokumenteras.

Finns de uppskattade resurserna för kostnader och personella insatser till förfogande så kan nästa steg påbörjas. I många fall måste dock ännu ett beslut tas nämligen hur mycket resurser som ska sättas in för genomförandet av IT-säkerhetsåtgärderna. Här är det lämpligt att för beslutsfattaren (ledningen, IT-chef, IT-säkerhetsansvarig, …) förbereda en presentation i vilken resultaten från säkerhetsundersökningen visas. Ordnade efter skyddsbehov bör de konstaterade svaga punkterna (saknade eller otillräckligt genomförda IT-säkerhetsåtgärder) presenteras för att öka beslutsfattarens medvetande. Dessutom är det lämpligt att ta fram de kostnader som uppkommer för genomförandet av de saknade åtgärderna. I anslutning till denna presentation bör ett budgetbeslut tas.

Om tillräckliga medel inte kan ställas till förfogande för genomförande av alla saknade åtgärder så bör det noteras vilken restrisk som i så fall finns om några åtgärder inte genomförs eller genomförs senare. För detta syfte kan åtgärds-hot-tabellerna i hjälpmedlen till IT-grundskydd användas för att bestämma vilka hot som inte längre täcks tillräckligt. Restrisken som uppkommer bör beskrivas tydligt för tillfälligt uppkommande eller avsiktligt utlösta hot och presenteras för ledningsnivån för beslut. De följande stegen kan först utföras efter ledningsnivåns beslut att restrisken är acceptabel eftersom ledningsnivån måste ta ansvar för konsekvenserna.

Steg 4: Fastställa i vilken ordningsföljd åtgärderna genomförs

När den aktuella budgeten eller de personella resurserna inte är tillräckliga för att genast kunna genomföra samtliga saknade åtgärder måste en ordningsföljd för genomförandet fastställas. När ordningsföljden fastställs bör följande aspekter beaktas:

- Ordningsföljden för genomförande bör först vara orienterad efter hur livscykeln ser ut för åtgärderna. I varje komponent finns det en översikt över vilka åtgärder som bör genomföras i vilken livscykelfas, dvs. ordningsföljden i tiden. Det är naturligt att starta med åtgärderna i fasen ”planering och koncept” innan man arbetar med de i faserna ”genomförande” och ”drift”.
- För varje åtgärd anges dessutom en klassificering i vilken mån de behövs för IT-grundskydd-kvalificeringen. Kvalificeringsnivån (A-start, B-påbyggnad, C-certifikat, Z-tillägg) för en åtgärd ger ofta information om den vikt som den respektive åtgärden har i IT-säkerhetskonceptet. A-åtgärder är i många fall särskilt viktiga och bör därför genomföras med hög prioritet.
- För några åtgärder erhålls en tvingande tidsmässig ordningsföljd till följd av logiska sammanhang. Så är visserligen åtgärderna M 2.25 *Dokumentation av systemkonfigurationen* och *M 2.26 Utse en administratör och en ställföreträdare* båda mycket viktiga men utan administratör kan M 2.25 knappast genomföras.
- Åtskilliga åtgärder har en stor inverkan på flera områden, åtskilliga däremot endast en begränsad lokal verkan. Ofta är det ändamålsenligt att tänka på inverkan på flera områden.
- Det finns komponenter som har större inverkan på den eftersträvade säkerhetsnivån än vad andra har. En sådan komponents åtgärder ska behandlas prioriterat särskilt om svaga punkter inom områden med stort skyddsbehov härigenom elimineras. Så bör man alltid först säkra servrarna (t.ex. genom att genomföra

komponenten B 3.102 Server under Unix) och först därefter de anslutna klienterna.

- Komponenter med påfallande många saknade åtgärder representerar områden med många svaga punkter. De bör likaså behandlas prioriterat.

Beslutet vilka säkerhetsåtgärder som ska tillämpas eller skjutas upp och var restrisker accepteras bör även dokumenteras noggrant till följd av juridiska skäl. I tveksamma fall bör här ytterligare synpunkter hämtas in och likaså dokumenteras för att i senare tvister kunna visa att erforderlig aktsamhet har iakttagits.

Steg 5: Fastställa uppgifterna och ansvaret

När ordningsföljden i vilken åtgärderna ska genoföras har bestämts måste man därefter fastställa vem som måste genomföra vilka åtgärder och till vilken tidpunkt. Utan att ha fastställt detta fördröjs genomförandet erfarenhetsmässigt avsevärt respektive sker inte alls. Man ska därvid tänka på att den som har utsetts som ansvarig har tillräcklig kompetens och befogenheter för att genomföra åtgärderna samt att erforderliga resurser ställs till dennes förfogande.

Likaså ska det fastställas vem som ansvarar för kontrollen av genomförandet respektive till vem man ska anmäla att de enskilda åtgärderna har genomförts. Normalt lämnas meddelandet till den IT-säkerhetsansvarige. En regelbunden kontroll av hur genomförandet fortlöper bör ske så att genomförandeuppdragen inte drar ut på tiden.

Den nu färdigställda genomförandeplanen bör minst innehålla följande information:

- beskrivning av målobjektet som användningsmiljö
- den betraktade komponentens nummer
- åtgärdsrubrik respektive åtgärdsbeskrivning
- tidplan för genomförandet
- budgetram
- ansvariga för genomförandet och
- ansvariga för kontrollen av genomförandet.

Steg 6: Åtgärder i anslutning till genomförandet

Det är synnerligen viktigt att i god tid utforma åtgärder i anslutning till genomförandet och planera dem tillsammans med genomförandet. Till dessa åtgärder hör speciellt åtgärder för att öka medvetandet vilka har som mål att instruera de medarbetare som berörs av nya IT-säkerhetsåtgärder beträffande att åtgärderna är nödvändiga och konsekvenserna av dem samt öka deras medvetande om vikten av IT-säkerhet.

Dessutom måste de berörda medarbetarna utbildas i att genomföra och använda de nya IT-säkerhets-åtgärderna. Om denna utbildning inte genomförs kan åtgärderna inte genomföras och har inte någon verkan. Vidare skulle medarbetarna känna att de inte har fått tillräcklig information vilket ofta leder till en avvisande hållning gentemot IT-säkerhet.

När de nya IT-säkerhetsåtgärderna har genomförts och introducerats bör den IT-säkerhetsansvarige kontrollera att den nödvändiga acceptansen finns hos medarbetarna. Om det visar sig att de nya åtgärderna

---

inte accepteras betyder det ett förprogrammerat misslyckande. Orsakerna ska utredas och åtgärdas. Ofta räcker det att de berörda erhåller extra information.

Exempel:

För att närmare beskriva stegen ovan beskrivs nedan ett fiktivt exempel i sammandrag. Först bör tabellen med de konsoliderade åtgärderna som ska genomföras inklusive kostnadsuppskattningarna, som är ett resultat av stegen 1 - 3, visas:

Målobjekt	Komponent	Åtgärd	Prioritet			Kostnad	Anmärkning
			1	2	3		
Hela organisationen	B 1,9:	M 2.11 Reglering av användningen av lösenord	T			a) 0 euro b) 2 AD c) 0 euro/år d) 0 AD/år	
Serverrum R 3.10	B 2,4:	M 1.24 Undvikande av vattenförande ledningar			F	a) 20000 euro b) 12 AD c) 0 euro/år d) 0 AD/år	Denna åtgärd är inte ekonomiskt genomförbar. Som ersättning genomförs åtgärd Z 1.
Serverrum R 3.10	B 2,4:	Z 1 Installation av vattenavledande plåtar med övervakning genom vattenvarnare och signal till övervakningsrum				a) 4000 euro b) 3 AD c) 0 euro/år d) 0 AD/år	Ersätter åtgärd M 1.24
Server S4	B 3.101	M 1.28 Lokal avbrottsfri elförsörjning	F			a) 1000 euro b) 1 AD c) 0 euro/år d) 0 AD/år	
Grupp klienter C1	B 3.207	Z 2 autenticering med aktiva kort och lokal kodning av hårddiskarna				a) 1400 euro b) 2 AD c) 0 euro/år d) 2 AD/år	Denna extra åtgärd ersätter åtgärden M 4.1 i komponent B 1.9.

Förklaring:

• Åtgärd

Z 1 = Tilläggsåtgärd 1 (tillägg till IT-grundskydd-åtgärder)

• Prioriteter

T = delvis uppfylld, F = saknas, är inte genomförd

• Kostnader:

a) = engångsinvestering

b) = personell insats en gång (AD = arbetsdagar)

---

c) = återkommande investering

d) = återkommande personell insats (AD = arbetsdagar)

Därefter visas en genomförandeplan vilken efter ledningsbeslutet skulle erhållas ur tabellen ovan.

Genomförandeplan (version 01.09.2004)						
Målobjekt	Komponent	Åtgärd	Genomförande till	Ansvarig	Budgetram	Anmärkning
Hela organisationen	B 1.9	M 2.11 Reglering av användningen av lösenord	31.12.04	a) Müller b) Meier	a) 0 euro b) 2 AD c) 0 euro/år d) 0 AD/år	
Serverrum R 3.10	B 2.4	Z 1 Installation av vattenavledande plåtar med övervakning genom vattenvarnare och signal till övervakningsrum	30.04.05	a) Schmitz b)Hofmann	a) 1000 euro b) 1 AD c) 0 euro/år d) 0 AD/år	Installation av plåtarna enbart under ledningar med färsk- och avloppsvatten
Server S4	B 3.101	M 1.28 Lokal avbrottsfri elförsörjning	31.10.04	a) Schulz b) Meier	a) 500 euro b) 1 AD c) 0 euro/år d) 0 AD/år	
Grupp klienter C1	B 3.207	Z 2 autenticering med aktiva kort och lokal kodning av hårddiskarna	31.12.04	a) Schulz b) Meier	a) 1400 euro b) 2 AD c) 0 euro/år d) 2 AD/år	

Förklaring:

• Ansvarig person:

a) = ansvarig för genomförande av åtgärden

b) = ansvarig för kontroll av genomförandet

• Budgetram: För genomförandet av åtgärden finns till förfogande

a) = engångsinvestering

b) = personell insats en gång (AD = arbetsdagar)

c) = återkommande investering

d) = återkommande personell insats (AD = arbetsdagar)

Punkter att utföra:

- sammanfatta saknade eller endast delvis genomförda IT-grundskydd-åtgärder eller kompletterande säkerhetsåtgärder i en tabell
- konsolidera IT-säkerhetsåtgärder, dvs. stryka överflödiga åtgärder, anpassa allmänna åtgärder till förhållandena och kontrollera att alla åtgärder är ändamålsenliga
- bestämma engångskostnader och återkommande kostnader samt insatser för åtgärderna som ska genomföras
- bestämma reservåtgärder för åtgärder som inte kan finansieras eller utföras
- få till stånd beslut, vilka resurser som bör sättas in för att genomföra åtgärderna
- vid behov visa restrisk och inhämta ledningsnivåns beslut
- fastställa ordningsföljden för genomförandet av åtgärderna, motivera och dokumentera
- bestämma tidpunkter för genomförandet och anvisa ansvar
- kontrollera genomförandeförlopp och att tidplan innehålls
- utbilda och öka medvetandet hos berörda medarbetare
- kontrollera huruvida IT-säkerhetsåtgärderna accepteras och vid behov förbättra.

5 Upprätthålla IT-säkerheten och kontinuerliga förbättring

För att kunna upprätthålla IT-säkerhetsprocessen och kontinuerligt förbättra den måste inte enbart lämpliga IT-säkerhetsåtgärder implementeras och dokument fortlöpande uppdateras utan IT-säkerhetsprocessen måste regelbundet kontrolleras med avseende på effektivitet. En resultatkontroll och bedömning av IT-säkerhetsprocessen genom ledningsnivån bör äga rum regelbundet (ledningens bedömning). Vid behov (t.ex. vid ökat antal IT-säkerhetsincidenter eller viktiga ändringar av förutsättningarna) måste sammanträden hållas utöver det planerade sammanträdesprogrammet. Alla resultat och beslut måste dokumenteras så att de är spårbara.

För kontroll och förbättring av IT-säkerhetsprocessens effektivitet bör metoder och mekanismer etableras vilka å ena sidan kontrollerar genomförandet av de beslutade åtgärderna och å andra sidan kontrollerar deras verkan och effektivitet. IT-säkerhetsstrategin bör därför även vara riktlinjer för mätning av att målen uppfylls. Basen för sådana mätningar kan exempelvis vara:

- detektion, dokumentation och utvärdering av IT-säkerhetsincidenter
- genomförande av övningar och tester för simulering av säkerhetsincidenter och dokumentation av resultaten
- interna och externa revisioner
- certifiering enligt fastställda IT-säkerhetskriterier.

Resultatkontrollen för de genomförda åtgärderna bör ske inom ramen för interna revisioner. I samband med detta är det viktigt att sådana revisioner inte utförs av de personer som har utvecklat säkerhets-konceptet. För denna uppgift kan det vara ändamålsenligt att anlita externa experter.

Eftersom insatsen vid revisioner beror på IT-nätverkets komplexitet och storlek går det bra att tillgodose kraven även för små myndigheter och företag. I vissa fall kan det för små institutioner räcka med en årlig teknisk kontroll av IT-systemen, en genomgång av befintlig dokumentation och en workshop vid vilken problem och erfarenheter med IT-säkerhetskonceptet diskuteras.

Punkter att utföra:

- integrera mätning av måluppfyllelsen i IT-säkerhetsstrategin
- kontrollera genomförandet av de beslutade åtgärderna
- kontrollera verkan och effektivitet av de beslutade åtgärderna.

5.1 Kontroll av IT-säkerhetsprocessen på alla nivåer

IT-säkerhetskontrollen ska ovillkorligen kontrolleras så att å ena sidan fel och svaga punkter kan registreras och elimineras och å andra sidan IT-säkerhetsprocessen kan optimeras vad gäller dess effektivitet. Mål är bland annat förbättring av hur strategi, åtgärder och organisatoriska förlopp fungerar i praktiken.

De viktiga aspekterna som därvid måste studeras redovisas nedan.

Införande av genomförandeplanen

Med hjälp av uppgiftslistan och tidplanen som måste ingå i genomförandeplanen går det att kontrollera huruvida och i vilken omfattning denna är uppfylld. En ändamålsenlig resursplanering är en viktig förutsättning för att de planerade IT-säkerhetsåtgärderna ska utföras. Därför är det vid kontrollen klokt att

tänka på huruvida tillräckliga ekonomiska och personella resurser har ställs till förfogande. IT-säkerhets-processens kontroll är inte enbart avsedd för kontroll av aktiviteterna inom ramen för IT-säkerhets-konceptet utan även för att i god tid lägga märke till planeringsfel och för att anpassa IT-strategin om denna visar sig vara orealistisk.

IT-strategins lämplighet

För att framgångsrikt kunna styra IT-säkerhetsprocessen måste institutionsledningen ha en överblick över i vilken omfattning IT-säkerhetsmål kunde uppnås med hjälp av den insatta IT-säkerhetsstrategin.

Uppdatering av säkerhetsmål, förutsättningar och säkerhetskoncept

I ett längre perspektiv är det även nödvändigt att kontrollera de uppsatta IT-säkerhetsmålen och förutsättningarna. Speciellt i snabbt föränderliga branscher är en motsvarande anpassning av IT-säkerhetspolicyn och IT-säkerhetsstrategin i detta fall av elementär betydelse.

Även förändringar inom institutionen (t.ex. användning av nya IT-system) och organisatoriska ändringar (t.ex. lägga ut verksamheter på entreprenad) måste redan vid planeringsfasen integreras i IT-säkerhets-konceptet. IT-säkerhetskonceptet och den tillhörande dokumentationen måste uppdateras efter varje relevant ändring. Detta måste även beaktas i institutionens förändringsprocess. Därför måste IT-säkerhetsprocessen integreras i institutionens förändringshantering.

Lönsamhet

En annan punkt som konstant ska hållas under uppsikt är lönsamheten vad gäller IT-säkerhetsstrategin och specifika IT-säkerhetsåtgärder. Kostnaderna för IT-säkerheten är visserligen svåra att fastställa. För den fortsatta planeringen är det emellertid ofta till hjälp att kontrollera huruvida de faktiskt uppkomna kostnaderna motsvarar de ursprungligen budgeterade kostnaderna eller om andra mindre resurskrävande IT-säkerhetsåtgärder kan införas. Det är likaså viktigt att regelbundet visa nyttan av de befintliga IT-säkerhetsåtgärderna.

Integrering av resultaten i IT-säkerhetsprocessen

Resultatkontrollens resultat är nödvändiga för förbättringen av IT-säkerhetsprocessen. Det kan i samband med detta visa sig att IT-säkerhetsmålen, IT-säkerhetsstrategin eller IT-säkerhetskonceptet bör ändras och att IT-säkerhetsorganisationen bör anpassas till kraven. I vissa fall är det ändamålsenligt att grundläggande förändra IT-miljön eller att förändra affärsprocesser, t.ex. när IT-säkerhetsmål inte eller endast omständ-ligt (och därmed dyrt) kan uppnås. Om stora förändringar utförs och omfattande förbättringar införs sluter sig managementcirkeln åter och planeringsfasen startar på nytt.

Kontrollen av de enskilda ämnena måste utföras av lämpliga personer som garanterar att nödvändig kompetens och oberoende föreligger. Fullständighets- och sannolikhetskontroller bör inte utföras av de personer som har utarbetat konceptet. Kontrollresultat och rapporter ska i allmänhet betraktas som kritiska och konfidentiella och måste därför skyddas särskilt väl.

Punkter att utföra:

- beakta rollkonflikt mellan utfärdare och den som kontrollerar och säkerställ konfidentialitet för undersökningsresultaten
- kontrollera att genomförandeplanen följs
- kontrollera lämplighet och aktualitet för säkerhetsmål, -strategier och -koncept
- kontrollera lämpligheten av resurserna som har ställts till förfogande och lönsamheten för säkerhetsstrategin och –åtgärderna

---

• för över resultaten av kontrollerna till IT-säkerhetsprocessen i form av förbättringar.

5.2 Informationsflöde i IT-säkerhetsprocessen

Rapporter till ledningsnivån

För att företags- respektive myndighetsledningen ska kunna fatta rätt beslut vid styrning av IT-säkerhetsprocessen behöver de nödvändig information. Den ska ha sammanställts i ledningsrapporter som bland annat ska innehålla följande:

• resultat av revisioner

• rapporter över IT-säkerhetsincidenter

• rapporter över hittillsvarande framgångar och problem med IT-säkerhetsprocessen.

Ledningsnivån måste regelbundet och i lämplig form informeras av IT-säkerhetsledningen om resultaten av kontrollerna och IT-säkerhetsprocessens status. Då bör problem, bra resultat och förbättringsmöjligheter redovisas. Ledningsnivån tar till sig ledningsrapporterna och vidtar eventuellt nödvändiga åtgärder.

Dokumentation

Dokumentationen av IT-säkerhetsprocessen på alla nivåer är av flera skäl avgörande för processens framgång. Här gäller bland annat att endast genom tillräcklig dokumentation:

• kan träffade beslut spåras

• kan processer upprepas och standardiseras

• kan brister och fel konstateras så att de kan undvikas i framtiden.

Beroende på en dokumentations innehåll och syfte kan man skilja mellan följande typer av dokumentation:

Teknisk dokumentation och dokumentation av arbetsförlopp (målgrupp: experter)

Här beskrivs aktuell version av affärsprocesser och de därtill kopplade IT-systemen och -tillämpningarna. Ofta är detaljeringsgraden för teknisk dokumentation ett omstritt ämne. En pragmatisk inställning vid utformning av användbar dokumentation är att andra personer med jämförbara kunskaper inom området ska kunna förstå den och att administratören visserligen ska vara hänvisad till sitt kunnande men inte till sitt minne för att åter bygga upp system och tillämpningar. Vid säkerhetsövningar och säkerhetsincidenter bör den tillgängliga dokumentationens kvalitet bedömas och den vunna insikten användas för förbättringar. Till sådan typ av dokumentation hör:

- installations- och konfigurationsanvisningar
- anvisningar för en omstart efter en säkerhetsincident
- dokumentation av test- och godkännademetoder
- anvisningar för förhållningssätt vid störningar och IT-säkerhetsincidenter.

• Anvisningar för IT-användare (målgrupp: IT-användare)

IT-säkerhetsåtgärderna måste dokumenteras på ett för IT-användarna begripligt sätt. Dessutom måste medarbetarna vara informerade om dessa riktlinjers existens och betydelse och de måste ha relevant utbildning så att de utan problem kan följa dem. Denna grupp av dokumentation omfattar:

- arbetsförlopp och organisatoriska föreskrifter
- tekniska IT-säkerhetsåtgärder
- förhållningssätt vid IT-säkerhetsincidenter.

• Dokumentation av ledningsbeslut (målgrupp: ledningsnivå)

IT-säkerhetsstrategi, riktlinjer och andra grundläggande beslut inom IT-säkerhetsprocessen måste dokumenteras så att dessa alltid är spårbara och kan upprepas.

Informationsflöde och rapporteringsvägar

För att upprätthålla IT-säkerhetsprocessen är det av elementär betydelse att direkt uppdatera rapporteringsvägar och tillvägagångssätt för informationsflödet. Där utöver utgör resultaten från utförda övningar, tester och revisioner även en användbar grund för förbättring av informationsflödet.

Utnyttja synergieffekter för informationsflödet

Många institutioner har redan definierat processer för tillhandahållande av servicetjänster eller IT-supporten. Ofta lyckas det att utnyttja synergieffekter för att integrera IT-säkerhetsaspekter i redan befintliga processer. Exempelvis skulle rapporteringsvägar integreras i IT-supporten eller resursplaneringen utökas med aspekter från förebyggande av nödsituationer.

Mycket information som samlas in av säkerhetsskäl kan användas för andra ändamål. IT-säkerhetsåtgärder har även andra positiva sidoeffekter, speciellt optimeringen av processer är värdefull. Exempelvis fastställandet av informationsägare eller inordning av information efter enhetliga bedömningskriterier är relevant för flera områden inom en institution. En översikt över affärsprocessers beroende av IT-system och IT-tillämpningar är likaså inte enbart ändamålsenlig för IT-säkerhetsledningen. Den möjliggör t.ex. även att IT-kostnader fördelas exakt på enskilda affärsprocesser eller produkter i stället för att de fördelas som allmänna omkostnader.

Punkter att utföra:

• informera ledningsnivån om resultaten av kontroller och statusen hos IT-säkerhetsprocessen

• vid behov inhämta beslut avseende erforderliga korrektionsåtgärder

• på ett förståligt sätt dokumentera hela IT-säkerhetsprocessen och hålla informationen uppdaterad

• vid behov bedöma kvaliteten på dokumentationen och eventuellt förbättra eller uppdatera

• uppdatera rapporteringsvägar som gäller för IT-säkerhetsprocessen

• söka synergier mellan IT-säkerhetsprocessen och andra ledningsprocesser.

5.3 IT-grundskydd-certifiering

För att utåt tydligt kunna visa på ett framgångsrikt genomförande av IT-grundskydd-åtgärderna har BSI utvecklat ett certifieringsschema enligt IT-grundskydd. IT-grundskydd-certifikatet eller ett IT-grundskydd-intyg erbjuder företag och myndigheter möjligheten att påvisa vad de företagit med avseende på IT-säkerhet. Det kan utgöra ett kvalitetsmärke vid kontakter med såväl kunder som affärspartners och på så sätt ge konkurrensfördelar.

Intresset för ett IT-grundskydd-certifikat har olika orsaker:

• företag som svarar för IT-verksamheter vill med hjälp av detta certifikat ha ett förtroendegivande bevis på att de har genomfört åtgärderna enligt IT-grundskydd

---

- samarbetande företag vill få information om vilken grad av IT-säkerhet som deras affärspartners kan garantera.
- av institutioner som ansluts till ett nät krävs beviset för att visa att de har en tillräcklig IT-säkerhet så att en anslutning till nätet inte medför att oacceptabla risker uppstår
- företag och myndigheter vill visa kunder respektive allmänheten att de arbetar för en tilläcklig IT-säkerhet.

Eftersom IT-grundskydd med dess rekommendationer avseende standardsäkerhetsåtgärder numera utgör en defactostandard för IT-säkerhet är det lämpligt att använda den som ett allmänt erkänt underlag för IT-säkerhet.

Kostnader och insatser för att erhålla ett IT-grundskydd-certifikat är (jämförelsevis) små. I vissa fall kan det visserligen vara ganska dyrbart för ett företag eller en institution att helt genomföra åtgärdsrekommendationerna i IT-grundskydd-katalogerna. För att även ge dessa organisationer en möjlighet att utåt visa att de jobbar med IT-säkerhet så finns det **två förnivåer** till IT-grundskydd-certifikatet:

- revisionsintyget ”startnivå” kan delas ut när de ovillkorligen nödvändiga standardsäkerhetsåtgärderna enligt IT-grundskydd har genomförts (genomförande av alla åtgärder i steg A)
- revisionsintyget ”påbyggnadsnivå” kan delas ut när de viktigaste standardsäkerhetsåtgärderna enligt IT-grundskydd har genomförts (genomförande av alla åtgärder i steg A och B).

För båda kvalificeringsnivåerna krävs en kontroll genom en extern revisor. Efter att en revisionsrapport har upprättats utifrån revisionsmetodbeskrivningen (i dokumentet ”Certifiering enligt ISO 27001 utifrån IT-grundskydd - kontrollschema för ISO 27001 revisioner”) i vilken kontrollen av genomförandet av alla de för kvalificeringsnivån erforderliga åtgärderna dokumenteras kan intyget utfärdas av en licensierad revisor. Certifieringsorganet kontrollerar inte revisionsrapporter från intyg men kan begära att få se dem för att kunna ställa frågor. Intygen gäller i två år och kan inte förlängas eftersom de är förnivåer till certifikatet. En återkvalificering kan endast göras på en högre nivå.

Grunden för att erhålla ett IT-grundskydd-certifikat är likaså att en revision utförs av en extern revisor som är licensierad hos BSI. Revisionens resultat är en revisionsrapport som presenteras för certifieringsorganet som beslutar om IT-grundskydd-certifikatet ska utdelas. Kriterier för metoden finns förutom i ISO 27001 i det i detta dokument beskrivna IT-grundskydd-tillvägagångssättet och i BSI:s IT-grundskydd-kataloger i respektive aktuell version respektive i de omedelbart föregående versionerna. Revisionsmetodbeskrivningen beskriver tillvägagångssättet för kontroll av revisionsrapporten och för utdelning av IT-grundskydd-certifikatet.

För att bli licensierad IT-grundskydd-revisor måste en revisor först styrka sina kunskaper på området. För att göra det måste kunskaperna som rör IT-grundskydd och kvalificeringsschema visas på ett välunderbyggt sätt. Det är nödvändigt att ha minst två års yrkeserfarenhet inom IT-säkerhet och att ha utfört minst tre projekt relaterade till IT-grundskydd. Dessutom måste de blivande revisorerna delta i en utbildning avseende kvalificeringsschemat. I anslutning till denna utbildning genomför BSI en kontroll av de förvärvade kunskaperna och vid godkänt resultat erhålls licensen. En licens gäller under fem år. Alla licensierade revisorer finns redovisade på en lista som BSI har publicerat på www.bsi.bund.de/gshb/zert.

Med ett IT-grundskydd-certifikat visas att IT-grundskydd med framgång har genomförts i det betraktade nätet. Dessutom visar ett IT-grundskydd-certifikat även att den aktuella institutionen:

- lägger stor vikt vid IT-säkerhet

- har en fungerande styrning av IT-säkerhet och dessutom
- vid en bestämd tidpunkt uppnått en definierad IT-säkerhetsnivå.

Ytterligare information om certifieringen och licensieringen som IT-grundskydd-revisor finns på www.bsi.bund.de/gshb/zert/schema.htm

Punkter att utföra:

- läsa BSI:s information om kvalificerings- och certifieringsschemat för IT-grundskydd
- kontrollera huruvida satsningarna avseende IT-säkerhet bör visas genom ett IT-grundskydd-certifikat eller revisionsintyg
- vid behov kontrollera huruvida IT-säkerhetsledningen och IT-säkerhetsnivån uppfyller de motsvarande förutsättningarna
- vid behov initiera kvalificerings- respektive certifieringsprocessen.