Bundesamt
für Sicherheit in der
Informationstechnik

BSI-standard100-3

Riskanalys på grundval av IT-Grundschutz (IT-grundskydd)

Version 2.0

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

Februari 2004	Version 1.0
December 2005	Version 2,0

1.2 Målsättning

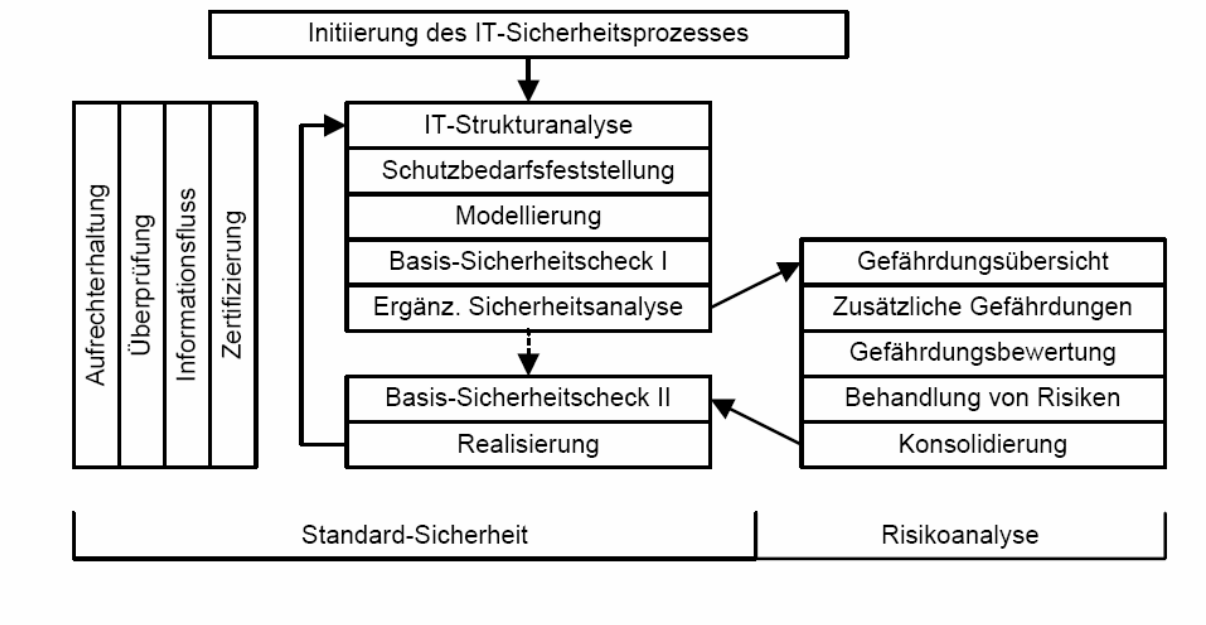
Nedan förklaras en metodik hur en förenklad analys av IT-risker kan utföras med hjälp av de i IT-grundskydd-katalogerna [GS-KAT] angivna hoten. Potentiella användningsområden för en sådan analys är inom myndigheter och företag exempelvis IT-komponenter eller IT-områden

- 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.

I dessa fall är följande frågor aktuella:

- Vilka hot för informationsbearbetningen har genom införandet av de relevanta IT-grundskydd-komponenterna ännu inte beaktats tillräckligt eller till och med inte alls?
- Måste eventuellt extra IT-säkerhetsåtgärder, vilka omfattar med än IT-grundskydd-modellen, planeras och genomföras?

Det föreliggande dokumentet beskriver en metodik som anger hur det för bestämda målobjekt, med en så liten insats som möjligt, kan fastställas huruvida och i vilket avseende det finns ett behov att begränsa IT-risker utöver IT-grundskydd.



I IT-säkerhetshandboken [SHB] och i några andra tillvägagångssätt för risk- och säkerhetsanalys betraktas bland annat även *sannolikheter för inträffande* av skadehändelser för beslut om hantering av risker. I praktiken har det emellertid visat sig svårt att uppskatta dessa sannolikheter eftersom det inte finns underlag för tillförlitliga skattningar. Även tolkningen av sannolikheterna är ofta tveksam. I den här beskrivna metodiken betraktas därför sannolikheter för inträffande inte explicit utan endast implicit inom ramen för inventering och bedömning av risker.

1.3 Målgrupp

Detta dokument riktar sig dem som ansvarar för IT-säkerhet, IT-säkerhetschefer, IT-experter, IT-rådgivare och alla intresserade som har ledningsansvar avseende informationssäkerhet eller som svarar för genomförande av IT-riskanalyser.

Användare av den i detta dokument beskrivna metodiken [GS-VOR] bör vara förtrogna med IT-grundskydd-tillvägagångssättet.

1.4 Tillämpning

Detta dokument beskriver en metodik för genomförande av IT-riskanalyser som kompletterar ett befintligt IT-säkerhetskoncept. Som hjälpmedel används de hot som beskrivs i IT-grundskydd-katalogerna.

Det rekommenderas att steg för steg arbeta igenom metodiken som visas i kapitel 2 - 8.

1.5 Litteraturförteckning

[GS-KAT] IT-Grundschutz-Kataloge, BSI, *http://www.bsi.bund.de/gshb*

[GS-VOR] BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, *http://www.bsi.bund.de/gshb*

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

2 Förarbeten

Innan den egentliga riskanalysen startar bör följande förarbeten, som anges i IT-grundskydd-tillvägagångssättet, vara avklarade:

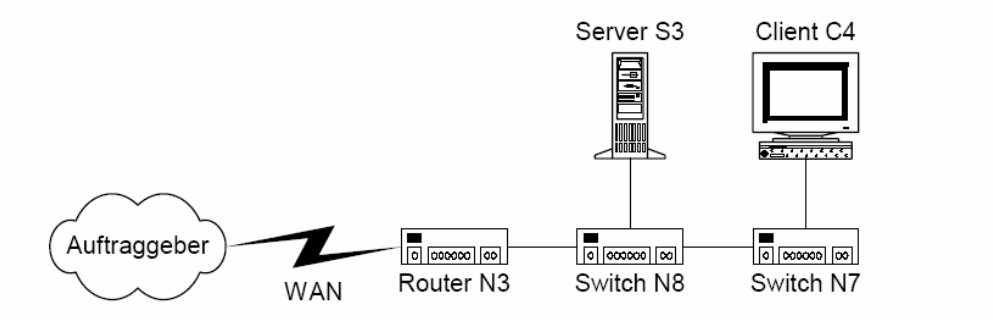
- En systematisk *IT-säkerhetsprocess* bör ha *initierats*. Dess uppgift är att styra aktiviteterna inom området IT-säkerhet i ordnade banor. Exempelvis måste lämpliga roller och uppgifter definieras. Ytterligare information om initieringen av IT-säkerhetsprocessen finns i kapitel 3 i IT-grundskydd-tillvägagångssättet.
- För IT-nätverket måste en *IT-strukturanalys* ha utförts enligt kapitel 4 i IT-grundskydd-tillvägagångssättet. Därigenom tas den viktigaste informationen om IT-nätverket fram, till exempel den korrigerade nätplanen samt en lista med de viktigaste IT-tillämpningarna med beroende till IT-systemen.
- Därefter måste *skyddsbehovet fastställas* enligt kapitel 4.2 i IT-grundskydd-tillvägagångssättet. Som resultat föreligger skyddsbehovet för IT-tillämpningarna, IT-systemen, de använda IT-lokalerna samt en förteckning över de kritiska kommunikationsförbindelserna. Skyddsbehovet är kopplat till grundvärdena *konfidentialitet*, *riktighet* och *tillgänglighet* och fastställs i tre nivåer *normalt, stort* och *mycket stort*.
- En *modellering* enligt kapitel 4.3 i IT-grundskydd-tillvägagångssättet och kapitel 2 i IT-grundskydd-katalogerna måste genomföras. Därvid fastställs för varje komponent i IT-grundskydd-katalogerna för vilka målobjekt i det verkliga IT-nätverket den ska användas. Standardsäkerhetsåtgärderna, som anges i de enskilda komponenterna, utgör grunden för det betraktade IT-nätverkets IT-säkerhetskoncept.
- Innan riskanalysen utförs måste en *grundläggande säkerhetskontroll* enligt kapitel 4.4 i IT-grundskydd-tillvägagångssättet utföras. På så sätt konstateras vilka standardsäkerhetsåtgärder som redan har genomförts för det aktuella IT-nätverket och var det ännu finns brister.
- Därefter måste en *kompletterande säkerhetsanalys* genomföras enligt kapitel 4.5 i IT-grundskydd-tillvägagångssättet. Vid den kompletterande säkerhetsanalysen bestäms för vilka målobjekt som en riskanalys bör genomföras och för vilka målobjekt ingen analys behövs.

De målobjekt som i den kompletterande säkerhetsanalysen har valts ut för en riskanalys betecknas nedan som *betraktade målobjekt* eller som *betraktade komponenter*.

Exempel:

En leverantör har en kommunikationsförbindelse till huvudkunden. Via denna förbindelse meddelar kunden ständigt det aktuella behovet av produkter i respektive färger, storlekar och typer. För att minimera datavolymen överförs endast ändringarna i förhållande till det tidigare meddelade behovet. Leverantören använder dessa behovsmeddelanden som underlag för sin planering av produktionskapaciteter. På så sätt finns en garanti att leverantörsföretaget producerar och levererar det antal varor som behövs i olika färger, storlekar och typer.

Den tekniska lösningen för kommunikationsförbindelsen är en hyrd linje till kunden. Redan ett bortfall på två timmar kan medföra en avsevärd överproduktion eller leveransproblem och därmed stora kostnader för företaget. Följande delområde i IT-nätverket har därför ett stort skyddsbehov med avseende på tillgänglighet:



(kund)

De berörda komponenterna finns i rummen M.723 (serverrum), M.811 (teknikrum) och E.5 (styrcentral i tillverkningsområdet). Inom ramen för den kompletterande säkerhetsanalysen beslutades det att för alla andra komponenter med stort skyddsbehov det inte krävs någon riskanalys.

3 Upprättande av översikten över hot

En lämplig utgångspunkt för riskanalyserna är de för de betraktade målobjekten relevanta hoten som finns angivna i IT-grundskydd-katalogerna. Till skillnad från vad som gäller i IT-säkerhetshandboken undersöks hot, svaga punkter och risker härvid inte separat.

Målet för de följande arbetsstegen är att upprätta en översikt över hot som finns för IT-nätverkets betraktade målobjekt. För det ändamålet är det lämpligt att först reducera IT-nätverket till de betraktade komponenterna.

1. Första steget är att från IT-nätverkets modellering stryka alla målobjekt eller grupper av målobjekt för vilka det enligt kompletterande säkerhetsanalys inte finns behov av en riskanalys. Det vill säga att de målobjekt som inte betraktas stryks ur modelleringen. Härvidlag kan i regel strykningar endast ske i skikten 2 till 5 eftersom komponenterna i skikt 1 i regel gäller alla eller åtminstone många målobjekt.

   Exempel: (utdrag)

Nr	Komponentens rubrik	Målobjekt	
B 2.3	Kontorsrum	~~Rum M.501~~	stryka
B 2.4	Serverrum	Rum M.723	
B 2.6	Rum för teknisk infrastruktur	Rum M.811	
B 3.101	Allmän server	~~S2~~	stryka
B 3.101	Allmän server	S3	
B 3.105	Server under Novell Netware 4.x	~~S2~~	stryka
B 3.105	Server under Novell Netware 4.x	S3	
B 3.205	Klient under Windows NT	~~C2~~	stryka
B 3.207	Klient under Windows 2000	C4	
B 3.301	Säkerhetsgateway (brandvägg)	N3	

2. Därefter stryks från den kvarvarande tabellen alla komponenter för vilka det inte längre finns något målobjekt och någon grupp av målobjekt. Dessa komponenter är uppenbarligen inte relevanta för de betraktade målobjekten.

I några fall kan komponenter strykas från skikt 1 när det är uppenbart att det ämne som behandlas i komponenten är irrelevant för den aktuella riskanalysen.

Exempel:

- I allmänhet kan komponenterna B 1.3 *Koncept för försörjning i nödsituationer* och B 1.8 *Hantering av säkerhetsincidenter* utelämnas när det i riskanalysen endast behandlas delområden som har ett normalt skyddsbehov med avseende på tillgänglighet.
- I allmänhet kan komponenten B 1,7 *Kryptokoncept* utelämnas när det i riskanalysen endast behandlas delområden som har ett normalt skyddsbehov med avseende på konfidentialitet och riktighet.

Detta steg ger som resultat en tabell i vilken ingår de komponenter som är relevanta för de betraktade målobjekten. Komponenterna i steg 1 är därvid viktiga för alla eller många målobjekt. Komponenterna i de övriga fyra skikten hänför sig däremot till speciella målobjekt eller grupper av målobjekt.

Exempel: (utdrag)

Nr	Komponentens rubrik	Målobjekt
B 2.4	Serverrum	Rum M.723
B 2.6	Rum för teknisk infrastruktur	Rum M.811
B 3.101	Allmän server	S3
B 3.105	Server under Novell Netware 4.x	S3
B 3.207	Klient under Windows 2000	C4
B 3.301	Säkerhetsgateway (brandvägg)	N3

3. Varje komponent från IT-grundskydd-katalogerna hänvisar till en lista av hot. För varje målobjekt i tabellen sammansätts dessa hots nummer och rubrik ur komponenterna och tillordnas aktuellt målobjekt.
4. Som resultat erhålls en tabell som tillordnar varje målobjekt en lista med relevanta hot. Ur den lista bör alla hot, som nämns två eller flera gånger, tas bort.
5. Därefter bör hoten sorteras i tabellen efter ämne per målobjekt. Några hot i IT-grundskydd-katalogerna behandlar liknande säkerhetsproblem eller olika varianter av samma hot (t.ex. G 1.2 *Bortfall av IT-systemet* och G 4.31 *Bortfall av eller fel på nätkomponenter*).
6. För att underlätta den efterföljande analysen bör det i tabellen för varje målobjekt noteras det skyddsbehov som inom ramen för fastställandet av skyddsbehov har bestämts med avseende på de tre grundvärdena konfidentialitet, riktighet och tillgänglighet. Denna tillordning kan slopas för det överordnade målobjektet *totalt IT-nätverk*.

Denna tabell visar en *översikt över hot/risker* för de betraktade målobjekten. Den tjänar som utgångspunkt för den följande *inventeringen av extra risker/hot*.

Exempel: (utdrag)

Kommunikationsserver S3	
Konfidentialitet:	normal
Riktighet:	stor
Tillgänglighet:	stor
G 1.2	*Bortfall av IT-systemet*
G 3.2	*Utrustning eller data förstörda pga. vårdslöshet*
G 4.1	*Strömavbrott*
G 5.57	*Nätanalys-verktyg*
G 5.85	*Förlust av riktighet hos skyddsvärd information*
osv.	

Rum M.811	
Konfidentialitet:	normal
Riktighet:	normal
Tillgänglighet:	stor
G 1,4	*Brand*
G 1.5	*Vatten*
G 2.6	*Obehörigt tillträde till lokaler med skyddsbehov*
G 5.3	*Obehörig inpassering i en byggnad*
G 5.5	*Vandalism*
osv.	

4 Inventering av ytterligare hot

För de betraktade målobjekten finns det i vissa fall enstaka extra hot som ligger utöver de i IT-grundskydd-modellen förutsedda hoten. Dessa måste även beaktas. I IT-grundskydd-katalogerna är i regel endast sådana hot *inte* upptagna vilka

- orsakas av en speciell teknik, en speciell produkt eller ett speciellt tillämpningsfall eller
- som vid vanliga användningsscenarier endast medför skador under mycket speciella förhållanden eller
- som förutsätter att en angripare har mycket goda fackkunskaper, möjligheter och medel.

Exempel på detta är en hel etablering slås ut uppsåtligt med hjälp av vapen eller ett tekniskt komplicerat angrepp med aktiv hjälp från en intern administratör.

För IT-säkerheten relevanta risker är sådana som

- kan leda till nämnvärda skador och
- i föreliggande tillämpningsfall och användningsmiljö är realistiska.

Vid inventeringen av ytterligare hot bör det respektive målobjektets skyddsbehov beaktas med hänsyn till IT-säkerhetens tre *grundvärden - konfidentialitet, riktighet och tillgänglighet*:

1. Om målobjektet beträffande ett visst grundvärde har skyddsbehovet *mycket stort* bör man prioriterat söka efter sådana hot som negativt påverkar detta grundvärde. Vid denna skyddskategori kan man utgå från att det finns relevanta hot vilka inte finns i IT-grundskydd-katalogerna.
2. Även om målobjektet beträffande ett visst grundvärde har skyddsbehovet *stort* bör man söka efter sådana hot som negativt påverkar detta grundvärde. Vid denna skyddskategori finns det i vissa fall relevanta hot vilka inte finns i IT-grundskydd-katalogerna.
3. Om målobjektet avseende ett visst grundvärde har skyddsbehovet *normalt* är de i IT-grundskydd-katalogerna angivna hoten i regel tillräckliga för detta grundvärde och då också de rekommenderade säkerhetsåtgärderna.

Oberoende av det betraktade målobjektets skyddsbehov är inventeringen av ytterligare relevanta hot särskilt viktig när det i IT-grundskydd-katalogerna inte finns någon lämplig komponent för målobjektet. Det samma gäller om målobjektet används i ett användningsscenario (miljö, tillämpning) som inte är förutsett i IT-grundskydd-katalogerna.

Följande frågeställningar ska beaktas vid inventeringen av ytterligare hot:

- Vilka möjliga händelser inom området force majeure utgör en särskild fara för IT-nätverket?
- Vilka *organisatoriska brister* måste absolut undvikas för att IT-säkerheten ska vara garanterad?
- Vilka *mänskliga felhandlingar* kan speciellt påverka den säkra IT-driften negativt?
- Vilka speciella säkerhetsproblem kan uppkomma vid respektive betraktat målobjekt till följd av *tekniska fel*?
- Vilken särskild risk hotar genom uppsåtliga angrepp från externa gärningsmän? Här avses personer som inte tillhör den egna institutionen och som inte heller genom speciella överenskommelser har tillgång till eller åtkomst av interna resurser.

- Hur kan interna gärningsmän genom uppsåtliga handlingar negativt påverka den korrekta och säkra driften av aktuellt målobjekt? Här hotar särskild risk till följd av befintliga åtkomsträttigheter och insiderkunskaper.

För varje betraktat målobjekt kontrolleras först huruvida ytterligare hot måste beaktas. Källor för dessa speciella hot är exempelvis

- tillverkarens dokumentation
- förteckningar på Internet avseende svaga punkter och
- egna hotanalyser.

Vid inventeringen av ytterligare hot kan det dessutom ett bra resultat erhållas om IT-grundskydd-hotkatalogerna G 1 till G 5 på nytt utnyttjas som källor. Möjligtvis finns där angivet fler relevanta hot vilka dock hittills inte har beaktats eftersom de motsvarande komponenterna exempelvis inte ingår i modelleringen.

I praktiken är det ofta så att ytterligare hot samtidigt gäller för flera målobjekt. De identifierade ytterligare hoten läggs till i hotöversikten.

Viktigt: Om relevanta hot inte beaktas kan det medföra luckor i det resulterande IT-säkerhetskonceptet. I tveksamma fall bör man därför analysera huruvida och – om ja – vilka hot som ännu saknas. Härvid är det ofta tillrådligt att utnyttja externa konsulttjänster.

I praktiken har det visat sig bra att för inventering av ytterligare hot genomföra en gemensam brainstorming med alla berörda medarbetare. Följande personer bör delta: IT-säkerhetsansvariga, projektledare, administratörer och användare av respektive betraktat målobjekt och vid behov även externa sakkunniga. Deltagarnas uppdrag bör vara tydligt formulerat och tiden för brainstormingen vara begränsad. Erfarenhet visar att två timmar är en ändamålsenlig övre tidsgräns. En IT-säkerhetsexpert bör leda brainstormingen.

Exempel: (utdrag)

Vid en brainstorming identifierar företaget bland annat följande extra hot:

Komplett IT-nätverk	
G 2.B1	*Otillräcklig synkronisering av operativa system och backup-system*
	På grund av de stora kraven på tillgänglighet finns det dubbla komponenter i kommunikationssystemet till kunden. Om backup-komponenterna inte motsvarar modern teknik finns risken att en fungerande förbindelse inte kan etableras med kunden.
G 5.70	*Manipulation genom anhöriga och besökare*
	Detta hot finns i IT-grundskydd-katalogerna och finns angivet vid komponent B 2.8 *Hemarbetsplats*. Denna komponent ingår dock inte i modelleringen av det föreliggande IT-nätverket. Dock måste hotet G 5.70 beaktas eftersom besökare regelbundet kommer genom företagets lokaler. G 5.70 tas därför med extra i riskbedömningen.
osv.	

Växel N7	
Konfidentialitet:	normal
Riktighet:	normal
Tillgänglighet:	stor
G 2.B2	*Skada på informationsteknik i tillverkningsområdet*
	Klienten C4 och växeln N7 används i företagets tillverkningsområde och är därför speciellt utsatta för fysiska hot. Apparaterna kan skadas, förstöras eller deras livslängd kan förkortas.
osv.	

Klient C4	
Konfidentialitet:	normal
Riktighet:	stor
Tillgänglighet:	stor
G 2.B2	*Skada på informationsteknik i tillverkningsområdet*
	se växel N7
G 4.B1	*Tillverknings- och kommunikationsprogramvara är inte kompatibla*
	Klienten C4 används inte enbart för kommunikationen med kunden utan på den körs även program som utgör ett stöd i tillverkningen. Genom att programmen inte är kompatibla kan det leda till avbrott och därmed är tillgängligheten förlorad.
osv.	

5 Bedömning av hot

I nästa steg gås hotöversikten igenom systematiskt och kontrolleras för varje målobjekt och för varje hot huruvida de hittills genomförda eller åtminstone förutsedda IT-säkerhetsåtgärderna ger ett tillräckligt skydd. I regel rör det sig om standardsäkerhetsåtgärder från IT-grundskydd-katalogerna. Kontrollen sker med hjälp av IT-säkerhetskonceptet och följande kontrollkriterier:

- Fullständighet

  Ger standardsäkerhetsåtgärderna skydd mot alla aspekter av det aktuella hotet? (Exempel: Har även husets bakdörr beaktats?)

- Mekanismstyrka

  Motverkar de i standardsäkerhetsåtgärderna rekommenderade skyddsmekanismerna det aktuella hotet i tillräcklig grad? (Exempel: Är föreskrifterna om minsta nyckellängd tillräckliga?)

- Tillförlitlighet

  Kan de planerade säkerhetsmekanismerna inte kringgås för enkelt? (Exempel: Hur lätt kan användare skaffa sig tillträde till serverrummet och därigenom kringgå åtkomstkontrollen för filer?)

Resultatet av kontrollen markeras i hotöversikten för varje hot separat i kolumnen *OK* (*J/N*).

OK=J betyder att de redan införda eller åtminstone i IT-säkerhetskonceptet planerade IT-säkerhetsåtgärderna erbjuder ett *tillräckligt skydd* mot det aktuella hotet eller att det aktuella hotet ändå *inte* är *relevant* för den planerade riskanalysen (exempelvis eftersom ett annat grundvärde berörs).

OK=N betyder att de redan införda eller åtminstone i IT-säkerhetskonceptet planerade IT-säkerhetsåtgärderna *inte* erbjuder ett *tillräckligt skydd* mot det aktuella hotet.

Tips: Inom ramen för bedömningen av hot diskuteras ofta första idéer vilka kan användas för att möta hot. Dessa förslag är användbara för de efterföljande arbetsstegen och bör därför noteras.

Bedömningen av hot ger en översikt över vilka hot mot de betraktade målobjekten som beaktas tillräckligt genom IT-grundskydd-katalogernas åtgärder (*OK=J*), och var risker ännu finns kvar (*OK=N*). Hanteringen av dessa risker behandlas i nästa avsnitt.

Exempel: (utdrag)

En bedömning av hot har genomförts vid leverantörsföretaget med hjälp av den kompletterade hotöversikten. Resultatet är bland annat att IT-grundskydd-åtgärderna inte är tillräckliga för följande hot (*OK=N*):

Kommunikationsserver S3		
Konfidentialitet:	normal	
Riktighet:	stor	
Tillgänglighet:	stor	
G 1.2	*Bortfall av IT-systemet*	*OK=N*
	Bortfall av server S3 måste förebyggas på ett tillförlitligt sätt. Åtgärderna i IT-grundskydd-katalogerna är inte tillräckliga.	
G 5.85	*Förlust av riktighet hos skyddsvärd information*	*OK=N*
	Den information som kunden sänder beträffande behov av varor får inte förvanskas. I annat fall kan det uppstå avsevärd överproduktion eller leveransproblem och därmed höga kostnader för företaget.	
osv.		

Klient C4		
Konfidentialitet:	normal	
Riktighet:	stor	
Tillgänglighet:	stor	
G 1.2	*Bortfall av IT-systemet*	*OK=N*
	För kommunikation med kunden används på klienten C4 speciell programvara vars installation är besvärlig och tidskrävande.	
G 2.B2	*Skada på informationsteknik i tillverkningsområdet*	*OK=N*
	Användning av IT i maskinella tillverkningsområden behandlas endast marginellt i IT-grundskydd-katalogerna.	
osv.		

6 Riskhantering

Inom ramen för bedömningen av hot erhålls i praktiken för det mesta flera hot som inte kan motverkas genom åtgärderna i IT-grundskydd-katalogerna. Dessa *kvarvarande hot* kan ge upphov till risker för driften av IT-nätverket.

Därför måste det beslutas hur de kvarvarande hoten ska hanteras. Vid detta beslut måste ledningsnivån absolut involveras eftersom avsevärda risker eller merkostnader kan uppkomma i vissa fall. För varje hot i den kompletterade hotöversikten med *OK=N* finns följande alternativ:

A. Riskreducering genom fler säkerhetsåtgärder: Det kvarvarande hotet elimineras genom att en eller flera extra IT-säkerhetsåtgärder, som i tillräcklig grad motverkar hotet, utarbetas och genomförs. Som informationskällor beträffande extra säkerhetsåtgärder finns exempelvis:

- tillverkarens dokumentation och service när det berörda målobjektet är en produkt
- standarder och kända framgångsrika arbetssätt, som exempelvis har tagits fram av kommittéer inom området IT-säkerhet
- andra publikationer och service som exempelvis erbjuds på Internet eller av specialföretag
- erfarenheter som har vunnits inom den egna institutionen eller hos samarbetspartners.

B. Riskreduktion genom omstrukturering: Det kvarvarande hotet elimineras genom att affärsprocessen eller IT-nätverket omstruktureras. Anledningar till detta beslut kan till exempel vara:

- alla verksamma motåtgärder är mycket dyra, det kvarvarande hotet kan trots det inte accepteras
- omstruktureringen är hur som helst lämplig av andra skäl t.ex. för att sänka kostnader
- alla verksamma motåtgärder skulle medföra avsevärda inskränkningar för systemets funktion eller användarvänligheten.

C. Riskacceptans: Det kvarvarande hotet accepteras och därmed även den risk som hotet medför. Anledningar till detta beslut kan till exempel vara:

- endast under vissa speciella förutsättningar leder hotet till en skada
- mot det aktuella hotet är inga verksamma motåtgärder kända för närvarande och hotet kan i praktiken knappast undvikas.
- insatser och kostnader för verksamma motåtgärder överskrider det värde som ska skyddas.

D. Risköverföring: Risken som uppkommer genom det kvarvarande hotet överförs till en annan institution till exempel genom ett försäkringsavtal eller genom att verksamheten läggs ut på entreprenad. Anledningar till detta beslut kan till exempel vara:

- de möjliga skadorna är av rent ekonomisk art
- det har i alla fall av andra skäl planerats att lägga ut IT-driften
- avtalspartnern är av ekonomiska och tekniska skäl bättre rustad att hantera risken.

För att förberedda ett välunderbyggt beslut beträffande vilket av de fyra alternativen för riskhantering som väljs bör det genomföras en brainstorming som tar upp vilka extra IT-säkerhetsåtgärder (alternativ A) som i princip kommer i fråga. Därvid bör de ovan nämnda informationskällorna utnyttjas.

Tips: I några fall går det endast att identifierar IT-säkerhetsåtgärder mot bestämda, men inte alla, delaspekter av ett hot. Här uppkommer frågan hur man hanterar hotet (alternativ A eller C/D). Det aktuella hotet bör i detta fall delas upp i två hot som därefter behandlas separat med alternativ A respektive C/D.

Det bör även beaktas vilka IT-säkerhetsåtgärder som redan finns för det aktuella målobjektet. Härvid kan resultaten från den grundläggande säkerhetskontrollen (se kapitel 4.4 i IT-grundskydd-tillvägagångssättet) användas.

De hypotetiska insatserna och kostnaderna för eventuellt erforderliga IT-säkerhetsåtgärder och information om redan befintliga IT-säkerhetsmekanismer är viktiga beslutsstöd.

- Vid alternativ A kompletteras de extra IT-säkerhetsåtgärderna i IT-säkerhetskonceptet. Det räcker med en entydig hänvisning till den motsvarande detaljerade beskrivningen av åtgärderna. Om de extra IT-säkerhetsåtgärderna motverkar det berörda hotet tillräckligt korrigeras den aktuella *OK*-statusen i hotöversikten från *N* till *J*.
- Alternativ B medför i regel att för de berörda delarna av IT-nätverket och även IT-säkerhetsprocessen måste startas på nytt. Det startar i allmänhet vid IT-strukturanalysen. Naturligtvis kan den hittills framtagna informationen och dokumenten utnyttjas.
- Vid alternativ C måste den resulterande risken absolut visas tydligt. Ledningsnivån fattar beslutet vilket dokumenteras spårbart.
- Vid alternativ D är en korrekt utformning av avtal en av de viktigaste aspekterna. Speciellt när verksamheter läggs ut på entreprenad bör personer solida, juridiska kunskaper utnyttjas. Ledningsnivån fattar beslutet vilket dokumenteras spårbart.

Viktigt: Hanteringen av hot mot vilka det i IT-grundskydd-katalogerna inte beskrivs tillräckligt verksamma motåtgärder kan vara avgörande för totalrisken för IT-driften. Man bör här överväga att utnyttja externa konsulttjänster.

Efter att ett beslut har fattats för varje kvarvarande hot i hotöversikten och några av de beskrivna handlingsalternativen har valts kan IT-säkerhetskonceptet för det betraktade IT-nätverket färdigställas.

Exempel: (utdrag)

För de hot som i kapitel 0 har identifierats med *OK=N* har följande beslut träffats:

Kommunikationsserver S3	
Konfidentialitet:	normal
Riktighet:	stor
Tillgänglighet:	stor
G 1.2	*Bortfall av IT-systemet*
"A"	Extra IT-säkerhetsåtgärder
M 6.B1	*Ha ett komplett reservsystem för kommunikationen med kunden i reserv* Ett komplett reservsystem för kommunikation med kunden hålls i reserv. Detta omfattar alla tekniska komponenter inklusive kommunikationsförbindelser. Reservsystemet förvara i rum E.3. Det säkerställs att reservsystemet alltid har samma konfiguration som produktionssystemet och att det är klart att använda inom 30 minuter. Kommunikationen med kunden sker via en uppringd linje. Det kompletta reservsystemet inklusive uppringd linje testas minst en gång per kvartal och i samband med varje ändring av konfigurationen.
G 5.85	*Förlust av riktighet hos skyddsvärd information*
"C"	Riskacceptans: Risken reduceras visserligen något genom de i överförings- och IT-systemen inbyggda säkerhetsmekanismerna. Säkerhetsincidenter, som kan medföra förvanskad behovsinformation och därmed högre kostnader för företaget, är dock fortfarande tänkbara. Denna restrisk accepteras av företagsledningen som tar ansvar för detta eftersom alla verksamma motåtgärder är oekonomiska.
osv.	

Klient C4	
Konfidentialitet:	normal
Riktighet:	stor
Tillgänglighet:	stor
G 1,2	*Bortfall av IT-systemet*
"A"	Extra IT-säkerhetsåtgärder
M 6.B1	*Ha ett komplett reservsystem för kommunikationen med kunden i reserv* Tips: se kommunikationsserver S3
G 2.B2	*Skada på informationsteknik i tillverkningsområdet*
"A"	Extra IT-säkerhetsåtgärder
M 1.B1	*Användning av en särskilt skyddad industri-pc i tillverkningsområdet* De största hoten mot klienten C4 i tillverkningsområdet kommer från luftföroreningar, vattenstänk och vibrationer. Istället för en standard-pc används därför en industri-pc som är speciellt skyddad mot fysiska hot. Industri-pc:n måste uppfylla följande krav: - lämplig för montering i standardiserade 19 tums skåp - integrerad eller utfällbar display - lätt utbytbart luftfilter - skydd mot vatten enligt kapslingsklass IP 54 - skydd mot vibrationer minst 0,2 g vid 0 - 500 Hz.
osv.	

7 Konsolidering av IT-säkerhetskonceptet

Om extra åtgärder har lagts till standardsäkerhetsåtgärderna i samband med behandlingen av kvarvarande hot måste IT-säkerhetskonceptet därefter konsolideras. Konkret innebär det att IT-säkerhetsåtgärderna för varje målobjekt måste kontrolleras med hjälp av följande kriterier:

IT-säkerhetsåtgärdernas lämplighet för att avvärja hot

- Täcks de relevanta hotens alla aspekter fullständigt?
- Är de träffade motåtgärderna i överensstämmelse med säkerhetsmålen?

Samverkan mellan IT-säkerhetsåtgärderna

- Samverkar åtgärderna när de relevanta hoten ska avvärjas?
- Ger åtgärdernas samverkan en verksam totaleffekt?
- Strider åtgärderna inte mot varandra?

IT-säkerhetsåtgärdernas användarvänlighet

- Är de vidtagna åtgärderna toleranta mot hanterings- och driftfel?
- Är de vidtagna åtgärderna tydliga för användarna?
- Är det uppenbart för användarna när en åtgärd inte fungerar?
- Kan användarna på ett enkelt sätt kringgå åtgärden?

IT-säkerhetsåtgärdernas lämplighet

- Är de vidtagna åtgärderna lämpliga för de aktuella hoten?
- Står kostnaderna och insatserna för genomförandet i ett korrekt förhållande till skyddsbehovet för de berörda målobjekten?

På denna grund bör IT-säkerhetskonceptet ordnas och konsolideras:

1. Olämpliga IT-säkerhetsåtgärder bör förkastas och efter ingående analyser ersättas genom verksamma åtgärder.
2. Motsägelser och inkonsekvenser beträffande IT-säkerhetsåtgärderna bör elimineras och ersättas med enhetliga och till varandra anpassade mekanismer.
3. IT-säkerhetsåtgärder som användarna inte accepterar är verkningslösa. Praktiska lösningar, som hindrar användarna så lite som möjligt, bör tas fram.
4. För komplicerade eller för dyra IT-säkerhetsåtgärder bör revideras eller förkastas och ersättas med passande skyddsåtgärder. Å andra sidan utgör för svaga åtgärder ett hot mot IT-säkerheten. Även de bör revideras eller ersättas.

Det kan mycket väl vara lämpligt att förutom riskanalysen även använda fler metoder för att förbättra IT-säkerheten, exempelvis penetrationstester. Därvid görs ett försök att simulera angreppsmetoden som en intern eller extern gärningsman använder. Resultaten kan medföra att ändringar görs i IT-säkerhetskonceptet.

Exempel: (utdrag)

Vid konsolideringen av IT-säkerhetskonceptet för leverantörsföretaget konstaterades bland annat följande:

- Även för det i åtgärd M 6.B1 krävda reservsystemet måste IT-grundskydd-katalogernas relevanta åtgärder genomföras. Skillnader i förhållande till produktionssystemet finns endast vad gäller placeringen och WAN-anslutningen. Reservsystemet ska alltså integreras i IT-grundskydd-modelleringen.
- De på grund av IT-grundskydd förutsedda åtgärderna M 6.53 *Redundant utformning av nätkomponenterna* genomförs för växeln N7 genom åtgärden M 6.B1. När M 6.B1 har genomförts har även M 6.53 genomförts för målobjektet N7. Åtgärd M 6.53 kan därför för N7 strykas ur IT-säkerhetskonceptet.
- För två år sedan beslutades att åtgärden M 5.68 *Användning av kodningsmetod för nätkommunikationen* kan undvaras. En gemensam projektgrupp med kunden har kommit fram till att detta beslut inte längre motsvarar dagens tekniska rön. Föreskrifterna för konfigureringen av routrarna revideras därför med kort varsel.
- De extra IT-säkerhetsåtgärderna M 1.B1 utnyttjas för de speciella infrastrukturella förhållandena hos klient C4. I tillverkningsområdet används förutom denna klient ytterligare informationsteknik som visserligen inte ingår i riskanalysen men som trots det måste skyddas på lämpligt sätt. Företaget tar genomförandet av åtgärden M 1.B1 som anledning till att utarbeta en riktlinje för säker drift av informationsteknik i tillverkningsområdet.

osv.

8 Återkoppling i IT-säkerhetsprocessen

När konsolideringen av IT-säkerhetskonceptet är klar kan säkerhetsprocessen fortsätta på det sätt som beskrivs i IT-grundskydd-tillvägagångssättet. Det kompletterade IT-säkerhetskonceptet utgör därmed en grund för följande arbetssteg:

- *Grundläggande säkerhetskontroll* (kapitel 4.4 i IT-grundskydd-tillvägagångssättet). Inom ramen för förarbetena har en grundläggande säkerhetskontroll redan genomförts för de enligt IT-grundskydd-modellen förutsedda åtgärderna. Eftersom riskanalysen i regel medför ändringar av IT-säkerhets-konceptet så ska de nytillkomna eller ändrade åtgärdernas genomförandestatus därefter kontrolleras. Eventuellt föråldrade resultat bör uppdateras till aktuell nivå.
- *Genomförande av säkerhetsåtgärder* (kapitel 4.6 i IT-grundskydd-tillvägagångssättet). De i IT-säkerhetskonceptet för de enskilda målobjekten förutsedda IT-säkerhetsåtgärderna måste genomföras i praktiken så att de kan vara verksamma. Detta omfattar bland annat uppskattning av kostnader och insatser samt att ordningsföljden för genomförande fastställs.
- *Upprätthålla IT-säkerheten och kontinuerlig förbättring* (kapitel 5 i IT-grundskydd-tillvägagångssättet). 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 även regelbundet kontrolleras med avseende på effektivitet.
- *Kontroll av IT-säkerhetsprocessen på alla nivåer* (kapitel 5.1 i IT-grundskydd-tillvägagångssättet). Regelbundet måste bland annat följande kontrolleras: Genomförandet av genomförandeplanen, IT-säkerhetsstrategins lämplighet, att IT-säkerhetsmålen är aktuella och IT-säkerhetsprocessens lönsamhet. Kontrollernas resultat tas in i den fortsatta utvecklingen av IT-säkerhetsprocessen.
- *Informationsflöde i IT-säkerhetsprocessen* (kapitel 5.2 i IT-grundskydd-tillvägagångssättet). Ledningsnivån måste regelbundet och i lämplig form informeras om resultaten av kontrollerna, IT-säkerhetsincidenter, IT-säkerhetsprocessens status och vid behov om ytterligare aspekter av IT-säkerheten. Då bör problem, bra resultat och förbättringsmöjligheter redovisas.
- *IT-grundskydd-certifiering* (kapitel 5.3 i IT-grundskydd-tillvägagångssättet). I många fall är det önskvärt att för en myndighet respektive ett företag att inåt och utåt tydliggöra vikten av IT-säkerhet och det framgångsrika genomförandet av IT-grundskydd. För detta ändamål har BSI skapat lämpliga mekanismer genom IT-grundskydd-intyget och certifieringen enligt ISO 27001 baserat på IT-grundskydd.
- *Koppling till GSTOOL* (se *http://www.bsi.bund.de/gstool*). Om styrningen av IT-säkerheten stöds genom GSTOOL eller en annan programvara bör riskanalysens resultat arbetas in där i så stor grad som möjligt. För GSTOOL gäller detta i synnerhet för nya eller ändrade IT-säkerhetsåtgärder som inte finns i denna form i IT-grundskydd-katalogerna.