

**MOTIVERING TILL OCH TILLÄMPNING AV
FÖRESKRIFT 47**

**OM HANTERING AV TELEFÖRETAGENS
INFORMATIONSSÄKERHET**

MPS 47

INNEHÅLL

INNEHÅLL	1
1 LAGSTIFTNING	2
1.1 FÖRESKRIFTENS LAGSTIFTNINGSGRUND.....	2
1.2 ÖVRIGA BESTÄMMELSER I ANSLUTNING TILL OMRÅDET.....	2
2 SYFTET MED FÖRESKRIFTEN OCH DESS ÄNDRINGSHISTORIA	2
2.1 SYFTET MED FÖRESKRIFTEN	2
2.2 CENTRALA ÄNDRINGAR OCH ÄNDRINGSHISTORIA	3
2.3 DEFINITIONER	3
3 MOTIVERING TILL ENSKILDA PARAGRAFER OCH ANVISNINGAR FÖR TILLÄMPNING	6
3.1 1 § TILLÄMPNINGSOMRÅDE.....	6
3.2 2 § ORGANISERING AV INFORMATIONSSÄKERHETEN	7
3.3 3 § STYRDOKUMENT FÖR INFORMATIONSSÄKERHET	8
3.4 4 § RISKHANTERING	11
3.5 5 § INFORMATIONSSÄKERHETSÅTGÄRDER	22
3.6 6 § UPPFÖLJNING AV HANTERINGEN AV INFORMATIONSSÄKERHETEN	24
4 REFERENSFÖRTECKNING	26
5 BILAGOR	28
5.1 FÖRENKLAT EXEMPEL PÅ RISKBEDÖMNING	28

1 LAGSTIFTNING

Syftet med detta kapitel är att ge användaren av denna föreskrift en helhetsbild av de författningar som föreskriften grundar sig på. Vidare presenteras i kapitlet annan väsentlig lagstiftning i anslutning till området.

1.1 Föreskriftens lagstiftningsgrund

Kommunikationsverkets förslag till föreskrift baserar sig på 19 och 20 § i lagen om dataskydd vid elektronisk kommunikation [1].

Kommunikationsverket kan med stöd av 19 § 4 momentet i lagen om dataskydd vid elektronisk kommunikation ge ett teleföretag närmare föreskrifter om ovan i 1–3 mom. avsett dataskydd för tjänster. Enligt paragrafens 1 moment ska ett teleföretag och den som tillhandahåller mervärdestjänster handha dataskyddet för sina tjänster. Enligt paragrafens 3 moment är ett teleföretag ansvarigt gentemot abonnenterna och användarna för det dataskydd som avses i 1 mom. också i fråga om sådan tredje part som helt eller delvis utför nättjänsten eller kommunikationstjänsten.

1.2 Övriga bestämmelser i anslutning till området

I detta avsnitt beskrivs andra föreskrifter som Kommunikationsverket meddelat och som anknyter till ämnesområdet för denna föreskrift. Syftet med avsnittet är att ge föreskriftens användare en bättre möjlighet att få en helhetsbild av skyldigheterna gällande kommunikationsnät och -tjänster.

Föreskrift 54 om säkerställande av kommunikationsnät och kommunikationstjänster [2]. Syftet med föreskriften är att säkerställa kommunikationsnätens och -tjänsternas funktions säkerhet, dataskydd och informationssäkerhet under normala förhållanden, i störningssituationer under normala förhållanden och i undantagssituationer. Därför ställer föreskriften minimiskyldigheter för teleföretag bland annat gällande säkerställandet av effektmatningen för de apparater som används i genomförandet av kommunikationsnät och -tjänster, apparaternas fysiska skydd samt säkerställandet av apparaterna och förbindelserna.

2 SYFTET MED FÖRESKRIFTEN OCH DESS ÄNDRINGSHISTORIA

Syftet med detta avsnitt är att ge föreskriftens användare information om målen för föreskriften. I avsnittet går man också igenom de mest betydande ändringarna beträffande de skyldigheter och rekommendationer som gällde före föreskriften.

2.1 Syftet med föreskriften

Hanteringen av dataskyddet har beskrivits på ett heltäckande sätt bland annat i standarden ISO 27001 (Information Security Management – Specification With Guidance for Use) [3]. Ett

heltäckande iakttagande av denna standard kan vara alltför tungt i synnerhet för små teleföretag i Finland.

I föreskriften beskrivs de minimikrav för administrationen av informationssäkerheten som varje teleföretag bör uppfylla i sin verksamhet. Genom kraven strävar man efter att säkerställa den grundläggande informationssäkerhetsnivån för den televerksamhet som teleföretagen bedriver och som fungerar som grund för säkerställandet av kommunikationsnätens och -tjänsternas informationssäkerhet. I kraven fokuserar man särskilt på fortlöpande utveckling, planering, genomförande och utvärdering av hanteringen av informationssäkerheten. Genom föreskriften strävar man efter att minska de skadliga verkningar som informationssäkerhetsrisker orsakar televerksamheten.

2.2 Centrala ändringar och ändringshistoria

Efter ikraftträdandet av föreskriftens föregående version har Kommunikationsverket meddelat tjänstespecifika föreskrifter, såsom om e-posttjänster (M11) [4] och internetförbindelsetjänster (M13) [5]. De skyldigheter som ställts i de tjänstespecifika föreskrifterna har i viss mån överlappat de skyldigheter som ställts i den föregående versionen av denna föreskrift. Genom ändringen av föreskriften har man strävat efter att avlägsna överlappningarna. Samtidigt har man även strävat efter att specificera kraven gällande administrationen av informationssäkerheten bland annat vad gäller hanteringen av risker.

2.3 Definitioner

I detta avsnitt beskrivs de definitioner som används i föreskriften.

2.3.1 Televerksamhet

Televerksamhet definieras i kommunikationsmarknadslagen. Enligt lagen avses med televerksamhet nättjänster eller kommunikationstjänster. Med allmän televerksamhet avses tillhandahållande av nättjänster eller kommunikationstjänster för en grupp av användare som inte har avgränsats på förhand.

Med nättjänst avses i kommunikationsmarknadslagen tjänster som tillhandahålls av ett nätföretag och med kommunikationstjänst tjänster som tillhandahålls av ett tjänsteföretag. Med nätföretag avses ett företag som tillhandahåller ett kommunikationsnät som det äger eller på någon annan grund förfogar över för överföring, distribution eller tillhandahållande av meddelanden. Med tjänsteföretag avses i sin tur ett företag som överför meddelanden i ett kommunikationsnät som det förfogar över eller har fått tillgång till av ett nätföretag eller som distribuerar eller tillhandahåller meddelanden i ett masskommunikationsnät.

Typiska nät- och kommunikationstjänster är till exempel telefonitjänster, bredbandstjänster, e-posttjänster och masskommunikationstjänster.

2.3.2 Dataskydd

Dataskyddet definieras i lagen om dataskydd vid elektronisk kommunikation. Enligt lagen avses med dataskydd administrativa och tekniska åtgärder genom vilka säkerställs att uppgifter är tillgängliga endast för dem som har rätt att använda dem, att uppgifterna inte kan ändras av andra än av dem som har rätt till detta och att uppgifterna och informationssystemen kan utnyttjas av dem som har rätt att använda uppgifterna och systemen.

2.3.3 Informationssäkerhetsrisk

Med informationssäkerhetsrisker avses i denna föreskrift en sådan oavsiktlig eller avsiktlig faktor som äventyrar televerksamhetens konfidentialitet, integritet eller tillgänglighet. Informationssäkerhetsrisker skiljer sig från informationssäkerhetsshot genom att informationssäkerhetsriskernas sannolikhet och verkningar har bedömts.

Informationssäkerhetsrisker kan till exempel orsakas av:

- mänskliga misstag,
- brister i eller underlåtenhet att iaktta instruktioner till personalen,
- stölder,
- kapacitetsbrister,
- fel i apparater,
- fel i applikationer,
- spridning av skadliga program,
- telekommunikationsstörningar,
- vandalism,
- eldsvåda och
- fel och försummelser begångna av en underleverantör eller en aktör som ingår i partnerskapsnätverket.

2.3.4 System för hantering av informationssäkerhet

Med system för hantering av informationssäkerhet avses i denna föreskrift en del av teleföretagets ledningssystem som baserar sig på bedömning och hantering av risker. Av teleföretaget förutsätts kännedom om dess verksamhetsmiljö och beaktande av verksamhetsmiljöns särdrag i utvecklingen av systemet för hantering av informationssäkerhet. Systemets krav baserar sig förutom på affärsstrategin i allmänhet även på informationssäkerhets- och dataskyddslagstiftningen, Kommunikationsverkets föreskrifter, andra bestämmelser samt kundernas och intressenternas krav och avtal.



Krav på teleföretagets informationssäkerhet baserar sig på informationssäkerhets- och dataskyddslagstiftningen samt andra bestämmelser, till exempel:

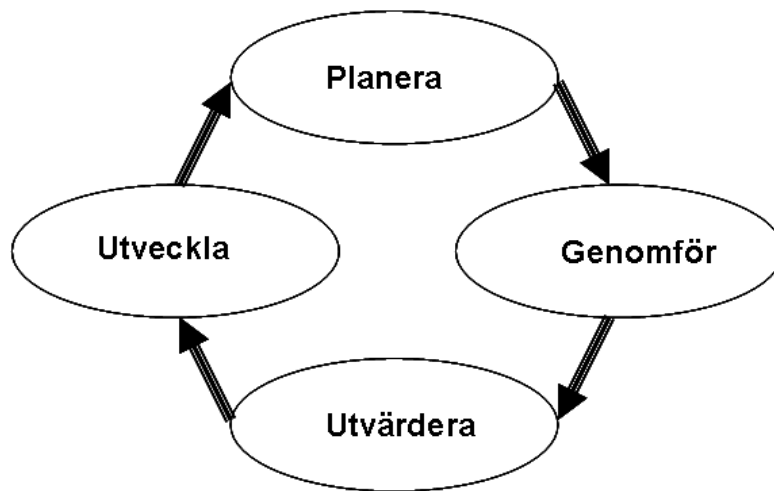
- kommunikationsmarknadslagen,
- lagen om dataskydd vid elektronisk kommunikation och
- Kommunikationsverkets föreskrift 47/2009 M.

Även andra krav gällande informationssäkerheten kan ställas på teleföretagets verksamhet, till exempel:

- kundernas krav,
- standardfamiljen ISO 27000,
- PCI DSS,
- HIPAA,
- SOX,
- EuroSOX,
- VAHTI-anvisningar och
- andra länders lagstiftning.

Syftet med hanteringssystemet är att stödja utvecklingen, planeringen, genomförandet och utvärderingen av informationssäkerheten.

Systemet för hantering av informationssäkerhet beskrivs i allmänhet som en process i fyra steg:



Planering:

Vid planeringen skapas policyn, definieras målsättningarna och objekten samt nödvändiga funktioner för informationssäkerheten.

Genomförande:

Vid genomförandet tillämpas informationssäkerhetspolicyn, -kontroller och -funktioner.

Utvärdering:

Vid utvärderingen mäts åtgärdernas inverkan på de målsättningar, policyn och praktiska erfarenheter som fastställts vid planeringen.

Utveckling:

I utvecklingsfasen utvecklas systemet för hantering av informationssäkerhet utifrån resultaten av utvärderingen. Utvecklingsmål kan bland annat vara informationssäkerhetspolicyn och informationssäkerhetsfunktioner.

3 MOTIVERING TILL ENSKILDA PARAGRAFER OCH ANVISNINGAR FÖR TILLÄMPNING

I detta kapitel går vi igenom motiveringen till respektive paragraf och dess tillämpningsanvisningar.

3.1 1 § Tillämpningsområde

Denna föreskrift tillämpas på verksamhet i anslutning till genomförandet av teleföretagens allmänna nät- och kommunikationstjänster. Föreskriftens tillämpningsområde omfattar till exempel internetförbindelsetjänster och e-posttjänster samt telefonitjänster enligt

kommunikationsmarknadslagen. Föreskriften tillämpas även på televerksamhet som är av ringa betydelse [6].

Denna föreskrift tillämpas inte på myndighetsverksamhet i myndighetsnät som avses i kommunikationsmarknadslagen eller i andra kommunikationsnät som konstruerats för att tillgodose behov i anslutning till allmän ordning och säkerhet, landets försvar, räddningsuppgifter, befolkningskydd eller trafiksäkerhet till lands, till sjöss, på räls eller i luften. Föreskriften tillämpas inte heller på tillfälligt tillhandahållande av kommunikationsnät eller -tjänster. Med tillfälligt tillhandahållande avses enhetliga perioder på högst två månader.

Tillämpningen av föreskriften avgränsas till att gälla televerksamhet och omfattar inte sådan verksamhet som inte direkt inverkar på kommunikationstjänsternas och -nätens funktion eller på slutanvändarnas dataskydd och informationssäkerhet.

3.2 2 § Organisering av informationssäkerheten

Motivering:

Säkerställandet av data, datasystem och verksamhetsförutsättningar förutsätter att informationssäkerhetsfunktionerna är effektivt organiserade i företaget. Den grundläggande förutsättningen är att ansvarsområdena och skyldigheterna för informationssäkerhetsfunktionerna har definierats.

Tillämpning:

Systemet för hantering av informationssäkerhet ska omfatta den högsta ledningens uppfattning om hur ansvaret för informationssäkerheten är fördelat inom organisationen. Ansvaret och skyldigheterna för informationssäkerheten kan vara både administrativa och operativa. Det finns skäl att granska ansvaret för informationssäkerheten i synnerhet då det sker ändringar i organisationen. Det kan till exempel handla om en ändring i personalen eller en ändring av verksamhetsomgivningen på grund av företagsarrangemang.

Ansvaret för informationssäkerheten kan fördelas mellan olika grupper. Vad gäller det administrativa ansvaret kan man som exempel nämna informationssäkerhetsgruppen. Exempel på operativa grupper är abuse- och cert/csirt-grupperna.

Exempel på administrativt ansvar för informationssäkerheten är utveckling av system för hantering av informationssäkerhet och styrdokument, upprätthållande av företagets informationssäkerhetsläge, beaktande av informationssäkerhetsfrågor i riskhanteringen och kontinuitetsplaneringen, upprätthållande och utveckling av ändamålsenliga datasystem samt korrekt allokering av resurser till informationssäkerhetsfunktioner och -investeringar samt beaktande av informationssäkerhetsfrågor i synnerhet i utbildningen av nyckelpersonal.

Eftersom dessa ansvarsförhållanden gäller flera delområden inom företagets ledningssystem är det motiverat att styra och övervaka genomförandet av informationssäkerhetsansvaret på ett koordinerat sätt. Betydelsen av en fungerande samordning är desto viktigare ju mer utspritt ansvaret för informationssäkerheten är i företagets organisation. Beroende på företagets storlek ska ansvaret för utvecklingen och uppföljningen av informationssäkerhetsärenden fördelas mellan en eller flera informationssäkerhetsansvariga. Informationssäkerhetsärenden ska hanteras som en del av ledningens normala rapportering.

För de primära samordnade åtgärderna vid hanteringen av kränkningar av informationssäkerheten och upprätthållandet av kontaktpunkten används i vissa sammanhang benämningen CERT (Computer Emergency Response Team) eller CSIRT (Computer Security Incident Response Team). I anslutning till tillhandahållandet av internetjänster har kontakt- och servicestället vad gäller informationssäkerhetsbrott mot kunderna och de externa intressenterna traditionellt benämnts Abuse-funktionen.

Föreskrifter för hanteringsberedskapen vad gäller enskilda teletjänster meddelas separat vid behov. Teleföretaget ska dock alltid ha en grundläggande beredskap för att hantera informationssäkerhetsbrott och -risker som har en betydande inverkan på företagets verksamhet och dess kunder.

Med administrativt ansvar kan man till exempel avse ansvar för:

- planering av informationssäkerhetspolicy,
- planering av personalens informationssäkerhetsutbildning,
- uppföljning av teleföretagets interna informationssäkerhetsnivå,
- planering och organisering av riskhanteringen samt
- hantering och planering av projekt som förbättrar informationssäkerheten.

3.3 3 § Styrdokument för informationssäkerhet

Motivering:

Informationssäkerheten utgör en del av kvaliteten på den televerksamhet som teleföretaget erbjuder. Styrdokumentet för informationssäkerhet är grundläggande dokument om informationssäkerhet genom vilka organisationens ledning visar de övergripande målen och de allmänna principerna för informationssäkerheten. Dokumenten skapar en grund för en systematisk utveckling och hantering av informationssäkerheten och hjälper att rikta investeringarna i informationssäkerhet.

Tillämpning:

Teleföretaget ska planera styrdokumenterna om informationssäkerhet enligt sina egna risker och behov. Till exempel teleföretagets informationssäkerhetsgrupp eller en annan tillräckligt omfattande enhet inom organisationen bereder dokumenterna som ledningen godkänner. Den aktör som berett dokumenterna kan också ansvara för deras publicering och en ändamålsenlig informering om dem till alla medarbetare inom organisationen. Styrdokumenterna ska vara lättillgängliga för alla medarbetare till exempel via organisationens intranätsidor. Dessutom ska dokumenterna ingå i inskolningsprogrammet för nya medarbetare. Teleföretaget ska se till att iakttagandet av huvudprinciperna för informationssäkerheten i dokumenterna övervakas.

Av styrdokumenterna för informationssäkerhet bör följande ärenden framgå vad gäller teleföretagets televerksamhet:

- informationssäkerhetsmål,
- ansvar för informationssäkerheten,
- informationssäkerhetsorganisation och
- metoder för upprätthållande och utveckling av organisationens egen informationssäkerhet till exempel vad gäller interna revisioner.

Teleföretaget ska skriftligt dokumentera hur följande specialområden har beaktats i praktiken och genomförts i den mån som de är lämpliga på teleföretagets televerksamhet:

- Personalsäkerhet
 - Ansvar och skyldigheter i anslutning till personalens informationssäkerhet.
 - Personalens informationssäkerhetskompetens och utveckling av den.
 - Kartläggning av nyckelpersonsrisker genom eventuella bakgrundskontroller.
 - Förebyggande av ansvars- och uppgiftshelheter som är farliga för televerksamheten.
 - Anvisningar för förfarandet när arbetsförhållandet slutar.
- Maskinvaru- och programvarusäkerhet
 - Tillräcklig dokumentation för att korrigera upptäckta sårbarheter.
 - Tillgång till reservdelar.
 - Allmän hanteringsprocess för ändringar av systemen.
- Telekommunikationssäkerhet
 - Kraven gällande telekommunikationssäkerheten behandlas närmare i de tjänstespecifika föreskrifterna, som till exempel i föreskriften om e-posttjänsternas informationssäkerhet och funktionsduglighet (M11)[4] och föreskriften om Internetförbindelsetjänsternas informationssäkerhet och funktionsduglighet (M13)[5].
- Datamaterialsäkerhet
 - Säkerställande av informationens konfidentialitet, integritet och användbarhet: hur klassificeras informationen och hur instrueras personalen i hanteringen av informationen.
- Driftssäkerhet

- Ansvar för registret för användarrättigheter: delning, ändring, och radering av användarrättigheter.
- Förebyggande av att användarrättigheter samlas på hög.
- Förhindrande av att utomstående kommer åt den hanterings- och konfigurationsinformation som anknyter till tillhandahållandet av kommunikationstjänsterna samt kundernas fakturerings-, abonnemangs- och logguppgifter.
- Ingripande i kränkningar och missbruk av informationssäkerheten
 - Verksamhetsansvar för att upptäcka betydande händelser i informationssäkerheten och ingripande i dem.
 - Verksamhetsanvisningar och processer för återhämtning från informationssäkerhetsproblem.
 - Bedömning av hotets allvar.
 - Anmälan till myndigheter.
 - Meddelanden om avvikelser.
 - Verksamhet efter avvikelser.
 - Missbruk och underlåtenhet att iaktta instruktioner från personalens sida.

Vad gäller fysisk säkerhet finns närmare anvisningar i föreskriften Kommunikationsverket M54. Bestämmelser om skyldigheten att anmäla kränkningar av informationssäkerheten samt fel och störningar i allmän televerksamhet finns i föreskriften Kommunikationsverket M9 [7].

Teleföretaget ska därtill fastställa tillräckligt detaljerade anvisningar för enskilda rutiner som är väsentliga för informationssäkerheten. I praktiken innebär detta fastställande av detaljerade anvisningar bland annat för hanteringen av identifieringsuppgifter i televerksamhet.

I avtal om anlitan av underleverantörer/underleverantörsfunktioner ska man se till att gränserna för informationssäkerhetsansvaret har fördelats tillräckligt noggrant mellan teleföretaget och underleverantören. Det totala ansvaret för tjänsternas informationssäkerhet innehas dock alltid av teleföretaget oberoende av om funktioner har lagts ut eller inte.

I underleverantörsavtal finns det skäl att införa hänvisningar till förpliktande bestämmelser gällande televerksamhet och sanktioner för brott mot bestämmelserna.

Försörjningsberedskapscentralen har publicerat rekommendationer [8], som man kan hänvisa till vad gäller hanteringen av verksamhetens kontinuitet. Dessa rekommendationer handlar om:

- ledning,
- styrning av verksamheten,
- personal och hantering av personalresurser,
- partnerskap och
- utvärdering av hanteringen av verksamhetens kontinuitet.

3.4 4 § Riskhantering

Motivering:

En av de viktigaste komponenterna i hanteringssystemet för informationssäkerhet är en effektiv riskhantering. Med detta avses i allmänhet identifiering av betydande risker i anslutning till företagets affärsverksamhet, bedömning och åtgärdande av riskerna efter att de identifierats samt övervakning av genomförandet av åtgärderna. Den viktigaste uppgiften för hanteringssystemet är att skydda organisationen och dess förmåga att utföra sina fastställda uppgifter under normala förhållanden, störningar under normala förhållanden och undantagsförhållanden med beaktande av ekonomiska faktorer. Riskhantering kan utgöra en del av företagets beredskaps- eller kontinuitetsplanering.

Om teleföretagens beredskapsskyldighet bestäms i 90 och 128 § i kommunikationsmarknadslagen [9].

Enligt 90 § i kommunikationsmarknadslagen har teleföretagen skyldighet att förbereda sig för undantagsförhållanden. Genom beredskapsplanering och förberedelser för undantagsförhållanden ska teleföretag sörja för att deras verksamhet fortgår så störningsfritt som möjligt även under sådana undantagsförhållanden som avses i beredskapslagen [10] och vid störningar under normala förhållanden.

Enligt 128 § i kommunikationsmarknadslagen ska allmänna kommunikationsnät och -tjänster samt kommunikationsnät och -tjänster som ansluts till dem planeras, byggas och underhållas så att de fungerar så tillförlitligt som möjligt även vid sådana undantagsförhållanden som avses i beredskapslagen och vid störningar under normala förhållanden och att tillgången till nödtjänster är tryggad på ett så tillförlitligt sätt som möjligt även vid störningar i nätet.

Målsättningen för riskhanteringen är bland annat att:

- snabba upp återhämtningen från informationssäkerhetsproblem i televerksamheten,
- minska kostnader och skador som informationssäkerhetsproblemen förorsakar televerksamheten,
- rikta investeringar som förbättrar informationssäkerheten i televerksamheten,
- förbättra televerksamhetens kvalitet och produktivitet,
- ekonomiskt optimera de risker som hänförs till televerksamheten och
- förebygga riskerna mot televerksamhet.

Genom kraven på riskhanteringen strävar man efter att säkerställa att teleföretaget är medvetet om följderna om riskerna realiserar och huruvida de riskminskande åtgärderna är tillräckliga.

Tillämpning:

Bland annat följande standarder och publikationer har utarbetats om riskhanteringen:

- ISO/IEC TR 13335-3, Information technology – Guidelines for the management of IT Security – Techniques for the management of IT Security. [11],
- ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management [12],
- NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology [13],
- Enisa: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools [14],
- COSO ERM (Enterprise Risk Management – Integrated Framework (2004)) [15],
- BS 31100:2008, Risk management. Code of practice [16],
- ISO 31000 Risk management – Principles and guidelines [17],
- The Institute of Risk Management (IRM), Risk Management Standard [18] och
- SM-RH: riskhantering i små och medelstora företag [19].

I denna föreskrift ställs inga skyldigheter på iakttagandet av en viss standard.

Riskhanteringsmodellerna varierar mellan företagen, och det finns inte en enda modell som skulle passa varje företag. Det viktiga är att sammankoppla målen för företagets riskhanteringssystem med målen för dess verksamhet och se till att de stöds av företagets ledning.

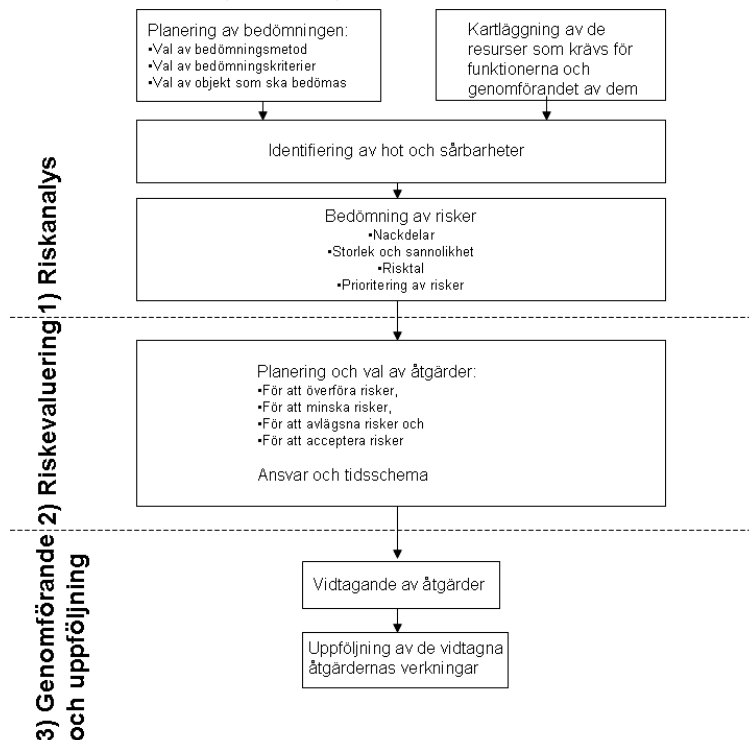
Minimikraven för riskhanteringen kan anses vara att:

- Teleföretaget har klassificerat de med tanke på televerksamheten viktigaste och mest kritiska funktionerna, processerna och systemen.
- Informationssäkerhetsriskerna i anslutning till televerksamheten har kartlagts.
- Teleföretaget regelbundet följer upp informationssäkerhetsnivån i anslutning till sin televerksamhet. Informationssäkerhetsnivån kan följas upp till exempel med stickprov, informationssäkerhetsinspektioner och informationssäkerhetsrevisioner.

Bestämmelser om viktighetsklassificeringen av kommunikationsnätens och -tjänsternas funktion finns i Kommunikationsverkets föreskrift 54/2008 M. Teleföretag kan utnyttja en viktighetsklassificering enligt föreskriften 54 för att kartlägga riskerna i anslutning till slutanvändarnas uppfattning om tjänstens användbarhet.

Informationssäkerhetsriskerna i anslutning till televerksamhet ska kartläggas vad gäller de för televerksamheten viktigaste och mest kritiska funktionerna, processerna och systemen, och åtgärderna för att minimera, avlägsna och överföra riskerna ska dokumenteras.

Riskhanteringen kan grovt indelas i tre olika faser:



3.4.1 Riskanalys

Med riskanalys avses de systematiska åtgärder genom vilka man strävar efter att identifiera hot och sårbarheter för informationssäkerheten som äventyrar genomförandet av televerksamheten, samt att bedöma följderna av de hot som eventuellt realiseras. Riskanalysen ska planeras, genomföras och dokumenteras omsorgsfullt. Riskanalysen borde göras upp i relation till en på förhand fastställd målnivå. Med detta avses till exempel krav på kommunikationstjänstens tillgänglighet enligt Kommunikationsverkets föreskrift eller ett kundavtal. Genom riskanalysen strävar man i synnerhet efter att identifiera de hot som äventyrar uppnåendet av de mål som ställts på föremålet.

Riskanalysen består av fem delområden:

- planering av utvärderingen,
- identifiering av informationssäkerhetshot som äventyrar televerksamheten,

- identifiering av utsatta system och funktioner,
- bedömning av riskernas storlek och sannolikhet samt
- prioritering av risker.

Risakanalysen ger svar på följande frågor om det granskade objektet:

- vad kan hända? (Hot)
- varför kan hotet förverkligas? (Sårbarheter)
- vad är sannolikheten för att hotet ska förverkligas och vilka följder får förverkligandet på televerksamheten? (Sannolikhet och storlek)
- hur stor är risken? (Risktal)
- vilka är de största riskerna? (Prioritering)

De viktigaste målsättningarna för risakanalysen är att:

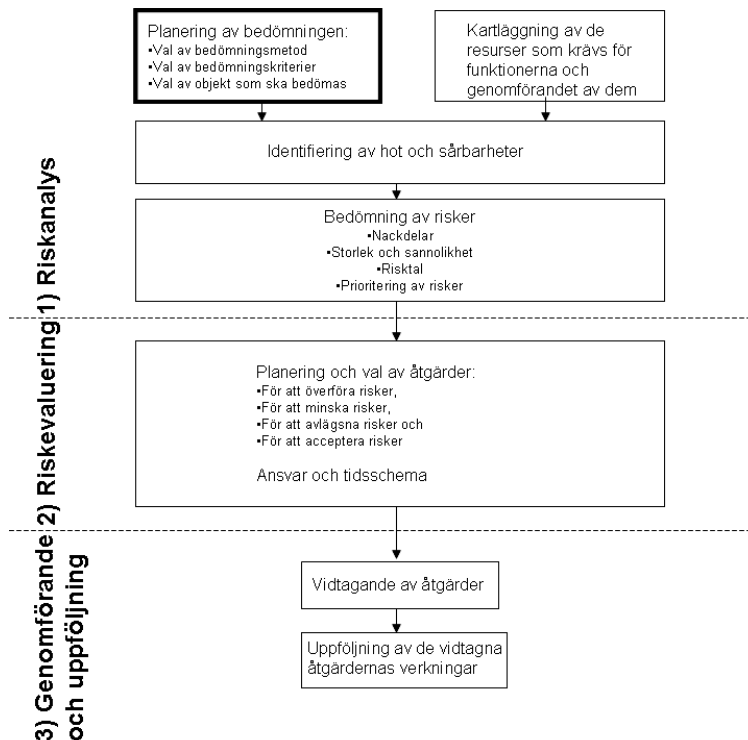
- stödja informationssäkerhetsledningen och styra investeringarna,
- förbättra informationssäkerheten och
- identifiera de informationssäkerhetsrisker som inverkar på televerksamheten och deras storlek.

På grund av målsättningarna för risakanalysen borde de som utför analysen ha god kännedom om den verksamhet som objektet för risakanalysen bedriver, om målen för dess verksamhet samt om de krav som ställs på verksamheten.

3.4.1.1 Planering av riskbedömningen

En viktig del av den systematiska utvecklingen av televerksamhetens informationssäkerhet är att bedöma informationssäkerhetsriskerna. Med hjälp av bedömningen utreder man de funktioner, uppgifter och system som är viktiga för televerksamheten.

Grunden för en god riskanalys skapas redan under planeringen och beredningen av risakanalysen, där man identifierar det bedömda objektets operativa mål, avgränsar de delområden som inte omfattas av analysen och väljer den mest ändamålsenliga analysmetoden. Genom en grundlig planering och beredning kan man säkerställa att de resurser som reserverats för riskbedömningen används effektivt, att målsättningarna för risakanalysen uppfylls och att den bästa möjliga operativa nyttan uppnås.



Planeringen av riskbedömningen ska omfatta de använda metoderna för riskbedömningen, kriterierna för riskbedömningen och objekten för bedömningen samt de ämnesområden som bedömningen riktar sig till. De bäst lämpade metoderna för bedömning av risker i anslutning till personalen kan nödvändigtvis inte tillämpas på bedömningen av riskerna i anslutning till datasystemen.

Innan bedömningen inleds ska man utreda bedömningens syfte, objektets operativa mål, sättet och tidsschemat för genomförandet av bedömningen. Målsättningarna för riskbedömningen kan till exempel kopplas till antalet bedömningar, tidsschemat eller antalet förbättringsåtgärder som bedömningen resulterar i.

Vid planeringen av bedömningen är det motiverat att beakta televerksamhetens omfattning och organisationens möjligheter. Om till exempel syftet med teleföretagets affärsverksamhet är att endast erbjuda e-posttjänster i liten skala, kan metoderna för riskbedömningen vara mycket enkla. Minimikravet på planeringen av riskbedömningen är dock att även de förenklade bedömningsmetoderna är dokumenterade.

Vid riskbedömningen lönar det sig att utnyttja till exempel tidigare informationssäkerhetsgranskningar, "nära ögat"-situationer och annat informationssäkerhetsmaterial.

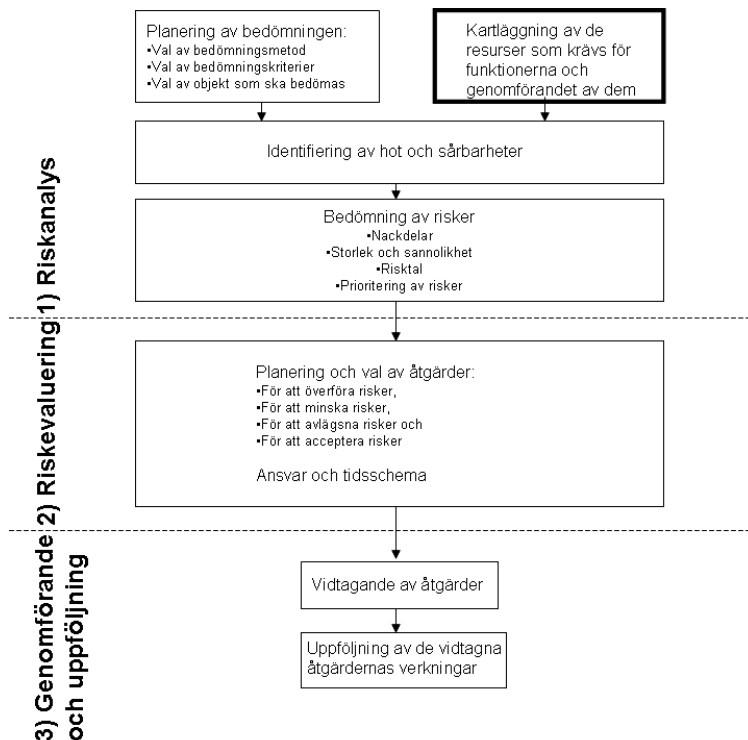
Teleföretaget ska säkerställa att de personer som deltar i bedömningen är tillräckligt förtrodda med den använda riskbedömningsmetoden.

I planeringsskedet ska man också komma överens om registreringen, lagringen och hanteringen av bedömningens resultat.

3.4.1.2 Kartläggning av funktionerna och de resurser som behövs för genomförandet av dem

Grundförutsättningen för identifieringen av systemen och funktionerna är att kartläggningen av de för televerksamheten centrala systemen och funktionerna har gjorts åtminstone vad gäller följande delområden:

- utrustningsutrymmen,
- maskinvara och programvara,
- telekommunikationsförbindelser,
- datamaterial och
- systemens underhålls- och stödpersoner.

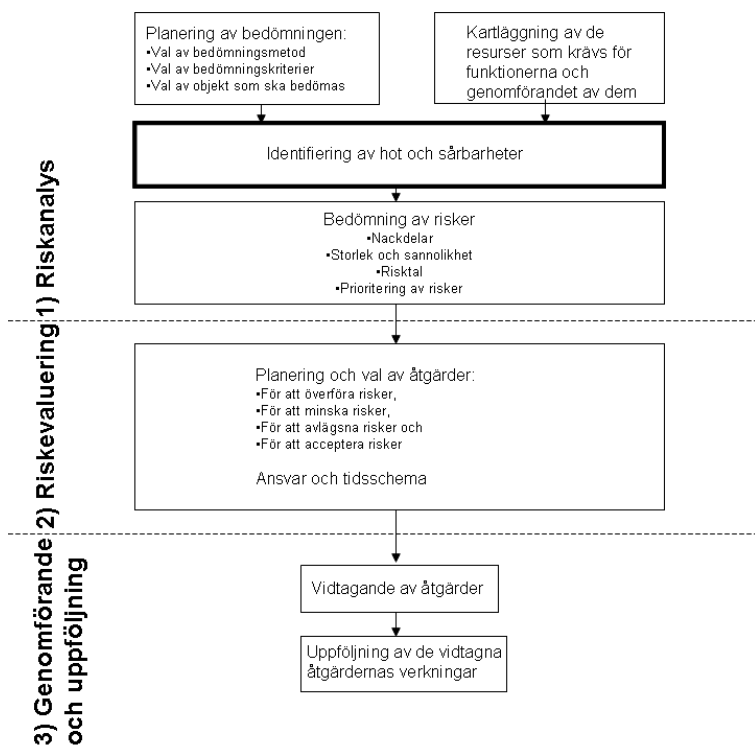


Teleföretag kan utnyttja en viktighetsklassificering enligt föreskriften 54 för att kartlägga riskerna i anslutning till slutanvändarnas uppfattning om tjänstens tillgänglighet. I föreskrift 47 förutsätts därtill att teleföretagen kartlägger risker i anslutning till system som hanterar känsliga uppgifter med tanke på datasäkerheten. Sådana system är till exempel fakturering, teleavlyssning och teleövervakning.

Kartläggningen förbättrar teleföretagets möjligheter att bedöma hur kritiska och känsliga datasystemen och de hanterade uppgifterna är och vilka resurser som behövs. Dessutom gör kartläggningen det lättare att rikta de informationssäkerhetsfrämjande åtgärderna.

3.4.1.3 Identifiering av hot

Med hot avses i detta sammanhang en situation som äventyrar televerksamheten och vars sannolikhet eller storlek inte har bedömts. Definitionen av hot beror på det valda riskanalysobjektet och avgränsningen. Vid definitionen av hot ska man utnyttja resultaten av de informationssäkerhetsrevisioner som gjorts på riskanalysobjektet samt tidigare realiserade risker eller informationssäkerhetsavvikelser. Informationssäkerhetsrevisionerna kan genomföras antingen som interna revisioner eller köpas av utomstående tjänsteleverantörer. Vi rekommenderar att revisioner görs, beroende på objektets kritiskhet, med 6 till 24 månaders mellanrum och alltid då betydande förändringar inträffar i det bedömda objektet.



Realiseringen av hotet an knyter alltid till en sårbarhet, dvs. utsatthet för en faktor som hotar televerksamheten. Sårbarheterna kan antingen vara tekniska eller icke-tekniska, och de kan till exempel anknyta till:

- maskinvara och programvara,
- processer och
- personal.

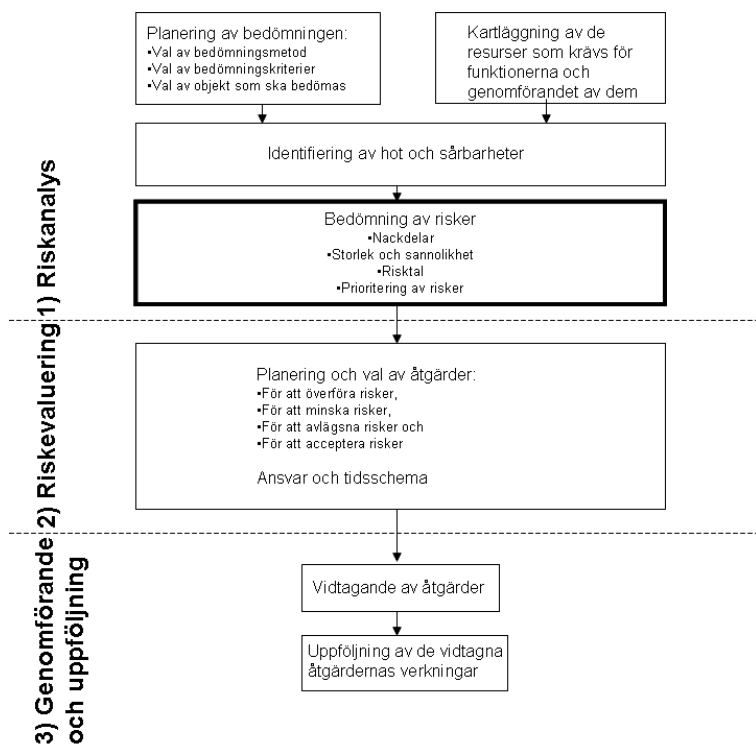
Med hot som anknyter till maskinvara och programvara avses till exempel att ett skadeprogram förhindrar apparatens eller programvarans funktion.

Med hot som anknyter till processer kan man till exempel avse dröjsmål i återhämtningen från ovan nämnda skadeprogram. Sårbarheten kan till exempel bero på avsaknaden av överenskomna rutiner.

Hot som anknyter till personalen kan vara att en viss tjänst saknar ansvarig person. Exempel på den här sårbarheten är att den ansvariga insjuknar eller säger upp sig.

3.4.1.4 Riskbedömning

Med riskbedömning avses bedömning av storleken på en identifierad risk och sannolikheten för att den realiserar.



Storlek:

Med storlek avses följderna av att hotet realiserar för den verksamhet som hotet riktar sig mot. Storleken kan öka med tiden varvid risken för temporära avbrott i tjänsten kan vara mindre än långvarigare avbrott.

Sannolikhet:

Med sannolikhet avses sannolikheten för att hotet realiserar.

Vid bedömningen av sannolikheten ska man beakta de åtgärder som redan vidtagits för att förebygga hotet.

Storlek och sannolikhet kan beskrivas till exempel på skalan 0–3, där 0 innebär ingen inverkan eller sannolikhet och 3 mycket betydande inverkan eller sannolikhet för att risken realiserar.

Risktal:

Risker beskrivs ofta med ett risktal som kan vara hotets storlek multiplicerat med hotets sannolikhet. Utifrån risktalet kan man klassificera riskerna enligt hotets sannolikhet och storlek.

Klassificering av risker:

De analyserade riskerna kan prioriteras till exempel enligt risktalet. Prioriteringen av risker enligt deras inverkan på affärsverksamheten är en allmänt använd metod, i synnerhet i större företag. Det som är viktigt är emellertid att de upptäckta riskerna har klassificerats på något sätt så att de tillgängliga resurserna kan inriktas på de mest allvarliga riskerna.

Klassificeringen av riskerna fungerar som en rekommendation, som stödjer beslutsfattandet när man planerar och riktar korrigerande åtgärder. Riskklassificeringen kan i sin enklaste form uttryckas på följande sätt då skalan för hotets sannolikhet och storlek är 0–3:

risktal	rekommendation
[0-1]	Obetydlig risk. Kräver inga åtgärder.
[2]	Acceptabel risk. Beslutet om att godkänna risken ska dokumenteras.
[3-4]	Måttlig risk: Risken kan godkännas temporärt. Åtgärder för att minska risken med tillgängliga resurser rekommenderas.
[6]	Betydande risk: Åtgärder för att minska risken så fort som möjligt rekommenderas.
[9]	Outhärdlig risk: Omedelbara åtgärder för att minska risken rekommenderas.

Dokumentation:

Dokumentationen ska innehålla sådana uppgifter utifrån vilka man i efterhand kan bedöma genomförandet av riskhanteringen samt riskkartläggningens och åtgärdernas tillräcklighet.

Dokumentationen ska omfatta åtminstone följande områden:

- riskanalys
 - Målsättningar för riskanalysen.

- Avgränsningar av riskanalysen.
- Resultat av riskanalysen.
- Slutrapport om riskanalysen.
- riskevaluering
 - Lista över de största riskerna.
 - Lista över de mest kritiska bristerna.

3.4.2 Riskevaluering

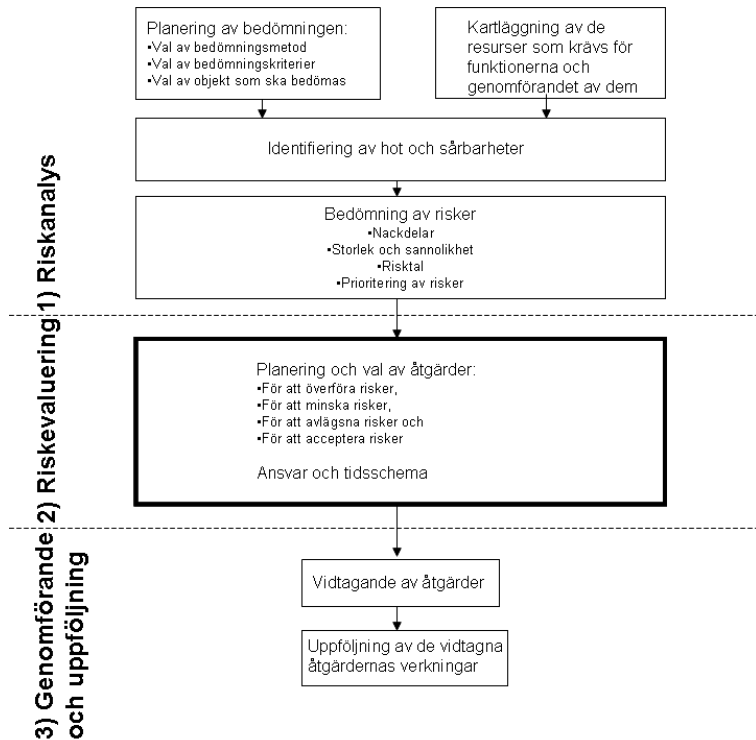
Vid riskevaluering lyfter man fram de viktigaste utvecklingsbehoven utifrån riskbedömningens resultat. Av detta sammandrag av riskbedömningen framgår bland annat:

- de största riskerna,
- de mest kritiska bristerna och
- föremålen för tilläggsutredningar.

3.4.2.1 Planering och val av åtgärder

Vid valet av informationssäkerhetsåtgärder utifrån riskanalysen finns det skäl att beakta de krav som de tvingande bestämmelserna ställer, kostnaderna för lösningarna, personalresurserna, företagets risktagningens vilja och de förluster som uppkommer genom att risken realiserar. Med dessa avses åtgärder för att:

- överföra risken,
- minska risken,
- undvika risken,
- acceptera risken,
- förebygga riskerna och
- förbättra upptäckten av risker.



Om en betydande risk inte kan avlägsnas helt och hållet ska teleföretaget göra upp en återhämtningsplan för den eventualitet att risken realiserar.

Med överföring av risker avses att kostnaderna för en realiserad risk överförs till tredje part till exempel genom försäkringar eller avtal. Teleföretaget bär dock det totala ansvaret för televerksamhetens informationssäkerhet om risken realiserar.

Med minskning av risker avses förebyggande av skador och delning av risker.

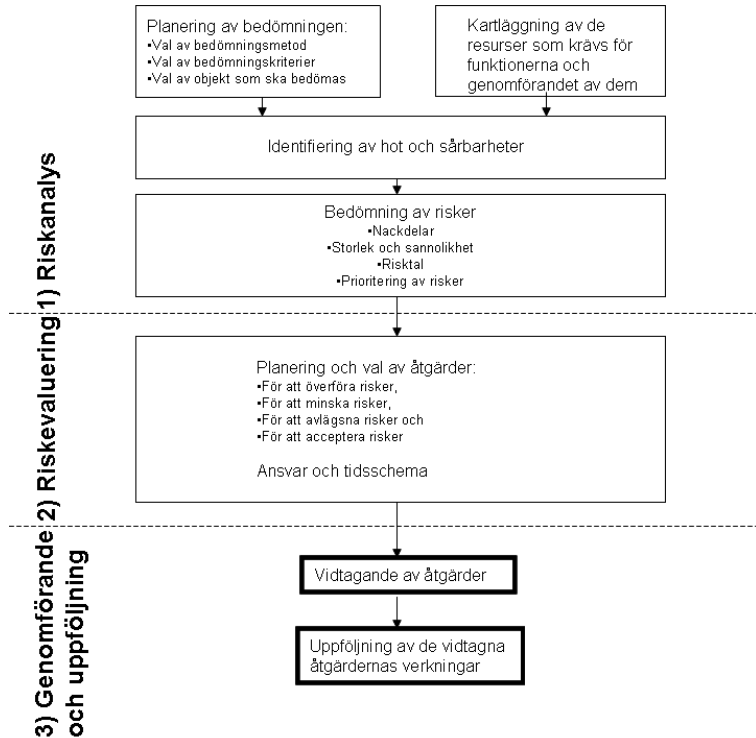
Genom undvikande av risker strävar man efter att göra sig av med en produkt, tjänst, avtalspart eller verksamhet som medför en alltför stor risk.

Risker med liten inverkan kan ofta accepteras om riskerna inte strider mot lagstiftning och bestämmelser. Om flera obetydliga risker realiserar samtidigt kan situationen dock förändras väsentligt till exempel vad gäller televerksamhetens kvalitet. När beslut om att acceptera risker fattas ska man från fall till fall beakta ur vilket perspektiv och under vilka förhållanden risken kan accepteras samt de följder och kostnader som uppkommer genom att risken realiserar.

Ägaren till en verksamhet eller tjänst ska se till att riskerna accepteras. Beslut om att acceptera risker fattas i enlighet med företagets beslutsfullmakter.

3.4.2.2 Ansvar och tidsschema för åtgärderna

Detta avsnitt anknyter till 5 § i föreskriften och behandlas i avsnitt 3.5 Informationssäkerhetsåtgärder i detta dokument.



3.5 5 § Informationssäkerhetsåtgärder

Tillämpning:

En plan ska uppgöras för de valda informationssäkerhetsfrämjande åtgärderna, och i den ska man bland annat fastställa de ansvariga personerna för de åtgärder som man beslutat vidta samt för genomförandet av och tidsschemat för uppföljningen av dem.

Exempel på informationssäkerhetsfrämjande åtgärder vad gäller överföring av risker är:

- undvikande av vissa produkter, protokoll eller metoder,
- undvikande av diffusa avtalspartner och
- nedläggande av verksamhet med alltför stora risker.

Exempel på informationssäkerhetsfrämjande åtgärder vad gäller minskning av risker är:

- personalutbildning i informationssäkerhet,
- verksamhetsdirektiv,
- införande av informationssäkerhetsfrämjande produkter,
- reservsystem,
- regelbundna uppdateringar av informationssäkerheten,
- uppdaterade säkerhetskopior,
- säkerhetsklassificering av dokumentationen och
- passagekontroll.

Upptäckt av risker kan förbättras till exempel genom regelbundna revisioner av objekten, införande av riskhantering i produktutvecklingen i ett så tidigt skede som möjligt, främjande av personalens medvetenhet om informationssäkerhet och anvisningar för rapportering i problemsituationer.

Till exempel personalrisker kan förebyggas med hjälp av ersättare och datasystemrisker med hjälp av reservsystem.

Teleföretaget ska fastställa detaljerade och tillräckliga anvisningar för väsentliga rutiner i anslutning till informationssäkerheten. Dessa anvisningar kan gälla till exempel följande delområden:

- förfarande vid besök,
- hantering av passagerättigheter,
- distansanvändning av system för teletrafik och
- hantering av känsligt datamaterial (t.ex. identifierings-, fakturerings- och kunduppgifter).

3.5.1 Datamaterialsäkerhet

Teleföretaget ska ha en gällande anvisning för hantering av datamaterial som är viktigt för televerksamheten. Anvisningen ska omfatta bland annat följande frågor:

- allmänna principer för bedömning av datamaterialets säkerhetsklass och konfidentialitet samt hemlighållandet av datamaterial,
- hanterings- och ändringsrättigheter vad gäller fördelningen av läsrättigheter till datamaterialet, ändringsrättigheter och fördelningen av dessa rättigheter,
- fastställande av konfidentialitetsklass,
- offentlighet av uppgifter eller dokument: till exempel rätten att tala om ett ärende offentligt,
- dokumentets egenskaper: papper, stämpel och andra märkningar
- förvaring och kryptering
- utskrifter och kopiering
- mottagning, distribution, sändning och transport,
- dokumentering av hanteringen av uppgifter och dokument och
- arkivering och hantering av dokument eller upphörande av hanteringsrätten samt förstörande av uppgifter och dokument.

Separata användar- eller användargruppspecifika behörigheter att hantera material ska fastställas för allt säkerhetsklassificerat datamaterial. Samtidigt ska man se till att utomstående inte kommer åt säkerhetsklassificerat datamaterial. Säkerhetsklassificerat datamaterial ska dock vara tillgängligt för dem som har rätt att hantera det.

Anvisningen för hantering av teleföretagens datamaterial kan i tillämpliga delar basera sig på till exempel finansministeriets datasäkerhetsanvisning för hantering av datamaterial inom statsförvaltningen [20].

Teleföretaget ska se till att datamaterial som är väsentligt för kommunikationsnätens och kommunikationstjänsternas tillgänglighet har uppdaterade säkerhetskopior, som förvaras i låsta utrymmen och separat från ifrågavarande apparater. Säkerhetskopiorna ska kunna tas i användning om det ursprungliga datamaterialet skadas till exempel på grund av fel i programvara, apparater eller en olycka i utrustningsutrymmet. Sådant datamaterial består till exempel av användaruppgifter och konfigurationsuppgifter.

3.5.2 Ingripande i missbruk och informationssäkerhetsproblem

Teleföretaget ska kunna reagera på brott och hot mot informationssäkerheten, som å ena sidan inverkar på teleföretagets förmåga att producera tjänster som teleföretag och som å andra sidan väsentligt äventyrar informationssäkerheten för teleföretagets kunder.

Ingripandet i missbruk av nät- och kommunikationstjänster samt informationssäkerhetsproblem ska vara organiserat och åtminstone omfatta följande funktioner:

- Beredning av anvisningar och processer för ingripande i missbruk och informationssäkerhetsproblem.
- Rapportering om missbruk och informationssäkerhetsproblem.
- Ansvar och funktioner för undersökningar och förundersökningar av missbruk och informationssäkerhetsproblem och bedömning av deras storlek.
- Ansvar och funktioner för begränsning av skador, åtgärdande av missbruk och informationssäkerhetsproblem samt information till den högsta ledningen.
- Anmälan till myndigheter.
- Ansvar och funktioner för återhämtning från missbruk eller informationssäkerhetsproblem.
- Funktioner för förebyggande av att händelsen upprepas.

3.6 6 § Uppföljning av hanteringen av informationssäkerheten

Motivering:

Nya tekniker och tjänster medför nya utmaningar för kommunikationstjänsternas och -nätens informationssäkerhet. Hanteringen av informationssäkerheten ska därför vara fortlöpande, reagera på förändringar och utgöra en del av företagets normala verksamhet från planering av kommunikationstjänster och -nät till underhåll.

Tillämpning:

Organisationens ledning ska se till att det finns tillräckligt med resurser för planering, genomförande, bedömning och upprätthållande av systemet för hantering av informationssäkerheten.

Systemet för hantering av informationssäkerheten ska underhållas regelbundet och uppdateras vid behov. Ändringsbehoven ska granskas en gång om året och alltid vid behov. Behovet av ändringar av hanteringssystemet kan uppstå på grund av till exempel organisationsreformer eller ändringar av företagets strategi.

4 REFERENSFÖRTECKNING

- [1] Lag om dataskydd vid elektronisk kommunikation (516/2004 jämte ändringar), uppdaterad lagstiftning
<http://www.finlex.fi/sv/laki/alkup/2004/20040516>
<http://www.finlex.fi/fi/laki/ajantasa/2004/20040516>
- [2] M54 Föreskrift om säkerställande av kommunikationsnät och kommunikationstjänster
<http://www.ficora.fi/attachments/suomiry/5vB4GW4xt/Viestintavirasto542008M.pdf>
<http://www.ficora.fi/attachments/ruotsiav/5vB4Pcjsx/Kommunikationsverket542008M.pdf>
- [3] Information Security Management - Specification With Guidance for Use
<http://www.iso.org/iso/home.htm>
- [4] M11, Föreskrift om e-posttjänsternas informationssäkerhet och funktionsduglighet
<http://www.ficora.fi/attachments/ruotsiav/5AWNeO3Pw/Kommunikationsverket11A2008M.pdf>
<http://www.ficora.fi/attachments/suomiry/5AWLwAxxQ/Viestintavirasto11A2008M.pdf>
- [5] M13, Föreskrift om Internet-förbindelsetjänsternas informationssäkerhet och funktionsduglighet
<http://www.ficora.fi/attachments/ruotsiav/5B36zJiZG/Kommunikationsverket13A2008M.pdf>
<http://www.ficora.fi/attachments/suomiry/5AWLt8K4m/Viestintavirasto13A2008M.pdf>
- [6] Statsrådets förordning (675/2003) om televerksamhet som är av ringa betydelse
<http://www.finlex.fi/sv/laki/alkup/2003/20030675>
<http://www.finlex.fi/fi/laki/kokoelma/2003/20030106.pdf>
- [7] M9, Föreskrift om skyldighet att anmäla kränkningar av informationssäkerhet samt fel och störningar i allmän televerksamhet
<http://www.ficora.fi/attachments/ruotsiav/5hw9QIBN0/Kommunikationsverket09C2009M.pdf>
<http://www.ficora.fi/attachments/suomiry/5hw8uQW3c/Viestintavirasto09C2009M.pdf>
- [8] Försörjningsberedskapscentralen: Avtalsbaserad beredskap inom informationssamhällssektorn
http://www.huoltovarmuus.fi/documents/3/SOPIVA_julkaisu.pdf
- [9] Kommunikationsmarknadslag (393/2003), uppdaterad lagstiftning
<http://www.finlex.fi/sv/laki/ajantasa/2003/20030393>
<http://www.finlex.fi/fi/laki/ajantasa/2003/20030393>
- [10] Beredskapslag (1080/1991), uppdaterad lagstiftning:
<http://www.finlex.fi/sv/laki/ajantasa/1991/19911080>
[http://www.finlex.fi/fi/laki/ajantasa/1991/19911080?search\[type\]=pika&search\[pika\]=valmiuslaki](http://www.finlex.fi/fi/laki/ajantasa/1991/19911080?search[type]=pika&search[pika]=valmiuslaki)
- [11] ISO/IEC TR 13335-3, Information technology – Guidelines for the management of IT Security – Techniques for the management of IT Security
<http://www.iso.org/iso/home.htm>
- [12] ISO/IEC 27005:2009 Information technology – Security techniques – Information security risk management
<http://www.iso.org/iso/home.htm>
- [13] NIST Special Publication 800-30, Risk Management guide for Information Technology Systems, Recommendation of the National Institute of Standards and Technology
<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>
- [14] Enisa: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools
http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf

[15] COSO ERM (Enterprise Risk Management – Integrated Framework (2004))
<http://www.coso.org/-ERM.htm>

[16] BS 31100:2008, Risk management. Code of practice.
<http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030191339>

[17] ISO 31000 Risk management – Principles and guidelines
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170

[18] The Institute of Risk Management (IRM), Risk Management Standard
<http://www.theirm.org/publications/PUstandard.html>

[19] PK-RH: riskhantering för små och medelstora företag
www.pk-rh.fi/riskilajit/tietoriskit/tietoriskit

[20] Finansministeriet: finansministeriets informationssäkerhetsanvisning för statsförvaltningens informationsmaterial
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3386/3388_fi.pdf

5 BILAGOR

5.1 Förenklat exempel på riskbedömning

I detta förenklade och avgränsade exempel beskrivs riskhanteringsprocessen i ett litet teleföretag som erbjuder e-posttjänster enligt modellen i avsnitt 3.4. Exempelföretaget har cirka 750 kunder som köper e-posttjänster. I exemplet har riskbedömningen av e-posttjänsterna endast beskrivits för en riskfaktor. I allmänhet exponeras e-posttjänster även för många andra risker, och dessa ska också bedömas.

5.1.1.1 Riskanalys

Riskanalysens målsättningar:

Genom riskbedömningen strävar man efter att utreda e-posttjänstens inverkan på affärsverksamheten i en situation där kompetent underhållspersonal inte är tillgänglig. I bedömningen uppskattar man också situationens ekonomiska inverkan. Bedömningen baserar sig på intervjuer med nuvarande ansvariga personer och chefen.

Avgränsning av riskanalysen:

Föremålet för riskanalysen är den e-posttjänst som teleföretaget erbjuder sina kunder och som står för cirka 30 procent av företagets kassaflöde. Denna analys fokuserar på drift och uppdatering av e-posttjänsten. Målsättningen för upprätthållandet är att säkerställa att e-postsystemet fungerar utan störningar i alla situationer. Tillgången på personal och dess kompetens är förutsättningar för driften och utvecklingen av e-postsystemet.

Riskanalysens resultat:

Som bedömningsmetod används en så kallad analys av potentiella problem.

Som bedömningskriterier för riskens storlek används skalan 0–3, där siffran

- 0 innebär att hotet saknar betydelse för företagets affärsverksamhet,
- 1 innebär att hotet har liten betydelse för företagets affärsverksamhet,
- 2 innebär att hotet har stor betydelse för företagets affärsverksamhet och
- 3 innebär att hotet har mycket stor betydelse för företagets affärsverksamhet.

Vid bedömningen av sannolikheten för att hotet ska realiseras används motsvarande skala.

Riskerna prioriteras enligt risktalet, dvs. enligt hotets sannolikhet multiplicerat med hotets storlek. Skalan för risktalet är 0–9 där:

- 0–1 innebär obetydlig risk,
- 2 innebär acceptabel risk,
- 3–4 innebär måttlig risk,
- 6 innebär betydande risk och

- 9 innebär outhärdlig risk.

För närvarande ansvarar två personer för upprätthållandet av e-posttjänsten. Den ena personens arbetsavtal för viss tid upphör efter tre månader och personen har meddelat att han flyttar utomlands för att studera.

Det centrala hotet är att det uppstår störningar i systemets funktion till exempel på grund av en överraskande ökning av mängden skräppost. För slutkunderna tar sig störningarna i verksamheten uttryck i form av försenade e-postmeddelanden som i längden kan orsaka betydande ekonomiska förluster för företag. Dröjsmål är sannolika om kompetent underhållspersonal inte är tillgänglig.

Sårbarheter:

- Den för viss tid anställda arbetstagarens arbetsförhållande upphör efter tre månader.
- Om den enda underhållspersonen insjuknar eller annars är frånvarande.

Hotets storlek: E-posttjänsten utgör cirka en tredjedel av företagets kassaflöde. Betydelsen av att e-posttjänsten fungerar för företagets affärsverksamhet är mycket betydande och därför ges hotet storlekssiffran 3.

Hotets sannolikhet: Sannolikheten ökar på grund av den kommande semesterperioden, eftersom den nuvarande underhållspersonen är tre veckor på semester i juli. Betydande fel i e-postsystemet har uppdragats cirka en gång i månaden. Utifrån ovan beskrivna grunder gavs hotet sannolikhetssiffran 2.

Risktal: hotets storlek * hotets sannolikhet = 3 * 2 = 6.

Risikanslysens slutrapport:

Utifrån risikanalysen upptäcktes en betydande risk i upprätthållandet av e-posttjänsten och det rekommenderas att risken minskas så fort som möjligt.

Tillgången till underhållspersonal på kort sikt är inte nödvändigtvis betydande om driftsstörningar inte sker under frånvaron. Då frånvaron förlängs ökar verkningarna betydligt. Samtidigt ökar också sannolikheten för driftsstörningar. Eftersom e-postsystemet inte är funktionsdugligt utan underhållspersonalens specialkompetens, orsakar en störning i tjänstens funktion som sker då underhållspersonen är frånvarande betydande ekonomiska förluster för företaget och har en negativ effekt på företagets image.

I denna bedömning orsakar bristen på tillgänglig underhållspersonal under driftsstörningar en betydande risk på grund av riskens storlek och sannolikhet. Risken är tydligt kopplad till företagets kärnverksamhet.

5.1.1.2 Riskevaluering

Åtgärder:

En fungerande e-posttjänst är inskriven i bolagets centrala mål för affärsverksamheten. Uppnåendet av målen för affärsverksamheten förutsätter åtgärder för att minska den bedömda risken. Detta görs genom att i god tid utse en annan underhållsperson för e-postsystemet innan den gamla arbetstagaren lämnar bolaget, så att man undviker en situation där endast en person ansvarar för underhållet. En utbildningsplan uppgörs för underhållspersonalen för att garantera den nödvändiga kompetensen även i framtiden.

Ansvar och tidsscheman:

Den närmaste chefen för underhållspersonalen ansvarar för åtgärderna. Vid behov inleder denne omedelbart en intern rekryteringsprocess.

5.1.1.3 Genomförande och uppföljning

Den närmaste chefen för underhållspersonalen rapporterar om vidtagandet av de överenskomna åtgärderna och rapporterar om lägets framskridande till sin egen chef.

Uppföljning av åtgärdernas inverkan:

Underhållspersonalens resurser och kompetens uppföljs i fortsättningen som en del av den årliga riskanalysen av omgivningen för e-posttjänsten och som en del av det dagliga chefsarbetet.