Kapitel 9 Fysisk och miljörelaterad säkerhet

Fysisk säkerhet syftar till att skydda organisationens lokaler, utrustning och informationskapital. Brister i fysisk säkerhet kan medföra att de logiska säkerhetsskydden sätts ur spel. Nyttan med ett behörighetskontrollsystem försvinner om okrypterade kommunikationskanaler kan avlyssnas och system- och tillämpningsloggar förlorar sitt värde som kunskapskälla eller bevismaterial om de kan manipuleras av obehöriga, etc.

Fysisk säkerhet handlar inte enbart om skydd mot kriminella handlingar. Naturolyckor och -katastrofer som brand, översvämning, oväder eller kraftig åska samt olyckor och katastrofer som orsakas av fel i tekniska system eller mänskliga misstag eller slarv utgör ett ännu större hot mot organisationens informationstillgångar.

Vid utformning av fysiska skydd är det lätt att fastna i tekniska frågor och att överskatta säkerhetsprodukternas skyddsförmåga. Man får aldrig glömma att fysiska skydd – lås, larm, belysning, intern-tv och så vidare – bara fungerar effektivt med tillräckliga personella resurser och korrekta administrativa rutiner.

9.1 Säkrade utrymmen

Mål: Att förhindra obehörigt fysiskt tillträde, skador och störningar i organisationens lokaler och information.

Kritiska eller känsliga informationsbehandlingsresurser bör inrymmas i säkra utrymmen inom ett avgränsat skalskydd med lämpliga säkerhetsspärrar och tillträdeskontroller. De bör fysiskt skyddas mot otillåten åtkomst, skada och störning.

Skyddet bör stå i proportion till förekommande risker.

9.1.1 Skalskydd

Ett sätt att skapa fysiskt skydd är att bygga rent fysiska hinder runt verksamhetens områden och lokaler eller mindre delar av den. Dessa fysiska hinder, som brukar kallas skalskydd, kan i sin yttre del bland annat bestå av stängsel eller staket. De inre delarna baseras på byggtekniska konstruktioner som förstärkt betongvägg, ståldörr eller galler.

Oforcerbara skalskydd – skalskydd som med säkerhet motstår ett kompetent och målinriktat angrepp – finns inte. Skalskyddets funktion är dels att avskräcka en angripare, dels att försvåra och fördröja ett påbörjat angrepp. Förutom det mekaniska skyddet måste komplettering ske med lämpliga larm och riktiga larmåtgärder för att fylla sin funktion.

9.1.2 Tillträdeskontroll

Tillträde till säkrade utrymmen bör kontrolleras. Detta kan ske manuellt via exempelvis en bemannad reception, eller automatiserat med hjälp av id-kort med behörighetskod eller någon annan teknisk metod. I båda fallen är det lämpligt att såväl inpassering som utpassering registreras för att medge spårbarhet.

Vid automatisk inträdeskontroll till särskilt känsliga utrymmen är det av vikt att systemet hindrar ”insmitning” tillsammans med en behörig person. I organisationen bör det finnas en central funktion för administration av behörighetstilldelning.

9.1.3 Skydd av kontorsbyggnader, rum och utrustning

Säkrade utrymmen innanför skalskyddet måste i vissa fall försåtskyddas. Det innebär att de övervakas för att upptäcka obehörig verksamhet. Detta kan bland annat ske med larm och/eller med hjälp av TV-övervakning.

Speciellt värdefull utrustning eller annan tillgång bör punktskyddas, alltså säkras med ett separat skydd som bara har till uppgift att övervaka denna tillgång.

Vid utformning av skydd är det viktigt att man även ser förbi de rent kriminella hot som finns, och tittar på de hot som finns inom såväl den interna som den externa miljön, men också de oönskade konsekvenser som kan bli följden av mänskliga misstag och rent slarv.

9.1.4 Skydd mot externa hot och miljöhot

Identifiering av tänkbara hot och genomförd riskanalys är en förutsättning för att kunna bedöma vilket fysiskt skydd som krävs för att skydda organisationens informationstillgångar. Det är väsentligt att beakta miljöpåverkande faktorer som omkringliggande fastigheter och dess verksamhet, risk för översvämning, jordskred etc.

9.1.5 Arbete i säkrade utrymmen

Extern och egen personal som normalt inte har behörighet till utrymmet bör övervakas kontinuerligt vid arbete i säkrade utrymmen. Detta sker enklast genom närvaro av egen personal eller med hjälp av TV-övervakning.

9.1.6 Allmänhetens tillträde, leverans- och lastutrymmen

Utrymme för godsmottagning måste organiseras så att de begränsar onödigt tillträde till känsliga områden. Inkommande gods ska registreras och godkännas av egen personal vid leveranstillfället och eventuella avvikelser från förväntad leverans ska kvitteras av leverantören. Allt inkommande gods ska dessutom kontrolleras så att det inte bär med sig eventuella farligheter.

9.2 Skydd av utrustning

Mål: Att förhindra förlust, skada, stöld eller skadlig påverkan på tillgångar och avbrott i organisationens verksamhet.

Utrustning bör skyddas mot fysiska hot och miljömässiga hot

Skydd av utrustning (även sådan som används utanför organisationens lokaler, och vid bortflyttning av egendom) krävs för att minska risken för obehörig åtkomst av information och skydda mot förlust och skada. Det bör också beaktas var utrustning installeras och hur den avvecklas. Särskilda åtgärder kan krävas för att skydda mot fysiska hot och för att skydda försörjningsutrustning, t.ex. elförsörjning och kablage.

9.2.1 Placering och skydd av utrustning

Vid placering och skydd av utrustning bör man bland annat tänka på

- hot från intern och extern miljö,
- risken för obehörig åtkomst,
- risken för obehörig insyn,
- risken för avlyssning.

Speciellt känslig utrustning och utrustning som behandlar känslig eller kritisk information bör placeras så att onödigt tillträde minimeras och så att utformningen av punktskydd för utrustningen underlättas.

Miljöförhållanden ska övervakas på ett sådant sätt att ”negativ påverkan” på IT-utrustningen och dess användning kan upptäckas på ett mycket tidigt stadium.

Brand utgör alltid en miljörisk som är viktigt att ha rätt skyddsåtgärder mot. Förutom byggteknisk sektionering (indelning i brandzoner), minimal brandbelastning, lämpliga släcksystem och relevanta brandlarm är det viktigt att det finns utrymningsplaner som övas regelbundet.

9.2.2 Tekniska försörjningssystem

De vanligaste orsakerna till störningar i elförsörjningen är avgrävda kraftkablar, åska och interna kraftvariationer som kan bero på bland annat fläktregulatorer och hissmotorer.

Ett genomtänkt skyddssystem mot störningar i elförsörjningen är A och O för effektiv tillgänglighet. Skyddssystemet ska omfatta skydd mot exempelvis elavbrott, spänningsspikar/transienter och statisk elektricitet.

Används avbrottsfri elförsörjning UPS, ”uninterruptable power supply” måste man tänka på att elkraft ska säkerställas även till IT-utrustningens kringmiljö som klimatanläggningar och arbetsbelysning. Av vikt är också att UPS-systemet regelbundet testas samt att de aktuella underhållsrutinerna följs.

För särskilt avbrottskänsliga eller kritiska IT-system bör skyddsåtgärder som dubblerade och av varandra oberoende matningsvägar för elkraft och egen reservkraftsgenerator övervägas.

9.2.3 Kablageskydd

Starkströmsledningar samt data- och telekablar bör skyddas mot åverkan och avlyssning samt elektromagnetisk störning. Fiberoptiska data- och telekablar eliminerar risken för elektromekanisk störning och minimerar hotet

för avlyssning. De är, ur säkerhetssynpunkt, att föredra framför traditionellt trådkablage utom i miljöer med risk för radioaktiv strålning.

9.2.4 Underhåll av utrustning

Förutsättningarna för en störningsfri driftsmiljö är att följa leverantörens rekommenderade underhållsplan för utrustningen. Hemlig eller på annat sätt känslig information måste skyddas vilket kan vara problematiskt i samband med underhållsarbete. I verksamhet vars informationsbehandling har bäring på rikets säkerhet bör all underhållspersonal säkerhetsprövas.

9.2.5 Säkerhet för utrustning utanför egna lokaler

Risker i samband med användning av utrustning utanför de egna lokalerna måste analyseras särskilt. Detta gäller för informationsbärare i vid mening och omfattar bland annat persondatorer, handdatorer, mobiltelefoner och pappersdokument. Vid utformning av skyddsåtgärder måste man beakta att säkerhetsrisker kan variera avsevärt mellan olika platser och vid olika tidpunkter. Samtidigt bör aktuella skyddsåtgärder diskuteras med organisationens försäkringsbolag. Viktigt att även beakta riskerna då utrustning lämnas ut för service externt.

9.2.6 Säker avveckling eller återanvändning av utrustning

Lagringsmedia som innehåller känslig information eller licensierade program bör förstöras, avmagnetiseras eller överskrivas på ett säkert sätt i samband med avveckling eller återanvändning. Alla verksamheter accepterar inte ”överskrivning” som en säker metod. Det kan också finnas speciella bestämmelser för fysisk förstöring av IT-utrustning.

9.2.7 Avlägsnande av egendom

Ut- och införsel av säkerhetsklassad IT-utrustning måste godkännas och registreras vid ut- och inpassering. Det måste dessutom finnas klara riktlinjer/regler för hur sådan utrustning ska hanteras. Säkerhetsklassningen måste vara realistisk och rimlig. Säkerhetsåtgärder som förhindrar ett effektivt arbete eller som omotiverat inskränker de anställdas handlingsfrihet kommer förr eller senare att kringgås.

Exempel

1 – Brand

En söndagskväll för lite mer än sex månader sedan utbröt en brand på övervåningen hos företaget Pappum Nova i byggnaden intill Medytekk. Branden spred sig snabbt över till Medytekks huvudbyggnad, först till över- och sedan till bottenvåningen. Pappum Nova och Medytekk saknade båda brandlarm. Industriområdet är tämligen folktomt på kvällarna så det dröjde länge innan branden uppmärksammades. Resultatet blev katastrofalt. Båda våningsplanen brändes ut och bland annat datarummet och arkivet totalförstördes. IT-utrustningen kunde lätt ersättas men att samtliga reservkopior förintades av branden tillsammans med alla pappersdokument, både i arkivet och i kontorsrummen, fick katastrofala följder. Omfattande och väsentlig forskningsinformation gick förlorad, liksom kund-, leverantörs- och personaldata. Medytekk kunde inte heller betala sina räkningar, fakturor kunde inte följas upp, bokföringen kunde omöjligen rekonstrueras, etc.

Dessutom förlorades en stor del av de egenutvecklade programmen för forskningsstöd. Forskningsarbetet kunde visserligen fortsätta men de aktuella projekten fördyrades avsevärt.

Som ett resultat av ovanstående fick Medytekk ett (oförtjänt) dåligt rykte som företag och affärspartner. Efterfrågan på företagets forskningsprodukter minskades – i princip till noll.

Det hade nu gått sex månader och Medytekk ska rekonstrueras efter det att nära femton års hårt arbete gått upp i rök.

Vad borde Medytekk ha tänkt på?

2 – Kidnappning och utpressning

B-G Sjöström jobbade över på Medytekk en torsdagskväll. Efter att han ringt hem flera gånger utan att någon svarade började han bli orolig och beslutade sig för att åka hem.

Vid hemkomsten var huset mörkt. Telefonen ringde just när han fick av sig kläderna och försökte hitta något meddelande från sin fru Marianne. En grov, manlig röst meddelade att hans fru och dotter kidnappats och uppmanade honom att möta kidnapparna vid sluthållplatsen för den lokala bussen, några minuters promenadväg från Sjöströms hus. Rösten uppmanade honom att ta med sig huvudnyckeln till Medytekk, och varnade honom för att kontakta polisen – det kunde gå illa för både hustrun och dottern i så fall. Efter mötet vid busshållplatsen åkte kidnapparna till Medytekk där de förstörde samtliga dataservrar och tog med sig säkerhetsskåpet med alla reservkopior. Sjöström fick 24 timmar på sig att överlämna 1 miljon kronor i små valörer i utbyte mot reservkopiorna. Han uppmanades dessutom att skynda sig hem och befria hustrun och dottern som var fastbundna och inlåsta i vinkällaren.

Vad borde Medytekk ha tänkt på?

3 – Donation av pc

Ett av Medytekks hittills största forskningssatsning har arbetsnamnet ”Projekt A 6”. Det syftar till att framställa en ny smärtstillande substans, som förväntas revolutionera smärtbehandling och bedöms ha ett mycket stort kommersiellt värde. Forskningen har tagit mycket tid och resurser och har belastat Medytekks ekonomi hårt. Forskningen har dock varit mycket lyckad, och det återstår bara ett begränsat antal tester. Medytekk har börjat förhandla med ett antal intresserade läkemedelsföretag.

Bestörtnigen är därför mycket stor en måndagsmorgon då en av huvudstadens större morgontidningar rapporterar om en sensationell medicinsk nyhet från ett stort utländskt läkemedelsföretag. Det gäller en ny smärtstillande substans som verkar bygga på samma principer som Medytekks.

Efter en försiktig förfrågan och mera detaljerad produktinformation från läkemedelsföretaget står det klart för Medytekks ledning att det måste vara resultatet från Projekt A 6 som utgör grunden för den utländska produkten. Stefan Eriksson är mycket upprörd och anlitar en utomstående säkerhetsexpert för att utreda händelsen.

Säkerhetsexperten kan efter ett tag konstatera att för några månader sedan har forskarna i Projekt A 6 framfört krav på kraftigare persondatorer vilket har blivit tillgodosett. B-G Sjöström – vars farmor var född i Estland och som är mycket aktiv i olika aktiviteter för att stödja de baltiska länderna – beslöt då att Medytekk skulle donera den gamla utrustningen till en baltisk forskningsorganisation. Innan persondatorerna skickades iväg raderades alla program- och datafiler med hjälp av operativsystemets raderingsfunktion.

Det förekommer ett visst samarbete mellan några forskare från den baltiska forskningsorganisationen och det aktuella läkemedelsföretaget – bland annat finansierar läkemedelsföretaget några pågående forskningsprojekt. Flera av forskarna har dessutom tidigare anklagats för illojal hantering av känsliga forskningsdata och säkerhetsexperten misstänker att forskningsinformation från Projekt A 6 har läckt från den baltiska forskningsorganisationen till läkemedelsföretaget.

Vad borde Medytekk ha tänkt på?

Vad kan vi lära oss av dessa exempel?

Exempel 1 – Brand

Medytekk borde ha tänkt på att vidta effektiva åtgärder mot brand (som är den allra största enskilda risken för näringsverksamhet) genom att

- installera automatiskt brandlarm i huvudbyggnaden,
- förvara viktiga dokument i säkerhetsskåp,
- förvara datamedia i datamediaskåp, eller i säkerhetsskåp med datamediainsats (brand- och stöldskydd),
- förvara reservkopior på säkert avstånd från det normala driftstället (se även SS ISO/IEC 17799, Kapitel 8 Styrning av kommunikation och drift).

Medytekk borde också

- diskuterat brandrisken och eventuella gemensamma åtgärder för att minska konsekvenserna av en brand med Pappum Nova,
- övervägt byggnadstekniska åtgärder för att brandsäkra datarummet och arkivet.

Exempel 2 – Kidnappning och utpressning

Medytekk borde ha tänkt på att

- förvara reservkopior på ett säkert sätt även med hänsyn till stöld, till exempel genom en extra kopia i ett bankfack.

Medytekk borde också ha tänkt över

- innehav och förvaring av huvudnycklar, genom att exempelvis endast ha två huvudnycklar: den ene hos det lokala vaktbolaget (med en särskild procedur för utkvittering), den andra i ett bankfack.

Exempel 3 – Donation av pc

Medytekk borde ha tänkt på att

- bättre säkra avveckling/återanvändning av IT-utrustning genom att överskriva data på ett säkert sätt på fasta hårddiskar, alternativt fysiskt förstöra dessa.

Medytekk borde också

- undersökt den baltiska forskningsorganisations verksamhet ur bland annat säkerhetssynpunkt innan man bestämde sig för att donera persondatorerna.

Checklista – Fysisk och miljörelaterad säkerhet

Fråga	Ja	Delvis	Nej
Har man vid riskanalysen beaktat potentiella hot från den externa miljön?			
Har den interna miljön utformats med hänsyn till säkerhetskrav, det vill säga, är säkerheten inbyggd i miljön?			
Är skalskyddet entydigt definierat?			
Är kraven på brandskydd uppfyllda utan att övriga säkerhetsaspekter har ignorerats?			
Är alla branddörrar larmade och självstängande?			
Finns det ett fungerande administrativt system för tilldelning och fråntagning av behörigheter för fysiskt tillträde?			
Fungerar den operativa tillträdeskontrollen utan störningar och/eller klagomål?			
Är lokalerna utformade så att onödigt tillträde till säkrade utrymmen har minimerats?			

Fråga	Ja	Delvis	Nej
Är larmsystemet fackmässigt installerat och regelbundet testat?			
Finns det klara regler, inklusive entydig ansvarsfördelning, för aktivering och avaktivering av larm?			
Förvaras reservkopior och annan reservutrustning på ett säkert avstånd från driften?			
Är övervakning av säkrade utrymmen ordnad för normala förhållanden? Finns det beredskap för ovanliga situationer?			
Finns det rutiner för hantering och användning av utrustning för fotografering och video-, ljud- eller annan upptagning i känsliga utrymmen?			
Kontrolleras inkommande gods med avseende på eventuell farlighet?			
Är rutinerna för godsmottagning utformade så att ansvar för inleverans, mottagning och leveransavvikelser kan spåras och fastställas vid en eventuell tvist eller misstanke om brott?			
Är all it-utrustning placerad och skyddad på ett riktigt sätt? Har onödigt tillträde till känsliga utrymmen minimerats?			
Har åtgärder vidtagits mot potentiella hot som stöld, brand, vatten, EMI, etc.?			
Finns det en policy mot intagning av mat och drycker, rökning med mera i närheten av it-utrustning?			
Är ovanstående policy accepterad av berörd personal?			
Har konsekvenserna av störningar i elförsörjningen (avbrott, spikar, statisk elektricitet, etc.) beaktats tillräckligt?			
Har eventuella UPS tillräcklig kapacitet?			
Sker underhåll och test av eventuella UPS: er enligt leverantörens anvisningar?			
Är startbatteri- och drivmedelsförsörjningen till eventuella reservkraftsgeneratorer säkrad?			
Gäller ovanstående även i en större kris- eller katastrofsituation?			
Är starkströmsledningar och data- och telekablar skyddade mot skada, avlyssning och EMI?			
Finns det administrativa system för underhåll av it-utrustning där misstänkta fel, verkliga fel samt underhållsaktiviteter registreras (och planeras i tillämpliga fall)?			
Är säkerhetsskyddet för utrustning som används utanför de egna lokalerna tillräckligt? Omfattar det alla typer av it-utrustning (person- och handdatorer, mobiltelefoner, pappersdokument, etc.)?			
Är försäkringsskyddet för utrustningen ovan tillfredställande?			
Finns det klara regler och procedurer för hur utrustning ska avvecklas eller återanvändas?			
Är det säkerställt att känsliga IT-resurser inte lämnas oskyddade när de inte används?			
Sker ovanstående så långt som möjligt med hjälp av tekniska skydd och så litet som möjligt genom förhållningsregler för användare?			
Är reglerna för avlägsnande av egendom acceptabla ur säkerhetssynpunkt?			
Är reglerna ovan sådana att de inte leder till ineffektivitet i arbetet eller missnöje bland personalen?			