Teknisk rapport SIS/TK 318 N46
Version 6.00 2006-08-07

SWEDISH STANDARDS INSTITUTE

LIS
Ledningssystem för informationssäkerhet

Ge din information rätt säkerhet

Handbok i informationssäkerhetsarbete

Baserad på standarderna:
ISO-ISO/IEC 27001 Ledningssystem för informationssäkerhet - Krav
SS-ISO/IEC 17799 Riktlinjer för styrning av informationssäkerhet

DNV
SVENSKT NÄRINGSLIV
CONFEDERATION OF SWEDISH ENTERPRISE
Öhrlings
PRICEWATERHOUSECOOPERS
SWEDAC
SVENSK BRAND & SÄKERHETS CERTIFIERING AB

Innehållsförteckning

Förord

Information är förmodligen en av de mest värdefulla tillgångarna i din verksamhets. Nya snabba, kreativa och komplexa möjligheter att skapa, använda och utbyta information skapas varje dag. Elektronisk information och synen på information som den centrala tillgången omvandlar vårt sätt att leva och arbeta. Men riskerna är stora att information går förlorad, förvanskas eller kommer i fel händer. Följderna av sådana incidenter är ibland förödande.

Den internationella standarden SS-ISO/IEC 27001 står för ett affärsmässigt synsätt för att styra informationssäkerheten i din verksamhet. Standarden specificerar hur alla verksamheter kan bygga upp ett ledningssystem för informationssäkerhet (LIS) som tillhandahåller en organisationsanpassad säkerhetsnivå. Aktivt riskanalysarbete är kärnan i SS-ISO/IEC 27001. Din organisation måste identifiera sina informationstillgångar och förstå de risker och hot som finns mot dessa. Standarden SS-ISO/IEC 17799 ger råd för vad som kan göras för att minska sårbarheten hos informationstillgångarna.

Inom SIS, Swedish Standards Institute, har projekt LIS nu verkat i snart tio år. Projektets första delmål var att ta fram de två standarderna SS-ISO/IEC 27001 och SS-ISO/IEC 17799. För att underlätta införandet av LIS, i framför allt mindre och medelstora företag, väcktes idén om en handbok som ger en praktisk handledning och exempel från verksamheter. Beslut om att ge ut denna handbok har tagits av SIS tekniska kommittén TK 318 Ledningssystem för informationssäkerhet.

Denna handbok hjälper dig att bygga ett LIS via SS-ISO/IEC 27001 med stöd av SS-ISO/IEC 17799. Alla gråtonade rutor i handboken är hämtade från SS-ISO/IEC 17799 och innehåller de mål som finns inom dessa delområden.

Fler exemplar av denna handbok i pdf-format finns att hämta gratis via Internet från SIS:s webbplats: www.sis.se eller från SWEDACs hemsida: www.swedac.se.

Förändringshistorik

Version	Utkom	Förändringar
1.0	2001-01-17	-
2.10	2002-03-05	Anpassning till nya SS-ISO/IEC 17799
3.0	2004-01-23	• Beskrivning av ledningssystem utgör nya Kapitel 2 och anpassning till nya SS 62 77 99-2, utgåva 2 (processinriktning, etc.) • Korrigering av hänvisningar för att få ett Ledningssystem för informationssäkerhet, LIS • Tillägg av avsnitt rörande handledning för LIS planeringsfas i Appendix 4 • Redaktionella förändringar (Kapitel 13 är numera Appendix 2, Kapitel 2 är numera Appendix 3 och Kapitel 14 är numera Appendix 5)
6.0	2006-07-10	• Anpassningar till SS-ISO/IEC 27001:2006 och SS-ISO/IEC 17799:2005

Revideringen till version 6.0 har utförts av:

- Gunnar Lindström, SWEDAC, med stöd av deltagare i TK 318.

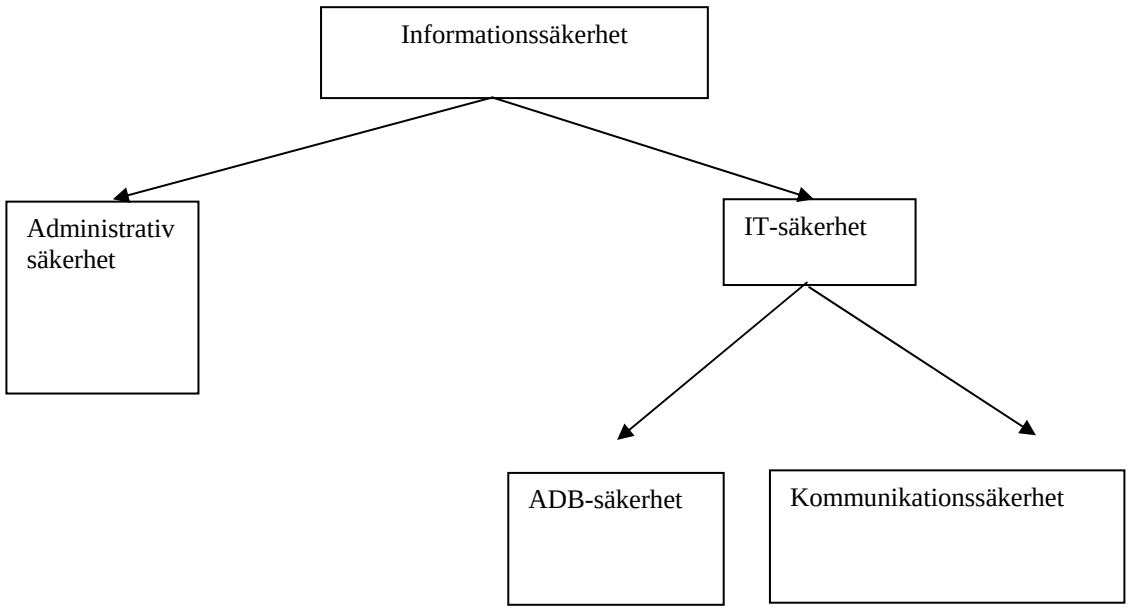
Medverkande vid det ursprungliga framtagande av denna skrift var:

- Johan Karlsson, frilansjournalist som sammanställde handboken i version 1.0
- Jan-Olof Andersson, Riksbanken
- Göran Antonsson, Clemens Wallen Östlund Advokater AB
- Anders Carlstedt, Öhrlings Price Waterhouse Coopers
- Per Anders Eriksson, Arthur Andersen
- Thomas Keisu, StoSec
- Gunnar Lindström, SWEDAC – ordförande i arbetsgruppen
- Per Lundin, Svensk Brand- och Säkerhetscertifiering AB
- Inger Nordin, DNV Certification AB
- István Orci, Statskontoret
- Thomas Osvald, Thomas Osvald IT-Konsult
- Bengt Rydstedt, SIS, Swedish Standards Institute
- Jan Svenson, Protect Data Konsult

Kapitel 1 Inledning

Idag är informationssäkerhet ett begrepp som är av stor betydelse för att säkerställa en organisations lönsamhet och även dess fortsatta existens.
Denna handbok är framtagen under SIS projekt TK 318 vilket allmänt benämns LIS-projektet.
LIS står för Ledningssystem för Informationssäkerhet. LIS motsvaras i engelskan av ISMS, Information Security Management System. De viktigaste standarderna i den växande familjen inom detta område är kravstandarden för ledningssystem informationssäkerhet SS- ISO/IEC 27001 samt Riktlinjer för styrning av informationssäkerhet SS-ISO/IEC 17799:2005. (Denna standard kommer under 2007 få beteckningen SS-ISO/IEC 27002)
Handboken är tänkt att fungera som ett komplement till riktlinjerna och även att användas vid utbildning inom området. Handboken är utformad som en teknisk rapport och som en följd av detta är en del av standardens text återgiven ordagrant i handbokens gråtonade rutor. Handbokens kapitelindelning och disposition följer helt standardens disposition. I slutet av varje kapitel finns en checklista och övningsexempel. Övningsexemplen utgår från ett fiktivt företag ”Medytekk” vilket är beskrivet under en bilaga till boken.

Informationssäkerhet är ett begrepp vilket av många felaktigt förknippas med IT-säkerhet. Nedanstående figur beskriver relationen mellan de underordnade begreppen.



Nyckelbegreppen som omfattas av informationssäkerhet är

- Sekretess
- Riktighet
- Tillgänglighet
- Spårbarhet

Handboken bygger på standarden SS-ISO/IEC 17799, Ledningssystem för informationssäkerhet - Riktlinjer för styrning av informationssäkerhet.
Vid internrevision av informationssäkerheten bör standarden SS-ISO/IEC 27001, Ledningssystem för informationssäkerhet - Krav användas. Detta gäller även då bedömning görs av underleverantörers informationssäkerhet. Certifieringsorgan vilka certifierar ledningssystem för informationssäkerhet gör detta mot SS-ISO/IEC 27001. I den normativa bilagan till SS-ISO/IEC 27001 är dispositionen lika med rekommendationerna i SS-ISO/IEC 17799. I SS-ISO/IEC 27001 är det däremot **skall-krav** och inte rekommendationer.

SS-ISO/IEC 27001 följer samma struktur som SS-EN ISO 9001, Ledningssystem för kvalitet och SS-EN ISO14001 Miljöledningssystem och kan med fördel integreras med dessa i ett verksamhetssystem.

SIS
Swedish Standards Institute

ISO
Internationella standardiseringsorganisationen (International Organization for Standardization)

IEC
Internationell standardiseringsorganisation (International Electrical Commissions) Standardisering inom elektronik och telekommunikation

2 Termer och definitioner

Termerna och definitionerna 2.1 till och med 2.17 är de vilka nämns under kapitel 2 i SS-ISO/IEC 17799:2005.

Termerna och definitionerna utan beteckning är ett urval av kompletterande termer och definitioner vilka förekommer i denna handbok.

2.1
Tillgång
Allt som är av värde för organisationen

2.2
Skyddsåtgärd
Handling, procedur eller tekniskt arrangemang som genom att minska sårbarheten möter identifierat hot

2.3
Vägledning
Beskrivning som klargör vad som ska göras och hur, för att nå målen i policys

2.4
Informationsbehandlingsresurser
Informationsbehandlingssystem, -tjänst eller stödjande infrastruktur, eller lokaler som inhyser resurserna

2.5
Informationssäkerhet
Förmågan att bevara sekretess, riktighet och tillgänglighet hos information. Därutöver kan begreppet innefatta t.ex. autenticitet, spårbarhet, oavvislighet och tillförlitlighet

2.6
Informationssäkerhetshändelse
En fastställd förekomst av ett tillstånd i ett system, nätverk eller för en tjänst som indikerar ett tänkbart brott mot informationssäkerhetspolicyn eller brister i skyddsåtgärder, eller en ny och okänd situation som kan påverka säkerheten

2.7
Informationssäkerhetsincident
En eller flera händelser som kan tänkas få eller kunnat få allvarliga konsekvenser för verksamheten och hota informationssäkerheten

2.8
Policy
Övergripande avsikt och viljeinriktning formellt uttryckt av ledningen

2.9
Risk
Produkten av sannolikheten för att ett givet hot realiseras och därmed uppkommande skadekostnad

2.10
Riskanalys
Process som identifierar säkerhetsrisker och bestämmer deras betydelse

2.11
Riskbedömning
Övergripande process för riskanalys och riskutvärdering

2.12
Riskutvärdering
Process som jämför uppskattad risk mot given riskbedömningsgrund för att fastställa riskens betydelse

2.13
Riskhantering
Samordnande aktiviteter för att styra och kontrollera en organisation med avseende på risk

2.14
Riskbearbetning
Bearbetningsprocess för val och införande av åtgärder för att begränsa risker

2.15
Tredje part
Person eller organisation som anses fristående från de berörda parterna i den aktuella frågan

2.16
Hot
Möjlig, oönskad händelse med negativa konsekvenser för verksamheten *

2.17
Sårbarhet
Brist i skyddet av en tillgång exponerad för hot

Kompletterande termer och definitioner

ADB
Automatisk Databehandling (ADB) är ett begrepp som används i datalagen

ADB-säkerhet
Säkerhet beträffande skydd av datorsystem och dess data syftande till att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling

Arkivering
Arkivering är en långtidslagring. Viktiga beslut att ta vid lagring är vad som skall lagras, hur länge, på vilket media och vilken säkerhet krävs

Attack
Aktiviteter som syftar till att åstadkomma skada på verksamheten eller verksamhetens resurser

Autenticering
En kontroll av en användares identitet för att säkerställa att användaren verkligen är den han eller hon utger sig för att vara

Avveckling
Att lägga ned, stänga ett system eller organisation

Certifiering av ledningssystem för informationssäkerhet
En formell certifieringsprocess där ett certifieringsorgan genom bedömning fastställer att det implementerade ledningssystemet uppfyller kraven i standarden

Elektronisk handel/Elektroniska affärer
Parter utväxlar affärsinformation via olika former av elektronisk kommunikation

Elektroniska signaturer/Digitala signaturer
Omvandling av ett meddelande (eller ett kondensat av detta) på ett sätt som endast avsändaren kan utföra och som tillåter mottagaren att kontrollera meddelandets äkthet, innehåll och avsändarens identitet

Hotbild
Hot som bedöms förekomma mot en viss verksamhet

Intrång
Oönskad interaktion och aktiviteter mot system
- i strid med systemets policy
- som kan medföra förändringar, störningar eller skada

Kontinuitetsplan
Dokument som beskriver hur verksamheten skall bedrivas när identifierade, kritiska verksamhetsprocesser allvarligt påverkas eller störs under en längre, specificerad tidsperiod, d.v.s. en typ av reservplan för verksamheten

Kryptering
Omvandling av klartext till kryptotext med ett krypteringssystem och kryptonyckel i syfte att förhindra obehörig åtkomst

Kvarvarande risk
Skyddsåtgärder tar inte bort risken till fullo. Det finns alltid en viss sannolikhet att den kvarvarande risken realiseras och medför skada i någon form

Lösenord
Teckensträng som anges för att verifiera användaridentitet

Resurs
1. något som används eller förbrukas när en operation utförs
2. systemkomponent med viss fastställd funktion för lagring, överföring eller bearbetning

Riskacceptans
Den medvetna handlingen att leva med riskens konsekvens/er

Riskreduktion
Att minska risken genom att mildra, förebygga eller föregripa den. Det kan ske genom att undvika risken, överföra den genom exempelvis försäkringar eller genom att reducera hotet, sårbarheten eller den möjliga påverkan. Det kan också ske genom att upptäcka oönskade händelser, reagera på dessa och vidta åtgärder

Svaghet
Se Sårbarhet

Upphovsrätt
Upphovsrätt ger rättsligt skydd till personer som skapat något med så kallad verkshöjd. Exempel på sådant skapande kan vara litterära verk, bilder, musik och programvara

*Definitioner vilka används för olika former av hot

Avsiktligt hot
Hot och aktivitet som syftar till att skada verksamheten

Oavsiktligt hot
Hot och aktiviteter som existerar trots att illasinnad avsikt saknas. Brist på kompetens och utbildning kan vara en anledning

Yttre hot
Hot som har sitt ursprung utanför organisationen

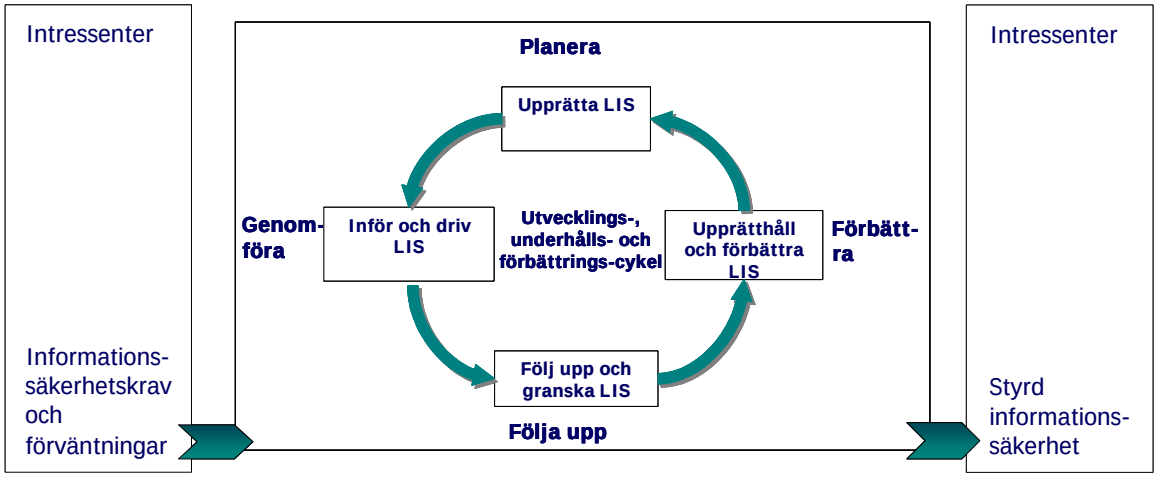
Inre hot
Hot mot säkerheten som orsakas av individer inom organisationen

Kapitel 3 Standardens struktur

3.1 Avsnitt

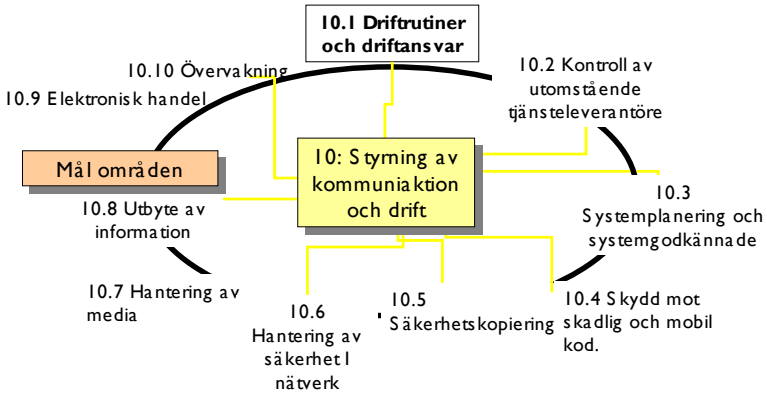
Standarden SS-ISO/IEC 17799 omfattar elva avsnitt för styrning av säkerhet samt en inledande beskrivning av riskbedömning och riskhantering. Kapitelindelningen och även underliggande rubriker överensstämmer med standarden SS-ISO/IEC 17799:2005.
Vid certifiering av ett ledningssystem eller annan bedömning av överensstämmelse mot krav som exempelvis vid internrevision används standarden SS-ISO/IEC 27001 Ledningssystem för informationssäkerhet - Krav.
Denna standard har en disposition vilken i stort överensstämmer med kravstandarderna SS-EN ISO 9001, ledningssystem för kvalitet och SS-EN ISO 14001, ledningssystem för miljö. Standarden innehåller även under bilaga C en korsreferenslista till SS-EN ISO 9001:2000 och SS-EN ISO 14001:2004.
SS-ISO 27001 har en bilaga A vilken är utformad som en checklista där de olika punkterna direkt överensstämmer med motsvarande kapitel och underrubrik i SS-ISO/IEC 17799:2005.

Att implementera och förvalta ett ledningssystem för informationssäkerhet är att systematiskt styra verksamheten utgående från kraven på verksamheten, se nedanstående figur.

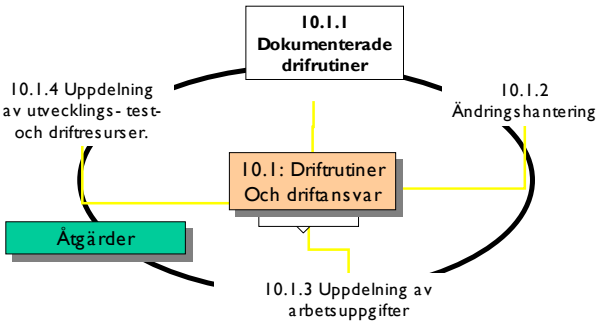


3.2 Indelning inom huvudområden

För varje område beskriver standarden SS-ISO/IEC 17799 ett mål för styrning och vilka åtgärder som kan tillämpas för att uppnå detta. Standarden ger även vägledning för införande av åtgärder och i flera fall även viktig övrig information.



Exempel på utformning av ett målområde



Kapitel 4 Riskbedömning och riskhantering

4.1 Allmänt

Riskhantering är att hantera risker och därmed möjliga oönskade händelse eller skador som en organisation kan drabbas av. Detta kan göras på många olika sätt och sättet bör anpassas till organisations inre och yttre miljö. Riskhanteringen görs enligt ett antal steg i en riskhanteringsprocess.

Error! Objects cannot be created from editing field codes.

Figur 1 Riskhanteringsprocess

Processen består av ett antal aktiviteter:

1. Kommunikation
2. Etablering av miljö; intern & extern
3. Riskbedömning som består av
    a. Riskanalys som består av
        i. Identifiera risker
        ii. Analysera risker
    b. Riskutvärdering
4. Riskbearbetning
5. Utvärdering

4.1.1 Kommunikation

Denna del av processen är viktig för varje steg i hela processen. För att uppnå en effektiv riskhanteringsprocess måste det finnas möjlighet för interna diskussioner mellan olika interna intressenter men också med externa intressenter.

Det är viktigt att kartlägga organisationens interna och externa intressenter. Organisationen bör utveckla en kommunikationsplan med dessa. Planen bör innehålla processen för en sådan kommunikation. En effektiv kommunikationsplan ger möjlighet att samla in olika synpunkter och perspektiv från olika kompetensgrupper, förstå intressenternas krav och förväntningar etc. för att den vidare delen av processen som riskbedömning och riskhantering blir rätt. Kommunikationen bidrar till att riskhanteringsprocessen tar hänsyn till intressenternas krav och förväntningar.

4.1.2 Etablera extern och intern miljö

För att få en effektiv riskhanteringsprocess måste alla tillgångar och resurser båda internt och externt identifieras och ligga som grund för att upprätta rätt säkerhetskrav. Rätt säkerhetskrav måste alltså baseras på både intern och extern miljö.

4.1.3 Etablering av extern miljö

Att etablera extern miljö betyder att definiera relationen mellan organisationen och dets externa miljö. Detta inkluderar:

- Politisk situation, social och kulturell miljö
- Externa intressenter så som
    - Styrelse och ägare
    - Kunder och affärsrelationer
    - Konkurrenter
    - Leverantörer
    - Etc.

Det är viktigt att upprätta en policy för extern kommunikation.

4.1.4 Etablering av intern miljö

Att etablera en intern miljö innebär att definiera organisationens verksamhet och interna intressenter. Detta inkluderar att identifiera kultur, struktur(er), organisation(er), processer, tillgångar som kapital etc.

Det är viktigt att upprätta en policy för intern kommunikation.

4.1.5 Riskbedömningsgrund eller kriterier för riskbearbetning

Definiera kriterier för hur en risk skall utvärderas och identifiera riskhanteringskrav är viktigt. Detta skall göra med hänsyn tagen till den interna och externa miljön.

För att ta beslut för om riskkriterierna är det viktigt att ta hänsyn till:

- konsekvenserna
- intressenternas krav
- etc.

4.2 Bedömning av säkerhetsrisker

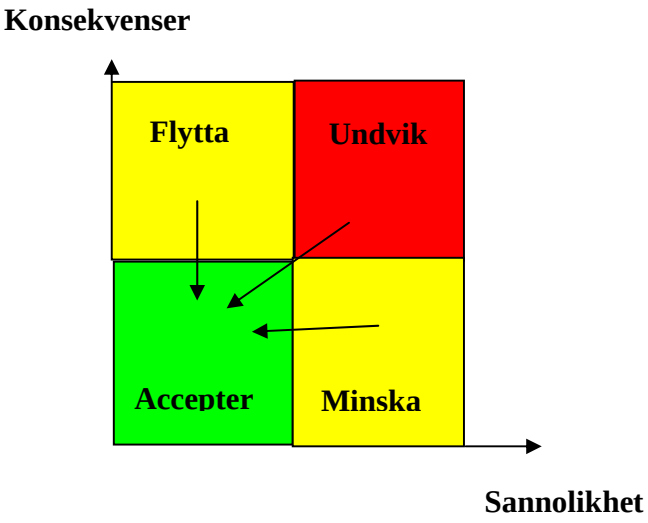
Riskbedömningen innebär att hantera risker på ett systematiskt sätt och består av två delar:

1. Riskanalys
2. Riskutvärdering

4.2.1 Riskanalys

Riskanalysen är en viktig del. Denna består av två steg:

1. Identifiera risker
2. Analysera risker



4.2.2 Identifiera risker

Här är det viktigt att identifiera alla risker i en organisation, såväl nya som de vilka eventuellt redan är under hantering. I detta steg skall alla risker identifieras; de som kanske kan inträffa, de som redan finns och är identifierade. Här identifieras också olika oönskade händelser som skall kunna inträffa och källor eller orsaker till dessa.

Resultatet är en lista av risker och källor för olika oönskade händelser.

4.2.3 Analysera risker

Analysera risker betyder definiera och förstå risknivå och riskernas natur. Det ger input till ett senare beslut om risken skall hanteras eller inte.

Riskanalysen skall innehålla alla riskkällor, negativa och positiva konsekvenser med hänsyn till intressenterna. Analysering av risken skall ske genom att kombinera konsekvenser och intressenter.

4.2.4 Riskutvärdering

Riskutvärdering är en process som jämför uppskattad risk mot given riskbedömningsgrund (eller kriterier för riskhantering) för att fastställa riskens betydelse. Detta görs mot det underlag som är tagit fram under steget Etablering av miljö. De risker som värderas som acceptabla hanteras inte vidare utan övervakas och utvärderas kontinuerligt.

De risker som utvärderas till att tas hand om och minska eller eliminera skall hanteras i steget Hantering av säkerhetsrisker.

4.3 Bearbetning av säkerhetsrisker

Efter en värdering av riskerna och en prioritering av de risker som skall hanteras skall en plan för hanteringen göras. Besluten omfattar:

- Går det att reducera riskerna
- Helt undvika risker
- Överföra risker till andra

Planen skall innehålla tydliga roller och ansvar.

4.3.1 Utvärdering

Riskbearbetning är en kontinuerlig process och denna skall ständigt utvärderas. Detta kan ske genom aktiv granskning eller på annat sätt.

Kapitel 5 Säkerhetspolicy

5.1 Informationssäkerhetspolicy

Mål: Att ange ledningens viljeinriktning och stöd för informationssäkerhet i enlighet med organisationens verksamhetskrav och relevanta lagar och föreskrifter.

Organisationens ledning bör klart ange en viljeinriktning i enlighet med verksamhetens mål och visa sitt stöd och åtagande för informationssäkerhet genom att fastställa och underhålla en informationssäkerhetspolicy för hela organisationen.

Informationssäkerhetspolicyn är ledningens instrument för att klart ange inriktningen och visa sitt engagemang för informationssäkerheten – "det här är vår avsikt, så här vill vi ha det och så når vi dit".

Att tillföra företagskulturen en ny dimension – "i vår verksamhet är säkerhet ett självklart inslag i arbetet". Den ger ökad trygghet, trivsel och bidrar till ett bättre resultat. Den ska också vara en plattform för konsekvent agerande, göra de anställda medvetna om säkerhetens betydelse samt visa vägen för att uppnå säkerhetsmålen.

Informationssäkerhetspolicyn ska besvara följande frågor:

- Vad är det som ska skyddas?
- På vilken nivå ska skyddet vara?
- Vem är ansvarig för informationssäkerheten?
- Hur bedrivs informationssäkerhetsarbetet?
- Var gäller informationssäkerhetspolicyn?
- Hur ska informationssäkerhetspolicyn följa verksamheten och hotbilden?
- Vilka rättigheter och skyldigheter har medarbetarna?
- Hur ska incidenter hanteras?
- Påföljder då informationssäkerhetspolicyn ej följs?

För att en informationssäkerhetspolicy ska få avsedd effekt är det några punkter som bör beaktas vid framtagandet av informationssäkerhetspolicyn. Den ska

- vara relevant i förhållande till organisationens verksamhet,
- vara långsiktig,
- vara övergripande,
- visa ambitionsnivå och inriktning,
- vara kommunicerbar med organisationens samarbetspartners,
- ha ett enkelt språk,
- vara kortfattad,
- föras ut på ett tydligt sätt.

Det finns tillfällen då informationssäkerhetspolicyn har ett extra stort värde. Det kan röra sig om verksamheter som har speciellt skyddsvärd information som personuppgifter och finansiell verksamhet. Det kan också vara att säkerheten precis blivit en viktig fråga och det finns ett behov av att markera vad som gäller. Ytterligare ett exempel kan vara att man går in i ett nytt verksamhetsområde.

Organisationer som har ett markant säkerhetsinslag i sin verksamhet – nationella som internationella, privata som statliga – har en av ledningen uttalad och antagen informationssäkerhetspolicy som

- kan delges interna och externa intressenter vilket minskar risken för missförstånd och kan öka affärsmöjligheter och minska affärsrisken/-riskerna,
- underlättar granskning av det verkliga tillståndet med hänsyn till informationssäkerhetspolicyn.

En informationssäkerhetspolicy ska peka ut den övergripande inriktningen, slå fast de principer som ska gälla och tydliggöra organisationens inställning till arbetet, i detta fall informationssäkerhetsarbetet.

En informationssäkerhetspolicy är ett centralt och viktigt dokument som utgör grunden för organisationens övergripande och detaljerade säkerhetsmål.

Det är organisationens högsta ledning som fastställer informationssäkerhetspolicyn och därmed också ansvarar för dess innehåll och att den uppfylls. Ansvar, befogenheter, arbetssätt och beslutsordning i speciella frågor liksom verksamhetsinriktning på kort sikt (1–3 år) kan vidareutvecklas inom organisationen och beslut ska framgå av ett upprättat protokoll.

Organisationen måste kunna redovisa och dokumentera på vilket sätt man följer upp sina åtagande enligt informationssäkerhetspolicyn. Det ska därför med hjälp av fastlagda rutiner dokumenteras och säkerställas vilka resultat som uppnåtts för att leva upp till innehållet i och innebörden av informationssäkerhetspolicyn.

Såväl leverantörer och entreprenörer som kunder och samarbetspartners ska informeras om organisationens informationssäkerhetspolicy och syn på säkerhet samt de önskemål och krav som är förknippade med detta. Det innebär exempelvis att organisationens entreprenörer måste leva upp och ta hänsyn till organisationens informationssäkerhetspolicy.

5.1.1 Policydokument för informationssäkerhet

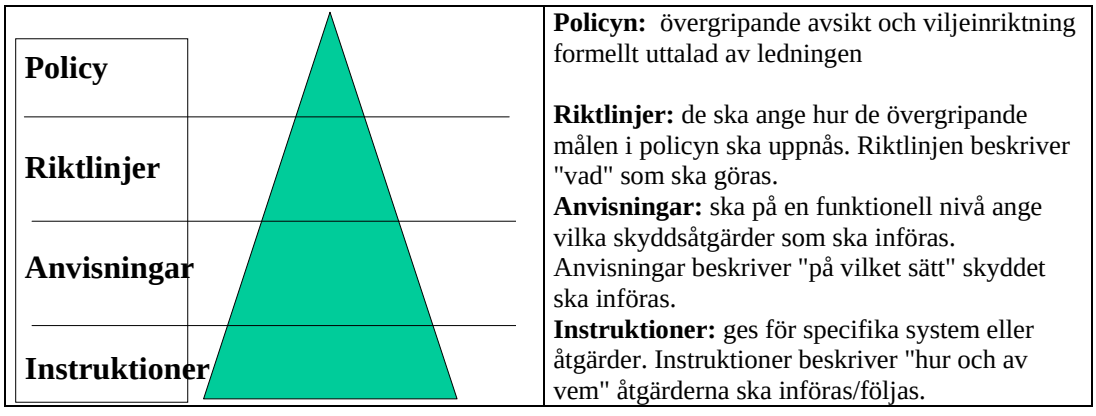
Informationssäkerhetspolicyn måste växa fram stegvis och vara förankrad i verksamheten. Den ska vara godkänd av ledningen. Efter beslut ska informationssäkerhetspolicyn förankras i verksamhetens alla delar.
Informationssäkerhetspolicyn kan utgöra en del av ett större policydokument. Policyn bör minst omfatta:

- Definition av begreppet informationssälerhet
- Ledningens viljeinriktning
- Mål och metoder för styrning
- Incidentrapportering
- Normer och krav på efterlevnad samt konsekvenser vid överträdelse
- Kontinuitetsplanering

En informationssäkerhetspolicy kan tas fram enligt följande steg:

1. Gå igenom frågelistan (*se punkt 3.2 Underlag för att skriva en informationssäkerhetspolicy*) och skaffa svar på frågorna. Välj struktur och mall (*se punkt 3.3 Exempel på informationssäkerhetspolicy*) för hur informationssäkerhetspolicyn ska utformas.
2. Ta ställning till de svar du fått på frågorna.
3. Stäm av relevansen i informationssäkerhetspolicyn genom att intervjua nyckelpersoner i verksamheten.
4. Förankra informationssäkerhetspolicyn i verksamheten.
5. Fastställ informationssäkerhetspolicyn i ledningen.
6. Inför och förankra den i organisationen.
7. Vid behov, minst årligen, revidera informationssäkerhetspolicyn.

Parallellt med arbetet att ta fram informationssäkerhetspolicyn bör en plan hur den ska förankras i verksamheten tas fram. I större organisationer kan det vara bra med en mix av åtgärder som exempelvis en kortfattad folder, presentationer ute i verksamheten, via intranet eller informationssäkerhetspolicyn som en bilaga i lönebeskedet.
En informationssäkerhetspolicy antagen av ledningen visar ledningens viljeinriktning och utgör en vägledning för den fortsatta utvecklingen av informationssäkerhetsarbetet och hur det ska bedrivas. En del i detta arbete är att ta fram det underliggande regelverket baserat på organisationens processer.



Figuren ovan visar på olika nivåer av dokumentation och vad varje nivå bör omfatta.

Checklista att använda vid utformning av policy, riktlinjer, anvisningar och instruktioner:

- Säkerhetsansvar och säkerhetsorganisation.
- Säkerhetsplan.
- Incidenthantering.
- Risk- och sårbarhetsanalys.
- Lagar och bestämmelser.
- Informationsklassning.
- Hantering av information.
- Datariktighetsskydd.
- Tillgänglighetsskydd.
- Spårbarhet.

- Logiskt åtkomstskydd.
- Fysisk säkerhet.
- Personal.
- Nyckelpersoner.
- Externa resurser/användare.
- Information och utbildning.
- Persondatorer och arbetsstationer.
- Nätverk, tele- och datakommunikation.
- E-post och Internet.
- Systemutveckling/miljö.
- IT-drift.
- Systemförvaltning.
- Ändringshantering.
- Kontinuitetsplanering

Omfattningen kan begränsas med hänsyn till organisationens storlek.

5.1.2 Granskning av informationssäkerhetspolicyn

Informationssäkerhetspolicyn bör granskas med planerade intervall eller då större förändringar med påverkan på verksamheten inträffar. Ett minimum är att policyn granskas i samband med ledningens genomgång. Det bör finnas rutiner för detta.
Vid granskning bör nedanstående beaktas:

- Resultat från tidigare ledningens genomgång
- Resultat från internrevisioner och oberoende granskningar
- Rapporterade säkerhetsincidenter
- Åtgärder för att förbättra informationssäkerheten och de processer som berörs

Underlag för att skriva en informationssäkerhetspolicy

Det är viktigt att skaffa sig underlag innan man börjar skriva informationssäkerhetspolicyn. I texten nedan finns ett antal frågor som är viktiga att ställa sig innan man börjar skriva.

1. Vilket mål har organisationen för sin verksamhet?
2. Vad är prioriterat i verksamheten?
3. Vad säger IT-strategin?
4. Finns det något fastställt dokument som beskriver dokumentnivåer i verksamheten (policy, riktlinjer, anvisningar, instruktioner)?
5. Finns det någon allmän säkerhetspolicy för organisationen?
6. Vilken information ska omfattas av informationssäkerhetspolicyn?
7. Vilka problem ska lösas med informationssäkerhetspolicyn?
8. Vad ger analyserna för underlag till informationssäkerhetspolicyn (risk-, affärsberoende- och säkerhetsanalys)?
9. Kan avsteg från informationssäkerhetspolicyn tillåtas? Hur ska sådana avsteg regleras/hanteras?
10. Vilka påföljder kan vara aktuella om informationssäkerhetspolicyn inte följs?
11. Krav på riktlinjer för informationssäkerheten?
    – internet?
    – e-post?
    – personlig integritet?
    – användningssätt?
    – konfidentiell/sekretessbelagd information?
    – programvarulicenser?
    – utläggning (outsourcing)?
12. Finns det en revideringsperiod för informationssäkerhetspolicyn?
13. Vilka hot finns mot organisationen (i dag och i framtiden)?
14. Mot vilken typ av information riktas hoten?
15. Har sannolikheten för och konsekvensen av dessa hot analyserats?
16. Vilka resurser ska skyddas?
17. Sekretess/riktighet/tillgänglighet?
18. Fred-, kris- och krigsaspekten, påverkar detta hur informationssäkerhetspolicyn utformas?
19. Vilken är den önskade nivån för informationssäkerhet?
20. Skyddskrav på utrustning och information utanför arbetsplatsen?
21. Tredje parts tillgång till information?
22. Hur fördelas kostnaderna för informationssäkerhetsåtgärder?
23. Hur mycket har investerats i fysiska skyddsåtgärder?
24. Hur mycket kostar den personella bevakningen per år?
25. Är ledningen involverad i säkerhetsarbetet?
26. Vem hanterar säkerhetsfrågor i organisationen?
27. Vem har ansvaret för säkerhetsfrågor i organisationen?
28. Finns det en säkerhetschef eller motsvarande?
29. Beslutsnivåer för säkerhetsfrågor?
30. Känner cheferna till verksamhetens säkerhetsregler?
31. Finns det en samordningsgrupp för säkerhet?
32. Vilka instruktioner om informationsskydd finns i dag?
33. Finns det anvisningar om klassificering av information?
34. Hur sker kunskapsspridningen rörande säkerhetsfrågor?
35. Finns det någon intern utbildning i säkerhet?
36. Finns det behov av utbildning i säkerhet?
37. Är informationssäkerhet kopplad till det övriga arbetet/säkerhetsarbetet?
38. Vem ska ha tillgång till vilken information?
39. Åtkomsträttigheter?
40. Loggning?
41. Extern kommunikation?
42. Externa beroenden?
43. Förekommer distansarbete?
44. Får användare ta hem arbetsutrustning?
45. Incidenthantering?
46. Kritiska händelser de senaste 3 åren?
47. Hur ser skadestatistiken ut?
48. Hur bedriver organisationen det skadeförebyggande arbetet?
49. Finns rutiner för att hantera skador/incidenter?
50. Erfarenheter av skador/incidenter?
51. Förändringar som gjorts i system/rutiner efter en skada/incident?
52. Medverkandes ansvarsområden?
53. Hur stor är personalomsättningen?

Exempel på informationssäkerhetspolicy

Informationssäkerhetspolicy för Medytekk

Daterad 2005-xx-xx.
Fastställd av företagsledningen 2005-xx-xx.
All personal ska tilldelas ett personligt exemplar av informationssäkerhetspolicyn.
Informationssäkerhetspolicyn kommer att presenteras vid interna möten under hösten.

Motiv
Vi som arbetar på Medytekk använder IT för att stödja, utveckla och effektivisera verksamheten. Vårt företag är beroende av informationsbehandlingen. Kraven på snabb och relevant information inom olika funktioner av Medytekks verksamhet ökar. Att säkerställa hög tillgänglighet och samtidigt innehålla nödvändiga krav på sekretess är väsentligt ur affärssynpunkt.

Definition
Informationssäkerhet inbegriper all säkerhet kring Medytekks totala informationsbehandling. Såväl organisatoriska åtgärder som fysiska och logiska skyddsåtgärder inbegrips. Exempel på säkerhetsrelaterade åtgärder är en fastställd informationssäkerhetspolicy, ansvarsfördelning, utbildning, riskanalys, katastrofplan, behörighetsregler, informationsklassning, säkrad driftmiljö, åtkomstskydd i datorer, regler för hantering av datamedia, behörighetsadministration, säkerhetskopiering, regler för extern kommunikation och modemuppkopplingar etc och kontroll av uppgiven identitet vid till exempel påloggning med hjälp av aktiva kort (förstärkt autentisering).

För att tillgodose kraven som ställs på informationssystemen, där så gott som all Medytekks information hanteras på ett eller annat sätt, är det nödvändigt att hanteringen av information sker på ett så tillförlitligt sätt som möjligt. Informationssäkerheten ska motverka risker för såväl obehörig läsning och förändring av data som för förlust av data. Informationssäkerheten syftar även på informationens kvalitet, riktighet och tillgänglighet.

Nyckelord för informationssäkerheten är att säkra informationens

- sekretess,
- tillgänglighet,
- riktighet,
- spårbarhet.

Informationssäkerhetspolicyn utgör ett komplement till Medytekks målbeskrivning och IT-strategi, som anger inriktningen för den totala informationsbehandlingen. Informationssäkerhetspolicyn är det grundläggande underlaget för informationssäkerhet och berör samtliga anställda, samarbetspartners och konsulter.

Informationssäkerhetspolicyn ger inriktningen och de övergripande målen för hur informationssäkerhetsarbetet ska bedrivas inom företaget - för verksamheten, personalen, kunderna och samarbetspartners.

Tillhörande dokument
Riktlinjer för informationssäkerhet är ett deldokument till informationssäkerhetspolicyn som beskriver riktlinjerna för informationssäkerhetsarbetet. Detta deldokument innehåller motiv, mål, tidplan, definition, omfattning och ansvarsfördelning.

Som ett komplement till den övergripande informationssäkerhetspolicyn och riktlinjerna kommer dokument att finnas i form av anvisningar inom olika områden för informationssäkerhetsarbetet. Dessa samlas i en informationssäkerhetshandbok som sammantaget visar hur informationssäkerhetsarbetet ska bedrivas. För specifika områden kan det även finnas instruktioner på en mer detaljerad nivå som beskriver vad som gäller. Dessa dokument beskriver tillsammans alla fysiska och logiska åtgärder som syftar till att förebygga eller minimera oönskade konsekvenser av olika händelser på informationssystemsområdet.

Mål för informationssäkerheten
Målsättningen med denna informationssäkerhetspolicy är att säkerställa sekretess, tillgänglighet och spårbarhet för verksamhetens information och data, samt att reducera risken för skador på verksamheten oavsett orsak och angripare.

- Avsikten med denna informationssäkerhetspolicy är att skydda organisationens informationstillgångar mot alla typer av hot - interna eller externa, avsiktliga eller oavsiktliga.
- Det ska finnas skyddsmekanismer som utifrån nedanstående punkter säkerställer informationens
  – sekretess,
  – tillgänglighet,

– riktighet,
– spårbarhet.

- Informationssäkerhetsarbetet ska bedrivas enligt standarden SS-ISO/IEC 27001.
- Alla anställda inom organisationen som i sina arbetsuppgifter berörs av IT ska vara medvetna om informationssäkerhetsfrågornas betydelse samt ha kunskaper om vad som gäller för att bevara och utveckla en säker och stabil IT-miljö.
- Informationssäkerheten ska vara en integrerad del i Medytekks ordinarie verksamhet och stödja verksamheterna i att uppnå de uppsatta målen för kvalitet och effektivitet.
- Till grund för informationssäkerhetsåtgärder ska föreligga dokumenterade bedömningar eller genomförda riskanalyser.
- Skydden för kända hot ska vara uppbyggda till rätt nivå med hänsyn till skyddskostnad och konsekvens för Medytekks verksamhet vid eventuellt tillfogad skada.
- Alla säkerhetsincidenter, konstaterade eller misstänkta, ska rapporteras till och utredas av informationssäkerhetschefen.
- Uppföljning av riskanalyser, skyddsåtgärder och utbildningsinsatser ska ske kontinuerligt.
- En kontinuerlig drift ska garanteras genom att säkerställa driftmiljön för samtliga datordriftställen.
- Medytekk ska ha egen IT-personal, det vill säga anställda med rätt kompetens och som fortlöpande utbildas i takt med att datorsystemen utökas och förändras.
- Känslig data ska skyddas mot otillbörlig åtkomst inom och utom företaget med hjälp av behörighetskontroll och i vissa fall kryptering.
- Säkerhetsarbetet ska skydda personalen i dess tjänsteutövning.
- Kommunikationslösningar ska vara gjorda så att resursdatorer och nätverk skyddas mot driftsstörningar och intrång. Driftstörningar och intrång ska kunna följas upp med hjälp av dokumenterad historik (loggar).
- Man ska leva upp till gällande lagar och kommersiell sekretess. Exempelvis ska personuppgiftslagen (PUL) följas så att den personliga integriteten beaktas i användningen av personregister. Bokföringslagen ska följas vad gäller ansvarsfördelning och behandlingshistorik för att uppnå en tillförlitlighet och en god intern kontroll av redovisningen.

Omfattning

Informationssäkerhetspolicyn rör all informationsbearbetning oavsett driftmiljö, alltså oberoende av om datorbearbetningen sker i resursdator (stor-, minidator, eller server) eller persondator.

Informationssäkerhetspolicyn gäller även om datorbearbetningen sker externt och via datakommunikation eller motsvarande. Med datorbearbetning menas hela informationssystemet: system-/programutveckling, källdataframställning, registrering, dataöverföring, bearbetning, datalagring, utdatahantering, arkivering och makulering.

Genomförande

För att nå de uppsatta målen ska resurser avdelas för att systematisk genomföra

- riskbedömningar och konsekvensanalyser,
- riktlinjer och handlingsplan,
- informationssäkerhetshöjande åtgärder,
- utbildning och information.

Årligen ska en plan för säkerhetsarbetet inom varje avdelning upprättas. Planen ska innehålla en beskrivning av säkerhetsläget samt de planerade åtgärderna som ska vidtas för att höja säkerhetsnivån. Planerna sammanställs till en handlingsplan och en budget för informationssäkerheten för hela Medytekk. Ledningen fattar beslut om planen, dess genomförande och budget.

Övergripande ansvar

Företagsledningen är ytterst ansvarig för mål och ramar för informationssäkerhetsarbetet och bär det yttersta ansvaret för skador som kan inträffa. Ledningen följer upp informationssäkerhetsläget genom att ta del av säkerhetsplanen.

Ansvarsfördelning

Informationssäkerhetschefen sammanställer avdelningarnas säkerhetsplaner och upprättar en säkerhetsplan för hela Medytekk samt svarar för initiering och uppföljning av informationssäkerhetsarbetet enligt planen.

Informationssäkerhetssamordnaren är ansvarig för att informationssäkerhetsåtgärder genomförs enligt ledningens och informationssäkerhetschefens beslut. Samordnaren ska leda informationssäkerhetsarbetet inom respektive tilldelat ansvarsområde och är även registeransvarig för avdelningens personregister.

Den system-/driftansvarige har det operativa ansvaret för att beslutade åtgärder genomförs. Ansvaret kan gälla ett eller flera IT-system. Den ansvarige är skyldig att omgående meddela säkerhetsproblem och misstanke om eller redan inträffade incidenter till informationssäkerhetssamordnaren eller informationssäkerhetschefen.

Användaren ska verka för en god informationssäkerhet inom sitt område och följa de regler och riktlinjer som gäller inom Medytekk. Nivån på informationsskyddet inom företaget beror på hur varje enskild person hanterar verktygen för informationsbehandling såsom datorer, disketter, datakommunikation (e-post, fax etc).

Dotterbolag/partners

I enlighet med företagsägarnas enhälliga beslut vid fastställandet av denna informationssäkerhetspolicy år 2005, gäller samma informationssäkerhetspolicy för dotterbolag och partners.

Informationssäkerhetspolicyns giltighet

Planering av framtida informationsstrategier ska ske i samarbete med respektive företagsledning. Informationssäkerhetschefen ska arbeta för att informationssäkerheten i samtliga bolag uppnår jämlika nivåer till det fjärde kvartalet 2006. Revidering av informationssäkerhetspolicyn samt riktlinjerna kommer att göras därefter för att i ny upplaga börja gälla fr.o.m. 2007

Checklista – Informationssäkerhetspolicy

Fråga	Ja	Delvis	Nej
Ger informationssäkerhetspolicyn ledningens viljeinriktning och stöd för informationssäkerhetsarbetet?			
Har ledningen fastställt informationssäkerhetspolicyn?			
Är det beskrivet hur informationssäkerhetspolicyn ska underhållas och på vilket sätt?			
Är informationssäkerhetspolicyn förankrad i verksamheten och finns det ett system för detta?			
Finns det en definition av informationssäkerhetsbegreppet?			
Tar informationssäkerhetspolicyn hänsyn till hoten från anställda och utomstående?			
Visar informationssäkerhetspolicyn mål och omfattning samt vikten av informationssäkerhet?			
Är ansvaret definierat?			
Finns det reglerat hur rapportering av incidenter ska gå till?			
Hänvisar informationssäkerhetspolicyn till andra styrande dokument inom organisationen?			
Är det klart och tydligt beskrivet vem som är ägare till informationssäkerhetspolicyn?			

.

Kapitel 6 Organisation av informationssäkerheten

Att ha kontroll över organisationens informationstillgångar är nödvändigt för att säkerställa kontinuitet av verksamheten. För att på ett säkert sätt hantera informationstillgångarna behöver en infrastruktur upprättas för informationssäkerhetsarbetet.

Säkerhetsorganisationens storlek och sammansättning är beroende av vilken verksamhet som bedrivs (produktion/tillverkning, tjänsteföretag etc.), vilken hotbild som finns och organisationens storlek.

6.1 Intern organisation

Mål: Att hantera informationssäkerheten inom organisationen.
Ett ledningssystem bör upprättas för att initiera och styra införandet av informationssäkerhet inom organisationen.

Ledningen bör godkänna informationssäkerhetspolicyn, tilldela roller i säkerhetsarbetet, samt samordna och granska införandet av säkerhet i hela organisationen.

Om det är nödvändigt bör en enhet för specialistrådgivning i säkerhetsfrågor inrättas och göras tillgänglig för hela organisationen. Kontakter med externa säkerhetsspecialister eller –grupper, inklusive relevanta myndigheter bör utvecklas för att kunna följa med i säkerhetstrender i olika branscher. Syftet är att kunna följa utvecklingen av standarder och riskanalysmetoder samt även för att etablera lämpliga kontakter när det gäller hantering av säkerhetsincidenter. Ett tvärfunktionellt sätt att hantera informationssäkerhet bör uppmuntras

6.1.1 Ledningens engagemang för informationssäkerhet

För att arbetet med informationssäkerhet ska kunna bedrivas på ett strukturerat sätt bör man, speciellt i större organisationer, ta ställning till att inrätta en ledningsgrupp för detta. I ledningsgruppen bör nyckelpersoner i organisationens ledning ingå. Gruppen kan med fördel utgöra en del av den befintliga ledningsgruppen.
Att roller och ansvar identifieras och fastställs är av stor betydelse för informationssäkerheten.

I organisationer är det i dag vanligt att nyckelpersoner från ledningen inte finns representerade i liknande forum. Gruppen består då endast av säkerhets- och/eller informationssäkerhetschef samt olika linjechefer. För att kunna driva säkerhetsfrågor på ett effektivt sätt är det nödvändigt att även inkludera vd och andra nyckelpersoner på ledningsnivå. Säkerhetsarbetet ska emellertid ske i linjeorganisationen och är allas ansvar.

För att få kontinuitet i säkerhetsarbetet bör gruppen sammanträda med relativt täta tidsintervall. Alla aktiviteter och beslut bör dokumenteras i protokoll.

Vid ledningens genomgång ska frågor som granskning och godkännande, övervakning, uppföljning, stödjande och analyserande arbete, kravställande etc. tas upp. Även periodiska granskningar av informationssäkerhetspolicyn samt omvärldsanalys bör behandlas. Ansvar för genomförande av fastställda aktiviteter bör finnas hos en person inom gruppen, gärna företagsledningens representant.

I mindre organisationer kan frågor som rör informationssäkerhet behandlas i samband med exempelvis ordinarie ledningsgruppsmöte.

6.1.2 Samordning av informationssäkerhetsarbetet

I framför allt större organisationer är det oftast nödvändigt att inrätta ett forum med representanter på ledningsgruppsnivå för samordning av de aktiviteter som ska genomföras. Samordningen ska syfta till att utjämna skillnader mellan funktioner, avdelningar och geografiska platser inom organisationen.

Ett sådant forum kan till exempel se närmare på hur gemensamma metoder och processer kan användas för att få bättre möjlighet till utvärdering och jämförelse. Det kan också röra sig om att samordna stödet för organisationen i gemensamma frågor och att granska och tydliggöra behovet av åtgärder vid exempelvis säkerhetsincidenter och bristande efterlevnad av regelverk. Alla aktiviteter bör även här dokumenteras tillsammans med rapporter och beslut.

6.1.3 Fördelning av ansvar för informationssäkerhet

Ansvaret för att skydda organisationens tillgångar bör vara tydligt definierat. Ledningen har det yttersta ansvaret för informationssäkerheten och måste vara medveten om vad som krävs för att arbetet med informationssäkerhet ska bli så effektivt som möjligt. Genom den informationssäkerhetspolicy och det

underliggande regelverket som ledningen fastställt bör fördelning av ansvar och befogenheter i organisationen framgå.

Om möjligt bör en informationssäkerhetschef utses med ett överordnat ansvar för samordning av informationssäkerhetsfrågor.

6.1.4 Godkännandeprocess för informationsbehandlingsresurser

I många organisationer saknas riktlinjer för hur anskaffning av ny utrustning för informationsbehandling ska ske. När det saknas en dokumenterad process för detta ges utrymme för att felaktig utrustning anskaffas. Detta kan äventyra organisationens information både vad gäller sekretess, riktighet och tillgänglighet, vilket i sin tur äventyrar organisationens affärsverksamhet.

En grundprincip bör vara att personlig utrustning inte används på arbetsplatsen utan att en riskanalys har genomförts och att rustningen godkänts.

Utrustning bör väljas så att den svarar mot såväl de uppställda säkerhets- och kontrollkraven som affärsbehoven i verksamheten, men också så att den är kompatibel med annan utrustning.

Godkännande av syfte, användning och säkerhet kring utrustning är några punkter som klart måste framgå i en dokumenterad beslutsprocess. Det bör också stå klart vem som godkänner utrustningen.

6.1.5 Sekretessavtal

Vid anställning såväl som vid kontraktsskrivning med konsult bör ett sekretessavtal upprättas. Avtalet ska vara så skrivet att det entydigt definierar vad sekretessen avser samt vilka befogenheter och vilket ansvar för sekretessbehandlad information som gäller.
Inom den offentliga sektorn är sekretess reglerat i lagstiftning för de anställda och personer som anlitas av offentliga uppdragsgivare. Sekretessförbindelse är i dessa fall inte möjlig att använda utan ersätts i stället av en sekretesserinran. Denna skrivs inte under utan, som namnet säger, erinrar om gällande lagstiftning.

6.1.6 Myndighetskontakt

Det är viktigt att utgående från sin egen verksamhet identifiera vilka myndigheter man kan tänkas behöva kontakt med och även identifiera eventuella kontaktpersoner på dessa myndigheter. Inom den egna organisationen bör det finnas fastställda rutiner för hur kontakter skall tas. Beträffande informationssäkerhetsincidenter och hur dessa skall rapporteras kan det vara lämpligt att lyssna med berörda myndigeter och få deras synpunkter på lämplig hantering.

6.1.7 Kontakt med särskilda intressegrupper

För att säkerställa snabba åtgärder vid exempelvis säkerhetsincidenter är det viktigt för organisationen att etablera nätverk med andra företag, organisationer och myndigheter. Nätverken ger bland annat möjligheter att hålla sig informerad om nya hot och hur de kan bemötas. Det är också möjligt att få råd i säkerhetsfrågor, bygga upp kompetens inom organisationen och så vidare.

Personliga nätverk är oftast det bästa och snabbaste sättet att få kunskap om hur akuta problem kan lösas. Medlemskap i säkerhetsorganisationer och information via Internet är andra instrument.

Utbyte av information bör begränsas så att konfidentiell information ej delges obehöriga. Det är därför alltid på sin plats att hålla sig à jour med vad som för tillfället är konfidentiell information, samt hur länge skyddet gäller. Detta för att säkerställa att samarbetet sker på korrekta grunder

6.1.8 Oberoende granskning av informationssäkerhet

Oberoende granskningar av att styrmedel och tillämpningar som införts i organisationen verkligen fyller sina syften och svarar mot den fastställda informationssäkerhetspolicyn bör ske med jämna mellanrum. En oberoende granskning kan ske såväl av en extern (tredje part) som intern resurs. Det viktiga är att den som genomför granskningen inte är en del av den verksamhet som ska granskas eller på annat sätt medverkat till uppbyggnaden av det som granskningen omfattar.

6.2 Utomstående parter

Mål: Att bibehålla säkerheten hos organisationens information och resurser för informationsbehandling som är åtkomlig, bearbetas, kommuniceras till eller styrs av utomstående parter.

Säkerheten hos organisationens information och informationsbehandlingsresurser bör inte minskas genom introduktionen av utomstående parters produkter eller tjänster.

All åtkomst till organisationens informationsbehandlingsresurser liksom utomståendes bearbetning och kommunikation av information bör styras.

Där organisationen har behov av att arbeta med utomstående parter som kan kräva åtkomst till organisationens information och informationsbehandlingsresurser eller att ta emot eller lämna en produkt eller tjänst från eller till en utomstående part bör en riskbedömning göras för att avgöra säkerhetskonsekvenser och behov av styrning. Metoder för styrning bör överenskommas och definieras i överenskommelse med den utomstående parten.

6.2.1 Identifiering av risker med utomstående parter

Vid genomförandet av riskanalysen bör man först identifiera de informationsbehandlingsresurser som den utomstående parten måste få åtkoms till. Avstämning mot organisationens åtkomstpolicy bör göras för att säkerställa att behoven ryms inom denna. Riskerna skiljer sig mellan fysisk och logisk åtkomst. Med fysisk åtkomst menas bland annat tillgång till arkiv, värdeskåp och utrymmen för servrar. Den logiska åtkomsten innefattar exempelvis tillgång till organisationens databaser, ekonomisystem och personalinformation.

Om information lagras i databaser och den där skyddas på ett visst sätt är det inte ovanligt att den skrivs ut och blir tillgänglig i pappersformat. Hantering och lagring av information brukar då ofta ske på andra premisser – ofta felaktiga – än vad som ursprungligen var fallet när den var lagrad på datamedia. Detta utan att involverade personer förstår att de gör fel.

En annan faktor att beakta är skälen för åtkomst från tredje part. Vilka risker finns till exempel när det gäller fysisk och logisk åtkomst då organisationen behöver utnyttja inhyrd servicepersonal för sina IT-system?

Många organisationer köper i dag färdiga programvaror, exempelvis ekonomisystem. Programvarorna ska uppdateras och anpassas i olika skeden och det kräver i de flesta fall att tredjepartskunskap måste användas för att genomföra arbetet. Finns medvetenhet om riskerna med detta? Finns vetskap om vilken tillgång till organisationens övriga informationsresurser som möjliggörs i samband med arbetet?

Eventuella behov av sekretessavtal bör alltid övervägas. Utomståendes åtkomst till organisationens informationsresurser bör tillåtas först när eventuella avtal skrivits under och de säkerhetsåtgärder införts som har bedömts vara nödvändig.

6.2.2 Hantering av säkerhet vid kundkontakt

I de fall då organisationens kunder önskar eller ha behov av att få tillgång till organisationens information bör detta föregås av en genomgripande analys. Vid riskhantering måste även beaktas de möjligheter till begränsningar som kan genomföras. Rutiner för att skydda organisationens tillgångar kan behöva upprättas.
Vilken information kunden skall ges tillgång till och förutsättningarna för detta bör regleras i ett avtal med kunden.

6.2.3 Hantering av säkerhet i avtal med utomstående

Tredjepartsåtkomst bör alltid baseras på ett formellt avtal. Avtalet är en mycket viktig form för att reglera säkerhetsvillkoren mellan parterna. När avtalet upprättas bör det även avtalas om de fall där andra parter ska omfattas av avtalet, som exempelvis tredjeparts samverkan med egna underleverantörer.

Avtalet bör omfatta alla nödvändiga säkerhetsvillkor och reglera ansvarsförhållanden. Det bör också omfatta möjligheten att omförhandla eller förändra avtalet, om och hur skadestånd ska utgå, ägareförhållande till gemensamt utfört arbete, möjlighet att genomföra revision och kontroll etc.

Av vikt är också att se över likheter och olikheter mellan den egna organisationen och den motsatta parten innan en affärsrelation upprättas. Att ta hänsyn till då är främst inställningen till, och behovet av säkerhet för hantering av information. Ref. Sekretessavtal Kapitel 6.1.3.

Detta ställer höga krav på kontraktsgenomgången och den riskanalys som denna omfattar.

Exempel

Ledningskonferens

För två månader sedan publicerades delar av en affärsplan, som ledningen på Medytekk jobbar med, i kvällspressen.

Tidpunkten för publiceringen stämde väl överens med när ledningsgruppen på Medytekk hade varit på en helgkonferens där affärsplanen diskuterades och strategier lades upp.

Hur borde Medytekk ha skyddat sig?

Operatörsansvar

Medytekk har vid ett antal tillfällen haft problem med sina servrar och vid ett tillfälle var informationen på back up-media ofullständig.

Normalt brukar det inte vara problem med återläsning av säkerhetskopior, men vid det senaste tillfället lyckades man inte återskapa informationen och informationen blev ofullständig.

Detta berodde på att back up-körningen avbrutits under natten och den ansvarige teknikern hade inte gjort en ny tidigt nästa dag. Säkerhetskopiering gjordes dessutom endast en gång i veckan. Många forskare blev ursinniga och menade att en veckas arbete gått förlorat. Ansvaret för säkerhetskopieringen när den ordinarie teknikern var borta var oklart.

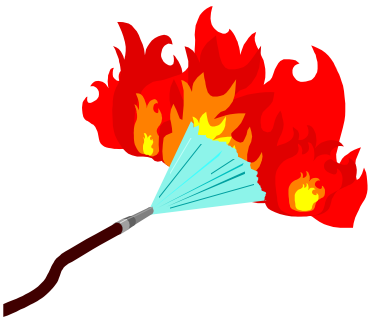
Vad borde Medytekk ha tänkt på?

Tredjepartsavtal

För en tid sedan uppmärksammades ledningen på att resultat från delprover i projekt A6 blivit kända av medarbetare i projekt B3.

Det visade sig att gästforskarna, som delade lägenhet, diskuterat sina rön, stick i stäv med den sekretesspolicy som ledningen hade och trodde fanns inskriven i avtalen med forskarna.

Vad borde Medytekk ha tänkt på?

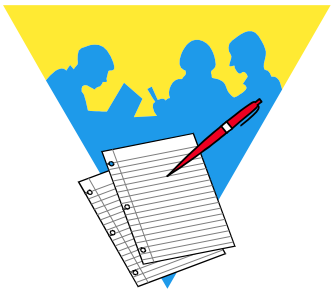


Försäkringsskydd

För tre år sedan inträffade en brand på FoU-avdelningen. Skadorna var relativt begränsade men saneringsarbetet tog tre veckor.

Det visade sig att försäkringsskyddet för avbrottet i verksamheten inte täckte skadan fullt ut.

Vad borde Medytekk ha tänkt på?



Organisation och ansvar – IT-avdelningen

It-chef Lennart Jakobsson har påpekat för vd att it-avdelningen är överbelastad med arbete och att det är viktigt att en strategi tas fram.

Medytekk expanderar kraftigt varje år och företaget har ingen it-strategi. Lennart har påtalat problemet för vd, Stefan Eriksson, men har fått en ganska sval respons. Lennart har tillsammans med sin

ersättare arbetat som administratörer och svarar för driften av nät och servrar. En annan person svarar för stöd till de anställda och fungerar även som nätverkstekniker. Den fjärde personen på avdelningen arbetar i huvudsak med applikationer och applikationsutveckling.

Vad borde Medytekk ha tänkt på?

Vad kan vi lära oss av dessa exempel?

Exempel 1 – Ledningskonferens

Medytekk borde ha tänkt på att försäkra sig om att konfidentiell information inte kommer i obehöriga händer genom att

- ha regler för klassning av information,
- ha regler för hantering av klassad information,
- säkerställa personalens lojalitet.

Dessutom borde Medytekk tänka på sekretessfrågan vid samtal vid val av konferensanläggning samt vad som får diskuteras utanför konferenssalen.

För att säkerställa att information inte läcks ut från ledningsnivå i framtiden borde Medytekk tänka på att

- införa ett system för klassning av information,
- införa en sekretessklausul i anställningsvillkoren.

Exempel 2 – Operatörsansvar

Medytekk borde ha tänkt på att utbildad personal som ansvarar för säkerhetskopiering fanns tillgänglig för att minska sårbarhet vid sjukdom, semester eller annan frånvaro.

För att säkerställa detta i framtiden borde Medytekk tänka på att

- identifiera viktiga funktioner och säkerställa att det finns utbildade ersättare vid frånvaro,
- säkerställa funktion hos utrustning för säkerhetskopiering genom kontinuerlig validering.

Exempel 3 – Tredjepartsavtal

Medytekk borde tänka på att

- se över tredjepartsavtalen för att säkerställa att sekretessen efterlevs,
- säkerställa att tredje part erhåller motsvarande information och utbildning i informationssäkerhet som den egna personalen har,
- klargöra säkerhetsnivåerna för varje avgränsat projekt,
- se till att riskanalys för de enskilda projekten utförs och dokumenteras,
- tydliggöra ansvar och befogenheter för projektledare i utvecklingsprojekt.

Exempel 4 – Försäkringsskydd

För att säkerställa att försäkringsskyddet är det rätta borde Medytekk tänka på att

- genomföra riskanalys som ger svar på vilka konsekvenser produktionsbortfall får,
- uppdatera sin försäkringsplan,
- utse en ansvarig för försäkringsfrågor inom företaget,
- upprätta kontinuerlig kontakt med försäkringsmäklare och försäkringsbolag.

Exempel 5 – Organisation och ansvar IT-avdelning

För att säkerställa att IT-avdelningen fungerar i framtiden borde Medytekk tänka på att

- definiera ansvar och befogenheter för tjänsten som IT-chef.

Checklista – Organisation av informationssäkerheten

Fråga	Ja	Delvis	Nej
Finns det en ledningsgrupp för informationssäkerhet?			
Är ansvaret för informationssäkerhetsarbetet tydligt definierat?			
Finns det en beslutsprocess för hur anskaffning av informationsbehandlingsresurser ska ske?			
Nyttjar organisationen egna experter vid säkerhetsincidenter?			
Nyttjar organisationen externa experter vid säkerhetsincidenter?			
Finns det förutsättningar inom organisationen att skapa nätverk med andra företag, organisationer eller myndigheter?			
Finns fastställda processer för hur oberoende granskning av informationssäkerheten ska ske?			
Finns det tredjepartsavtal som innehåller säkerhetsaspekter vid utläggning (outsourcing)?			
Genomförs riskanalyser innan tredjepartsåtkomst av organisationens informationsbehandlingsresurser tillåts?			

Kapitel 7 Hantering av tillgångar

Information och data som skapas, inhämtas, distribueras, bearbetas och lagras i en organisation är en av dess viktigaste tillgångar. Graden av tillgänglighet, sekretess och riktighet hos informationen är i många fall en utslagsgivande faktor för en organisations effektivitet, trovärdighet och långsiktiga konkurrensförmåga. Men det förutsätter att man har kännedom om vilka informationstillgångar som finns, deras karaktär och värdet för organisationen.

Att säkerställa att man har uppdaterad och korrekt kunskap om organisationens informationstillgångar är nödvändigt för att bedriva ett effektivt informationssäkerhetsarbete. En förutsättning för att på ett effektivt sätt fördela ansvaret för informationstillgångarna är att klassificera informationen med avseende på behov, prioritet och skyddsnivå. En korrekt klassificering och styrning av informationstillgångarna utgör ett viktigt underlag för informationssäkerhetsarbete och riskhantering, såväl i det dagliga arbetet som när det gäller strategiska beslut som rör informationstillgångarna.

7.1 Ansvar för tillgångar

Mål: Att uppnå och upprätthålla lämpligt skydd av organisationens tillgångar.

Alla tillgångar bör redovisas och ha en utsedd ägare.

Ägare bör utpekas för alla tillgångar och ansvaret för underhåll av lämpliga skyddsåtgärder bör utpekas. Införandet av särskilda skyddsåtgärder kan delegeras av ägaren om det anses lämpligt, men ägaren förblir ansvarig för att tillgångarna ges rätt skydd.

Att identifiera, värdera och dokumentera organisationens informationstillgångar är en mycket viktig del i ett aktivt säkerhetsarbete. Utöver identifiering och dokumentation bör varje tillgång också tilldelas en ägare. Respektive ägare ansvarar sedan för att en korrekt skyddsnivå införs och vidmakthålls. Skyddsnivån bör motsvara de krav som fastställts i organisationens system för klassificering av informationstillgångar.

7.1.1 Förteckning över tillgångar

Inom organisationen bör det finnas en upprättad inventarieförteckning över organisationens informationstillgångar. Några exempel är

- programvaror,
- databaser som exempelvis kundregister och leverantörsregister
- fysiska tillgångar,
- nyckelpersoner,
- immateriella tillgångar som patent och varumärken.

Varje identifierad tillgång bör ha en definierad och registrerad ägare. Även ägarens ansvar för den enskilda tillgången bör vara klarlagd och dokumenterad.

För att ett effektivt återställande efter exempelvis en stöld ska kunna genomföras bör det även dokumenteras var i organisationen varje tillgång normalt finns.

7.1.2 Ägarskap för tillgångar

Alla informationstillgångar bör ha en utsedd ägare. Det är väsentligt att ta hänsyn till hur tillgångarna används i verksamheten så att det finns en naturlig koppling mellan verksamhetsprocesser och ägarskap av tillgångar. Vid förändringar av verksamheten kan detta medföra att ägarskapet måste omprövas. Ägarskap innebär att säkerställa att informationstillgångar är rätt klassade och att de har ett skydd som står i relation till den fastställda klassningen. Rutinuppgifter kan delegeras men ansvaret för att de utförs kvarstår hos ägaren.

7.1.3 Godtagbar användning av tillgångar

Viktigt är att upprätta såväl rutiner som instruktioner för hur informationstillgångarna får användas. I de fall då tillgångarna även nyttjas av utomstående som exempelvis leverantörer, kunder, inhyrda konsulter etc. bör

avtal upprättas där villkor och krav tydligt framgår. Vid upprättande av instruktioner och avtal måste dessa givetvis avspegla den skyddsnivå vilken står i relation till hur tillgången klassats.
Glöm inte bort den utrusning och de informationstillgångar vilka används utanför kontoret som exempelvis bärbara datorer och mobiltelefoner.
Vid avveckling av utrustning är det nödvändigt att ta hänsyn till den information vilken kan finnas lagrad i utrustningen. Se information under punkten 9.2.6.

7.2 Klassificering av information

Mål: Att säkerställa att informationstillgångar får en lämplig skyddsnivå.

Informationen bör klassificeras för att ange behov, prioritet och förväntad grad av skydd vid hantering av informationen.

Information är känslig och kritisk i varierande grad. Vissa informationstillgångar kan behöva utökat skydd eller särbehandling. En modell för informationsklassificering bör användas för att definiera ett lämpligt antal skyddsnivåer och anvisa behov av särskild hantering.

Genom att upprätta och implementera ett system av informationsklasser inom organisationen skapas ett instrument för att effektivt kunna bestämma hur stora mängder information som ska skyddas och hanteras. Respektive klass bör tydligt avspegla värdet och betydelsen av tillgångarna.

De informationstillgångar som är viktiga för verksamheten bör analyseras för att få reda på hur stor tillgångens betydelse egentligen är. I analysarbetet bör parametrarna tillgänglighet, riktighet och sekretess vara grundbegrepp. Tillgången tillförs sedan en informationsklass som motsvarar dess betydelse för verksamheten.

7.2.1 Riktlinjer för klassificering

Det bör vara den utsedde ägaren eller den som skapat eller inhämtat informationen som ansvarar för att den också klassificeras. Det gäller oavsett vilken typ av information det är frågan om eller hur den lagras.

Ett effektivt klassificeringssystem vinner på att vara enkelt, och antalet klasser bör fastställas redan från början. För att säkerställa att beslut tagits angående klass bör även icke känslig information ges en identitet genom att exempelvis märkas som ”oklassificerad”. Exempel på klassning är oklassificerad, hemlig och kvalificerat hemlig. Ett annat exempel är oklassificerad, endast internt bruk, hemligt, kvalificerat hemligt och kvalificerat hemligt med restriktioner.

Information upphör ibland att vara känslig efter en viss tid eller genom att den exempelvis publiceras offentligt. Organisationens riktlinjer bör ta hänsyn till detta, och göra det möjligt för ägaren eller den som klassificerat informationen att regelbundet ompröva klassificeringen. På så sätt undviks på sikt onödiga kostnader för en eventuell överklassificering Lämpligt är att alltid kombinera klassen med ett bäst före datum ex. Kvalificerat hemligt t.o.m. 2008-06-21. Ett alternativ till datum kan vara en händelse som exempelvis annonsering. Ex. Kvalificerat hemligt t.o.m. annonsering.

Värt att notera är att den faktiska betydelsen av likartade benämningar av informationsklasser ofta skiljer sig åt mellan olika organisationer. Därför bör klassificerade dokument som härstammar från källor utanför den egna organisationen hanteras med särskild försiktighet om man är osäker på vad som gäller i det enskilda fallet.

7.2.2 Märkning och hantering av information

För att vara säker på att informationen hanteras riktigt är det av stor betydelse att det finns fungerande rutiner för märkning och hantering. Rutinerna ska självklart vara anpassade till det klassificeringssystem som organisationen antagit. Särskilt viktigt är detta för information som tillhör ”känsliga” eller ”kritiska” klasser. När ”utdata” som kan klassas som just ”känslig” eller ”kritisk” genereras i form av utskrifter, skärmbilder, e-post eller filöverföringar bör klassificeringen framgå tydligt. Om det går att märka informationen med fysiska etiketter är detta att föredra. Går inte det bör informationen i stället märkas elektroniskt. Rutiner och riktlinjer bör på detta område även omfatta information som tidigare klassats som känslig av andra organisationer.

Följande punkter betraktas som särskilt känsliga

- kopiering,
- lagring,

- överföring via post, fax, e-post,
- överföring via tal (även mobiltelefon, röstbrevlåda, telefonsvarare),
- förstöring,
- arkivering.

Inom varje informationsklass bör det finnas särskilda hanteringsrutiner för punkterna ovan.
Vid arkivering av information liksom vid avveckling av utrustning vilken innehåller inform är det väsentligt att beakta den klassning som informationstillgången har. Ref. 9.2.6

Exempel

1 – Förstörda data på lagringsmedia

För sex månader sedan slutade en av de anställda på Medytekks FoU Samtidigt återlämnade han sin bärbara dator till IT-avdelningen. Någon vecka senare visade det sig att de forskningsdata den anställde tagit fram saknades på företagets server. Forskaren kontaktades då och han berättade att han tagit egna kopior på diskett av de dokument och data som han bedömde som viktiga. ”Att lagra data på den centrala utrustningen kändes alldeles för osäkert – särskilt mot bakgrund av risken för virus”. Då disketterna senare återfanns hade forskarens kollegor formaterat om dem och de användes för andra ändamål.

Vad borde Medytekk tänkt på?

2 – Förlust av forskningsrapport

I samband med ett internt sammanträde försvann en viktig forskningsrapport.Den glömdes kvar efter ett sammanträde. Rapporten berörde centrala delar av bolagets forskningsresultat. Då personen som glömt den några timmar senare återvände till sammanträdesrummet var rapporten försvunnen. Senare visade det sig att bland annat en inhyrd IT-konsult disponerat rummet direkt efter mötet.

Vad borde Medytekk tänkt på?

3 – Spridning av känslig information

Jan är nyanställd laboratorieassistent. Som sådan har han tillgång till känslig information kring Medytekks verksamhet. Efter första veckan på nya jobbet blir han inbjuden på middag hos en av de nya kollegorna, Kalle. Efter middagen blir han, som en av flera gäster, föremål för värdinnans särskilda intresse. Hon visar sig vara mycket intresserad av Jans arbete. Då Jan har

stort förtroende för sin nya kollega ser han ingen anledning att inte kunna ha en ingående diskussion kring jobbet med Kalles sambo. Några dagar senare publiceras en anonym insändare i lokalpressen som i detalj beskriver förekomsten och omfattningen av djurförsök i Medytekks verksamhet.

Vad borde Medytekk tänkt på?

4 – Märkning av säkerhetskopior

Under en diskussion i samband med ett möte i ledningsgruppen väcker vd frågan hur det ”ser ut med företagets säkerhetskopior”. IT-chefen, som har stort förtroende för sina medarbetare, berättar att man regelbundet säkerhetskopierar väsentliga delar av datorsystemen. Samma eftermiddag beslutar sig IT-chefen för att för säkerhets skull kontrollera hur det förhåller sig. Det visar sig att det finns ett otal kassetter lagrade i det kassaskåp som är avsett för kopiorna. Någon enhetlig märkning eller struktur finns emellertid inte. Detta trots att han vid ett möte bara arton månader tidigare muntligen informerade sin personal om hur kopiorna ska märkas och lagras.

Vad borde Medytekk tänka på?

Vad kan vi lära oss av dessa exempel?

Exempel 1 – Förstörda data på lagringsmedia

Med ett system för klassificering och märkning av information hade man säkerligen minskat riskerna för att kritisk information hanteras som i exemplet. Med ett sådant system på plats bör de anställda vara medvetna om hur olika typer av information rutinmässigt ska hanteras och varför. Genom märkning minskar även risken för felaktigt hantering av information på grund av vad som brukar kallas ”den mänskliga faktorn”.

Exempel 2 – Förlust av forskningsrapport

Även inhyrda konsulter, tillfälligt anställda och vikarier bör informeras om rutiner kring hur man hanterar känslig eller kritisk information. Med ett fungerande system för klassificering och märkning av information ökar möjligheterna att säkerställa att även dessa personer informeras om interna föreskrifter. Ansvarsfrågan ska också regelmässigt regleras i avtal.

Exempel 3 – Spridning av känslig information

Medytekk borde ha tydliggjort att det är otillåtet att delge utomstående känslig information. Om Jan på ett bättre sätt känt till hur den information han har kunskap om klassificerats och vilka regler som gällde för just den klassen hade han antagligen vetat bättre än att i detalj beskriva sitt intressanta arbete.

Exempel 4 – Märkning av säkerhetskopior

Med klara regler för hur märkning av information ska gå till kunde detta ha undvikits. Reglerna bör också innehålla särskilda föreskrifter om hur den rutinmässiga kontrollen av kritisk information ska gå till för att fungera tillsammans med klassificeringssystemet.

Checklista – Klassificering och styrning av tillgångar

Fråga	Ja	Delvis	Nej
Har informationstillgångarna inventerats?			
Har en förteckning över informationstillgångarna upprättats?			
Har samtliga ägare av informationstillgångar fastställts och dokumenterats?			
Finns det fastställda informationsklasser?			
Är skyddsnivåer fastställda för respektive klass?			
Tillförs informationstillgångar rutinmässigt den informationsklass som motsvarar dess betydelse för organisationen?			

Fråga	Ja	Delvis	Nej
Finns det riktlinjer på plats som definierar rutiner för märkning och hantering av information?			

Kapitel 8 – Personalresurser och säkerhet

Människorna i en organisation brukar oftast kallas för ”kunskapskapitalet” och betraktas som den viktigaste resursen. Men de är inte enbart en förutsättning för verksamheten utan ingår också i hotbilden mot den. Väsentligt är att hotbilden inte enbart kommer från alla anställda utan också från personer med anknytning till organisationen som konsulter, praktikanter, entreprenadarbetare (städare, catering, växeltelefonist, IT-tekniker) etc.

Lojala medarbetare är en förutsättning för att säkerställa en kontinuerligt hög nivå av informationssäkerhet i en organisation. En god arbetsmiljö, i vid bemärkelse, bidrar till att höja säkerheten. Arbetsmiljöverkets föreskrifter AFS 2001: 1, Systematiskt arbetsmiljöarbete, ställer krav på organisationens ledningssystem inom arbetsmiljöområdet.

En verksamhet som vilar helt på en eller flera nyckelpersoner är sårbar. Det är viktigt att utforma organisation och befattningar så att beroendet av nyckelpersoner reduceras. Mångkunnighet hos de anställda minskar sårbarheten.

En organisation som värnar såväl informationssäkerhet som en god arbetsmiljö har förutsättningen att täcka in hela säkerhetsbegreppet för området personal och säkerhet.

8.1 Före anställning

Mål: Att säkerställa att anställda, leverantörer och utomstående användare förstår sitt ansvar och är lämpliga för de roller de avses ha och för att minska risken för stöld, bedrägeri eller missbruk av resurser.

Säkerhetsansvar bör klargöras före anställning i lämpliga befattningsbeskrivningar och i villkor och förutsättningar för anställningen.

Alla platssökande, leverantörer och utomstående användare bör kontrolleras på lämpligt sätt särskilt då det gäller känsliga arbetsuppgifter.

Anställda, leverantörer och utomstående användare av informationsbehandlingsresurser bör skriva under en förbindelse om sina säkerhetsroller och sitt ansvar.

Organisationens olika befattningar bör identifieras och analyseras utifrån ett riskperspektiv. En riskprofil för varje befattning som hanterar känsligt material bör tas fram som innehåller information om bland annat hantering av klassificerat material och ekonomiskt ansvar.

Vid rekrytering och omplacering av personal bör en avstämning ske mot befattningens riskprofil.

Ovanstående gäller inte enbart tillsvidareanställda utan även praktikanter och korttidsanställda.

Vid användning av en resursförstärkning som exempelvis inhyrda konsulter, bör en avtalsgenomgång innehålla en motsvarande avstämning mot den riskprofil som finns kopplad till uppdraget.

8.1.1 Roller och ansvar

Befattningsbeskrivningar eller motsvarande bör upprättas på ett sådant sätt att de omfattar den riskprofil som finns.

Formuleringen av det ansvar och de befogenheter som är kopplade till tjänsten bör vara entydiga. Viktigt är att befattningsbeskrivningen innehåller vilka informationssäkerhetstillgångar som befattningen ansvarar för och att ansvaret för såväl skydd som underhåll av dessa klart framgår.

8.1.2 Kontroll av personal

Vid all rekrytering eller anlitande av tillfällig personal bör följande områden beaktas

- **Identitet** bör kontrolleras på erforderlig nivå. Normalt via allmänt accepterade id-handlingar, som körkort, pass eller SIS-märkt id-handling.
- **Referenser** bör alltid kontrolleras.
- **Meritförteckning** bör kontrolleras utifrån både riktighet och rimlighet. Kvalifikationer bör vara bekräftade med betyg eller intyg.
- **Kreditupplysning** bör tas för befattningar där riskprofilen innefattar ekonomiskt ansvar och där ytterligare kontroll kan anses befogad.
- **Utdrag ur polisregister** kan vara befogat för känsliga befattningar. Ett sådant utdrag kan dock vara ofullständigt på grund av sekretessregler, varför det inte bör tillmätas ett alltför stort värde.

8.1.3 Anställningsvillkor och anställningsförhållanden

Anställningsvillkoren bör tydligt definiera det ansvar samt de rättigheter och skyldigheter en anställning medför utifrån ett informationssäkerhetsperspektiv. Frågor rörande upphovsrätt, användning och spridande av information, användning av organisationens resurser för egen del etc. är områden vilka bör regleras i anställningsvillkoren.
Rutiner för upphörande av anställning alternativt ändrad befattning bör finnas definierade i det regelverk vilket reglerar anställningsförhållanden.

8.2 Under anställningen

Mål: Att säkerställa att anställda, leverantörer och utomstående användare är medvetna om hot och problem som rör informationssäkerhet, sitt ansvar och sina skyldigheter samt är utrustade för att stödja organisationens säkerhetspolicy när de utför sitt normala arbete och att minska risken för mänskliga fel.

Ledningsansvar bör definieras för att säkerställa att säkerhet tillämpas under en persons hela anställningstid inom organisationen.

Tillräcklig nivå av medvetenhet, utbildning och övning i säkerhetsrutiner och korrekt användning av informationsbehandlingsresurser bör ges till alla anställda, leverantörer och utomstående användare i syfte att minimera möjliga säkerhetsrisker. Ett formellt disciplinärt förfarande för att hantera säkerhetsöverträdelser bör inrättas.

En medarbetare kan oavsiktligt åsamka organisationen höga kostnader och annan stor skada beroende på bristande introduktion och utbildning. Det är därför viktigt att introduktion och utbildning av nya medarbetare håller hög kvalitet. Detsamma gäller naturligtvis vid omplacering av redan anställda medarbetare. Lika viktigt är det att detta görs även när tillfällig personal och externa konsulter anlitas.
Generell kompetensutveckling av personalen är viktig eftersom den också påverkar medarbetarnas trivsel med arbetsuppgifterna och därmed ökar lojaliteten med organisationen.

8.2.1 Ledningens ansvar

Att säkerställa att medarbetarna i organisationen är lojala mot ledningen är en grundförutsättning för att de i sitt arbete skall leva upp till ställda informationssäkerhetspolicys. Ledningens agerande och framförallt förmågan att förankra och få acceptans för uppställda krav är därför mycket viktigt. Givetvis måste uppställda krav kunna motiveras utifrån genomförda analyser.
Då organisationen anlitar konsulter eller underleverantörer vilka kommer i kontakt med informationstillgångarna inom organisationen måste på motsvarande sätt som för egen personal säkerställas att krav är definierade, förstådda och accepterade
Den psykosociala arbetsmiljön har en mycket stor betydelse för lojaliteten. Medarbetare som mår dåligt förlorar lojaliteten och därmed tilltron till existerande rutiner. I extrema fall kan de bli ett direkt hot mot organisationen genom en drivkraft att avsiktligen vilja skada denna.

8.2.2 Informationssäkerhetsmedvetande, utbildning och övning

Alla i organisationen, även tillfälligt anställda och konsulter, bör få information om den gällande informationssäkerhetspolicyn. Information om det regelverk som ser till att policyn efterlevs bör också ges.
Grundläggande information bör ges redan vid introduktion på arbetsplatsen och därefter följas upp med kontinuerliga utbildningar. Utbildningens omfattning är beroende av den riskprofil och det ansvar och de befogenheter som gäller för befattningen.
Utbildningen bör följas upp minst en gång om året. I samband med uppföljningen bör också en omvärldsanalys eller annan aktuell information inom området presenteras. Resultatet av genomförda riskanalyser baserade på incidentrapporteringen bör också presenteras.
För att på sikt höja säkerheten i organisationen är det viktigt att de incidenter som inrapporteras hanteras på ett effektivt sätt. Det innebär att olika åtgärder, som att genomföra nya riskanalyser och andra omedelbara kortsiktiga åtgärder, vidtas så snart som möjligt.

8.2.3 Disciplinär process

De olika disciplinära åtgärder som kan vara aktuella är varning, omplacering till tjänst med annan riskprofil, uppsägning och polisanmälan. Åtgärderna måste ha ett tydligt stöd av ett regelverk som är väl förankrat hos de anställda och deras fackliga organisationer. I samband med information och utbildning i informationssäkerhet bör också information om detta regelverk ges. Det får aldrig råda någon tvekan om att när en disciplinär åtgärd används är det till följd av en avsiktligt illojal handling mot organisationen.

8.3 Upphörande av anställning eller förflyttning

Mål: Att säkerställa att anställda, leverantörer och utomstående användare lämnar organisationen eller ändrar anställningsförhållande på ett ordnat sätt.

Ansvar bör definieras för hanteringen av när en anställds, leverantörs eller utomstående användares lämnar organisationen och för att all utrustning återlämnas och att alla åtkomsträttigheter avslutas.

Förändring av ansvar och anställning inom en organisation bör styras på samma sätt som upphörande av respektive ansvar och anställning, i enlighet med detta avsnitt, och nya anställningar bör behandlas som beskrivs i avsnitt 8.1

8.3.1 Ansvar vid upphörande

Rutiner liksom att det är tydligt definierat vem som ansvarar för vad då en anställning upphör alternativt en anställd övergår till andra arbetsuppgifter bör finnas. Det vanliga i större organisationer är att personalavdelningen är övergripande ansvarig.

Om riskprofiler upprättats för befattningar inom organisationen bör en avstämning mot denna göras innan en medarbetare erbjuds en annan tjänst.

8.3.2 Återlämnande av tillgångar

Då en anställning upphör bör säkerställas att all mobil utrusning vilken används som informationsbärare återlämnats exempelvis bärbar dator och mobiltelefon. Säkerställ även att eventuella lösenord, smarta kort eller andra nycklar vilka ger åtkomst till information återlämnas och att register för tillgång till information uppdateras. Även då en medarbetare går över till nya arbetsuppgifter inom organisationen kan det vara lämpligt att ompröva tillgång till information.

8.3.3 Indragning av åtkomsträttigheter

Alla medarbetare i organisation måste ha tillgång till den information vilken är nödvändig för att de skall kunna utföra sina arbetsuppgifter med hög kvalitet. Samtidigt bör information vilken ej är nödvändig eller rent av olämplig att känna till skyddas. Vid förändring av arbetsuppgifter eller inför att en anställning upphör bör åtkomsrättigheter ses över. Begränsning av åtkomsträttigheter kan även utgöra en disciplinär åtgärd.

Exempel

1 – Rekrytering

För två år sedan var Medytekk AB tvunget att lägga ner ett projekt på grund av att två forskare gick till ett konkurrerande företag.

Projektet blev inte avslutat innan uppsägningstidens slut. Ledningen för Medytekk lyckades inte heller hyra tillbaka forskarna från konkurrenten för att avsluta projektet.

Vad borde Medytekk ha tänkt på?

2 – Förändring av anställningsvillkor

Vid starten av Medytekks produktion i Polen för ett år sedan fick man allvarliga leveransproblem.

Vid starten upptäcktes det att en stor del av de nödvändiga databaserna för produktions- och kvalitetsstyrning måste ha varit manipulerade, eftersom den färdiga slutprodukten inte uppfyllde kravspecifikationen.

När Medytekk för ett år sedan flyttade en del av sin produktion till Polen permitterades ett 30-tal medarbetare.

Vad borde Medytekk ha tänkt på?

3 – Militant djurrättsaktivist

Laboratorieassistenten Kalles sambo är militant djurrättsaktivist.

Hon har deltagit i ett antal aktioner mot företag och institutioner som, precis som Medytekk, sysslar med djurförsök. Hon var även med i den demonstration som föreningen "Stopp av djurförsök nu" hade utanför Medytekk.

Rykten har cirkulerat inom Medytekk vilka bekräftades i samband med demonstrationen utanför Medytekk.

Chefen för Test och Produktion hos Medytekk har blivit utsatt för vissa hot, antagligen från olika militanta djurrättsaktivister, hon har dock aldrig tagit dessa på allvar eller polisanmält dem.

Vad borde Medytekk ha tänkt på?

4 – Virusproblem

För en månad sedan var Medytekk AB tvungna att ta in en extern konsult för att få bukt med ett datorvirus som kommit in i företaget via e-post.

Konsulten upptäckte att en av orsakerna till problemet var att virusprogramvaran inte var uppdaterad. Uppdateringen av virusskyddet var inte prioriterad och ingick inte heller i säkerhetsutbildningen hos företaget. Konsulten upptäckte också att den instruktion som fanns på företaget för hur e-post fick användas inte följts.

Vad borde Medytekk ha tänkt på?

5 – Sjukligt spelberoende

Den administrative chefen Göran Rubens ägnar en allt större del av sin tid åt totospel på Solvalla. Spelandet har fått sådana konsekvenser att det privat resulterat i skilsmässa och att familjens gård i Knivsta har fått säljas för att täcka spelskulderna.

Stefan Eriksson, vd, har av sin sekreterare, Berit Qvick, hört talas om att Göran Rubens vid ett flertal tillfällen bett om förskott samt att han vid flera tillfällen sjukskrivit sig på onsdagar.

Vad borde Medytekk ha tänkt på?

Vad kan vi lära oss av dessa exempel?

Exempel 1 – Rekrytering

Medytekk borde ha tänkt på att kompetens- och resurssäkra forskningsprojektet via

- anpassad uppsägningstid till projekts varaktighet,
- sekretessavtal och
- identifiering av nyckelpersoner vid riskanalys för projektet.

Dessutom borde Medytekk tänka på sekretessfrågan om forskarna skulle ha hyrts tillbaka för att slutföra projektet.

För att säkerställa att framtida kompetensbehov täcks borde Medytekk tänka på att

- säkerställa personalens lojalitet via anställningsförmåner, rätt lönenivå, etc.,
- identifiera nyckelpersoner och arbeta för att minska beroendet av dem,
- se över sina anställningsvillkor, och att
- inkludera sekretess i anställningsvillkoren även efter anställningens upphörande.

Exempel 2 – Förändring av anställningsvillkor

Medytekk borde ha tänkt på att permittering av personal ofta kan innebära störningar i verksamheten när lojaliteten hos medarbetarna minskar eller när arbetsgivarens attraktivitet hos arbetstagaren minskar.

För att säkerställa en flytt utan problem borde Medytekk ha tänkt på att

- göra en riskanalys utifrån den nya hotbild som uppstår vid förändringen,
- uppdatera behörigheter,
- förstärka skalskyddet, och att
- informera de anställda bättre om företagets planer och konsekvenserna för personalen.

Exempel 3 – Militant djurrättsaktivist

Medytekk borde tänka på att

- diskutera frågan i utvecklingssamtal med Kalle,
- säkerställa tydlig informationshantering,
- utöka det fysiska skyddet och att
- eventuellt omplacera Kalle om riskanalysen visar att han utgör en stor risk.

Dessutom bör Medytekk tänka på att säkerställa att incidenter rapporteras och följs upp så att hot tas på allvar och att de utgör en del i framtida riskanalys.

För att säkerställa fortlevnad borde Medytekk tänka på att

- utöka sin omvärldsbevakning för att i framtiden vara förberedda för eventuell e-postbombning (spamming) och andra typer av hot, och att
- vara lyhörd vid personalrekrytering.

Exempel 4 – Virusproblem

Medytekk borde ha tänkt på att

- uppmärksamma alla anställda på de problem virus kan åstadkomma i en organisation,
- införa rutiner för hantering av disketter, cd-skivor, filer bifogade till e-post, och så vidare som förs in i organisationen, detta för att säkerställa att viruskontroll sker,
- säkerställa informationsflödet till organisationen från experter på området, exempelvis via medverkan i branschorganisationer och liknande och att

- ha en aktiv omvärldsbevakning för att så tidigt som möjligt få kunskap om nya virus så att åtgärder mot dessa kan sättas in.

Exempel 5 – Sjukligt spelberoende

För att säkerställa informationssäkerheten borde Medytekk tänka på att

- inrätta rutiner för personer som har personliga problem,
- sätta upp tydliga riktlinjer för vad som är tillåtet samt regler för hur överträdelser ska hanteras,
- tillsätta en krisgrupp som hjälper Göran Rubens att ta itu med sitt spelberoende och att
- i utvecklingssamtal följa upp personalens privata situation.

Checklista – Personal och Säkerhet

Fråga	Ja	Delvis	Nej
Har nyckelpersoner identifierats?			
Har riskprofiler för organisationens befattningar tagits fram?			
Framgår ansvar och befogenhet för informationssäkerhet av befattningsbeskrivning?			
Kontrolleras identitet, referenser och meritförteckning vid rekrytering?			
Är rutiner för sekretessavtal/-erinran införda?			
Ges anställda erforderlig information och utbildning vad gäller informationssäkerhet?			
Finns rutiner för rapportering och hantering av säkerhetsincidenter?			
Finns rutiner för disciplinära åtgärder mot anställda som bryter mot organisationens informationssäkerhetspolicy?			

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?			

Kapitel 10 Styrning av kommunikation och drift

En förutsättning för att de flesta informationssystem ska fungera är den underliggande kommunikationen. Varje enhet måste kunna lita på att nödvändiga resurser är tillgängliga vid behov. För att säkerställa och övervaka detta är ändamålsenlig drift en annan förutsättning för väl fungerande informationssystem.

Redan då en kommunikationslösning planeras är det viktigt att ta säkerhetsaspekter i beaktande. Infrastrukturen för såväl LAN som WAN påverkar i högsta grad säkerhetsnivån och dess möjligheter.

Kommunikation och drift kräver att kompetent personal finns såväl för att konfigurera och upprätta korrekta rutiner som för att övervaka och följa upp loggar och eventuella incidenter.

10.1 Driftrutiner och driftansvar

Mål: Att säkerställa korrekt och säker drift av informationsbehandlingsutrustning.

Ansvar och rutiner för ledning och drift av all informationsbehandlingsutrustning bör fastställas. Detta omfattar utveckling av lämpliga driftrutiner.

Uppdelning av arbetsuppgifter bör i förekommande fall tillämpas för att minska risken för försummelse eller avsiktligt missbruk av system.

För att säkerställa säker och korrekt drift krävs att ansvar och rutiner är fastställda för verksamhetens system för informationsbehandling. Därutöver krävs rutiner för att kunna hantera eventuella incidenter.

Det är viktigt att rutiner och ansvar är dokumenterade och att det är tydligt vem som gör vad.

10.1.1 Dokumenterade driftrutiner

Det bör vara en naturlig del i informationssäkerhetsarbetet att regelmässigt tillse att driftrutiner uppdateras vid förändringar. De dokument som behandlar driftrutiner bör betraktas som styrande dokument och hanteras som sådana. Samtliga identifierade rutiner som rör driften bör innehålla klara och tydliga instruktioner om tillvägagångssätt. Om så inte är fallet bör det finnas hänvisningar till de dokument som behandlar respektive rutin i detalj. Den här typen av dokumentation bör omfatta driften av hela den integrerade systemmiljön, inklusive kommunikation, säkerhetskopiering, underhåll, ledning och personsäkerhet i datahallar samt hantering av post.

10.1.2 Ändringshantering

Det bör finnas formella rutiner på plats för att säkerställa att erforderlig säkerhetsnivå kan upprätthållas även i samband med förändringar i informationsbehandlingsutrustning och -system. Tänk på att förändringar inom ett område även kan ha påverkan på andra delar av systemet.

10.1.3 Uppdelning av arbetsuppgifter

För att minska risken för missbruk av system brukar metoden att dela upp arbetsuppgifter användas. Om detta av praktiska skäl inom till exempel mindre organisationer inte är genomförbart ökar kraven på loggning, övervakning samt uppföljning av verksamheten.

Om en person exempelvis har kontroll över både utveckling och driftsättning kan denna göra förändringar utan att någon annan märker det.

10.1.4 Uppdelning av utvecklings- test- och driftresurser

En huvudregel, vilken inte nog kan betonas, är att resurser för drift, utveckling och test ska hållas åtskilda. För att säkerställa detta bör exempelvis program tillhörande de tre angivna kategorierna åtskiljas så långt det är möjligt genom användande av skilda processorer, domäner eller kataloger. Ej heller bör hjälpprogram från driftsystem vara åtkomliga för test- och utvecklingsarbete.

10.2 Kontroll av utomstående tjänsteleverantör

Mål: Att införa och bibehålla lämplig nivå på informationssäkerhet och utförande av tjänster i enlighet med utomstående leverantör av tjänster.

Organisationen bör kontrollera implementeringen av avtal, följa upp överensstämmelsen med avtalen och hantera ändringar för att säkerställa att utförda tjänster uppfyller alla krav avtalade med den utomstående parten.

10.2.1 Utförande av tjänster

Vid utläggning (outsourcing) av hela eller delar av organisationens informationsbehandling kvarstår ansvaret för informationssäkerheten på organisationen. För att organisationen även vid utläggning skall kunna bibehålla säkerhetsnivån för sin information bör säkerhetskraven regleras i avtal med den utomstående parten.

Det är av vikt att granska och bedöma såväl den organisatoriska som den tekniska säkerhetsnivån hos den utomstående parten så att nivåerna motsvarar den egna organisationens.

I utläggningsavtal bör framför allt följande punkter beaktas/regleras.

- Rättsliga krav och hur de ska uppfyllas.
- Åtgärder för att skapa medvetenhet om säkerhetsansvar.
- Hur riktighet och sekretess upprätthålls.
- Hur åtkomsten ska begränsas både logiskt och fysiskt.
- Hur verksamheten ska fortleva i händelse av en katastrof.
- Möjligheten att genomföra revisioner och kontroll av den utomstående organisationen.
- Krav på sekretess.
- Hur informationen får spridas och hur den ska förstöras.
- Uppdragets omfattning med avgränsningar.
- Typen av material som ska hanteras och dess säkerhetsklassificering.

10.2.2 Uppföljning och granskning av utomståendes utförande av tjänster

Innan man använder sig av externa resurser bör de särskilda risker detta kan medföra noga analyseras. Utfallet av en sådan analys bör ingå som en del i underlaget vid förhandlingar med leverantören.

Vid användning av externa leverantörer bör leverantörens hantering av följande områden särskilt beaktas:

- Riktlinjer för säkerhet och metoder för kontroll av efterlevnad,
- avbrottsplan,
- incidenthantering,
- säkerhetsorganisation,
- acceptans av systemägare.

10.2.3 Ändringshantering av tjänster från utomstående part

I avtalet med utomstående part bör det finnas beskrivet hur ändringshantering skall hanteras. Vid förändringar kan det beroende på hur pass kritisk informationen som behandlas är vara nödvändigt att analysera de risker som finns med hanteringen.

10.3 Systemplanering och systemgodkännande

Mål: Att minimera risken för systemfel.

Planering och förberedelse krävs i förväg för att säkerställa att tillgänglig kapacitet och resurser finns för att leverera den systemprestanda som krävs.

Planläggning för framtida kapacitetskrav bör göras för att minska risken för överbelastning av system.

Driftkraven hos nya system bör fastställas, dokumenteras och testas innan de godkänns och används.

Genom ett aktivt, förutseende och långsiktigt arbete med systemplanering vilket innefattar väl avvägda formella rutiner för systemgodkännande kan risken för systemfel minimeras.

10.3.1 Kapacitetsplanering

Genom en effektiv planering av resursbehovet, som även tar hänsyn till framtida behov, säkerställs att det finns tillgång till erforderliga resurser över tiden.

Särskild hänsyn bör tas till nya system- och verksamhetskrav samt utvecklingen av organisationens informationsbehandling. Genom att ha tillgång till denna typ av information bör ledningen via effektiv planering kunna undvika kapacitetsmässiga flaskhalsar.

10.3.2 Systemgodkännande

Ledningen ansvarar för att det i samband med systemgodkännande finns fastställda krav och kriterier som är definierade, överenskomna, dokumenterade och testade. Först därefter kan man godkänna ett system efter leverans, uppgradering eller motsvarande typ av förändring.

10.4 Skydd mot skadlig och mobil kod

Mål: Att skydda riktighet i program och data.

Försiktighetsåtgärder krävs för att förhindra och upptäcka att skadlig kod och icke godkänd mobil kod installeras.

Program och informationsbehandlingsresurser är sårbara för att skadlig kod, såsom virus, maskar, Trojanska hästar och logiska bomber installeras. Användarna bör göras medvetna om farorna med skadlig kod. Där det är lämpligt, bör ledningen införa skyddsåtgärder för att skydda mot, upptäcka och rensa bort skadlig kod liksom för att styra mobil kod.

För att skydda riktigheten i program och data bör införande av särskilda åtgärder övervägas.

10.4.1 Åtgärder mot skadlig kod

Ett effektivt skydd mot skadliga program förutsätter ett aktivt förebyggande arbete, som också omfattar åtgärder för att tillse att personalens säkerhetsmedvetande ligger på rätt nivå. Det krävs även styrning av åtkomst och ändringshantering.

Organisationens riktlinjer bör i de flesta fall omfatta följande punkter:

- ett formellt förbud i policy mot användning av program som ej godkänts samt mot att hämta hem datafiler eller program från externa källor som Internet,
- program för detektering av skadliga program samt stödprogram för återställande,
- regelbunden granskning av program och data i samband med kritiska verksamhetsprocesser,
- antivirusprogram, som också inbegriper kontroll av så kallade bifogade filer i e-post,
- fastställande av ledningsrutiner och ansvar för virusskydd,
- avbrottsplan,
- verifiering av – och tillgång till – information som rör skadliga program.

Okända program som installeras kan öppna bakvägar för obehöriga in i systemmiljön.

10.4.2 Åtgärder mot mobil kod

Mobil kod är kod som då den överförs till en dator automatiskt kör program. Mobil kod levereras ofta med såväl hårdvara som programvara. Innan användande av mobil kod tillåts bör verifieras att den inte på något sätt skadar de applikationer som används och de informationstillgångar som finns lagrade i systemet Säkrast är att spärra all användning av mobil kod som inte verifierats i en logiskt isolerad miljö.

10.5 Säkerhetskopiering

Mål: Att bevara informationens och informationsbehandlingsresursernas riktighet och tillgänglighet.

Rutinåtgärder bör fastställas för att införa den beslutade policyn och strategin (se också 14.1) för säkerhetskopiering av data och för att öva återställande av data inom rimlig tid.

Genom införandet av formella rutiner för säkerhetskopiering, reservkopiering av data, loggning, övervakning samt återkommande övningar av återställande ökar man möjligheterna att i alla lägen bevara riktigheten hos och tillgängligheten till verksamhetens kommunikations- och informationsbehandlingsresurser.

Ju tydligare och renare systemmiljön är desto svårare blir det att maskera otillåten användning.

10.5.1 Säkerhetskopiering av information

Det kan inte nog understrykas vikten av att organisationen har tillgång till ett antal generationer säkerhetskopior (minst tre när det rör sig om kritiska tillämpningar) av väsentlig verksamhetsinformation och program som finns lagrade utanför det normala driftstället. Samma krav på lagringsbetingelserna bör ställas på alla förvaringsplatser.

För att säkerställa att kraven i kontinuitetsplanen uppfylls bör följande punkter omfattas av regelbundna tester:

- rutiner för säkerhetskopiering samt återläsning av kopiorna,
- lagrade data på säkerhetskopior samt återstartsrutiner.

Utöver det bör även följande områden vara föremål för formellt fastställda rutiner:

- tidpunkter för säkerhetskopiering,
- permanent lagring av säkerhetskopior.

En säkerhetskopia är värdelös om den inte kan användas – testa därför regelbundet att den går att återläsa!

10.6 Hantering av säkerhet i nätverk

Mål: Att säkerställa skyddet av information i nätverk och i tillhörande infrastruktur.

Säker hantering av nätverk, som kan sträcka sig över organisationsgränserna, kräver noggrann hänsyn till dataflöde, legala konsekvenser, övervakning och skydd.

Ytterligare åtgärder kan också krävas för skyddet av känsliga data som överförs via allmänna nät.

För att nå en acceptabel nivå av säkerhet i nätverk och infrastruktur är det nödvändigt att effektivt kombinera de nedan angivna åtgärderna.

10.6.1 Skyddsåtgärder för nätverk

De formellt fastställda styrmedlen och åtgärderna för säkerhet i nätverksmiljöer bör ta hänsyn till behovet av skydd av data i nätverksmiljön. Ansvaret för att dessa rutiner både införs och används bör ligga hos nätverksansvariga, och dessutom vara skilt från ansvaret för datordrift. Även ansvarsfrågor beträffande lokal utrustning som exempelvis arbetsstationer och skrivare bör beaktas.

När det gäller åtkomst till organisationens resurser kan särskilda krav ställas på säkerheten som kan tillfredsställas genom exempelvis brandväggar och en lämplig indelning av nätverksmiljön.

För att kunna avgöra huruvida de mål organisationen ställt upp för kommunikationssäkerhet uppnåtts eller inte, kan det vara lämpligt att genomföra regelbundna intrångstester.

10.6.2 Säkerhet i nätverkstjänster

Erforderliga säkerhetsegenskaper och andra krav bör klarläggas och dokumenteras. Då nätverkstjänsterna utförs av en leverantör är det väsentligt att säkerhetskrav och nödvändiga arrangemang för att uppfylla dessa finns beskrivna i avtalet med leverantören

10.7 Hantering av media

Mål: Att förhindra obehörigt avslöjande, modifiering, borttagning eller förstörande av tillgångar och avbrott i organisationens verksamhet.

Lagringsmedia bör styras och skyddas fysiskt.

Lämpliga driftrutiner bör upprättas för att skydda dokument, datamedia (t.ex. databand och skivor), in- och utdata och systemdokumentation från obehörig åtkomst, förändring, borttagande och förstörande

10.7.1 Hantering av flyttbara datamedia

Flyttbara datamedia innebär inte bara ett praktiskt stöd för verksamheten utan även ett reellt hot när det brister i rutiner och hantering. Det är därför mycket viktigt att all lagrad information skyddas. Med rätt och fungerande rutiner kan man skydda media från skada, stöld och obehörig åtkomst. På så sätt skyddas verksamheten mot avbrott och förlust av tillgångar.

10.7.2 Avveckling av media

Det bör finnas väl avvägda riktlinjer på plats för att se till att information inte kommer i orätta händer då man tänker kassera lagringsmedia.

Dokumenterade riktlinjer och rutiner bör omfatta alla aktuella typer av lagringsmedia. Det kan behövas rutiner för loggning och attestering för att uppnå nödvändig säkerhetsnivå.

10.7.3 Rutiner för informationshantering

Inom organisationen bör det finnas tydliga riktlinjer med åtföljande rutiner för hantering av information. På så sätt kan risken för missbruk eller obehörig åtkomst minskas.

10.7.4 Säkerhet för systemdokumentation

Oavsett hur man väljer att lagra systemdokumentation måste det regelmässigt säkerställas att lagringsbetingelserna är korrekta vad gäller exempelvis åtkomsten av lagringsmedia vid fysisk förvaring.

10.8 Utbyte av information

Mål: Att bibehålla säkerheten hos information och programvara som utbyts inom organisationen och med någon extern enhet.

Utbyte av information och programvara mellan organisationer bör baseras på en formell utbytespolicy genomförd enligt överenskommelser om utbyte och bör vara i överensstämmelse med eventuell relevant lagstiftning (se avsnitt 15).

Det bör upprättas rutiner och normer för att under överföring av information skydda fysiska media som innehåller information.

Lagstiftarens krav, ingångna avtal och eventuella interna säkerhetskrav samt följder för verksamheten och säkerheten kring överföringen av information från en organisation till en annan bör utvärderas innan ett utbyte genomförs.

10.8.1 Policy och rutiner för informationsutbyte

Informationsutbyte kan idag ske med användning av många olika typer av utrustning. Det är dock viktigt att inte glömma bort traditionella röstmeddelanden, brev och fax. Hur informationsutbyte får ske bör vara reglerat i en policy. En förutsättning för att få en fungerande policy är att det inom organisationen finns ett system för klassning av information beroende på dess värde ur informationssäkerhetssynpunkt.
Regelverket kan exempelvis definiera vilken klass som är tillåten att använda vid kommunikation med e-post, när kryptering krävs etc.

10.8.2 Överenskommelse om överföring

I samband med upprättande av avtal om utbyte av information och program bör säkerhetsaspekterna utvärderas redan på ett tidigt stadium. Den egna organisations bedömning av hur känslig eller kritisk den aktuella informationen eller programmet är, eller kommer att vara, bör ligga till grund för avtalets utformning.

10.8.3 Fysiska media under transport

Vid transport av media bör rutiner finnas som innebär att det skyddas på ett sätt som återspeglar dess värde för organisationen.

10.8.4 Elektroniska meddelanden

E-post, EDI och andra former av elektroniska meddelanden måste ges ett skydd vilken står i relation till hur informationen klassats. Har informationen hög säkerhetsklassning kan det vara nödvändigt att använda annan metod för överföring av information.

10.8.5 Verksamhetsrelaterade informationssystem

Integrerade informationssystem innebär ofta stora fördelar och effektiviserar verksamheten. Samtidigt ökar sårbarheten och det kan vara nödvändigt att ha fungerande reservlösningar tillgängliga. För att minimera riskerna är det viktigt identifiera vilken information som skall vara tillgänglig och för vilka informationen skall vara tillgänglig. Bra fungerande rutiner för säkerhetskopiering av information är en nödvändighet.

10.9 Elektronisk handel

Mål: Att säkerställa säkra e-handelstjänster och en säker användning av dessa.

Säkerhetsförhållanden vid e-handel, inklusive direktanslutna transaktioner och kraven på skyddsåtgärder bör beaktas. Riktigheten och tillgängligheten hos information som publiceras elektroniskt via publikt tillgängliga system bör också beaktas.

10.9.1 Elektronisk handel

Det finns en rad tekniker som stödjer elektronisk handel. En generell skiljelinje går dock mellan lösningar som använder enskilda nät, som exempelvis EDI, eller publika nät som Internet. Med stöd av en väl genomförd risk-/sårbarhetsanalys kan man optimera tekniklösningar, säkerhetsorganisation och rutiner. Därigenom minskar risken för störningar som kan resultera i bland annat avtalstvister eller förlust av marknadens förtroende.

10.9.2 Direktanslutna transaktioner

Vid användande av direktanslutna transaktioner som exempelvis finansiella eller avtalsrelaterade är det väsentligt att analysera vilka risker som detta kan medföra och upprätta de skydd som är nödvändiga baserat utifrån riskanalysen.

10.9.3 Öppen information

Information som skall vara öppen och tillgänglig på exempelvis en webbplats bör skyddas på ett effektivt sätt för att motverka att informationen förvanskas vilket allvarligt kan skada organisationens rykte. Innan information görs allmänt tillgänglig måste organisationen försäkra sig om att såväl informationen som det sätt på vilket den presenteras är korrekt och uppfyller gällande lagstiftning som exempelvis personuppgiftslagen.

10.10 Övervakning

Mål: Att upptäcka obehörig informationsbehandling.

System bör övervakas och infornationssäkerhetshändelser registreras. Operatörs- och felloggar bör användas för att säkerställa att problem med informationssystem identifieras.

Organisationen bör följa alla relevanta lagkrav som är tillämpliga på dess övervakning och loggning.

Systemövervakning bör användas för att kontrollera effektiviteten hos använda skyddsåtgärder och verifiera att en modell för åtkomstpolicy följs.

10.10.1 Revisionsloggning

Loggning av användaraktiviteter är en grundläggande förutsättning för spårbarhet. Revisionsloggar som registrerar avvikelser, oregelbundenheter och andra säkerhetsrelaterade händelser bör föras och förvaras väl skyddade. Då loggning kan medföra registrering av konfidentiella persondata måste åtgärder införas för att säkerställa den personliga integriteten. Ur säkerhetssynpunkt bör inte systemansvarig eller systemadministratör ha möjlighet att radera eller förändra loggning av egna aktiviteter.

10.10.2 Övervakning av systemanvändning

Övervakning och på vilken nivå denna skall genomföras kräver att det finns en förståelse av vilka hot som finns. För att dimensionera övervakningsresurserna krävs riskanalyser. Berörd personal bör vara informerad om att övervakning sker och för att skapa förståelse för detta måste givetvis skälen som ligger till grund för övervakning redovisas.

10.10.3 Skydd av logginformation

Då systemanvändningen loggas är det nödvändigt att dessa loggar verkligen ger korrekt information. För att säkerställa detta måste loggarna ges nödvändigt skydd mot åtkomst och manipulering. Det bör finnas rutiner vilka beskriver vilka som har åtkomst till loggarna. Systemadministratörens roll är viktig att definiera. Det är inte självklart att denna befattning innebär full tillgång till alla loggar.

10.10.4 Administratörs- och operatörsloggar

Allt arbete som utförs av operatörer bör loggas. Operatörsloggar bör regelbundet kontrolleras av oberoende personal mot driftrutiner. Även operatörer är människor som kan göra misstag, omedvetet eller medvetet.

10.10.5 Loggning av fel

Tydliga regler bör finnas för rapportering och hantering av fel i informations- och kommunikationssystemen. Loggar bör föras över rapporterade fel, annars är det omöjligt att spåra fel och andra incidenter. Hanteringen av rapporterade fel bör innefatta:

- granskning av felloggar,
- granskning av korrigerande åtgärder.

10.10.6 Klocksynkronisering

Korrekt inställning och exakt funktion av datorklockor är väsentligt för att säkerställa giltigheten hos de loggar som förs. Det rekommenderas att samtliga datorklockor i organisationens nätverk ställs till en överenskommen standardtid.
!

Exempel

1 – Virus

För ett år sedan drabbades Medytekk av ett virus som spreds via e-post. Viruset kom in via Internet till en anställd, och vidarebefordrade sedan sig själv till alla användare i de drabbade användarnas adressböcker. Det förorsakade att en stor mängd e-brev skickades fram och tillbaka inom och utom företaget. Resultatet blev att servern som hanterar e-post blev överbelastad och "hängde" sig. Samma server hade också uppgiften att bland annat köra ett för forskarna viktigt analysprogram.

För att rensa server och starta analysprogrammet anlitades en konsult. Driften var nere i totalt tre dygn. Forskarna ansåg att detta var oacceptabelt, då viktiga beräkningar inte kunde genomföras under tiden.

Vad borde Medytekk ha tänkt på?

2 – Säkerhetskopiering

Då en hårddisk kraschade i en av servrarna förlorades viktig information. Då säkerhetskopian skulle återställas upptäcktes att den inte fungerade. Man försökte då återläsa äldre kopior men fann att inte heller dessa fungerade. Efter lite undersökningar kom man fram till att en ny typ av band för säkerhetskopiering hade börjat användas för två veckor sedan, och att inget av dessa fungerade. Man hade aldrig tidigare testat att återläsa någon av dessa kopior.

Vad borde Medytekk ha tänkt på?

3 – Militant djurrättsaktivist

Medytekk har i olika sammanhang haft problem med demonstrerande djurrättsaktivister. En gång tog sig hackers med sådana intressen in på företagets hemsida och ändrade den. I samband med detta spreds falsk information där det bland annat sades att företaget genomför plågsamma djurförsök. Aktivisterna uppmanade till bojkott av företagets produkter.

Vad borde Medytekk ha tänkt på?

Vad kan vi lära oss av dessa exempel?

Exempel 1 – Virus

Medytekk borde ha tänkt på att säkerställa att uppdatering av användarnas virusskydd sker automatiskt och regelbundet. Detta kan uppnås genom att:

- Medytekk prenumererar på virusuppdateringar från leverantören av programvaran,
- automatisk uppdatering av användarnas virusskydd sker då de loggar på nätverket,
- servrarna regelbundet genomsöks efter virus.

Genom utbildning av användare kan man tillförsäkra sig att de är medvetna om riskerna med "maskerade" bifogade filer och vid minsta tveksamhet inte öppnar dem.

Exempel 2 – Säkerhetskopiering

Medytekk borde ha bättre rutiner för att säkra att säkerhetskopiorna verkligen fungerar bland annat genom att:

- använda funktionen för verifiering av säkerhetskopiorna i direkt samband med att de tas,
- införa rutiner för att regelbundet testa att återläsning av både nya och äldre säkerhetskopior fungerar.

Exempel 3 – Militant djurrättsaktivist

Medytekk borde ha skyddat sin hemsida bättre, genom att bland annat:

- upprätta en brandvägg mellan Internet och den server som innehåller hemsidan,
- säkerställa att brandväggen är korrekt konfigurerad och att den övervakas på ett ändamålsenligt sätt,
- dela upp nätverket i ett flertal zoner så att hackers ej kan komma åt eller ändra information beträffande produktionen.

Checklista – Styrning av kommunikation och säkerhet

Fråga	Ja	Delvis	Nej
Tas rutinmässigt schemalagda säkerhetskopior av data?			
Tas rutinmässigt schemalagda säkerhetskopior av program?			
Tas rutinmässigt schemalagda säkerhetskopior av system?			
Tas rutinmässigt schemalagda säkerhetskopior av loggar?			
Har antivirusprogramvara installerats heltäckande på alla arbetsstationer och servrar?			
Sker regelbundna uppgraderingar av programvaror?			
Har behovet av kryptering fastställts?			
I de fall kryptering används har behovet av stark eller svag kryptering analyserats?			
Tas loggar från centrala delar i systemmiljön samt brandvägg?			
Kontrolleras konfigurationen av centrala delar i systemmiljön samt brandvägg regelbundet?			
Finns rutiner för rapportering av iakttagelser?			
Finns rutiner för uppföljning av iakttagelser?			
Finns rutiner för incidenthantering?			
Finns eskaleringsrutiner?			

Kapitel 11 – Styrning av åtkomst

Information representerar kunskap och kunskap är en av de viktigaste resurserna i varje organisation. Skydd av information är därför av vital betydelse för överlevnad och framgång. IT-system i moderna organisationer tillhandahåller en nödvändig infrastruktur för verksamheten. Störningar i dessa system kan få allvarliga, i värsta fall fatala, konsekvenser för organisationen i sin helhet.

Åtkomstskydd av information är datorvärldens motsvarighet till tillträdes- och användningsskydd av fysiska tillgångar i den fysiska världen. Det finns många kopplingar mellan informationssäkerhet och fysisk säkerhet, bland annat kräver IT-resurser fysiska skydd. Men det finns också betydande skillnader såväl när det gäller hot och risker som skyddsmetoder. I dagens samhälle har såväl informationssäkerhet som fysisk säkerhet sin givna och nödvändiga plats i framgångsrika verksamheter.

11.1 Verksamhetskrav på styrning av åtkomst

Mål: Att styra åtkomst till information.

Åtkomst till information, informationsbehandlingsresurser och verksamhetsprocesser bör styras på grundval av verksamhets- och säkerhetskrav.

Regler för styrning av åtkomst bör ta hänsyn till policies för spridning och behörighet till information.

11.1.1 Åtkomstpolicy

En organisations informationssäkerhetspolicy ska klart och tydligt ange de riktlinjer som gäller för tilldelning/fråntagning av åtkomsträttigheter till information, men också hur dessa rättigheters operativa användning ska kontrolleras.

Styrande för riktlinjerna är de krav som verksamheten ställer på organisationens samlade IT-resurser. Dessa krav kan vara av olika slag: funktionella, effektivitet, säkerhet, legala och avtalsmässiga. Informationssäkerhetspolicyn måste klarlägga de övergripande principer som ska gälla för informationsanvändning. En ofta tillämpad princip är ”behov-att-veta”-principen, som säger att varje medarbetare ska ha tillgång till exakt den information som krävs för att han eller hon ska kunna utföra sina arbetsuppgifter. En annan vanlig princip – som också styr utformningen av ”regler för styrning av åtkomst” – säger att ”det som inte är explicit tillåtet är förbjudet”.

Riktlinjerna och principerna ovan utgör grunden för det regelverk som ska styra åtkomst till IT-resurser i den operativa verksamheten

Operativ styrning av åtkomst kan ske på två olika sätt: obligatorisk- och frivillig åtkomststyrning. Vid obligatorisk åtkomststyrning måste åtkomsträttigheter definieras för samtliga användare till varje informationsresurs. Detta sker centralt som en systemadministrativ funktion. Vid frivillig åtkomststyrning definieras åtkomsträttigheter decentraliserat av ägaren till respektive informationsresurs. Obligatorisk åtkomststyrning är resurskrävande men att föredra ur säkerhetssynpunkt.

11.2 Styrning av användares åtkomst

Mål: Att säkerställa behörig användares åtkomst och förhindra obehörig åtkomst till informationssystem.

Formella rutiner bör finnas för styrning av åtkomsträttigheter till informationssystem och tjänster.

Rutinerna bör täcka alla stadier i användaråtkomstens livscykel, från registrering av nya användare till slutlig avregistrering av användare som inte längre behöver åtkomst till informationssystem och tjänster. Särskild försiktighet bör iakttas, där det är lämpligt, ifråga om behovet av att styra fördelning av privilegierade åtkomsträttigheter som tillåter användare att förbigå normala systemspärrar.

11.2.1 Användarregistrering

Systemet för användarregistrering ska omfatta samtliga användares ”livscykel som systemobjekt”, det vill säga sträcka sig från nyregistrering till slutlig avregistrering. En unik användaridentitet (tillsammans med lämplig loggning av användaraktiviteter) är en förutsättning för spårbarhet varigenom en användare kan göras ansvarig för sina handlingar. En rutin bör finnas och ett register upprättas vilket visar de åtkomsträttigeter varje individ tilldelats.

Viktigt är att alltid beakta de krav som finns för att skydda individers personliga integritet.

11.2.2 Styrning av särskilda rättigheter

Privilegierad behörighet – en åtkomsträtt som överträder normal åtkomstkontroll – ska tillämpas ytterst restriktivt. Det är väsentligt att tilldelning och användning av privilegierad behörighet sker så att spårbarheten upprätthålls. Olämplig tilldelning av priviligerad behörighet kan resultera i oönskade intrång i system.

11.2.3 Styrning av lösenord för användare

Tilldelning av lösenord bör ske genom en formell och sekretesskyddad rutin. Det är av vikt att

- utgivning av lösenord föregås av en säker användaridentifikation,
- regler för hur lösenord bör hanteras är fastställda,
- användaren har förstått och accepterat dessa regler.

Temporära lösenord bör användas sparsamt och utdelas endast efter positiv identifikation av användaren. De bör alltid tidsbegränsas. Används tillfälliga lösenord bör dessa vara av bra kvalitet och endast gälla för den första inloggningen.

11.2.4 Granskning av användares åtkomsträttigheter

Tilldelade behörigheter bör granskas efter varje förändring i arbetsuppgifter, men också med regelbundna intervall.

11.3 Användares ansvar

Mål: Att förhindra obehörig användaråtkomst och åverkan eller stöld av information och informationsbehandlingsresurser.

De behöriga användarnas medverkan är väsentlig för en effektiv säkerhet.

Användarna bör göras medvetna om sitt ansvar för att upprätthålla en effektiv styrning av åtkomst särskilt när det gäller användning av lösenord och säkerheten hos användarutrustning.

En policy som kräver ”renstädat skrivbord och tom bildskärm” bör införas för att minska risken för otillåten åtkomst till eller skada på pappersdokument, media och informationsbehandlingsresurser.

11.3.1 Användning av lösenord

Självvalda lösenord bör vara av bra kvalitet, genom att exempelvis bestå av minst sex tecken (varav minst två ska vara numeriska eller specialtecken) samt inte vara associerbara till användaren på ett enkelt sätt. Lösenorden bör hållas hemliga. Lagras de på pappers- eller datamedia bör detta ske på ett säkert sätt. Lösenord bör aldrig lagras oskyddat i det IT-system det används.

11.3.2 Obemannad användarutrustning

Användarutrustning utan tillsyn måste skyddas på ett tillfredställande sätt. Ett bra hjälpmedel är lösenordsskyddade skärmsläckare. Lämnas persondatorer eller terminaler obemannade under en längre tid bör användaren logga ut. Arbetsstationer eller terminaler ska normalt aldrig slås av utan utloggning.

11.3.3 Policy för renstädat skrivbord och tom bildskärm

Ett sunt och vaket säkerhetsmedvetande är en naturlig komponent i varje säkerhetssystem. Som en allmän grundregel gäller att känslig information aldrig lämnas oskyddad när den inte används. Det är bland annat viktigt att

- påloggade men obevakade persondatorer eller terminaler är lösenordsskyddade (eller skyddade på annat sätt) och har skärmar som slocknar när de inte används,
- känsliga elektroniska dokument eller pappersdokument inte lämnas obevakade på en öppen plats (inte enbart på grund av risk för sekretessbrott utan också på grund av risk för brand, vattenskada, etc.).

11.4 Styrning av åtkomst till nätverk

Mål: Att förhindra obehörig åtkomst till nätverkstjänster.

Åtkomst till både interna och externa nätverkstjänster bör styras.
Användaråtkomst till nätverk och nätverkstjänster bör inte äventyra nätverkstjänsternas säkerhet, genom att säkerställa:
(a) att det finns lämpliga gränssnitt mellan organisationens nätverk och nätverk som ägs av andra organisationer och publika nät;
(b) att lämpliga autenticeringsmetoder används för användare och utrustningar;
(c) att styrningen av användares åtkomst till informationstjänster fungerar.

11.4.1 Policy för användning av nätverkstjänster

Policyn för utnyttjande av nätverk och nätverkstjänster bör reglera tillgång och behörighet till just dessa. Policyn är av särskild betydelse om (delar av) organisationens IT-resurser är sammankopplade med andra interna eller externa nätverk eller nätverkstjänster.

11.4.2 Autenticering av användare för extern anslutning

Externa anslutningar kan innebära stora risker för obehörig åtkomst. Därför är det viktigt att rätt säkerhetsåtgärder vidtas. Exempel på sådana säkerhetsåtgärder är stark autenticering, dedikerad utrustning, privata linjer, motringning, etc. Vid automatisk uppkoppling till externa datorer bör även dessa autenticeras (autenticering av nod).

11.4.3 Identifiering av utrustning i nätverk

Automatisk identifiering av utrustning kan vara en bra lösning om speciell utrustning används eller anslutning sker från definierade anslutningspunkter. En riskanalys av aktuella hot kan innebära att automatisk identifiering bör kompletteras med annan teknik för autenticering.

11.4.4 Skydd av extern diagnos- och konfigurationsport

Diagnosportar för distansunderhåll bör vara avstängda och fysiskt skyddade när de inte används. När diagnosporten behöver användas bör uppkopplingen var styrd från organisationen.

11.4.5 Uppdelning i nätverk

Modern informationsteknik har introducerat nya samarbetsformer och nya former att inter-agera organisationer emellan, men också nya sätt att utföra traditionella arbetsuppgifter. Det har medfört många nya frågor och problem när det gäller informationssäkerhet med krav på radikalt nya lösningar.
Logiskt sektionerade nätverk med säkrad kommunikation mellan sektionerna är ett generellt försök att besvara och lösa flera av dessa frågor och problem. Ansatsen har introducerat en del nya säkerhetskoncept och -mekanismer, till exempel intranät, extranät, filtrerande router, brandvägg, DMZ (demilitarized zone) och VPN (virtual private network).

11.4.6 Skydd av nätverksanslutning

Användarnas möjligheter att anslutna till nätverket bör utgå från att det finns klart definierat vilken information som krävs för att utföra de arbetsuppgifter som innefattas i befattningen. Då behoven omfattar tillgång till delade nätverk och nätverk vilka går utanför organisationens avgränsningar kan särskilda restriktioner behövas.

11.4.7 Styrning av vägval

Regler för styrning av vägval kan vara nödvändigt för att inte överträda krav på åtkomstkontroll. Vid användning av delade nätverk och nätverk vilka går utanför organisationens avgränsningar kan detta vara extra viktigt.

11.5 Styrning av åtkomst till operativsystem

Mål: Att förhindra obehörig åtkomst till operativsystem.
Säkerhetsanordningar bör användas för att begränsa åtkomsten till operativsystem till endast behöriga användare. Dessa anordningar bör möjliggöra följande:
(a) autenticera behöriga användare i enlighet med en definierad åtkomstpolicy;
(b) registrera lyckade och misslyckade försök till autenticering av system;
(c) registrera användningen av särskilda systemprivilegier;
(d) slå larm när systemsäkerhetspolicys bryts;
(e) tillhandahålla lämpliga medel för autenticering;
(f) i tillämpliga fall begränsa användarens uppkopplingstid.

11.5.1 Säker påloggningsrutin

En påloggningsrutin bör dels tillåta effektiv och enkel påloggning av legitima användare, dels minimera möjligheten till obehörig åtkomst. Systeminformation, hjälprutiner, etc. ska inte visas förrän fullständig påloggning har skett. Antalet tillåtna inloggningsförsök ska begränsas och misslyckade försök ska loggas. Det är lämpligt att påloggningsrutinen varnar för obehörig användning av systemet.

11.5.2 Identifiering och autenticering av användare

Samtliga legitima systemanvändare ska tilldelas en unik användaridentitet. I speciella fall är det lämpligt att en användare, exempelvis en systemadministratör, tilldelas flera identiteter.

Autentisering innebär att en påstådd identitet verifieras. En användare kan styrka sin identitet genom att

- veta något (till exempel ”lösenord”),
- äga något (till exempel ”aktivt kort”),
- ”vara” något (till exempel ”fingeravtryck”).

11.5.3 Lösenordsrutin

Användning av lösenord är den vanligaste metoden för autentisering utom i särskilt känsliga tillämpningar, som till exempel elektronisk handel, där starkare metoder krävs. I vissa fall tilldelas permanenta lösenord men i normalfallet väljs lösenordet av användaren själv. Det är önskvärt att lösenordsrutinen

- kontrollerar att det valda lösenordet är av tillräckligt god kvalitet,
- tvingar användaren till lösenordsbyte med jämna tidsintervall,
- hindrar återanvändning av tidigare lösenord.

Lösenord bör aldrig visas eller lagras i klartext eller annan oskyddad form. Fabriksinställda lösenord i programvaror bör ändras i samband med installation.

11.5.4 Användning av systemhjälpmedel

Systemhjälpmedel bör användas mycket restriktivt och ej vara tillgängliga för vanliga användare. Särskilt gäller detta program vilka kan sätta system och tillämpnigsspärrar ur spel. All användning av systemhjälpmedel bör loggas.

11.5.5 Tidsfördröjd nedkoppling

Automatisk utloggning och nedkoppling av terminaler efter en viss tid av inaktivitet kan vara lämplig för att hindra obehörig åtkomst. Tillämpningen av detta bör följas upp.

11.5.6 Begränsning av uppkopplingstid

Restriktioner i uppkopplingstid kan användas för att öka säkerheten. Det kan ske genom att det exempelvis bara är möjligt att vara uppkopplad till IT-systemen under normal kontorstid En förutsättning är naturligtvis att verksamheten tillåter att man endast har tillgång till resurserna under normaltid.

11.6 Styrning av åtkomst till information och tillämpningar

Mål: Att förhindra obehörig åtkomst av information i tillämpningar.

Säkerhetsåtgärder bör utnyttjas för att begränsa åtkomst till och inom tillämpningssystem.

Logisk åtkomst till program och data bör begränsas till behöriga användare. Tillämpningssystem bör:
(a) styra användares åtkomst till data och tillämpningssystem enligt definierad åtkomstpolicy;
(b) ge skydd mot obehörig åtkomst via systemhjälpmedel och operativsystemprogram och mot skadliga program som har funktioner för att åsidosätta eller gå förbi systemets eller tillämpningssystemets styrning;
(c) inte äventyra säkerheten i andra system med vilka informationsresurser delas.

11.6.1 Begränsning av åtkomst till information

Tillämpningssystem bör utformas så att differentierad åtkomst till systemdata och systemfunktioner kan tillämpas. Enskilda användare bör tilldelas åtkomsträtt i enlighet med gällande policy och regler för åtkomst samt de specifika krav tillämpningssystemet ställer.

11.6.2 Isolering av känsliga system

Speciellt känsliga eller kritiska system kan kräva helt eller delvis dedikerade tekniska plattformar. Systemet bör ha en utsedd ägare och vara väl dokumenterat. Dedikering kan ske genom användning av logiska och/eller fysiska metoder.

11.7 Mobil datoranvändning och distansarbete

Mål: Att säkerställa informationssäkerheten vid användning av mobilutrustning och utrustning för distansarbete.

Det skydd som krävs bör stå i proportion till de risker dessa särskilda arbetsmetoder orsakar. Vid mobil bearbetning bör risker med att arbeta i en oskyddad miljö beaktas och lämpligt skydd användas. Vid distansarbete bör organisationen använda skydd för arbetsplatsen och säkerställa att lämpliga anordningar är installerade för detta arbetssätt.

11.7.1 Mobil datoranvändning och kommunikation

Användning av bärbar IT-utrustning (bärbar pc, handdator, mobiltelefon, etc.) innebär särskilda risker, i synnerhet om de används på oskyddade platser som konferenslokal, flygplats och hotellrum. Speciella skyddsåtgärder kan bli nödvändiga mot stöld obehörig insyn eller avlyssning. Vidare kan det krävas speciella maskin- och programvaror för till exempel säkerhetskopiering, kryptering och virusskydd.

Det viktigaste säkerhetsskyddet vid mobil datoranvändning är dock användaren själv. Ett högt säkerhetsmedvetande parat med goda kunskaper i olika säkerhetsprocedurer är en grundförutsättning för effektivt säkerhetsskydd. Detta gäller naturligtvis för all IT-användning, men är speciellt viktigt vid mobilt bruk. En klart uttalad policy för mobil databehandling samt klara och heltäckande säkerhetsprocedurer och en relevant utbildning är därför tre hörnstenar för en säker mobil datoranvändning.

11.7.2 Distansarbete

Vid regelbundet och omfattande distansarbete, dvs. arbete från en fast plats utanför organisationen exempelvis i hemmet, är det viktigt att legala-, försäkrings- och arbetsmiljöaspekter har utretts och beaktats ordentligt. Säkerhetsaspekter som bör beaktas särskilt är bland annat

- fysiskt skydd och förvaring (stöld, brand etc.),
- kommunikationsskydd,
- skydd mot obehörig insyn (familjemedlemmar, vänner, grannar, med flera),
- skydd mot obehörig användning,
- säkerhetskopiering och kontinuitetsplanering,
- revision och övervakning av säkerhet,
- stöd och underhåll av IT-utrustning.

Ett speciellt problem är personaldatorer som vanemässigt eller endast tillfälligtvis används för arbetsändamål. Dessa datorer är vanligen bristfälligt skyddade men ofta uppkopplade mot publika nät. Organisationen måste ha en klar policy och klara regler för om, hur och när personaldatorer kan användas i arbetet.

Exempel

1 – Slarv med lösenord

Kvällstidningarna var en dag fyllda av ”sensationella avslöjanden” om de ”omänskliga” djurförsök Medytekk utfört under de senaste åren. Kvällspressen uppehöll sig speciellt vid sådana försök som fick göras om på grund av slarv. Djurförsöken var noggrant beskrivna med antalet försök och djur av olika slag per försök noggrant angivna. Det var uppenbart att journalisterna på något sätt hade fått tillgång till all forskningsdata för de senaste åren.

Den efterföljande undersökningen visade att Ida, laboratorieassistent Kalle Larssons sambo, har lämnat Kalles användaridentitet och lösenord till Bengt ”CyberBee” Olsson, en av de ”datorvana” ungdomarna i föreningen ”Stopp av djurförsök nu”. CyberBee hade tidigare frågat henne om hon kunde komma åt information om Medytekks djurförsök. Bengt ”CyberBee” Olsson har sedan loggat in som Kalle, kopierat olika filer samt sammanställt det underlag som kvällspressen använde sig av.

Ida råkade se Kalles invändaridentitet och lösenord i Kalles almanacka av en tillfällighet. Kalles hade skrivit upp dessa uppgifter på en gul ”kom-i-håg”-lapp som han sedan klistrade på insidan av almanacksbindningen.

Vad borde Medytekk ha tänkt på?

2 – Internt virusangrepp

Medytekks IT-chef Lennart Jakobsson och hans medarbetare var förtvivlade när man drabbades av ett tredje virusangrepp på två veckor. Viruset spred sig snabbt även denna gång och både forskningen och administrationen befann sig i något som bäst liknar kaos. Man var tvungen att ta ner systemet under två dagar för ”städning” varje gång vilket stört arbetsrutinerna kraftigt. IT-enheten fick arbeta nästan dygnet runt under dessa dagar eftersom användarna inte fått tillräckligt mycket utbildning för att kunna städa själva. Till råga på allt var stämningen något otrevlig och många har ifrågasatt IT-enhetens kompetens. Lennart visste att Göran Rubens övervägde att anlita externa experter.

Efter det andra virusangreppet har Jakobsson låtit installera ett ytterligare virusskydd. Det verkar inte ha hjälp och speciellt förbryllande var att ingen annan tycks ha drabbats. Dessutom verkade de aktuella virusen vara okända för båda leverantörerna av antivirusprogram.

Mitt under det brinnande arbetet ringer VD:s sekreterare Berit Qvick och vill träffa Lennart omgående. Hon berättar att man har sett en av medarbetarna på ekonomienheten, Barbro Sällström, använda en diskett på ett misstänkt sätt under morgonen. Barbro Sällström tittade runt om kring som för att kolla att ingen ser henne innan hon satte disketten i diskettläsaren. Efteråt la hon disketten i sin handväska som om hon ville gömma den. Under den efterföljande intern- och polisutredningen erkände Barbro Sällström att det var hon som initierade virusangreppen på uppmaning av sin pojkvän.

Barbro Sällström var kär i en utländsk forskare, James G. Watson, som arbetade för Medytekk för ett år sedan. Hon och Watson fattade tidigt tycke för varandra och var sambor medan Watson var i Sverige. Watson var en mycket begåvad kemist men missköte sitt jobb på grund av sitt stora intresse för datorer och internet. Efter flera månaders strul i det projekt han var engagerad i fick han lämna Medytekk och lämnade Sverige. Han var mycket bitter och tanken på hämnd gnagde i hans bakhuvud hela tiden. Idén att hämnas genom interna virusattacker fick han från en av sina hackerkontakter som också försåg honom med några nya, okända virus.

Vad borde Medytekk ha tänkt på?

3 – Hackerintrång

Sven Holgersson ersatte under en period Lennart Jakobsson. Holgersson kom till arbetet sent en fredagskväll för att göra en del systemuppdateringar. Han började med att se om någon var inloggad som skulle behöva varnas om det kommande systemavbrottet. Holgersson trodde för all del inte att någon skulle vara det men märkte

till sin förvåning att Stefan Eriksson var inloggad på distans. Han stirrade misstroget på sin skärm; Stefan Eriksson var ju på Bahamas på semester!

Efter samråd på telefon med Lennart Jakobsson kontaktade Holgersson IT-brottsenheten på Rikskriminalen. Man lyckades snabbt identifiera förbindelsens andra ändpunkt och kunde gripa en ung hacker på bar gärning. Den unge mannen höll på att experimentera med olika hackerverktyg och lyckades av en tillfällighet ta sig in på Medytekks system. Han var mycket förvånad över hur lätt det var att knäcka de flesta lösenorden med hjälp av en ordboksattack. Någon egentlig skada för Medytekks uppstod inte. Samtliga lösenord fick dock ändras för säkerhets skull. Vid den efterföljande rättegången hävdade den unge hackern att han borde få ersättning från Medytekk i stället för böter och det villkorliga straffet. Genom hackerattacken har Medytekk blivit medveten om en stor svaghet i säkerhetssystemet.

Vad borde Medytekk ha tänkt på?

4 – ”Fejkade” löner

Göran Rubens var förbryllad. Flera av projektledarna har klagat över felaktiga lönekostnader i samband med de månatliga uppföljningsmötena. Det var inte fråga om några stora summor, men i alla fall. Han misstänkte först att en eller annan månadslön har blivit felkonterad och bad för några veckor sedan Helene Petterson, en av trotjänarna på ekonomienheten, att kontrollera löneredovisningen. Hon har dock inte hittat något av intresse.

Rubens bestämde sig för att själv gå igenom samtliga lönelistor för året. Till sin förvåning noterade han att flera utländska forskare – vilka har anlitats tidigare men, så långt han visste, inte under året – har fått lön för en eller två månader under året. Han bestämde sig att kontrollera saken med B-G Sjöström och respektive projektledare. Den fortsatta undersökningen visade att ingen av dessa forskare anlitats av Medytekk under året. En utskrift av deras personaldata avslöjade dessutom att de hade ett och samma bankkonto – ett konto som tillhörde Helene Petterson!

Helene Petterson erkände gråtande och berättade om en svårt alkoholiserad make, trasigt hemliv med förestående skilsmässa samt dålig ekonomi. Hon kom på sättet att ”skaffa extra pengar” när hon märkte att hon kunde ändra personaluppgifter på eget bevåg samt kände till användar-id och lösenord som tillhörde arbetskamrater med behörighet att skapa lönetransaktioner. När hon blev ombedd av Göran Rubens att granska löneredovisningen förstod hon att hon skulle bli avslöjad men kunde inte komma på något sätt att sopa igen spåren efter sig.

Vad borde Medytekk ha tänkt på?

Vad kan vi lära oss av dessa exempel?

Exempel 1 – ”Social engineering”

Medytekk borde ha tänkt på att

- informera och utbilda alla datoranvändare om hur lösenord ska hanteras, bland annat förvaring, samt den enskildes ansvar för att det hanteras säkert,
- periodiskt följa upp hur lösenord hanteras,
- klassificera forskningsinformation mera finkornigt och begränsa åtkomsträttigheter på ett bra sätt,
- tillåta extern åtkomst endast för anställda som behöver det för sitt arbete, exempelvis med hjälp av stark autentisering av användare och/eller utrustning.

Medytekk borde också ha övervägt att

- informera personalen om olika hot i företagets omgivning och klargöra för de anställda hur de förväntas agera (*se även kapitel 6 – Personal och säkerhet*).

Exempel 2 – Internt virusangrepp

Medytekk borde ha tänkt på att

- införa ett system för uppföljning och övervakning av driften som registrerar och varnar för avvikelser från normalt användarbeteende, exempelvis när en normalanvändare initierar exekvering av ett främmande program,
- införa en genomtänkt rutin för incidenthantering, genom att bland annat utbilda användarna i konsten att ”städa” efter ett virusangrepp.

Exempel 3 – Hackerintrång

Medytekk borde ha tänkt på att

- införa ett system för uppföljning och övervakning av driften som registrerar och varnar för avvikelser från normalt användarbeteende, exempelvis när en användare börjar använda datasystemet på för honom/henne ovanliga tidpunkter,
- använda lösenord av bra kvalitet, genom att kräva att alla lösenord är minst sex tecken långa och innehåller minst två siffror eller specialtecken.

Exempel 4 – Fejkade löner

Medytekk borde ha tänkt på att

- informera och utbilda alla datoranvändare om en lämplig hantering av lösenord – de måste hållas hemliga och det är den enskildes ansvar att de förvaras säkert,
- agera snabbt när det blev känt att personalen på ekonomienheten har ”lånat ut” sina personliga lösenord till varandra.

Medytekk borde också ha övervägt att

- föra en mera aktiv personalpolitik, bland annat för att stödja sina anställda vid eventuella personliga problem (se även SS-ISO/IEC 17799, Kapitel 6 Personal och säkerhet).

Checklista – Styrning av åtkomst

Fråga	Ja	Delvis	Nej
Finns det riktlinjer för tilldelning respektive fråntagning av åtkomsträttigheter till information?			
Har man fastställt övergripande principer för informationsanvändning?			
Finns det ett regelverk som styr den operativa åtkomsten till it-resurserna?			
Täcker regelverket rättsregler och avtalsmässiga skyldigheter?			
Finns det ett system för användarregistrering?			
Omfattar systemet hela livscykeln från nyregistrering till slutlig avregistrering?			
Behöver användning av särskilda rättigheter auktoriseras och kan den spåras?			
Sker tilldelning av lösenord genom en formell och sekretesskyddad rutin?			
Finns det klara regler för temporära och tillfälliga lösenord?			
Granskas tilldelade åtkomsträttigheter periodiskt?			
Finns det regler för utformning, användning och förvaring av lösenord?			
Känner användarna till dessa regler och har de accepterat dem?			
Finns det tekniska skydd och operativa procedurer för obemannad utrustning?			
Finns det riktlinjer för utnyttjande av nätverkstjänster?			
Finns det regler och teknisk utrustning för autentisering av externanslutningar inklusive extern anslutning av datorer?			
Är externa diagnosportar fysiskt skyddade när de inte används?			
Är kommunikationen säkrad i logiskt sektionerade nätverk?			
Finns det avtal/överenskommelse med leverantörer av nätverkstjänster för samarbete avseende säkerhet?			
Är metoden för identifiering och autentisering av användare tillfredställande med hänsyn till genomförd riskanalys?			
Finns det regler för användning av överfalls- och nödfallslarm?			
Finns det tillämpningar med begränsad uppkopplingstid?			
Hindrar begränsningen effektivt arbete enligt systemanvändarna?			
Är differentierad åtkomst till data och funktioner möjlig i de tillämpningssystem detta är önskvärt?			
Finns det revisionsloggar (avvikelseloggar) för användaraktiviteter?			
Finns det lämpliga system för driftsuppföljning och -övervakning?			
Sker loggning och loggranskning på ett säkert sätt?			
Finns det IT-verktyg för manipulering och sammanställning av loggar från olika utrustningar?			
Finns det en överenskommen standardtid för datorklockor i nätverket?			
Har det skett en särskild riskanalys för mobil datoranvändning?			
Har alla, enligt riskanalysen relevanta, skyddsåtgärder vidtagits?			
Har användarna av mobil utrustning fått en genomgripande utbildning i nödvändiga säkerhetsprocedurer?			
Finns det en policy och klara regler för distansarbete?			
Sker det en lämplighetsbedömning och en riskanalys i varje enskilt fall?			
Är användning av utrustning för distansarbete för privata ändamål reglerad?			
Regleras användning av personaldatorer i hemmiljö för arbetsändamål?			

Kapitel 12 Anskaffning, utveckling och underhåll av informationssystem

Att själv utveckla ett eget tillämpningssystem eller upphandla ett externt system utan att från första början ta hänsyn till och väga in säkerhetskraven kan bli mycket dyrt. Men redan innan det är dags att bygga in säkerheten i systemet finns det faktiskt en del allmänna och ganska självklara råd för hur man ska ta itu med systemutveckling och upphandling – råd som man måste följa för att, oavsett säkerheten, få ett system som fungerar som man önskar. Det är inte någon vits med bra säkerhet i ett system som inte fungerar.

12.1 Säkerhetskrav på informationssystem

Mål: Att säkerställa att säkerheten är en integrerad del av informationssystemet.

Informationssystem omfattar operativsystem, infrastruktur, verksamhetstillämpningar, inköpta standardprodukter, tjänster och användarutvecklade tillämpningar. Utformning och införande av det informationssystem som stödjer verksamhetsprocessen kan vara avgörande för säkerheten. Säkerhetskrav bör identifieras och överenskommas före utveckling och/eller införande av informationssystem.

Alla säkerhetskrav bör identifieras under ett projekts kravspecifikationsfas och motiveras, överenskommas och dokumenteras som ett led i den överordnade motiveringen för ett informationssystem.

12.1 Analys och specifikation av säkerhetskrav

Hur ska man undvika att trilla i de dyrbara systemutvecklingsfällorna? Att införa ett LIS är bra. Dessutom finns det anledning att tänka igenom några generella systemutvecklingsstrategier.

För det första måste man ha klara tydliga funktionella mål för vad man vill att systemet ska göra. Den som vill handla rationellt måste självklart alltid göra klart för sig varför han vill eller ska göra något och hur det ska göras för att nå det önskade resultatet. Detta är den kravspecifikation som så ofta försummas eller slarvas över och som ska gälla även säkerheten. Ansvaret för systemutvecklingen och dess olika delar och faser måste vara skriftligt definierat innan utvecklingsarbetet börjar. Normalt bör det vara den verksamhetsansvarige – systemägaren – som bär det slutliga ansvaret. Han kan naturligtvis behöva ta stöd av experter. Försök att begränsa komplexiteten. Det finns gränser för hur komplicerade system en människa kan överblicka och kontrollera. Det är bättre att bryta ner systemet i mera lätthanterliga bitar. Erfarenheten visar också att evolution är bättre än revolution. En stegvis utvecklingsstrategi är bättre än jätteklivet. För övrigt får ett utvecklingsprojekts tidplaner inte bli så långa att utgångslägets förutsättningar förändrats när man äntligen kommer i mål. Det hindrar inte att man kan dra nytta av en vision som ett mål att på sikt sträva mot. Annat som måste begränsas är teknikfixeringen. Det är systemägaren som ska ta ansvar och vara den som bestämmer.

Som det står i standarden: ”Alla säkerhetskrav bör identifieras under ett projekts kravspecifikationsfas och motiveras, överenskommas och dokumenteras som ett led i den överordnade motiveringen för ett informationssystem.”

I kravspecifikationen på nya eller utökade/ändrade system – egenutvecklade eller upphandlade programpaket – måste alltså säkerhetskraven specificeras. Hur höga säkerhetskrav man måste ha är beroende av värdet av den aktuella informationen för företaget, riskerna och riskhanteringen och den skada som kan bli resultatet av otillräcklig säkerhet.

Säkerhetsarbetets gång under systemutveckling kan illustreras enligt följande:

Strategi: Företagets riktlinjer för systemutveckling inklusive säkerhet.

Analys: Riskbedömning, krav enligt lag och avtal, informationsklassning, specifikation av säkerhetskrav.

Genomförande: Behörighet, avbrottsplan, eventuell kryptering, kontroller (indata- utdata- och bearbetningskontroller).

Test/överlämnande: Formellt överlämnande till drift.

Drift/underhåll: Dokumentation, loggning, ändringar (efter förnyad riskanalys).

Avveckling: Strategi- och policyfrågor etcetera, behandlas i andra avsnitt i denna handbok liksom riskanalys, informationsklassning, behörighetskontroll med mera.

I det följande behandlas planeringen av kontroller, kryptering och hur test och övergång till drift ska styras. Slutligen berörs frågor om upphandling av utvecklingsarbete och drift.

12.2 Korrekt bearbetning i tillämpningar

Mål: Att förhindra fel, förlust, obehörig förändring eller missbruk av information i tillämpningssystem.

Lämpliga skyddsmedel bör konstrueras i tillämpningssystem inklusive användarutvecklade tillämpningar för att säkerställa korrekt bearbetning. Dessa medel bör innefatta validering av indata, intern bearbetning och utdata.

Ytterligare skyddsmedel kan krävas för system som bearbetar eller kan påverka känslig, värdefull eller kritisk information. Sådana medel bör beslutas på grundval av säkerhetskrav och riskbedömning.

12.2.1 Validering av indata

Sisu (= "skräp-in-skräp-ut") är ett gammalt talesätt inom informationsbehandlingen. Det betyder förstås att utdata från ett informationssystem blir dåligt om inmatade data har dålig kvalitet. Det är alltså nödvändigt att noga kontrollera sina indata oberoende av hur denna inmatning sker. LIS ger ett antal exempel på lämpliga kontroller: dubbelinmatning av data (samma data registreras två gånger), rimlighetstester, gränsvärden etcetera. Nivån och omfattningen av kontrollerna, som kan bli kostsamma, bör bland annat bestämmas av informationens karaktär. I vissa fall kan det vara fråga om textbaserade data där ett och annat fel, som en felstavning, inte har någon stor betydelse. I andra fall kan det få förödande konsekvenser om en enda siffra felregistreras. En felinmatning i Medytekks läkemedelsrecept liksom i forskningsresultaten kan få mycket svåra och kostsamma följder.

Rätt inmatade data kan förvanskas genom bearbetningsfel. Också mot avsiktliga felhandlingar och sabotage kan man behöva skydd även om de förefaller mycket osannolika. Det kan krävas särskilda kontroller av bland annat ändrings- eller raderingsfunktioner, kontroll av att rätt programversion används, att program körs i rätt ordning och i samband med återstart efter fel.

Bearbetningskontroller av data kan omfatta buntkontroller för avstämningar, saldokontroll från en bearbetning till nästa, checksummering och rimlighetskontroller. Flera exempel på bearbetningskontroller finns i standarden.

Slutligen måste utdata kontrolleras på motsvarande sätt genom exempelvis rimlighetskontroller och avstämningar.

12.2.2 Styrning av intern bearbetning

Vid utformningen och hanteringen av tillämpningssystem bör kontroller läggas in för att upptäcka eventuella bearbetningsproblem. Det kan vara lämpligt att upprätta en checklista med lämpliga kontroller.

12.2.3 Meddelandeintegritet

Bedömning av eventuella säkerhetsrisker och meddelandets riktighet avgör vilket skydd som behövs. Kryptering (se 12.3) kan vara en lämplig metod då ett utökat skydd behövs.

12.2.4 Validering av utdata

För att säkerställa att utdata från ett tillämpningssystem är korrekt behövs rutiner för validering av data. Väsentligt är att det görs någon form av rimlighetskontroll för att testa om utdata är rimligt. Likaså en kontroll av att all indata verkligen har bearbetats.

12.3 Kryptering

Mål: Att skydda informationens sekretess, autenticitet eller riktighet med kryptering.

En policy för användning av kryptering bör utvecklas. Nyckelhantering bör finnas för att stödja användningen av krypteringsteknik.

12.3.1 Krypteringspolicy

Kryptering skyddar både informationens sekretess och dess riktighet. Dessutom kan kryptering garantera till exempel ett meddelandes äkthet (autenticitet). Tillämpade krypteringstekniker består av en formel (krypteringsalgoritm) som är allmänt känd och i bland till och med officiell standard. Algoritmen är låset som öppnas med krypteringsnyckeln. Krypteringsnyckeln, som består av en slumpvis genererad datasträng, används

tillsammans med algoritmen för att göra ett meddelande eller andra data obegripliga för den som är obehörig det vill säga saknar krypteringsnyckeln med vars hjälp den behörige kan ”låsa upp” och få tillbaka det okrypterade klartextmeddelandet. Skyddsvärdet av krypteringen är förstås helt beroende av att den hemliga nyckeln inte kommer i orätta händer. För ett företag som anser sig behöva kryptering är därför ett vattentätt system, inklusive tydlig ansvarsfördelning, för generering och distribution av nycklar en viktig (och svårlöst) fråga.

Kryptering och dekryptering (=upplåsning) av exempelvis en datafil tar naturligtvis en viss processortid i anspråk och få därmed en kostnad. I princip mera ju längre (och därmed säkrare) nyckel man använder. Även nyckelhanteringen kostar. Man bör därför fundera över om man verkligen behöver kryptering och om så är fallet, välja en algoritm och nyckellängd som är anpassad till den risk och sårbarhet som råder. Man bör inte skjuta mygg med kanon och inte heller välja krypto så att det krävs timslångt arbete för en superdator (eller veckor av pc-bearbetning) för att knäcka kryptot om filen eller meddelandet trots allt har begränsat intresse under kort tid.

Självklart måste det vara resultatet av riskanalysen som blir avgörande för beslut om kryptering. Ett sådant beslut liksom också valet av algoritm och nyckelhanteringsrutin är komplicerade frågor där det är lämpligt att ta råd av experter. Kryptering är dessutom belastat med diverse legala restriktioner, särskilt vid export och import. Även av det skälet finns anledning att inhämta expertråd.

Elektroniska signaturer kan användas i stället för handskrivna signaturer och därmed möjliggöra elektroniska, juridiskt bindande avtal, order, betalningar och så vidare vid bland annat e-handel mellan företag. Elektronisk signering är en kryptografisk teknik som utnyttjar ett unikt sammanhängande nyckelpar där den ena nyckeln (den privata) används för att signera till exempel en betalningstransaktion och den andra (den öppna) för mottagarens kontroll av signaturen. Eftersom endast den öppna nyckeln i paret kan tolka signaturen gjord med motsvarande privata nyckel kan alltså signaturens äkthet kontrolleras av mottagaren. Den privata nyckeln måste därför skyddas väl eftersom vem som helst som har tillgång till den kan ”förfalska” signaturen. Naturligtvis kan ett signerat elektroniskt meddelande även krypteras om man anser att obehöriga inte ska kunna ta del av innehållet. En ytterligare fördel med den elektroniska signaturen är att den kan säkra oavvislighet. Den som exempelvis skickat en beställning signerad med den privata nyckeln kan inte hävda att han inte gjort beställningen.

Ett särskilt problem utgör nyckelhanteringen. Krypteringen och den elektroniska signaturens tillförlitlighet hänger ju helt på att nyckeln som måste hållas hemlig inte hamnar i orätta händer. SS-ISO/IEC 17799 innehåller en rad förslag till hur ett nyckelhanteringssystem bör fungera genom bland annat framställning, distribution, lagring och ändring av nycklar. SS-ISO/IEC 17799 talar också om återkallande av förlorade nycklar liksom arkivering och förstöring av existerande nycklar.

12.3.2 Nyckelhantering

Har man valt att tillämpa krypteringsteknologi för kryptering av information och eller elektronisk signering krävs att det finns rutiner implementerade i organisationen för att stödja detta. Det är även nödvändigt med fysiskt skydd av den utrustning som används för framtagning, lagring och arkivering av nycklar.

12.4 Säkerhet i databaser och filer

Mål: Att säkerställa säkerheten i databaser och filer.

Åtkomst till databaser, filer och källkod till programmen bör styras och IT-projekt och stödaktiviteter utföras på ett säkert sätt. Försiktighet bör iakttas för att undvika avslöjande av känsliga data i testmiljöer.

12.4.1 Styrning av program i drift

Alla system som går i drift är normalt föremål för kontinuerlig ändring under sin livstid. Man bör vara mycket försiktig vid system- och programändringar. Uppdatering av driftens program måste ske under strikt kontroll och tester måste formellt godkännas innan det nya/ändrade programmet införlivas med programbiblioteket. Alla ändringar och uppdateringar bör dokumenteras så att de kan spåras i efterhand. Tidigare programversioner bör bevaras.

Försiktighet måste iakttas vid system- och programtester. Man bör om möjligt undvika att använda produktionens databaser. Blir det trots allt nödvändigt utnyttjar man en särskild kopia, anonymiserad om så är möjligt, som raderas efter fullbordad test. All testverksamhet bör loggas. Revisorer vill gärna ha ett revisionsspår att följa. Överlämnande av program eller system efter test bör ske efter strikta formella regler för att undvika sammanblandning, missförstånd och ansvarsproblem.

Standarden innehåller ett antal regler för hur ett källprogramarkiv ska skötas. Det rör ansvars- och åtkomstfrågor, uppdateringsrutiner för arkivet och utlämnande av källprogram till driften liksom även loggning av åtkomst och andra händelser och slutligen arkivering av inaktuella programversioner.

12.4.2 Skydd av testdata

Testdata vilken används vid system- och acceptanstest måste efterlikna ordinarie driftdata så långt det är möjligt. Ofta måste dock testdata modifieras så att den ej innehåller information vilken har inverkan på personlig integritet eller annan känslig information. Det är väsentligt att hålla testdata avskilt från produktionsdata samt att logga alla testaktiviteter.

12.4.3 Styrning av åtkomst till källprogramkod

Det är från ett informationsäkerhetsperspektiv viktigt att skapa ett starkt skydd med strikta åtkomsträttigheter för källprogramkod. Detta för att undvika såväl avsiktliga som oavsiktliga förändringar av funktioner i program. Rutiner för att säkerställa ändringshantering liksom loggning av alla vilka getts åtkomst till källprogramkod kan vara nödvändigt.

12.5 Säkerhet i utvecklings- och underhållsprocesser

Mål: Att bibehålla säkerheten i tillämpningssystemens program och information.

Projekt- och underhållsmiljöer bör styras noggrant.

De personer som är ansvariga för tillämpningssystem bör också ha ansvar för säkerheten i projekt- eller underhållsmiljön. De bör säkerställa att alla föreslagna systemändringar granskas för att kontrollera att de inte äventyrar säkerheten vare sig i systemet eller i driftmiljön.

12.5.1 Ändringshantering

En formell rutin för beslut och godkännande bör finnas för systemförändringar. Frågorna berör

- behörighet och behörighetskontroll,
- rätten att fatta beslut om ändring,
- kontrollen av att inte andra program eller system påverkas av den tilltänkta ändringen,
- registreringen för revisionsspår av alla programuppdateringar,
- att systemdokumentationen uppdateras,
- att driftdokumentation och dokumentation av användarrutiner ändras och anpassas,
- slutligen en ordnad arkivering av gamla versioner.

Upphandlade program bör om möjligt användas utan modifiering eller anpassning. Om så ändå måste ske bör man dels samråda med leverantören, dels behålla originalversionen av programpaketet och göra ändringarna i en tydligt identifierad kopia. Man bör endast upphandla program från välrenommerade programleverantörer som man kan anta kommer att finnas kvar på marknaden under överskådlig tid.

Om man uppdrar programutveckling åt en extern part är det viktigt med avtal som reglerar bland annat upphovsrätt, kvaliteten i arbetet, rätten till revision av arbetets kvalitet och kontroll över hur tester ska genomföras.

12.5.2 Teknisk granskning av tillämpningar efter ändringar i operativsystem

Innan ändringar i ett operativsystem installeras i produktionsmiljö är det väsentligt att analysera vilken negativ påverkan detta kan ha på såväl drift som säkerhet. Ansvar och rutiner för detta bör vara dokumenterade och väl kända.

12.5.3 Restriktioner mot ändringar i programpaket

Ur säkerhetssynpunkt är det att föredra att programpaket används i originalversion.
När det bedömts lämpligt att modifiera programpaket bör ändringen begränsas till det absolut nödvändigaste.

Det kan vara nödvändigt att ha ett godkännande från leverantören och förändringar kan även innebära att leverantören avsäger sig supportansvar.

Den förändrade versionen bör vara tydligt identifierad och utgå från en kopia av originalversionen.

12.5.4 Informationsläckor

Trojaner utnyttjar ofta dolda eller dåligt skyddade kanaler. Det är därför viktigt vidta nödvändiga åtgärder för att stoppa trojaner. Policies och effektiva rutiner liksom vidtagna åtgärder för att obehöriga ej skall komma åt nätverket är väsentligt.

12.5.5 Utlagd programutveckling

När programutveckling läggs ut till en leverantör bör detta ske under avtalsreglerade former. Vid upprättande av avtal är det särskilt viktigt att beakta:

- Kvalitet och säkerhetsfunktioner
- Test före leverans och installation
- Licensfrågor, äganderätt till koden och upphovsrätt

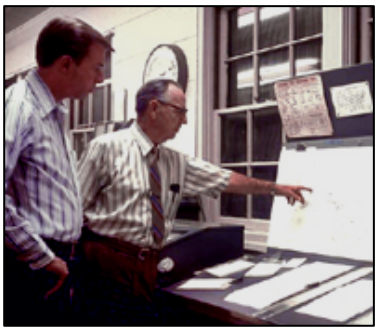
12.6 Hantering av teknisk sårbarhet

Mål: Att minska riskerna med utnyttjande av publicerade tekniska sårbarheter.
Skyddet för teknisk sårbarhet bör implementeras på ett effektivt, systematiskt och repeterbart sätt med åtgärder vidtagna för att bekräfta dess verkan. Dessa överväganden bör omfatta operativsystem och alla andra tillämpningar i drift.

12.6.1 Skydd av tekniska sårbarheter

För att säkerställa en hög informationssäkerhet är det nödvändigt att känna till vilka informationskällor som finns och använda dessa för att inhämta information. Rutiner för detta liksom att ansvarsfördelningen är definierad är viktigt för att lyckas. Programuppdateringar som skall åtgärda sårbarheter bör testas innan ändringen implementeras. En korrekt inventarieförteckning är nödvändig för att säkerställa att man har kontroll över alla svagheter.

Exempel



1 – Systemkontroller

I samband med användning av Amacyclin i Kosovo hade ett fall av förgiftning upptäckts. Man misstänkte att vaccinet var förorenat eller felsammansatt. FOI ville bland annat veta vilka kontroller som installerats i det system som styrde och kontrollerade produktionen och särskilt i det kvalitetskontrollsystem som varje vaccinsats genomgick före leverans. FOI tyckte att det fanns anledning att ifrågasätta kontrollen i produktionssystemen. All användning och alla leveranser av Amacyclin stoppades med omedelbar verkan i väntan på resultat av Medytekks utredning.

Vad hade Medytekk försummat?

2 – En bärbar förlust

Vid en lång (och ganska blöt) lunch hos ett utländskt konkurrentföretag – tillika presumtiv kund – blev en av Medytekks säljare bestulen på sin bärbara dator. På datorns hårddisk fanns bland annat vissa ännu inte patenterade forskningsresultat och Medytekks produktionsplaner för det kommande året. Materialet var avsett att utnyttjas i samband med förhandlingar med företaget. Datorn med innehåll bedömdes representera ett avsevärt värde för konkurrenten (cirka 5 miljoner kronor) och motsvarande förlust för Medytekk jämte en svåruppskattad goodwill-förlust i branschen.

Vad skulle Medytekks säljare ha gjort?

3 – Testslarv

Vid en kvalitetskontroll hos ett stort läkemedelsföretag tillika kund till Medytekk, konstaterades uppenbart felaktiga värden i Medytekks forskningsresultat. När saken undersöktes konstaterades att Medytekk förväxlat en filkopia avsedd för vissa programtester med den skarpa filen som avsågs varför resultatet blivit helt orimligt. Kunden uttryckte sitt utomordentliga missnöje med Medytekks slarv.

Vad borde Medytekk ha tänkt på?

4 – Systemupphandling

Medytekk köpte för något år sedan ett programpaket från en välrenommerad programleverantör. Medytekks forskare ansåg sig behöva förbättra systemet för att passa bättre i Medytekks miljö och gjorde därför vissa ändringar i programmen.

Vid senare uppdateringar visade det sig att ändringarna förorsakat icke förutsedda följdfel för vilka programleverantören inte ansåg sig kunna ta något ansvar. Leverantören begärde dessutom skadestånd för att hans system i strid med leveransavtal hade ändrats utan hans vetskap och godkännande.

Vad borde Medytekk ha tänkt på?

Vad kan vi lära av dessa exempel?

Exempel 1 – Systemkontroller

Medytekk borde ha planerat sitt systemutvecklingsarbete på ett mera professionellt sätt och ha

- gett IT-chefen tillfälle att upprätta en IT-strategi inklusive informationssäkerhetsstrategi,
- klargjort ansvarsfördelning där man bland annat utsett ansvariga systemägare innan systemutveckling påbörjats,
- gjort riskanalys och planerat säkerhet, styrning och kontroller innan systemutveckling påbörjats,
- installerat kontroller i systemet av indata, bearbetning och utdata, som till exempel rimlighets- och gränsvärdeskontroller.

Exempel 2 – En bärbar förlust

Med tanke på hur känslig som den information är som de resande säljarna ofta måste medföra i sina bärbara datorer vid kund- och mässbesök och hur lätt (och ofta) sådana datorer kan stjälas och glömmas på bland annat hotellrum, borde informationen krypteras på hårddisken. För att krypteringen ska fungera måste Medytekk

- upphandla ett passande kryptosystem,
- utveckla och installera ett tillförlitligt system för hantering (generering, distribution, lagring, ändring, förstörelse etcetera) av nycklar.

Medytekk bör också, med tanke på de pc-stölder som skett, installera kryptering i de känsligaste pc-systemen.

Exempel 3 – Testslarv

Medytekk borde ha utvecklat och fastställt regler och kontroller för testverksamhet som bland annat borde omfatta

- installation av säkra rutiner och kontroller för förvaring, utlämnande till drift, arkivering och förstöring av produktionsfiler,
- fysiskt där så är möjligt skilja förvaring och hantering av testfiler från produktionens filer,
- tillåta utnyttjande av produktionens data för teständamål endast då det är nödvändigt,
- om produktionens filer trots allt måste användas endast utnyttja avidentifierade kopior som förstörs efter genomförd test.

Exempel 4 – Systemupphandling

Medytekk borde besluta om policy och regler för upphandling av programprodukter/system som innebär att

- IT-chefen samordnar all sådan upphandling,
- upprätta lämpliga avtal med programleverantörer, som bland annat reglerar förfoganderätt, kvalitetskrav, tester, uppdatering och ändringar, säljarens underhållsansvar och eventuellt skadestånd.

Checklista – Anskaffning, utveckling och underhåll av informationssystem

Fråga	Ja	Delvis	Nej
Har både interna och externa användares/intressenters krav specificerats före utveckling/anskaffning av ett nytt eller förändrat system?			
Finns tydlig ansvarsfördelning för hela projektet?			
Finns en säkerhetskravspecifikation för systemet/projektet?			
Genomförs riskanalyser systematiskt i projektets olika faser?			
Tas en kontinuitetsplan fram under projektutvecklingen?			
Har kontrollrutiner utvecklats för systemet? • Indatakontroller? • Bearbetningskontroller? • Utdatakontroller?			
Har ett eventuellt behov av kryptering övervägts?			
Finns rutiner för godkännande av systemförändringar?			
Tillämpas rutiner/restriktioner för ändringar i upphandlad programvara?			
Skapas erforderliga loggar för uppföljning av säkerheten i systemet?			
Säkerställs det att testdata kontrolleras och skyddas?			
Sker utveckling och test av programvara i en egen, från driften avskild miljö?			
Sker överlämnande till drift enligt fasta rutiner?			
Finns rutiner för avveckling av system?			
Finns erforderlig dokumentation som bland annat beskriver systemet och dess kopplingar till andra system			

Kapitel 13 – Hantering av informationssäkerhetsincidenter

13.1 Rapportering av säkerhetshändelser och svagheter

Mål: Att säkerställa att informationssäkerhetsincidenter och svagheter hos informationssystem rapporteras på ett sådant sätt att korrigerande åtgärder kan vidtas i rätt tid.

Formella rutiner bör finnas för händelserapportering och eskalering. Alla anställda, entreprenörer och utomstående användare bör göras medvetna om rutinerna för rapportering av de olika typerna av händelser och svagheter som kan påverka säkerheten hos organisationens tillgångar. Det bör krävas att de rapporterar eventuella informationssäkerhetshändelser och –svagheter så snart som möjligt till den utsedda kontaktpunkten.

13.1.1 Rapportering av informationssäkerhetshändelser

Rutiner för incidentrapportering bör finnas. De ska säkerställa att incidenter rapporteras så snart de observerats. Rutinerna bör vara kända av alla i organisationen och så utformade att det inte finns några omotiverade byråkratiska hinder. Definitionen av vad som är en incident måste vara entydig och förstådd av alla.

13.1.2 Rapportering av säkerhetsbrister

För att förebygga uppkomsten av informationssäkerhetsincidenter bör alla säkerhetsbrister dokumenteras och hanteras i enlighet med en formell rutin. Bästa lösningen kan vara att använda samma rutin som för incidentrapportering.

13.2 Hantering av informationssäkerhetsincidenter och förbättringar

Mål: Att säkerställa att ett konsekvent och effektivt angreppssätt tillämpas på hanteringen av informationssäkerhetsincidenter.

Ansvarsfördelning och rutiner bör finnas för att effektivt hantera informationssäkerhetshändelser och brister så snart de har rapporterats En process för ständig förbättring bör tillämpas när det gäller att reagera på, följa upp, värdera och överordnat hantera informationssäkerhetsincidenter.

Där bevis krävs bör de insamlas i överensstämmelse med legala krav.

13.2.1 Ansvar och rutiner

För att effektivt kunna hantera eventuella incidenter bör en rad åtgärder övervägas. Även dessa bör behandlas på det sätt som tidigare angivits, alltså som formella rutiner som vilar på en strikt formell grund.

I rutiner för hantering av denna typ av beredskap bör säkerställas att rutinerna innefattar tillvägagångssätt för att kunna avhjälpa:

- driftavbrott och fel på informationssystem (även avsiktligt framkallade),
- störningar och felaktigheter på grund av inkorrekta data,
- sekretessbrott.

Dessa rutiner bör även inbegripa tillvägagångssätt för att utröna orsaken till störningen, rutinmässigt införande av lämpliga åtgärder för att förhindra upprepning samt säkra spårbarhet.

Väsentligt är även att former för vidarerapportering innefattas. Förutom att kontakta de som berörs direkt vid ett eventuellt återställande bör det även vara klarlagt vilka övriga instanser som ska informeras och i vilken ordning.

Vid ett intrång handlar det om att agera snabbt och korrekt. Det finns ofta inte tid för tveksamheter om intrång upptäcks medan de pågår.

13.2.2 Att lära av säkerhetsincidenter

För att utveckla ledningssystemet och förbättra skyddet av informationstillgångarna är det väsentligt att utvärdera rapporterade svagheter och incidenter. Analysen bör ske utifrån ett större perspektiv. Det räcker alltså inte att göra detta på ett övergripande sätt och bara titta på en enskild incident. Genom att klassa incidenter och använda statistiska tekniker kan mönster identifieras. Erfarenheterna från incidentrapporteringen bör tillämpas vid såväl genomförande av riskanalyser som vid uppdatering av informationssäkerhetspolicyn.

13.2.3 Insamling av bevis

När en informationssäkerhetsincident kan resultera i juridiska åtgärder mot en person eller organisation bör bevis insamlas för styrka händelsen. Rutiner för att hantera disciplinära åtgärder då medarbetare bryter mot regelverket vilket styr informationssäkerheten inom organisationen. Insamling av bevis och hur detta skall hanteras bör vara en del av detta regelverk. Det är nödvändigt att säkerställa att de åtgärder som vidtages är i enlighet med gällande lagstiftning. Saknas kunskap inom organisationen är det lämpligt att anlita juridisk expertis.

Checklista – Hantering av Informationssäkerhetsincidenter

Fråga	Ja	Delvis	Nej
Finns rutin för incidentrapportering?			
Finns rutin för rapportering av säkerhetsbrister?			
Har det definierats vad en incident är?			
Finns regler, metoder för att säkerställa spårbarhet?			
Finns rutiner för korrigerande åtgärder?			

Kapitel 14 Kontinuitetsplanering i verksamheten

Varför ska en organisation spendera delar av sin redan begränsade budget på någonting som kanske skapar värde för organisationen bara när eller om en kris/katastrof skulle inträffa? Sådana initiativ verkar ligga i konflikt med mer kortsiktiga prioriteringar, där fokus på kostnadskontroll och organisationens mål att generera vinst är viktigare.

Att det kan vara förödande att resonera på detta sätt visar bland annat tågolyckorna i Lilleström och Borlänge där farligt gods transporterades (bland annat gasol). Utrymningar och avspärrningar drabbade både organisationer och enskilda i omkring en vecka. Följderna vid allvarliga incidenter kan resultera i att företag måste läggas ner.

14.1 Informationssäkerhetsaspekter på kontinuitetsplanering i verksamheten

Mål: Att motverka avbrott i organisationens verksamhet och att skydda kritiska verksamhetsprocesser från verkningarna av allvarliga fel i informationssystemen eller katastrofer och att säkra återstart inom rimlig tid.

En ledningsprocess för kontinuitetsplanering bör införas för att minimera följderna för organisationen och återhämtning efter förlust av informationstillgångar (som kan vara ett resultat av t.ex. naturkatastrofer, olyckshändelser, utrustningsfel eller avsiktliga åtgärder) till en godtagbar nivå genom en kombination av förebyggande och återställande skydd. Detta förfarande bör identifiera kritiska verksamhetsprocesser, samt integrera krav på kontinuitet i verksamheten från informationssäkerhetsperspektiv med andra kontinuitetskrav utifrån aspekter som drift, personbemanning, material, transport och resurser.

Konsekvenserna av katastrofer, säkerhetsbrister, förlust av tjänster och tjänstetillgänglighet bör analyseras med hänsyn till inverkan på verksamheten. Avbrottsplan bör upprättas och införas för att säkerställa att viktiga funktioner kan återställas inom rimlig tid. Informationssäkerhet bör vara en integrerad del av den överordnade processen för kontinuitetsplanering och även av andra ledningsprocesser inom organisationen.

Kontinuitetsplanering för verksamheten bör innefatta åtgärder för att identifiera och minska risker, förutom den allmänna riskbedömningsprocessen, begränsa konsekvenserna av skadliga incidenter och säkerställa att den information som krävs för verksamheten är tillgänglig.

14.1.1 Att inkludera informationssäkerhet i verksamhetens kontinuitetsplanering

Kontinuitetsplanering är förmågan och beredskapen att hantera avbrott i en organisations verksamhet. Den syftar till att minska skador som förorsakas av avbrott. Dessutom ska den säkerställa att verksamhetens kritiska processer ligger på en accepterad lägsta nivå som kan garantera en finansiell och konkurrenskraftig position på lång sikt. Synonymt med begreppet kontinuitetsplan används också begrepp som katastrofplan, avbrottsplan och beredskapsplan.

Kontinuitetsplanering innefattar att etablera fungerade processer och en organisation som kan koordinera arbetet med att utarbeta och införa planen, genomföra granskningar och tester av planen och som kan hantera kontinuerlig anpassning av planen till nya risker och hot och förändringar i verksamheten.

Traditionellt har kontinuitetsplanering endast hanterat organisationens infrastruktur med den föreställningen att med alternativa lokaler kan organisationens verksamhet fortsätta som tidigare.

SS-ISO/IEC 17799 standardens definition av begreppet kontinuitetsplanering är dock större och vidare. Här är det organisationens verksamhet i kontinuitet som ska säkerställas. Kontinuitetsplanen ska utgå ifrån organisationens övergripande säkerhetspolicy, om sådan finns, och inte vara begränsad till dess informationssäkerhetspolicy. En kontinuitetsplan innefattar således mer än en plan för att skydda organisationens IT-verksamhet och information.

En kontinuitetsplan måste hållas aktuell. Planen, rutiner och organisationen kring den, samt lösningarna för att stödja den, måste kontinuerligt anpassas till förändringar i organisationens verksamhet, organisation och de risker som måste hanteras.

För att möjliggöra för organisationen att ta fram och underhålla en kontinuitetsplan, ha förmågan att verkställa den, samt ha en organisation för att underhålla den, bör arbetet med kontinuitetsplaneringen bedrivas i form av en ledningsprocess. Processen bör inkludera följande element:

- Definition av områden och strategi
- Hot- och riskanalys
- Avbrotts- och konsekvensanalys
- Etablering av en organisation för att utarbeta, införa och underhålla planen
- Framtagning och dokumentation av planen
- Förvaltning och underhåll
- Granskning, testning och övning.

Arbetet med kontinuitetsplanering bör inledas med att identifiera de områden som behöver skyddas. Detta inkluderar att identifiera verksamhetens mest kritiska processer och de produkter/tjänster dessa levererar och som måste skyddas.

Här bör man också reda ut frågor som:

- Var bör den lägsta nivån på en tjänst ligga i en katastrofsituation?
- Måste man erbjuda samma kontinuitet av service till alla kunder, eller kan man ha olika servicenivåer?
- Måste alla lokaler vara inkluderade i en kontinuitetsplan eller är vissa mer affärskritiska än andra?
- Är det bättre att titta på avdelningarna separat eller bör man betrakta affärsprocesserna tvärs igenom avdelningar?
- Är verksamhetens organisation och kultur sådan att det bästa tillvägagångssättet är att planen tas fram centralt medan genomförandet sker lokalt?

En förutsättning för att ta fram och dokumentera en kontinuitetsplan är att man har genomfört en riskanalys. Denna har som syfte att identifiera tänkbara händelser relaterat till såväl verksamhetens infrastruktur som dess affärsverksamhet och vilka kan orsaka avbrott i verksamheten. Dessa händelser bör sedan bedömas utifrån ett riskperspektiv där sannolikheten och konsekvensen av ett avbrott, inklusive omfattning och tid för att återställa, analyseras.

14.1.2 Kontinuerlig verksamhet och riskbedömning

I samband med riskanalysen bör också en avbrotts- och konsekvensanalys genomföras där olika händelsers påverkan på verksamheten beskrivs och analyseras. I denna fas är det viktigt att inkludera både dimensionerna affärsverksamhet och infrastruktur i analysen.

Affärsverksamhet inkluderar affärsrelaterade frågor rörande affärsfunktioner och affärs- processer, produkter och tjänster, viktiga kunder och leverantörer och olika affärsenheters specifika behov.

Infrastruktur täcker stora delar av IT-sidan som nätverk, datorer, kritiska applikationer, fastigheter, lokaler och logistik mm. Exempel på kontinuitetsplaner associerade med dessa risker inkluderar omlokalisering av kontor, redundanta datorhallar, dubblerade nätverk mm.

Allt för ofta fokuseras planeringen på risker relaterade till infrastrukturen (vad händer om nätverket inte längre är tillgängligt, vad händer om en byggnad brinner ner) när det finns många andra typer av risker som kanske skulle göra större skada än dessa.

I och med att dimensionen affärsverksamhet adderas, så kan man börja ställa sig frågor som: Vad händer om en viktig leverantör faller ifrån? Vilka är de kritiska produkter och tjänster som påverkas av att huvudkontor och de personer som jobbar där är otillgängliga? Denna dimension inkluderar även frågor som nöjda kunder, efterlevnad av lagar och regler, företagets livskraft på längre sikt samt mer immateriella element såsom företags- och varumärkesimage.

För många organisationer är kundomsorg nyckeln till framgång. Kontinuitet i kundservice bör vara del av de strategiska målen för ett kundfokuserat företag. Detta inkluderar inte bara möjligheten att snabbt kunna lösa nätverks problem, eller möjligheten att snabbt återuppta affärsverksamheten, utan också hur man hanterar kommunikation med kunderna.

Andra tänkbara katastrofsituationer där ingen direkt skada skett på tillgångar eller infrastruktur, men som ändå kräver omedelbar handling kan vara utpressning, dödsfall, negativ publicitet, strejk eller lockouter mm.

14.1.3 Utveckling och införande av kontinuitetsplaner innefattande informationssäkerhet

Det är viktigt att i tid etablera en organisation som kan utarbeta, införa och underhålla planen. Kontinuitetsplanering berör många avdelningar och kan kräva integration av många verksamheter, processer och rutiner.

När man etablerar denna organisation är det viktigt att exempelvis beakta följande:

- Ledningens stöd är absolut kritiskt för att kunna ta fram och underhålla en kontinuitetsplan. Kontinuitetsplanering är genomgripande av sin natur. Detta betyder att den berör alla nivåer och avdelningar inom ett företag och kräver en hög grad av kommunikation och integration. Det är viktigt att klargöra var och hur riskhanteringsbeslut att tas.
- Ansvaret för kontinuitetsplaner ska vara entydigt definierat. Det måste säkerställas att delat ägandeskap inte förekommer.
- Att skapa en kontinuitetsplan kan genomföras som ett antal projekt och delprojekt. Förvaltning, ägandeskap och beslutstagande befogenheter ligger inom linjeorganisationen.
- Olika organisationer har olika prioriteringar och begränsat med tid och resurser. Att skapa riskmedvetande och att involvera användarna i projektet med kontinuitetsplanering är viktigt för ett lyckosamt slutresultat.

En central del i etablerandet av en kontinuitetsplan är att involvera organisationen samt att bygga upp organisatorisk säkerhet exempelvis via krishantering. Detta är den organisation som effektuerar de rutiner som ska hantera avbrottet.

Speciellt måste denna organisation ha rutiner och regler för att upptäcka och aktivera planen när en oväntad händelse inträffar, och att försäkra sig om att dessa procedurer är kända av alla inblandade parter och att de fungerar effektivt.

14.1.4 Ramverk för kontinuitetsplanering i verksamheten

Arbetet med att utarbeta och dokumentera en kontinuitetsplan genomförs med fördel i projektform. Detta projekt bör inkludera följande områden

- Bygga upp riskmedvetenhet i verksamheten samt övertyga intressenter om nödvändigheten av kontinuitetsplanering
- Skapa reservrutiner och rutiner för återställande samt definiera ansvarsförhållanden för de kritiska områdena vilka ska inkluderas i planen
- Definiera en organisation med rätt ansvarsfördelning samt adekvata processer för att förvalta planen
- Dokumentera rutinerna samt rapportera status, föreslå åtgärder och beslut som bör tas av styrmöte på ledningsnivå
- En organisation för respons- och krishantering bör definieras som kan besluta när planen ska aktiveras. När bör man trappa upp från en händelse (som bör hanteras av den dagliga driften) till katastrof? Kan en katastrof vara definierad utifrån vilken inverkan den har på organisationen, eller bör ett avbrott av en tjänst som kraftigt påverkar en viktig kund också bli hanterad som en katastrof?

Huvuduppgiften i arbetet med att utarbeta och införa kontinuitetsplanerna är att koordinera den generella planeringsprocessen, samt att integrera de olika projekten och delprojekten i arbetet med att ta fram och implementera specifika avbrottsrutiner.

En kritisk framgångsfaktor är att projektet håller översikt på alla initiativ, och har myndighet att ta problem, konflikter eller frågor till en högre nivå, företrädesvis till styrmöte på ledningsnivå.

14.1.5 Provning, underhåll och ändring av kontinuitetsplaner

När projektet att bygga kontinuitetsplanen är avslutat är det stor risk att planen blir inaktuell inom några månader. Det är organisationens ansvar att hålla planen vid liv och att anpassa den till förändringar i verksamhet och organisation.

I organisationens ansvar ingår även att identifiera hinder som kan äventyra dess arbete. Typiska hinder kan vara bristande samarbete mellan avdelningar, inga incitament till att göra insatser för att underhålla planerna, brist på kommunikation, historiska svårigheter att göra medarbetare medvetna om olika rutiner och procedurer o.s.v.

Inom organisationen bör även följande frågeställningar beaktas:

- Vem tar ägaransvar av de olika delarna och lösningarna i den totala kontinuitetsplanen?
- Hur ska underhåll och distribution av planen organiseras för att säkerställa att alla involverade personer vet exakt vad de ska göra, baserat på den senaste versionen?

Det finns organisationer där en separat avdelning samordnar underhållet av kontinuitetsplanen och dess stödjande delar.

Avdelningen ligger i många organisationer organisatoriskt under IT-avdelningen. Denna placering upplevs ofta som ett hinder för integration med andra delar av organisationen, eller skapar svårigheter i kommunikation och förståelse av andra avdelningars ansträngningar rörande kontinuitetsplanering. På grund av dessa orsaker är oftast bästa placering av avdelningen någonstans i verksamheten där den kan ha överblick över hela organisationen.

Organisationen måste också definiera hur och när behovet finns för en granskning av planen. En normal granskning av kontinuitetsplanen måste vara väl organiserad och bör inkludera uppföljning av efterföljande rekommendationer från granskningen. Eftersom kontinuitetsplanen hanterar en mängd möjliga affärsrisker, kan det vara lämpligt att granskningen koordineras med organisationens internrevisionsavdelning om sådan finns. Många internrevisionsavdelningar utvecklas i riktning mot att granska organisationens affärsriskhantering och uppfyller en kontrollerande roll gentemot organisationens ledning.

Det är viktigt att försäkra sig om att kapaciteten för att verkställa planen finns, därför bör regelbundna tester och övningar genomföras. Tester kan göras av hela kontinuitetsplanen eller enskilda delar. Dock är det viktigt att testa helheten inkluderande krishanteringsrutiner för att säkerställa en verksamhet i kontinuitet om någonting händer.

En kritisk framgångsfaktor för att hålla en kontinuitetsplan vid liv är att regelbundet granska medvetenheten hos anställda och andra berörda. Att skapa ett separat program inom organisationen att utbilda och informera om kontinuitetsplanen kan vara ett sätt att höja medvetenheten.

Exempel

Normalt kan incidenter klaras av inom och med den normala organisationen, men då verksamheten drabbas av allvarligare skada och då tiden för maximerat avbrott överskrids, är det att betrakta som katastrof och då skall kontinuitetsplanen aktiveras

- Vad gör vi när och om allt plötsligt slutar att fungera?
- Vilka konsekvenser får det?
- Hur och när kan verksamheten komma igång?
- Vilka kostnader medför ett plötsligt stopp i verksamheten?
- Hur skall vi hantera personalen?

Det finns en mängd frågor att besvara som dyker upp och vi har kanske inga konkreta svar på frågorna. Det är säkert vid detta tillfälle varje företagsledare önskar att det funnits en väl fungerande kontinuitetsplan att tillgå. Varför har ingen tänkt på detta tidigare att det kunde hända, eller är det så att vi tyckt det varit onödigt ”det händer inte oss”, eller var det så att vi tyckte det kostade för mycket. Det kanske var så att vi planerat att utarbeta en kontinuitetsplan men inte kommit igång med arbetet. När det väl hänt är det för sent att vara efterklok.

Om man förutsätter att Medytekk kan klara sig 5 dygn utan delar av verksamheten eller IT-stödet

- Vad innebär 5 dygn utan produktion eller IT-stöd?
- Vad händer om allt blivit förstört av exempelvis en brand?
- Det kan vara så att grannföretaget drabbas av en incident som sprider sig till Medytekk med följden att Medytekk också blir utslaget helt eller delvis?

Vad som helst kan hända, smått som stort, och det gäller att vara förberedd på detta bland annat genom att ha en fungerande kontinuitetsplan med utbildad och tränad personal.

Följande exempel ger en fingervisning om vad som kan hända och med lite eftertanke kan dessa lösas med en kontinuitetsplan som är anpassad till er organisation.

1 – Naturkatastrof

För ca 3 år sedan drabbades verksamheten i Sverige av en allvarlig incident då blixten slog ned i Medytekk: s ställverk (elcentral) som försåg hela företaget med kraft. Blixten orsakade samtidigt en brand som totalförstörde ställverket och angränsande utrymmen (C testprod, Pretest djur och delar av produktionslokalen plan 2). I stort sett alla djur omkom p.g.a. rökgaserna.

Verksamheten drabbades hårt då produktion och verksamhet endast kunde bedrivas i mycket begränsad omfattning under ca två veckor, mitt under högproduktion.

Incidenten medförde att inga larm eller passagekontroller fungerade. Hissen drabbades också och var ur funktion.

Laboratoriet fick ett antal projekt starkt försenade, då försöksdjuren omkommit, vilket medförde att samtliga
pågående försök måste startas från början.

De lokala IT-systemen i dessa lokaler skadades och några servrar måste nyanskaffas. Vissa problem uppstod vid installationen av de nya servrarna, då säkerhetskopiorna inte var fullständiga och att en dags produktion av information måste återskapas manuellt, vilket medförde extra arbete på ca en vecka.

Vad borde Medytekk ha tänkt på?

2 – Explosion

Medytekk drabbades för ett år sedan av en explosion och brand i sitt laboratorium.

Laboratoriet blev totalförstört och ett flertal viktiga IT-utrustningar förstördes innehållande mängder av testresultat.

Samtliga försök förstördes, samtidigt som det fanns stor risk för smittspridning, då ett antal virus- och bakterieodlingar fanns i lokalerna.

Det kan inte säkerställas att dessa förstörts under branden då ett antal av dessa kan vara motståndskraftiga mot värme.

Hela området spärrades av och var i behov av sanering. Samtliga som beträdde området måste bära helskyddsdräkter.

Det bedömdes vid tillfället att det skulle ta minst flera månader innan verksamheten skulle kunna återupptas i full produktion.

Säkerhetskopior på den senaste och viktigaste informationen fanns inte annat än i den server som fanns i anslutning till laboratoriet och som totalförstörts. Resterna av hårddiskarna skickades till ett externt företag för att om möjligt kunna återskapa den viktigaste informationen. Dock upptäcktes att delar av informationen fanns i de två bärbara utrustningar som två av forskarna hade för hemarbete.

Försäkringsskyddet täckte inte skadorna.

Vad borde Medytekk ha tänkt på?

3 – Olycka

Medytekk drabbades nyligen återigen av en olyckshändelse. Det var restaurangköket som fattat eld genom överhettning av en flottyrkokare. Branden spred sig till intilliggande lokaler genom ventilationssystemet.

Ovanför restaurangköket finns den centrala datorhallen som skadades svårt vid branden. Säkerhetskopior fanns på annan plats, men det visade sig att den senaste säkerhetskopian (en vecka gammal) ej överförts till säkerhetsarkivet. Den senaste säkerhetskopian var ca två veckor gammal.

Kablar till och från datorhallen är förstörda då dessa dragits i anslutning till ventilationssystemet. Samtidigt med denna händelse blev den ansvarige IT-teknikern förolyckad då han var på väg till Medytekk för att om möjligt rädda något. IT-installationerna är mycket komplicerade och genom olyckan upptäcktes att ingen annan visste hur systemen var uppbyggda.

Vad borde Medytekk ha tänkt på?

Vad kan vi lära oss av dessa exempel?

Exempel 1 – Naturkatastrof

Med en kontinuitetsplan och förutseende åtgärder kunde incidenten (händelsen) ha begränsats till några dagar. Bland annat borde grundläggande åtgärder ha vidtagits enligt nedan:

- Verksamhetsanalys (identifiering av områden som behöver skyddas).
- Hot- och riskanalys.
- Kostnadskalkyl (riskvärdering).

Dessa för att identifiera risker och sannolikheten för att denna händelse kunde inträffa, samt vilka kostnader händelsen skulle medföra med och utan kontinuitetsplan.

Följande åtgärder hade i detta exempel minskat kostnader och tiden för driftstoppet:

- Kontinuitetsplan (reservrutiner).
- Säkerhets- och brandutbildad personal.
- Åskledare.
- Tillförlitligt brandlarm med tidig indikation.
- Dubblerad kraftförsörjning, kraftmatning från två oberoende ställverk.
- Favoriserad kraft till viktiga delar av verksamheten med UPS.
- Reservutrustning.
- Batteribackup på lås, larm och passagekontroll.
- Försöksdjuren i två oberoende byggnader.

Exempel 2 – Explosion

Hur skulle skadeverkningarna ha kunnat minskas? Vilka åtgärder borde ha vidtagits före olyckan?

Med en kontinuitetsplan kunde incidenten (händelsen) ha begränsats. Även i detta fall borde åtgärder ha vidtagits enligt nedan:

- Verksamhetsanalys (identifiering av områden som behöver skyddas).
- Hot- och riskanalys.
- Kostnadskalkyl (riskvärdering).

Dessa för att identifiera risker och sannolikheten för att denna händelse kunde inträffa, samt vilka kostnader händelsen kunde medföra med och utan kontinuitetsplan.

- Kontinuitetsplan (reservrutiner).
- Säkerhets- och brandutbilda personalen (katastrofutbildning).
- Uppdelning av laboratoriet (olika fastigheter).
- Endast ha mindre mängder brännbara ämnen i lokalerna och ha ett särskilt förråd i egen byggnad som är anpassad för förvaring av dessa ämnen.
- Automatisk brandsläckning på utsatta platser.
- Online säkerhetskopiering till annan fastighet.
- Säkerhetskopior bör alltid förvaras på två platser fysiskt skilda från varandra.
- Särskilt anpassat rum för odlingar med anpassat skydd mot brand etc.
- Inga känsliga IT-utrustningar i laboratoriet, endast terminaler till nätverket.

Ovanstående åtgärder bör ingå i en kontinuitetsplan.

Exempel 3 – Olycka

Även i detta fall borde åtgärder ha vidtagits enligt nedan:

- Verksamhetsanalys (identifiering av områden som behöver skyddas).
- Hot- och riskanalys.
- Kostnadskalkyl (riskvärdering).

Dessa för att identifiera risker och sannolikheten för att denna händelse kunde inträffa, samt vilka kostnader händelsen kunde medföra med och utan kontinuitetsplan.

- Kontinuitetsplan (reservrutiner).
- Felplacerad datorhall.
- Bättre rutiner för undanförsel av säkerhetskopior, alternativt onlinekopiering till server i annan byggnad.
- Kablar till nätverk och datorer bör alltid dras så de är skyddade eller på sådant sätt att kraft ventilationsrör ej kan påverka dessa.
- Nyckelpersonal.

Det visar sig om man granskar åtgärderna vid incidenter att många åtgärder återkommer vid olika händelser. Det är viktigt att analysera och skilja ut vad som är kärnverksamhet (det man tjänar pengar på) och prioritera åtgärder för kärnverksamheten.

Checklista – Kontinuitetsplanering för verksamheten

Fråga	Ja	Delvis	Nej
Finns en testad och fungerande kontinuitetsplan?			
Är den väl känd och dokumenterad?			
Finns ansvarig utsedd för kontinuitetsplanen?			
Har alla verksamheter deltagit vid utarbetandet av kontinuitetsplanen?			
Uppdateras kontinuitetsplanen vid förändringar och minst en gång om året?			
Är personalen väl förtrogen med kontinuitetsplanen?			
Är personalen övad och känner de till hur de skall agera?			
Finns organisation för att garantera verksamhetens kontinuitet?			
Finns enkla checklistor för vilka åtgärder som skall vidtas?			
Finns rutiner för bevakning vid allvarlig händelse?			
Finns fungerande larmlistor till nyckelpersoner?			
Finns reservrutiner och reservplats?			
Finns lokal för ledning av verksamheten vid avbrott?			
Finns en aktuell resursförteckning?			
Finns ansvariga utsedda att leda verksamheten vid kris/katastrof?			
Kan tillfälligt nätverk snabbt återskapas?			
Finns klara planer för återstart?			
Kan viktig information och utrustning snabbt flyttas om hot föreligger?			
Finns fungerande rutin för incidentrapportering?			
Finns och genomförs konsekvensanalyser vid incidenter?			
Kan verksamheten komma igång inom planerad tid?			

Kapitel 15 Efterlevnad

Organisationers verksamhet regleras av lagar och avtal. Många verksamheter måste också följa särskilda författningar eller krav som ställts upp av myndigheterna. Att handla i strid med regelverket kan naturligtvis orsaka skador för verksamheten, och då inte bara ur ett juridiskt perspektiv. Även om direkta skador uteblir finns det risk att förtroendet naggas i kanten, något som på sikt kan kosta organisationen väl så mycket. Därför är det väsentligt att organisationen följer det lagar och avtal som berör verksamheten.

15.1 Efterlevnad av rättsliga krav

Mål: Att undvika handlande i strid med författningar eller avtalsförpliktelser och andra säkerhetskrav.

Utformning, drift, användning och styrning av informationssystem kan påverkas av bestämmelser i lagar, författningar och säkerhetskrav i avtal.

Rådgivning i frågor om särskilda rättsliga krav bör inhämtas från organisationens juridiska rådgivare eller lämplig juridisk expertis. Rättsliga krav varierar från land till land och kan vara olika för information skapad i ett land och som överförs till annat land (s.k. trans-border data flow).

Verksamhetens informationssystem kan påverkas av bestämmelser i lagar, avtal och eventuella andra regler. Det gäller såväl systemens utformning som dess drift och användning. En komplicerande faktor är att hänsyn ofta även måste tas till andra länders lagar och regler. Organisationen bör ta sin juridiske rådgivare, jurist eller annan person med lämpliga kunskaper till hjälp.

15.1.1 Identifiering av tillämplig lagstiftning

För varje informationssystem bör organisationen göra klart vilka rätts- och avtalsregler som gäller. Därefter bör de personer som ansvarar för efterlevnaden utses. Personerna bör förses med de styrmedel som behövs för att efterlevnaden ska kunna följas upp.

15.1.2 Immaterialrätt

Immaterialrätten reglerar exempelvis upphovsrätt, patent och varumärkesskydd. Vid upphandling av programprodukter finns det i allmänhet restriktioner i licensavtalen. Brott mot dessa restriktioner, vanligen genom att extra kopior görs och installeras, kan leda till böter och mycket kraftiga skadestånd. Det är därför viktigt att organisationen har en policy som reglerar programvaruanvändningen. Policyn bör kompletteras med regler för upphandling och den praktiska programanvändningen, exempelvis hur det ska gå till om en programvara ska överlåtas till någon annan. Det bör särskilt regleras hur programvaror får hämtas från till bland annat internet. Som alltid bör man försäkra sig om att alla anställda känner till regelverket och vad avvikelser från det kan innebära.

Det bör också finnas uppdaterade register över vilka program organisationen har licenser för. Arkivering av bevis på innehav, som handböcker, installationsdiskar etcetera, kan vara ett stöd vid en eventuell process.

15.1.3 Skydd av organisationens register och andra redovisande dokument

Register och andra förtecknade uppgifter kan behöva skyddas för att inte bli avslöjade, förlorade, förstörda och förvanskade. Vissa uppgifter kan behöva skyddas för att lagen säger så medan andra är betydelsefulla för verksamheten som sådan. Därför bör ett system för säker lagring och hantering vara upprättat. Alla register bör vara utformade så att de är lätta att identifiera. Kategorisering efter typtillhörighet bör göras och uppgifter bör finnas om hur registret är lagrat och hur länge det ska behållas. Man bör också överväga valet av lagringsmedium så att det går att läsa uppgifterna under hela den tid som det är bestämt att registret ska finnas. När det är dags att gör sig av med ett register bör informationen makuleras på ett säkert sätt.

15.1.4 Skydd av persondata

Människors personliga integritet är en stor fråga. I Sverige har vi en lagstiftning som ska förhindra att personuppgifter hanteras på ett sätt som kan kränka den personliga integriteten. Många andra länder har liknande lagstiftning. Inom EU finns direktiv på området, som bland annat legat till grund för den svenska Personuppgiftslagen, PUL. Lagar och direktiv föreskriver i allmänhet vilka personuppgifter som överhuvud taget får registreras och behandlas, när det får ske samt vilka krav som ställs på den som hanterar uppgifterna. För register med personuppgifter ska ett individuellt ansvar vara fastställt.

För att kunna efterleva dessa krav måste det finnas en viss styrning. Exempelvis kan ett personuppgiftsombud utses i organisationen. Ombudet ska kunna vägleda ledning, personuppgiftsansvariga samt andra berörda i frågor som rör ansvar, regelverk och de rutiner som bör följas.

15.1.5 Förhindrande av missbruk av informationsbehandlingsresurser

Datorer, program och annan utrustning för informationsbehandling tillhör organisationen och finns där för att på olika sätt stödja verksamheten. Annan användning, utan ledningens vetskap och godkännande, kan ses som obehörig. Vissa länder har infört lagstiftning mot obehörig användning. Det kan då till och med vara brottsligt att använda företagets dator privat.

En annan aspekt på missbruk är att obehörigen skaffa sig tillgång till skyddad information. Även detta kan vara brottsligt, oavsett om det görs av anställda i verksamheten eller i form av externa intrång. Användarna i den egna organisationen bör informeras om vilken användning som är tillåten men också om eventuella påföljder som kan komma av ett missbruk. Att mottagaren fått denna information ska bekräftas. Vid försök att logga på till något av organisationens system bör användaren få ett meddelande om att obehörig åtkomst inte är tillåten. Fortsatta försök ska inte vara möjliga utan att användaren bekräftar meddelandet.

För att upptäcka ett eventuellt missbruk krävs naturligtvis uppföljning. Rutiner för detta bör därför finnas. Det innebär ofrånkomligen en viss övervakning av användarnas verksamhet i systemen, som i vissa fall innebära att organisationen i stället gör sig skyldig till lagbrott! Hur övervakningen får se ut varierar mellan olika länder, därför bör juridisk kompetens anlitas när rutinerna utformas.

15.1.6 Reglering av kryptering

Vissa länder har lagstiftning på krypteringsområdet. Det kan gälla restriktioner för import/export av utrustning för kryptering eller krav på statlig tillgång till krypteringsnycklar. Juridisk kompetens bör anlitas för att säkerställa att organisationen inte bryter mot gällande lagstiftning. Innan krypterad information eller utrustning flyttas till ett annat land bör det berörda landets lagstiftning utredas.

15.2 Efterlevnad av säkerhetspolicys, -standarder och teknisk efterlevnad

Mål: Att säkerställa att system följer organisationens säkerhetspolicys och –standarder.

Informationssystemets säkerhet bör granskas regelbundet.

Sådana granskningar bör ske mot tillämpliga säkerhetspolicys. De tekniska plattformarna och informationssystemen bör granskas vad avser efterlevnad av tillämpliga standarder för införande av säkerhet och dokumenterade säkerhetsåtgärder.

15.2.1 Efterlevnad av säkerhetspolicys och -standarder

För att säkerställa att säkerhetsrutinerna tillämpas bör regelbundna granskningar genomföras och omfatta:

- informationssystem,
- systemleverantörer,
- ägare av information och informationstillgångar,
- användare,
- ledningspersonal.

Arbetet bör aktivt stödjas av informationsägarna.

15.2.2 Kontroll av teknisk efterlevnad

Teknisk kontroll, utförd av specialister, krävs för att säkerställa att säkerhetslösningar är korrekt implementerade. Arbetet kan utföras manuellt eller med hjälp av lämpliga program- och rapportverktyg.

Exempelvis kan så kallade penetrationstester påvisa säkerhetslösningarnas effektivitet mot systemintrång. Här är det väsentligt att testerna inte äventyrar systemens säkerhet, varför såväl dess utförande som övervakning bör ske av kompetent personal.

15.3 Att beakta vid revision av informationssystem

Mål: Att maximera revisionens effektivitet och samtidigt minimera driftstörningar orsakade av revisionen.
Medel bör finnas för att skydda system i drift och revisionshjälpmedel under pågående revision av informationssystem. Skydd krävs också av revisionshjälpmedlen för att bevara deras riktighet och förhindra missbruk.

15.3.1 Styrning av revision av informationssystem

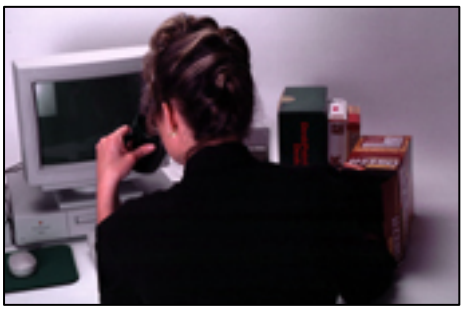
För att systemrevisionen inte i onödan ska störa den operativa verksamheten bör följande iakttas:

- samråd med tillämplig ledning,
- överenskommelse om vilka kontroller som ska granskas,
- revisor och revisionsprogram bör endast ha läsbehörighet (undantag kan göras för eventuella kopior av produktionsdata, vilka sedan bör raderas),
- erforderligt stöd från berörda IT-resurser,
- eventuella särskilda bearbetningar för revisionsändamål bör överenskommas,
- loggning av all åtkomst för att möjliggöra spårbarhet,
- dokumentation av samtliga revisionsrutiner samt ansvarsförhållanden.

15.3.2 Skydd av hjälpmedel för revision av informationssystem

Åtkomst till revisionshjälpmedel ska begränsas. Hjälpmedlen bör lagras åtskilda från utvecklings- och produktionssystem.

Exempel



1 – Olicensierade program

För ett par veckor sedan slutade IT-konsulten Stellan T Bråk innan han genomfört sitt uppdrag. Medytekk var inte nöjda med Stellans sätt att sköta sitt uppdrag och hade därför hos dennes arbetsgivare framfört önskemål om att byta ut honom. Stellan var inte på sitt bästa humör när han lämnade Medytekk.

Medytekk får en dag besök av representanter från BSA (Business Software Alliance). BSA säger sig ha fått tips om att piratkopior av program finns i företagets datorer och begär att få göra en genomgång. Alla datorer utom de som för tillfället inte finns i företagets lokaler undersöks. Det framkommer att ett antal datorer innehåller avancerad CAD/CAM-programvara, trots att företaget bara kan påvisa att en licens finns. Detsamma gäller diverse andra program för framställning av ritningar och flöden. Dessutom hittas några olicensierade spelprogram. Medytekk riskerar att antingen polisanmälas eller att ingå en uppgörelse i godo med BSA.

Vad borde Medytekk ha tänkt på?

2 – Musikfiler på nätet

Kapacitetsproblem konstateras på en av företagets servrar. Det visar sig att hårddisken i servern är full, vilket förvånar eftersom den nyligen bytts ut till en större. Vid analys upptäcks omkring 5 000 så kallade MP3-filer med musik. Ytterligare analys, denna gång av loggar, visar att filerna under lång tid laddats ned från internet och också vem som gjort det. Vid samtal med personen, Inge Snygg, framgår det att ett omfattande musikutbyte skett mellan Inge och ett par andra personer på företaget. Vidare har en cd-brännare på IT-avdelningen använts för att kopiera musikfiler från servern.

Inge hävdar att han hela tiden skött sitt jobb och att han ”inte visste att det inte var tillåtet”.

Vad borde Medytekk ha tänkt på?

3 – Datorn fast i tullen

Forskaren Fasth Ullén vid Medytekk åker utomlands för att medverka vid ett seminarium. Han ska där hålla föredrag och hoppas naturligtvis på nya internationella kontakter som kan leda till affärer. Hans föredrag har i form av bildspel och stödord lagrats i den bärbara datorn som är med på resan. Eftersom Fasth är säkerhetsmedveten har han låtit installera säkerhetsprogramvara på sin dator. Skulle datorn försvinna så kan ingen få tillgång till innehållet, som är krypterat i sin helhet.

Vid ankomst till flygplatsen i det främmande landet har Fasth otur och åker in i tullen. Tullaren kräver att Fasth ska slå på sin dator. När det framgår att informationen skyddas av kryptering säger tullaren att Fasth ska informera om krypteringsnyckeln. Fasth vägrar, då han inte ens vet vad krypteringsnyckel är. Lösenordet vill han förstås inte lämna ut.

Datorn stannar kvar i tullen tills Fasth åker hem igen utan att ha kunnat hålla något föredrag.

Vad borde Medytekk ha tänkt på?

Vad kan vi lära oss av dessa exempel?

Exempel 1 – Olicensierade program

Om det var Stellan T. Bråk som ”skvallrat” om olicensierade kopior eller om det kom fram till BSA på annat sätt är i sammanhanget inte relevant. Kopior av det slag som fanns vid Medytekk tas många gånger av bekvämlighetsskäl för att slippa beställa och vänta på ny licens. Många betraktar inte heller förfarandet som piratkopiering, då man ju ändå en gång betalat för programmet.

En policy med tillhörande regler för programanvändning förhindrar naturligtvis inte kopieringen i sig, men tydliggör företagsledningens inställning. Information till alla anställda om tänkbara följder, såväl för bolaget som för den enskilde, skulle sannolikt ha minskat risken för det inträffade.

Exempel 2 – Musikfiler på nätet

Regelverket för vad som får laddas ned och upphovsrätt är en fråga i sig vilken vi ej tar upp här.
Klart är dock att exemplet är ett fall av missbruk av företagets resurser. Eftersom företagsledningen inte explicit uttryckt att datorer och program är avsedda för arbetet och inget annat, kunde Inge hävda att han var i sin fulla rätt. Som i exemplet med otillåten kopiering av program skulle en tydlig policy med information till de anställda sannolikt ha minskat risken.

Exempel 3 – Datorn fast i tullen

Risken att tullen intresserar sig för en dator är naturligtvis låg. Ändå hände det här. Exemplet visar att okunskap om lagstiftningen på detta område faktiskt kan få oväntade följder. Om bolaget i förväg rådgjort med en jurist och informerat de anställda om vad som gäller på krypteringsområdet, hade säkerligen någon annan lösning för Fasths föredrag kunnat hittas före avresan.

Checklista – Efterlevnad

Fråga	Ja	Delvis	Nej
Finns i verksamheten, anställd eller konsulterad, person med erforderlig juridisk kompetens?			
Har relevanta lagar och avtal identifierats för verksamhetens informationssystem?			
Har ansvarig för att följa upp efterlevnaden utsetts och finns fungerande metoder för detta?			
Finns fungerande policy och regler för programupphandling och programanvändning?			
Finns aktuellt register över inköpta program?			
Finns system för säker lagring, hantering och destruktion av information?			
Finns utsedda ansvariga för skydd av personuppgifter?			
Finns policy som reglerar hur företagets system ska användas (skydd mot missbruk) och har de anställda informerats?			
Finns rutiner för att följa upp systemanvändningen?			

Appendix 1 – Exempelföretaget ”Medytekk AB”

Inledning

Detta kompendium innehåller information om företaget Medytekk AB. Företaget är helt fingerat och eventuella likheter med i verkligheten existerande företag ska betraktas som en ren tillfällighet. Detta gäller även för de personer och anställda som beskrivs i detta material.

Att utveckla ett nytt läkemedel är en komplicerad och tidskrävande process. Den kräver samverkan mellan specialister från olika områden inom biologi, medicin och teknik, såsom biokemi, toxikologi, patologi, fysiologi, farmakologi och klinisk dokumentation.

I genomsnitt tar det 10–15 år innan ett nytt läkemedel kan introduceras på marknaden från den inledande grundforskningen. För att reducera tiden från forskning till färdigt läkemedel som kan konsumeras utnyttjar många större läkemedelsföretag mindre forskningsföretag såsom Medytekk AB. Ca 10 procent av de resultat som Medytekk AB säljer blir till läkemedel.

De idéer som utvecklas syftar till att fylla ett medicinskt behov på marknaden. Kemister och farmakologer diskuterar vilka kemiska strukturer som bör undersökas och vilka biologiska testsystem som är lämpliga att använda för att den nya substansens effekter ska kunna ringas in. Visar det sig att det finns bärkraft i idén avancerar den till att bli ett projekt. Fler vetenskapsmän involveras i processen och för att skydda idén görs en patentansökan för de kemiska föreningar som är mest intressanta. Farmakologiska studier utförs för att ta reda på föreningarnas effekter, biverkningar, hur föreningarna tas upp, omsätts och utsöndras ur organismen. Det är också viktigt att ta reda på hur föreningen påverkar arvsanlag och foster samt undersöker eventuell skadlighet vid längre tids användning. Det är inom ramen för detta som Medytekk AB har sin verksamhet.

Efter försäljning av forskning och testresultat tar nästa fas vid. Kunskapen om de utvalda substanserna är nu så omfattande att köparen kan välja ut en läkemedelskandidat en så kallad **Candidate Drug, CD**. Efter dessa pre-kliniska studier ansöker läkemedelsföretaget om tillstånd att få göra studier på människa, så kallad Investigational New Drug (IND).

När tillstånd erhållits startas kliniska studier på människor. Detta arbete delas in i fyra faser. I fas I görs toleransstudier och undersökningar på friska försökspersoner om hur det blivande läkemedlet tas upp, bryts ner och utsöndras ur kroppen, så kallade farmakokinetiska studier. I fas II görs liknande försök på patienter i mindre grupper; och effekterna på sjukdomen följs upp. I fas III görs undersökningar på stora grupper av patienter och det blivande läkemedlet jämförs med konventionell terapi. Produktens effekter och säkerhet dokumenteras. Här bestäms produktens profil, vilken dosering och beredning som är lämpligast, vilka eventuella biverkningar läkemedlet kan medföra, i vilka fall det inte bör ges samt dess interaktion med andra läkemedel. Parallellt med de kliniska studierna genomförs toxikologiska tester och cancerstudier på djur.

Nu finns det underlag att göra en ansökan om att få sälja produkten som ett nytt läkemedel. Denna ansökan ställs till Läkemedelsverket, en så kallad **New Drug Application** (NDA-ansökan). Efter godkännande registreras substansen som läkemedel. I fas IV fortsätter de jämförande studierna. I syfte att upptäcka eventuella biverkningar samt för att upprätthålla kvalitén genomförs kontinuerligt studier under tiden som läkemedlet säljs på marknaden.

Appendix 1.1 Exempelföretaget ”Medytekk AB”

Medytekk AB grundades 1986 av två läkare, B-G Sjöström från Universitetssjukhuset i Umeå och Stefan Eriksson från Akademiska sjukhuset i Uppsala. De båda var gamla kamrater från studietiden i Lund. Genom ett gemensamt forskningsprojekt väcktes idén om att starta ett eget företag. Företaget började som ett handelsbolag och verksamheten finansierades egentligen helt genom anslag och bidrag från olika intresse organisationer.

Affärsidén var lika enkel som genial, utföra grundforskning inom väl avgränsat område och sälja resultaten till etablerade läkemedelsföretag. Själva forskningsresultaten säljs vanligtvis till en engångssumma med en klausul om att utnyttjas resultatet till att framställa ett läkemedel ska Medytekk AB erhålla en royalty om 15% av försäljningspriset. Idag finansieras verksamheten i huvudsak genom royalty intäkter från läkemedel. Företaget bedriver även mindre produktion av ett läkemedel som Medytekk själva tagit fram, antibiotikan Amacyklin. Detta är en speciell antibiotika mot så kallad råttpest.

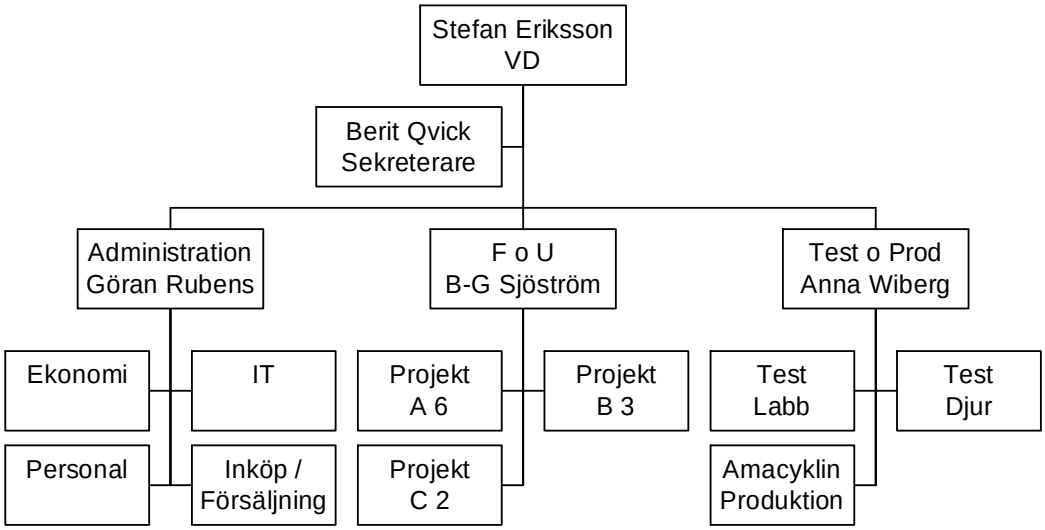
Idag omsätter företaget ca 170 miljoner kronor och har 98 anställda. Sedan hösten 1998 är företaget noterat på Stockholms fondbörs O-lista. De största ägarna är det två grundarna av företaget med vardera 30% av aktierna övriga 40% är fördelade på ett antal investment bolag och läkemedelsföretag.

Appendix 1.1.1 Lokalisering

Medytekk AB ligger i Uppsala närmare bestämt i Boländernas industriområde. Företaget flyttade till de nuvarande lokalerna för sex månader sedan. Flytten var ett resultat av de senaste åren expansion. I Boländernas industriområde

finns bl a en gymnasieskola, ett stort läkemedelsföretag, ett antal bilfirmor, verkstäder av olika karaktär samt det lokala bussbolaget, Uppsala Buss.

Appendix 1.1.2 Organisation



Appendix 1.1.3 Ledning

Ledningen inom Medytekk AB består utav, förutom vd Stefan Eriksson, de tre enhetscheferna. Ledningen genomför varje vecka ett formellt ledningsgruppsmöte och är företagets beslutande organ. Någon stående punkt för säkerhet finns ej med på agendan, inte ännu i alla fall.

Man skulle nästan kunna säga att sekreteraren, Berit Qvick, ingår i ledningsgruppen i och med att hon alltid medverkar vid dessa möten. Berit har varit anställd i företaget sedan det startade. Alla inom företaget vet att är det någon man ska fråga om det är något man undrar över så är det Berit, hon vet allt om alla. Hon har haft det lite svårt en period, i och med skilsmässan, och har varit sjukskriven kortare perioder lite då och då.

Appendix 1.1.4 Administrativa enheten (25 st)

Chefen för den administrativa enheten, Göran Rubens, är 47 år och har ett förflutet inom Uppsala Universitet. Han har arbetet för Medytekk AB i sju månader. I och med att han tidigare arbetet med frågor rörande säkerhet och skydd har han även fått detta som sitt ansvarsområde inom Medytekk AB. Han är således företagets säkerhetschef. Han har ingen formell utbildning inom området men funderar på att gå SAF Grundkurs i säkerhet.

Han har ännu inte hunnit med att aktivt arbeta och förbättra säkerheten inom företaget, han har dock en vilja och intention att ta itu med detta så snart som han hunnit bli varm i kläderna. Han vet att han bör börja med att göra en risk analys på företaget för att identifiera inom vilka områden de allvarligaste riskerna finns och utforma förslag på åtgärder. I och med att företaget hanterar mycket information som är vital funderar Göran på att även engagera IT-chefen Lennart Jakobsson i detta arbete.

Ekonomiavdelningen (6 st)
Ekonomiavdelning arbetar i huvudsak med den löpande redovisningen och fakturering till kunder. Samtliga anställda på avdelningen är kvinnor i åldern 34–57 år. De känner varandra ganska bra tycker de och de kompletterar varandra på ett bra sätt, ingen utav dem har någon tjänst eller uppgift som inte någon av de andra kan klara utav. Det har t o m hänt att de "lånat" ut de personliga lösenorden till varandra för att kunna lösa vissa uppgifter smidigt. Vissa utav dem brukar ersätta Berit Qvick då hon är sjuk eller ledig.

Personalavdelningen (4 st)
Personalavdelningen arbetar förutom med att rekrytera nya personer till företaget även med de externa kontakterna. Bland de externa kontakterna kan olika forskare och universitet runt omkring i världen nämnas. Det är så att Medytekk AB sponsrar olika forskningsprojekt och enskilda forskare, i och med denna sponsring får företaget tillgång till många av de senaste rönen och resultaten inom medicinforskningen. Avdelningen hanterar en mängd olika register rörande anställda, externa kontakter och personer som ingår i viss försöksverksamhet. Man har ännu inte helt anammat Personuppgiftslagen, PUL. Det beror till stor del på att man inte vet riktigt hur man ska tolka lagen, man har dock utsett en person som ska vara registeransvarig.

It-avdelningen (4 st)
IT-avdelningen är enligt IT-chefen, Lennart Jakobsson mycket överbelastad med arbete. Detta beror på att företaget expanderar kraftigt varje år och man inte har en IT-strategi. Lennart har påtalat problemet för VD, Stefan Eriksson men har fått en ganska sval respons. Lennart tillsammans med hans ersättare arbetar som administratörer och svarar för driften av nät och servrar. En annan person är svarar för supporten till de anställda och arbetar även en del som nätverkstekniker. Den sista personen på avdelningen arbetar i huvudsak med applikationer och applikationsutveckling. Själva IT-miljön beskrivs närmare i ett eget kapitel.

Inköp och Försäljningsavdelningen (10 st)
Avdelningen svarar för samtliga inköp av varor tjänster inom företaget, dock förekommer det att vissa utav forskarna kringgår dessa rutiner och anskaffar utrustning på egen hand. Avseende kemikalier och andra substanser som används i verksamheten finns det bara en leverantör i Sverige som kan leverera den kvalitet och kvantitet som erfordras, KEBO.

Avdelningen hanterar även externa kunder, det finns bland annat två stycken säljare som på heltid bearbetar befintliga och presumtiva kunder. Dessa två har ca 180 resdagar per år. Stor del av deras tid åtgår till besöka olika mässor runt om i världen och "smörja" kunder.

Appendix 1.1.5 Enheten för Forskning och Utveckling (FoU 34 st)

Enhetens storlek varierar beroende på antalet projekt som bedrivs. Vanligtvis pågår 3–5 olika projekt. Vissa av forskarna är projektanställda, detta gäller företrädesvis för de utländska forskarna.

Projekt A 6 (12 st)
Projekt A 6 är arbetsnamnet på det projekt som arbetar med att ta fram en ny smärtstillande substans. I forskarlaget ingår 12 personer, däribland två stycken forskare från universitetet i Austin, Texas. Dessa har en projektanställning som sträcker sig fram till och med nyårsskiftet.

Projekt B 3 (10 st)
Projekt B 3 arbetar med att utveckla en ny substans som kan ingå i en ny magsårsmedicin. I forskarlaget ingår 10 personer, utav dessa tio ingår en gästforskare från Folkets Hälsoministerium i Peking, Kina.

Projekt C 2 (11 st)
Projekt C 3 arbetar med att utveckla en substans som kan komma att ingå in ny typ av kombinationsvaccin mot flera av de vanligaste barnsjukdomarna såsom Röda hund, Vattkoppor, Mässling och Scharlakansfeber. I forskarlaget ingår 11 personer, samtliga är anställda inom Medytekk AB.

Appendix 1.1.6 Test och Produktion (34 st)

Testenheten arbetar med att genomföra olika typer av tester på de preparat och substanser som företaget utvecklat. Testerna genomförs i två olika miljöer. I den första miljön, laboratoriemiljön genomförs tester hur substanserna reagerar med andra etablerade mediciner och oönskade effekter dokumenteras. Testenheterna arbetar nära med de olika projekten för att återkoppla testresultaten till forskarlagen.

Då resultaten av substanserna är av sådan karaktär, samtliga oönskade effekter som går att identifiera i en laboratoriemiljö, genomförs tester på olika djur. Vanligtvis används möss, råttor och apor, i vissa fall utnyttjas även grisar då deras organ överensstämmer med människans storleksmässigt. Chefen för enheten, Anna Wiberg, har blivit utsatt för vissa hot, antagligen från olika djurrättsaktivister, hon har dock aldrig tagit dessa på allvar eller polisanmält dessa. Hon har dock tagit upp det inträffade på ett ledningsgruppmöte.

Den produktion som förekommer inom Medytekk AB är framställandet av antibiotikan Amacyklin, en speciell antibiotika mot Råttpest. Produktionen startades på uppdrag av svenska FOA (Försvarets forskningsanstalt) i samband med att flera fall av Råttpest rapporterades från de svenska FN-styrkorna i det forna Jugoslavien. Framställandet av antibiotikan är mycket känslig mot störningar i form av temperatur växlingar och feldosering av de olika ingående substanserna. Processen, från blandning av olika substanser till färdiga kapslar tar tre veckor. Produktionen sker löpande över hela året.

Pretest Labb (13 st)
De 13 laboratorietekniker och assistenter som arbetar på avdelningen är väl medvetna om de risker som är förenade med denna verksamhet. I många tester används olika typer av bakterier, vissa utav dem är mycket smittsamma. Verksamheten ställer höga krav på hur riskavfallet hanteras, allt avfall förvaras i frigolitfodrade papptunnor vilka märks med riskavfall. Avfallet hämtas på plats varannan vecka av Sellbergs.

Pretest Djur (8 st)
Det är denna avdelning som allmänheten knappt känner till, medvetet försöker man begränsa informationen kring denna avdelning då djurförsök i mångas ögon betraktas som kontroversiellt. Under en period genomfördes flera demonstrationer mot plågsamma djurförsök, speciellt efter en artikelserie i Uppsala Nya Tidning.

Amacyklin Produktion (12 st)
Detta är produktionsavdelningen inom Medytekk AB som producerar antibiotikan Amacyklin, en speciell antibiotika mot Råttpest. Produktionen startades på uppdrag av svenska FOA (Försvarets forskningsanstalt) i samband med att flera fall av Råttpest rapporterades från de svenska FN-styrkorna i det forna Jugoslavien.

Antibiotikan är helt utvecklad av Medytekk som har ett patent på Amacyklin som sträcker sig ytterligare 4 år. Inom företaget är man övertygad om att kunna sälja antibiotikan till andra intressenter än som nu är fallet enbart till FOA och Försvaret. Råttpest finns i många krigsområden och inom ledningen funderar man på att ta kontakt med FN och UNHCR, det borde även finnas ett intresse från andra håll.

Appendix 1.2 Utdrag ur årsredovisningen

Appendix 1.2.1 Resultaträkning i sammandrag (Tkr)

	2004	2005
Nettoomsättning	172 432	125 898
Kostnad för sålda varor	-62 163	-58 587
Bruttovinst	**110 269**	**67 311**
Försäljningskostnader	-18 406	-16 671
Adm. Kostnader	-12 918	-11 267
Forskning & Utvecklingskostnader	-39 242	-25 452
Valutakurs vinster	4 566	5 838
Valutakurs förluster	-6 352	-5 184
Rörelseresultat	**37 917**	**14 575**
Räntenetto	2 837	1 244
Resultat före skatt	**40 754**	**15 819**
Skatter	-6 729	-1 875
Redovisande resultat	**34 0251**	**13 944**

Appendix 1.2.2 Balansräkning i sammandrag (Tkr)

	2004	2005
Anläggningstillgångar	97 175	56 285
Övriga omsättningstillgångar	12 562	15 283
Varulager	4 275	5 830
Kundfordringar	51 067	38 718
Likvida medel	63 816	71 284
Summa tillgångar	**222 895**	**187 400**
Eget kapital	86 390	78 527
Minoritetsandel	5 752	7 392
Räntebärande skulder	74 297	78 293
Rörelseskulder	56 456	23 188
Summa skulder och eget kapital	**222 895**	**187 400**

Appendix 1.3 Säkerhetsskyddet inom Medytekk AB

För något år sedan hade Medytekk AB en student som gjorde ett examensarbete på företaget, examensarbetet handlade om säkerheten vid företaget. Som en del av arbetet ingick en kategorisering av företagets säkerhetsskydd. Han valde att dela in säkerheten i sju stycken områden.

1 Den stora skillnaden i resultat mellan 2004 och 2005 beror till största del på försäljning av Amacyklin som startade 2005.

Appendix 1.3.1 Fysiskt skydd

De flesta fysiska skyddsåtgärderna har vidtagits allteftersom de har aktualiserats. Någon medveten planering har inte förekommit inom Medytekk AB. Det som företaget benämner som stöldbegärlig egendom är i första hand datorerna.

Appendix 1.3.2 Områdesskydd

Delar av företaget är inhägnat med ett 230 cm högt Gunnebostängsel. Grindarna står öppna under dagarna (06.00–18.00), det är ett lokalt vaktbolag som svarar för öppning och stängning. Det finns en gånggrind som alltid är låst, den utnyttjas enbart under sena kvällar och helger. Samtliga anställda har nyckel till gånggrinden. Vaktbolaget som svarar för öppning och stängning genomför ingen rondering nattetid. På området finns viss belysning. Det är innanför staketet som de anställda kan parkera sina bilar, direkt utanför huvudbyggnaden finns tre gästparkeringar.

Appendix 1.3.3 Skalskydd

Det mekaniska skalskyddet i samtliga omslutningsytor är utformade för att svara mot försäkringsbolagets krav enligt Skyddsklass 2. Skalskyddet är kompletterat med en inbrottslarmanläggning, samtliga fönster och dörrar är försedda med magnetkontakter och fönstren även med glaskross detektorer. Testavdelningen har försett sina fönster med insynsskydd, detta insynsskydd ger dock inte någon reell förstärkning av glasytorna.

Appendix 1.3.4 Tillträdesskydd

Tillträdesskyddet består av ett nyckelsystem med fyra olika nivåer.

- **Nivå 1** ger tillträde till samtliga utrymmen utom IT-avdelningens lokaler och testavdelningen.
- **Nivå 2** ger tillträde samtliga utrymmen förutom testavdelningen, denna typ av nyckel innehas av personalen på IT-avdelningen och C Adm.
- **Nivå 3** ger tillträde till samtliga utrymmen förutom IT-avdelningens lokaler, denna typ av nyckel innehas av samtliga på Testavdelningen.
- **Nivå 4** kan likställas med en huvudnyckel, vilken ger tillträde till samtliga lokaler. Denna typ av nyckel innehas av Vd och C FoU, det finns dock en reservnyckel som sekreteraren Berit har förvarad i sitt kassaskrin.

Det är Berit Qvick som svarar för nyckelhanteringen inom Medytekk. I samband med att en anställd skriver på anställningsavtalet kvitteras även nycklarna.

Appendix 1.3.5 Punktskydd

Företaget har ett arkiv där alla viktigare handlingar förvaras, detta arkiv är utrustat med ett kodlås. Det är fyra personer på den administrativa avdelningen som delgivits koden till detta utrymme. Dörren är larmad och ingår i den befintliga inbrottslarmanläggningen.

På IT-avdelningen finns ett säkerhetsskåp som nyttjas till att förvara ”backup-media”. Det är tre personer som har nyckel till detta skåp, C IT-avdelningen och två stycken systemadministratörer.

Appendix 1.3.6 Incidenter och skador inom området

Vid ett flertal tillfällen har företaget drabbats av skadegörelse i form av klotter på husfasaderna, B-G Sjöström, C FoU, förmodar att det är skolungdomar från det närbelägna gymnasiet. Det var en period som det förekom mindre demonstrationer i området, det var föreningen mot plågsamma djurförsök. Dessa demonstrationer var inte enbart riktade mot Medytekk AB, även de andra läkemedelsföretagen drabbades.

Under de senaste åren har företaget drabbats tre inbrott, det senaste ägde rum i våras. Vid samtliga tillfällen har datorer och annan kontorsutrustning stulits, vid ett tillfälle stals handkassan på inköpsavdelningen.

Enligt vd, Stefan Eriksson, har ingen form av industrispionage förekommit, ingen som upptäckts i alla fall. Vid ett par tillfällen har det funnits misstanke om spionage eller att någon inom företaget läckt information till en konkurrent. I och med att varken han eller B-G Sjöström visste hur de skulle ta sig an problemet lät man det bero. Hans uppfattning är dock att hotet om industrispionage är något som man måste ta på fullaste allvar, men han har ingen bra lösning eller förslag på hur man ska skydda sig emot det.

Appendix 1.3.7 Brandskydd

Ingen formell utbildning av de anställda avseende hantering av brandsläckare eller kunskap om brands uppkomst och spridning förekommer inom Medytekk AB. Inom avdelningen för FoU nyttjas brännare och andra värmekällor för att skapa kemiska föreningar, i första hand utnyttjas Gasol och Acetylen som bränngas.

Appendix 1.3.8 Detektering

En brandlarmanläggning finns installerad i de utrymmen som FoU och Testavdelning finns lokaliserade i. Inom företaget vet man att anläggningen fungerar, larm har gått vid några tillfällen.

Appendix 1.3.9 Släckutrustning

Handbrandsläckare finns utplacerade i lokalerna och i erforderligt antal, dessa inspekteras och servas regelbundet. Samtliga släckare är skumsläckare.

Appendix 1.3.10 Incidenter och skador inom området

I samband med den senaste julledigheten skedde en incident, det var de bortglömda levande ljusen som orsakade en mindre brand i fika rummet. På morgonen hade det serverats glögg och pepparkakor, efter det att alla hade fikat färdigt glömde man att släcka ljusen. Från mossan i ljusstaken spred sig elden till träljusstaken och vidare till vaxduken, som tur var kom sekreteraren Berit tillbaka för lite påfyllning och upptäckte vad som höll på att hända. Hon lyckades att släcka elden genom att kasta en kastrull med vatten på elden. Som tack för sin insats fick hon de oöppnade flaskorna med glögg. Skadorna blev mycket ringa, en förstörd ljusstake, en vaxduk och brännmärken på köksbordet.

En annan incident inträffade på FoU avdelningen för tre år sedan. Den inträffade sent en tisdag kväll då ingen var kvar på företaget. Enligt utredningen visade det vara ett överslag i en elektrisk värmeplatta. Räddningstjänsten var på plats redan efter 8 minuter, Uppsalas största brandstation Victoria ligger inte mer är 2 km från Medytekk AB. Skadorna på utrustning och lokaler vart inte speciellt allvarliga, dock tog det tre veckor innan verksamheten kom igång på allvar på grund av det omfattande saneringsarbetet.

Appendix 1.4 Personalsäkerhet

Detta är ett område som Medytekk AB inte aktivt arbetat med. Det finns skyddsombud på företaget och arbetsmiljön bedöms av samtliga anställda som relativt bra. Något behov av personskydd har inte förelegat under den tid som företaget varit verksamt.

Appendix 1.4.1 Nyckelpersonal

På frågan om nyckelpersonal svarade vd Stefan Eriksson att det självklart fanns nyckelpersoner inom företaget men på din fråga om han kunde namnge dem blev svaret en aning svävande "det beror naturligtvis på vad man väger in i begreppet nyckelperson". Efter det att du förklarat för honom kriterierna för en nyckelperson och en stunds diskuterande förklarade han att de flesta personerna på företaget borde betraktas som nyckelpersoner med motiveringen att samtliga anställda har en unik kunskap och är mer eller mindre svåra att ersätta. Detta var tydligen något han inte tidigare hade tänkt på.

Appendix 1.4.2 Incidenter och skador inom området

För två år sedan var man tvungen att lägga ner ett påbörjat projekt på grund av att man förlorade två stycken forskare till en konkurrent. Man han inte med att avsluta projektet innan uppsägningstiden gick ut, ledningen inom Medytekk försökte t o m att hyra dessa forskare från deras nya arbetsgivare vilket inte var möjligt. Genom förlusten av dessa två forskare var man tvungen att lägga ner projektet.

Appendix 1.5 Informationssäkerhet

Ingen av personalen på IT-avdelningen har någon speciell säkerhetsutbildning, vilket har medfört att detta inte är ett prioriterat område. De anställda anser att det viktigaste är att allt fungerar så smidigt som möjligt. Alla är tekniskt kunniga och försöker hitta så smarta lösningar som möjligt, detta har medfört att dokumentationen avseende IT-miljön inte uppdateras regelbundet. Det finns vissa regler som samtliga följer, men de är inte formellt dokumenterade. IT-chefen Lennart Jakobsson skulle vilja upprätta en it-strategi, men det finns ingen tid för detta.

Appendix 1.5.1 Administrativ säkerhet

Avseende lagring och arkivering av dokumentation finns det fastställda regler och rutiner. Det finns en person som är ansvarig för arkivet och diarieför allt som ska arkiveras. Samma person har utsätts som registeransvarig på företaget. Något formellt klassificeringssystem har inte upprättats.

C Adm har funderat på att upprätta en säkerhetshandbok i och med att antalet anställda har ökat kraftigt de senaste två åren. I samband med introduktionen av nyanställda tecknas ett sekretessbevis och man går kort igenom vissa regler som gäller på företaget.

Appendix 1.5.2 IT-säkerhet

Samtliga PC är utrustade med antivirus program, uppdatering av programvaran sker genom att användarna själva laddar hem virusuppdateringar, genom funktionen "live update", från programvarutillverkarens hemsida.

Back-up tas varje natt, kopian som tas natten mellan torsdag och fredag blir veckokopia. Den sista veckokopian i månaden blir månadskopia och den sista månadskopian blir således årskopia. Det genomförs inga regelbundna tester huruvida det går att återskapa informationen eller ej, det finns ej heller några regler för hur många gången banden kan återanvändas. Kopiorna förvaras i ett låst säkerhetsskåp som står i it-avdelningens lokaler.

Varje användare har ett unikt användar-id och lösenord. Lösenordet måste minst vara fem tecken för att godkännas av systemet. Användar-id och lösenord krävs för åtkomst till det lokala nätverket. Personalen på Ekonomiavdelningen har ytterligare ett lösenord att hålla reda på för åtkomst till företagets ekonomi och redovisningssystem, det är samma parametrar som gäller för åtkomst.

Det finns en modempool på företaget som forskarna och säljarna utnyttjar. För åtkomst till nätverket avkrävs användarna användar-id och lösenord, dessa är desamma som vid ordinarie på-loggning. Uppkopplingen sker över publikt nät, någon form av kryptering används inte.

Appendix 1.5.3 Incidenter och skador

Man har haft problem med virus vid ett antal tillfällen, trots att man har ett anti-virus program. Vid det senaste tillfället var det ett virus som spreds via e-post, vid det tillfället var man tvungen att ta hjälp av en extern konsult för att få bukt med viruset. Han meddelade att den stora spridningen berodde till stor del på bristande uppdatering av programvaran.

Vid ett antal tillfällen har servrarna gått ner, omstart brukar inte vara något större problem i och med att man har ”backup”. Det var dock vid ett tillfälle som man skulle återskapa information från ”backup media” och det visade sig att informationen var ofullständig, detta berodde på att ”backup” körningen hade avbrutits under natten och den ansvariga teknikern hade inte kört en ny på morgonen och det var på den tiden som man körde ”backup” en gång i veckan. Många forskare blev ursinniga och menade att en veckas arbete gått förlorat.

Appendix 1.6 Drift- och produktionssäkerhet

Detta område var något som företaget inte hade funderat på förrän studenten redovisade sitt examensarbete.

Appendix 1.6.1 Avbrottsplanering

Någon avbrottsplanering har inte upprättats detta beror till stor del på att man inte gjort eller låtit göra en riskanalys på företaget och dess verksamhet. Vd, Stefan Eriksson, menar att det som kan få verksamheten att avstanna helt är avbrott i IT-miljön eller ett längre kraftbortfall. Något som kan orsaka avbrott för vissa delar av verksamheten är om någon forskare väljer att sluta innan ett projekt är avslutat eller någon nyckelperson råkar ut för en olycka eller blir långtidssjukskriven.

Appendix 1.6.2 El-säkerhet

Det finns ingen dubbel matning av kraft till företaget, ej heller någon form av reservkraft. Den enda utrustning som har någon form av skydd är servrarna som har utrustats med UPS (Uninteruptable Power Supply).

Appendix 1.6.3 Försäkringsskydd

Medytekk AB har inte haft någon utarbetad plan för vilka försäkringar som krävs eller behövs, för fyra år sedan anlitades en försäkringsmäklare som granskade företaget och dess verksamhet. Det var dennes bedömning av företaget som har legat till grund för utformningen av försäkringsskyddet. Ledningen inom Medytekk AB har inte haft någon anledning till att byta försäkringsgivare eller omförhandla sina villkor.

Appendix 1.6.4 Katastrofplanering

Någon katastrofplaneringen har aldrig upprättats, varför detta inte gjorts har vd Stefan Eriksson inget bra svar på "det har väl aldrig känts riktigt aktuellt". Inte ens då stora delar av torvlagret i Uppsala industriområde brann upp, vilket resulterade i rökskador hos flera olika företag i området.

Appendix 1.7 Beskrivning av byggnader och lokaler

I detta kapitel beskrivs företagets olika byggnader och vissa lokaler som kan vara av särskilt intresse.

Appendix 1.7.1 Huvudbyggnad

I huvudbyggnaden finns hela den administrativa enheten samlad, förutom kontorsutrymmen, konferensrum, datarum och arkiv finns även en mindre cafeteria/matsal.

Huvudbyggnaden är en tegelbyggnad i två våningar. Byggnaden är uppförd i slutet på 60-talet. Det mekaniska inbrottsskyddet uppfyller kraven enligt skyddsklass 2, dessutom är detta kompletterat med en inbrottsanläggning. Någon form av försåtskydd (ir-detektorer eller motsvarande) finns inte installerat. Vissa av mellan väggarna är av betongkonstruktion vilket ger ett gott skydd för brandspridning dock gäller detta inte för de dörrar som finns monterade. Dessutom är inte rörgenomföringar tätade.

Appendix 1.7.2 Datarum

Datarummet är beläget på andra våningen i anslutning till IT-avdelningens rum. Rummet är försedd med en mindre klimatanläggning den reglerar dock inte den relativa luftfuktigheten. För att reducera värmen har man monterat spegelfilm på fönstret. Någon form av driftlarm finns inte installerat i datarummet. En del av utrustningen är placerad direkt på golvet och en del är placerad i ett rack. Rummet saknar ett upphöjt datagolv, det finns vatten ledningar ovan innertaket. Genom avsaknaden av brandlarm har en brandvarnare satts upp. Utanför själva datarummet finns en brandsläckare av AB-typ.

För tillträde till IT-avdelningens lokaler krävs en nyckel av kategori Nivå 2 vilken innehas av samtliga på IT-avdelningen och C Adm. eller Nivå 4 vilken innehas av VD och C FoU. I praktiken är det alltså sju personer som har tillträde till dessa utrymmen förutom reservnyckeln som finns hos sekreteraren. Datarummet fungerar även som uppställningsplats för diverse utrangerad IT-utrustning.

Appendix 1.7.3 Arkiv

Det finns ett mindre arkiv på bottenvåningen där alla viktigare handlingar förvaras. Arkivet är utrustat med ett kodlås. Det är fyra personer på den administrativa avdelningen som delgivits koden till detta utrymme. Dörren är larmad och ingår i den befintliga inbrottslarmanläggningen. Rummet saknar brandlarmsanläggning och även i detta utrymme finns vattenledningar ovan innertak.

Appendix 1.8 Forskning och Utveckling

Enheten för FoU finns lokaliserade i byggnad som är sammanbyggd med huvudbyggnaden. Själva byggnaden är i ett plan. Samtliga mellanväggar är av gips konstruktion. Byggnaden inrymmer 6 större arbetsutrymmen vilka utnyttjas av de olika projekt som bedrivs samt 2 mindre kontor. I varje arbetsutrymme finns ett antal datorer och annan exklusiv testutrustning.

I och med renoveringen av byggnaden installerades ett brandlarm, detta var för övrigt ett krav från försäkringsbolaget. Handbrandsläckare finns i varje större arbetsutrymme. Samtliga anställda har tillträde till FoU lokaler. Det mekaniska inbrottsskyddet uppfyller kraven enligt skyddsklass 2, dessutom är detta kompletterat med en inbrottsanläggning. Någon form av försåtskydd (ir-detektorer eller motsvarande) finns inte installerat.

Appendix 1.9 Test och Produktion

Byggnaden där de bägge testavdelningarna och produktionsenheten finns är en fristående plåtbyggnad vilken har byggts av Medytekk AB. Samtliga mellanväggar är av gips konstruktion. Byggnaden innehåller förutom produktionsenheten två olika laboratorium varav ett används för djurförsök. Förutom dessa lokaler finns en mindre djuravdelning och ett fåtal kontor.

Det mekaniska inbrottsskyddet uppfyller kraven enligt skyddsklass 2, dessutom är detta kompletterat med en inbrottsanläggning. Någon form av försåtskydd (ir-detektorer eller motsvarande) finns inte installerat. En brandlarmsanläggning finns installerad i denna byggnad.

Det är endast innehavare av Nivå 3- och Nivå 4-nycklar som har tillträde till dessa lokaler, med andra ord samtliga anställda på testenheten samt vd och C FoU.

Appendix 1.10 Områdesbeskrivning

Företaget ligger i ett industriområde som heter Boländernas industriområde. Granne med huvudbyggnaden ligger ett företag som säljer bilder, posters och affischer, Pappum Nova. Granne med FoU ligger en ortopedisk klinik. I företagets närområde ligger ett antal bilfirmor och bilverkstäder, förutom detta finns ett antal mekaniska verkstäder samt flera företag inom samma bransch. I området finns även en gymnasieskola.

Området är lugnt under kvällar och helger. Det förekommer dock viss aktivitet m h t att det är flera företag som har produktion dygnet runt.

På bilden bredvid syns infarten till Pappum Nova, företaget som ligger granne med huvudbyggnaden.

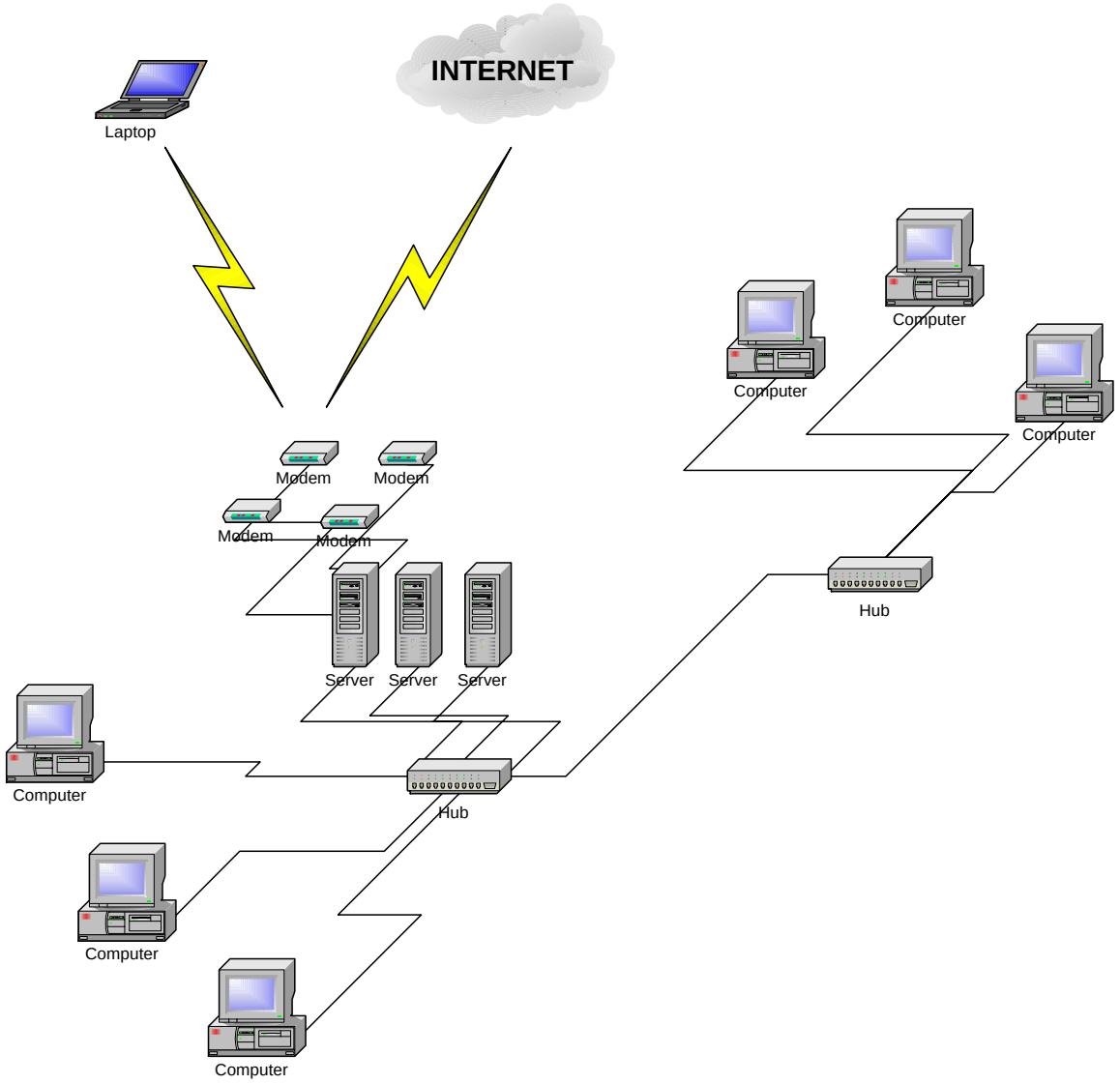
För att komma till Test & Produktionsenheten måste man åka genom den gemensamma grinden, alt gå igenom H-byggnaden för att komma ut på baksidan.

Innanför grindarna har personal både från Medytekk och Pappum Nova parkeringsplatser. Grindarna låses genom ett lokalt vaktbolag. Samtliga anställda på Medytekk har nyckel till gånggrinden med skylten. Det även genom denna grind som alla godstransporter till och från Medytekk går. En skiss över området finns som bilaga 1.

Appendix 1.11 Beskrivning av IT-miljön

Samtliga hårdvaror är av kända fabrikat såsom HP (servrar och desk top's), Dell (Lap top's), Novell (nätverkskomponenter) och Zyxxel (Modem). Utrustningen är i de flesta fall inte äldre än två år. Som operativsystem (OS) på servrarna används Windows NT 4 och på klienterna används Windows 2000. Basprogram är Office-paketet (inklusive MS Access och Internet Explorer) samt Norton AntiVirus. Förutom dessa standardprogram används olika programvaror för analys- och provningsverksamheten inom företaget. En del av dessa är egenutvecklade. Totalt finns det 98 användare inom företaget.

Appendix 1.11.1 Nätverksskiss



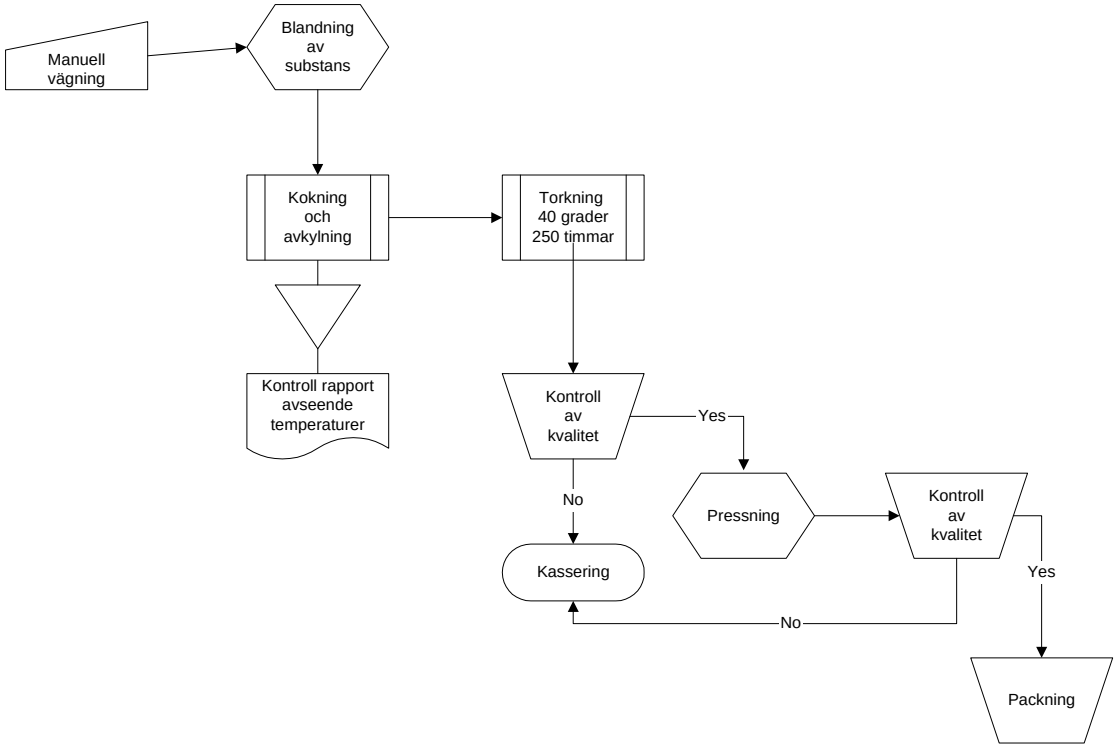
Appendix 1.12 Beskrivning av produktionen

Vägning av de substanser och ämnen som ska ingå i antibiotikan sker manuellt med hjälp av en elektronisk våg, därefter mals och blandas substansen. I kokning och avkylningsprocessen hettas blandningen upp och avkyls fyra gånger under kontrollerade förhållanden. Efter den sista upphettningen och nedkylningen tas en rapport ut för att kontrollera temperaturförhållandena under de tider produktionen varit obemannad. Efter den sista avkylningen ska substansen torkas i 250 timmar. Torkningen kan endast ske i en temperatur mellan 38 och 42 grader för att samtliga ämnen ska bibehålla sina specifika egenskaper. Efter det att torkningen avslutats kontrolleras kvaliteten på den färdiga substansen, för att sedan pressas in i gelékapslar. Efter ytterligare kvalitetskontroll förpackas det färdiga Amacyklinet. Skulle någon avvikelse ske i processen, till exempel fel blandning, temperatur avvikelser vid kokning eller nedkylning eller om torkning sker i utanför ovan avgivna gränsvärden måste hela satsen kasseras då antibiotikan inte får de

egenskaper som den ska ha. Skulle detta ske måste en ny sats tillverkas. Hela processen att framställa en sats Amacyklin tar tre arbetsveckor.

Appendix 1.12.1 Produktionsprocessen

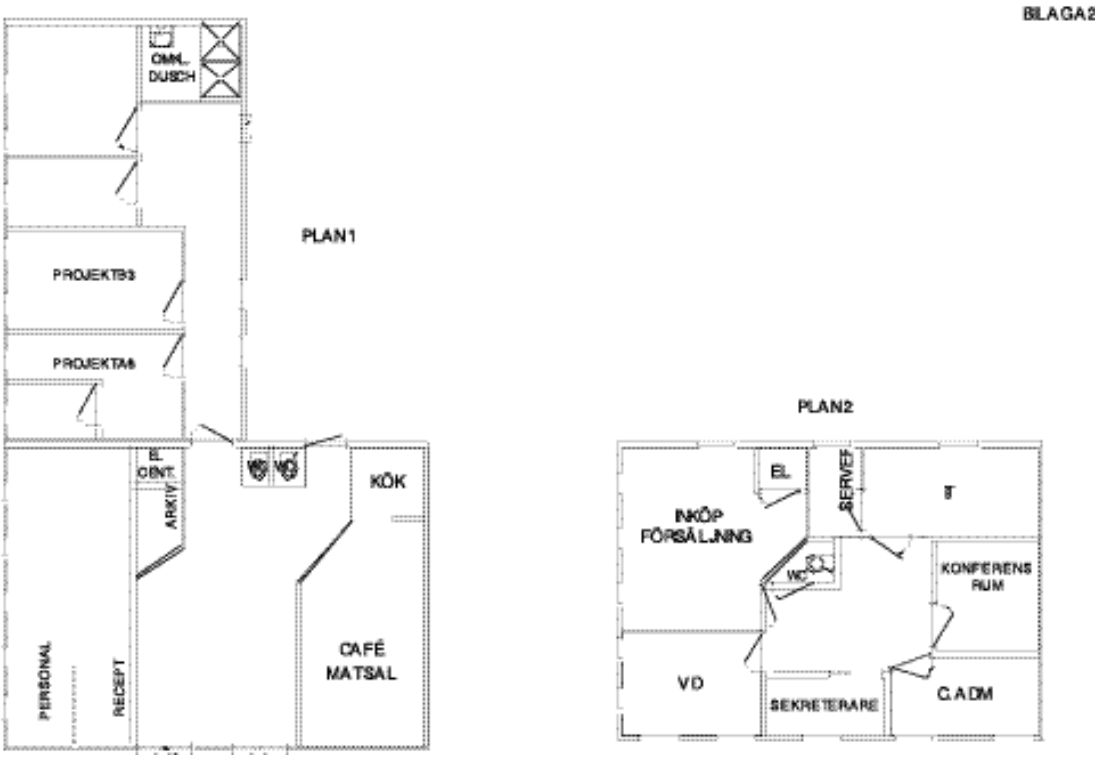
Det är de fyra första stegen som är kritiska för framställandet av Amacyklin av erforderlig kvalitet. Den utrustning som används i processen är mycket exklusiv, speciellt den elektroniska våg och mätutrustning som används för vägning av substanser och själva kokutrustningen är också exklusiv och är special beställd från Phoenix Labs i USA. Det finns manuella rutiner som är helt avgörande för framställandet av Amacyklin. Vägningen är en, men korrekt avläsning av loggar efter kokning och torkning är den enda kontroll funktion som säkerställer leverans av antibiotika av bestämd kvalitet.



Appendix 1.12.2 Situationsskisser

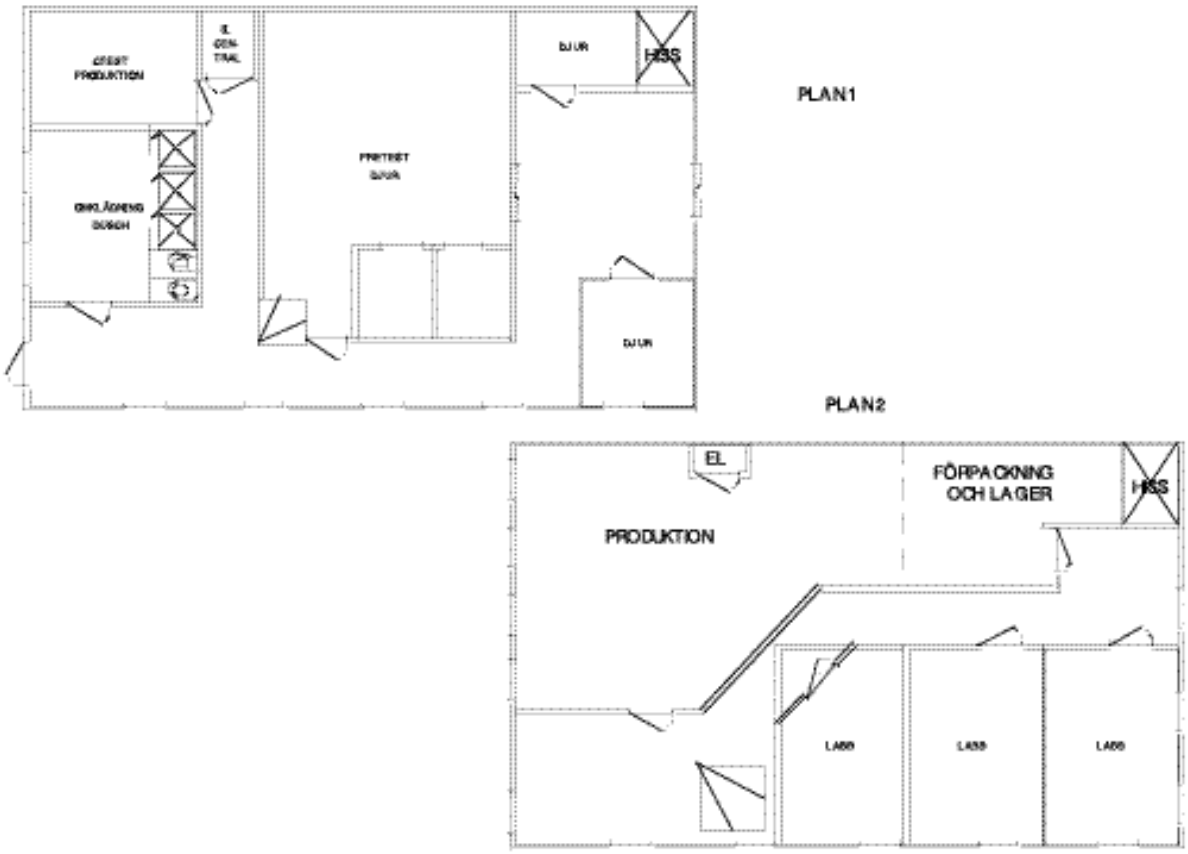
Exteriör

Plan 1 och 2 i huvud- och FoU-byggnad



Plan 1 och 2 test- och produktionsbyggnad

BILAGA 3



Appendix 2 – Lagrum, efterlevnad av rättsliga krav

Inledning

Det övergripande målet för efterlevnad av rättsliga krav i standarden framgår av **kapitel 15.1**, vari anges att målet är att undvika handlande i strid mot lagar och andra författningar, avtal och eventuella andra yttre säkerhetskrav. Övergripande medel för måluppfyllelse kan delas in i tre huvudgrupper, nämligen

- identifiering av organisationens rättsliga förpliktelser;
- säkerställande av efterlevnad inom organisationen; och
- agerande mot överträdelser.

Vad gäller identifiering av organisationens rättsliga förpliktelser kan dessa finnas dels i lagar och andra lägre stående författningar, såsom föreskrifter utfärdade av förvaltningsmyndighet, dels i avtal och andra typer av ”frivilliga” förbindelser. Det är självklart att dessa förpliktelser kan variera kraftigt mellan olika organisationer, och varje organisation måste själv hålla sig informerad om vilka regler som gäller. Kunskap om vilka rättsliga förpliktelser som gäller inhämtas säkrast genom en jurist, antingen organisationens egen eller en externt anlitad. Information kan även erhållas genom kontakt med branschförening, tillsynsmyndighet eller dylikt.

Säkerställande av efterlevnad rymmer avsevärt mer än enbart juridiska medel, men dessa kan i kombination med andra åtgärder av exempelvis teknisk natur bidra till efterlevnaden inom organisationen. Några av de viktigaste med juridisk anknytning är följande.

- utformning av säkerhetspolicy, innefattande bl.a. behörighets- och sekretessregler,
- fortlöpande information om gällande/nya/ändrade rättsregler och/eller avtalsförpliktelser,
- begränsning av informationsåtkomst, innefattande klassificering av information.

Agerandet mot överträdelser måste givetvis avpassas efter bland annat överträdelsens art och omfattning. Det är dock viktigt att åtgärder vidtas konsekvent och i enlighet med de riktlinjer organisationen ställt upp. Exempel på åtgärder är

- interna ”påföljder”, exempelvis varning, löneavdrag, avstängning från viss behörighet,
- uppsägning/avsked,
- skadestånd, och
- polisanmälan.

Interna påföljder bör alltid ske tillsammans med information om hur den anställde ska agera för att inte bryta mot de regler som gäller och åtföljas av en uppföljning av den anställdes fortsatta agerande. Riktlinjer för interna påföljder bör utarbetas tillsammans med den lokala fackliga organisationen.

Appendix 2.1 Exempel

Nedan följer några händelsebeskrivningar som ska tjäna som exempel och tankeväckare i säkerhetsarbetet. Exemplen tar sin utgångspunkt i Medytekk.

Appendix 2.1.1 Personuppgifter

På säljavdelningen har man under år 2004 upprättat ett dataregister över kontaktpersoner hos kunder som kan vara viktiga att bearbeta vid försäljning. Registret innehåller förutom uppgift om namn, direkttelefonnummer och e-postadress och dylikt även en ”profil” avseende respektive kontaktperson, innefattande uppgift om bland annat hur kontaktpersonen tidigare bemött Medytekks säljåtgärder och dennes fritidsintressen.

Eftersom registret innehåller personuppgifter aktualiseras tillämpning av personuppgiftslagen (PUL) på den behandling av personuppgifter som sker genom registret. Det innebär för det första att Medytekk bör utse ett personuppgiftsombud, som ska anmälas till Datainspektionen (DI), eftersom Medytekk annars måste anmäla registerbehandlingen till DI. Personuppgiftsombudet ska bland annat föra en förteckning över de behandlingar av personuppgifter som sker, varav bland annat ska framgå ändamålet med behandlingarna.

Utgångspunkten är att samtycke erfordras för att personuppgifter ska få behandlas, såvida inte registerbehandlingen omfattas av ett undantag från plikten på samtycke. Om Medytekk enbart hade registrerat namn, telefonnummer och e-postadress hade Medytekk sannolikt kunnat undgå kravet på samtycke genom att hävda att sådan behandling är nödvändig i kundförhållandet. När det gäller ”profiluppgifter” måste dock samtycke inhämtas från kontaktpersonerna. Ur bevishänseende är det lämpligt att samtycke inhämtas skriftligen, eller i vart fall dokumenteras genom e-mail.

De personuppgifter som behandlas måste hanteras på ett säkert sätt. I PUL 31 § ställs krav på att den personuppgiftsansvarige skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas.

Ett annat scenario som kan nämnas rör behandlingen av personuppgifter hos myndigheter. Allmänna handlingar innehåller inte sällan personuppgifter. I det fall någon begär att en myndighet skall lämna ut

personuppgifter men myndigheten misstänker att uppgifterna, om de lämnas ut, kommer att behandlas i strid med PUL så gäller sekretess för dessa uppgifter enligt sekretesslagen 7 kap 16 §.

Vad säger standarden?

- Standarden förutsätter att reglerna i PUL följs och anger i **kapitel 15.1.4** bland annat personuppgiftsombud bör utses.

Appendix 2.1.2 Missbruk av e-post

Ett e-brev avsett för en av de anställda på personalavdelningen – en man i 45-årsåldern – hamnar av misstag hos vd. Det visar sig komma från ”Svenska Folkviljan” (SFV), en organisation på den extrema högerkanten. När vd med hjälp av it-chefen kontrollerar den anställdes e-post uppdagas att mannen är medlem i SFV och att han haft en livlig korrespondens med andra medlemmar i såväl SFV som andra likasinnade organisationer.

För Medytekk är det givetvis väsentligt att inte på något sätt bli förknippat med sådana politiska organisationer och om så inte skett tidigare bör Medytekk snarast utfärda riktlinjer för de anställdas e-post- och Internetanvändning. Medytekk bör vidare kunna överväga uppsägning av den anställde (jfr AD: s dom nr 49/1999, där AD ansåg att saklig grund för uppsägning av en anställd vid PRO i Halland förelåg efter missbruk av organisationens e-post. Förhållandena var dock lite speciella i målet).

Händelsen aktualiserar även frågan om övervakning av personalens e-post- och Internetanvändning. Lagstiftning saknas (en utredning benämnd ”Personlig integritet i arbetslivet” utredningsdirektiv 2006:5 är nyligen tillsatt), men utgångspunkten är att arbetsgivaren har rätt att utfärda riktlinjer om e-post- och Internetanvändningen på företaget och att övervaka att dessa riktlinjer följs av de anställda. Om övervakning ska ske bör detta uttryckligen anges i riktlinjerna och det är av stor vikt att man säkerställer att de anställda är informerade om riktlinjerna, exempelvis genom att skriva på någon form av avtal/kontrakt. Finns inga riktlinjer bör arbetsgivaren vara mycket försiktig när det gäller att skaffa sig tillgång till information på de anställdas datorer, särskilt sådan information som betecknas som ”privat”, ”eget” eller liknande.

Om övervakningen sker genom att arbetsgivaren upprättar ett register över de anställdas e-post blir sannolikt personuppgiftslagen (PUL) tillämplig på registret, varför dess regler måste beaktas. Sker motsvarande övervakning hos en myndighet uppfyller registret troligen även kraven på att vara en allmän handling vilket innebär att om inte någon sekretessbestämmelse är tillämplig så skall registret vid förfrågan lämnas ut.

Vad säger standarden?

- I **kapitel 15.1.5** anges i relativt allmänna ordalag att all användning av informationsbehandlingsresurser för obehöriga ändamål bör ses som en orättmätig användning av resurserna, men att möjligheterna att lagligt övervaka användningen varierar mellan olika länder. Standarden förutsätter att företaget utfärdar riktlinjer för användningen av alla informationsbehandlingsresurser – däribland e-post och Internet – att användningen övervakas i möjlig och laglig utsträckning och att överträdelser åtgärdas på lämpligt sätt.

Appendix 2.1.3 Olaglig kopiering från Internet

I samband med undersökningen av en anställds e-post görs även en undersökning av vilka programvaror som används av de anställda på Medytekk. Det uppdagas då att ett flertal anställda använder programvaror för vilka licens inte tecknats. I flera har dessa programvaror hämtats hem från Internet.

Att utan tillstånd – licens – från upphovsrättsinnehavaren kopiera ett datorprogram är brottsligt och skadeståndsgrundande enligt upphovsrättslagen (53 och 54 § § URL). Medytekk bör snarast tillse att all personal informeras om dessa rättsregler och utfärda riktlinjer för inköp och användning av datorprogram samt för kontroll av att reglerna efterlevs. Ett register över gällande licenser bör upprättas och licensbevis med mera ska förvaras under ordnade former. För de datorprogram som behöver användas i verksamheten och för vilka licens ej betalats skall licens snarast tecknas. Övriga datorprogram ska avlägsnas från Medytekks datorer.

De anställda som begått upphovsrättsintrång har även gjort sig skyldiga till brott emot anställningsavtalet. Frågan om uppsägning kan aktualiseras, men sannolikt krävs omfattande eller upprepade förseelser för att saklig grund för uppsägning ska föreligga.

Vad säger standarden?

- I **kapitel 15.1.2** anges allmänt att lämpliga åtgärder ska vidtas för att säkerställa immateriell lagstiftning. Vad gäller upphovsrätt till programvaror definieras ett antal åtgärder som bör vidtas. Bland dessa kan nämnas
  • utfärdande av en skriftlig policy för efterlevnad av upphovsrättsskyddet som reglerar användningen av programvara,
  • regler för upphandling av programvaror,

- medvetenhet inom organisationen om upphovsrättsregler,
- register över programvaror, och
- kontroller av att endast godkänd och licensierad programvara används.

Appendix 2.1.4 Avhopp

En av Medytekks två säljare hoppar av till en konkurrent. Säljaren har givetvis haft full tillgång till Medytekks kundregister och en kort tid efter avhoppet har det konkurrerande företaget inlett en riktad säljkampanj mot ett flertal av Medytekks viktigaste kunder.

Händelsen aktualiserar frågan om innehållet i Medytekks anställningsavtal. Avtalen ska i samtliga fall innehålla en heltäckande sekretessbestämmelse, vilken ska gälla även efter anställningens upphörande och helst innehålla en skyldighet att utge ett vitesbelopp. Om säljaren har lämnat kundinformation till den nye arbetsgivaren har han brutit mot sekretessvillkoren, vilket aktualiserar vitet. För personal med så avgörande funktion som säljare bör avtalet även innehålla en konkurrensbegränsningsklausul, som förbjuder säljaren att bedriva/arbeta för en konkurrerande verksamhet under viss tid efter anställningens upphörande.

Säljaren har sannolikt inte gjort sig skyldig till brott mot straffbestämmelserna i lagen om skydd för företagshemligheter (FHL), eftersom han inte kommit över kundinformationen på olovligt sätt, men däremot har han sannolikt brutit mot FHL: s skadeståndsgrundande regler, genom att avslöja företagshemlig information som han fått del av under anställningen. Även det konkurrerande företaget kan ha brutit mot dessa regler (se 7 och 8 § § FHL, jfr Arbetsdomstolens – AD – dom 80/1998).

Vad säger standarden?

- Standarden anger i **kapitel. 8.1.3** att ett sekretessavtal ska ingå i anställningsavtalet för varje anställd. Standarden innehåller ingen föreskrift om konkurrensbegränsningsklausul.

Appendix 2.1.5 Externt intrång

På Medytekk upptäcker man att någon med ”konstig” systemtillhörighet via Medytekks modempool varit inne i företagets nätverk och hämtat information om ett av Medytekks mest lovande projekt.

Intrångsgöraren har sannolikt gjort sig skyldig till dels dataintrång (Brottsbalken – BrB – 4:9 c §), genom att olovligen ta sig in i nätverket, dels företagsspioneri (3 § FHL), genom att ta del av information om ett av projekten – vilket är att betrakta som företagshemlig information (jfr Stockholms tingsrätts dom 1996-10-16, målnr. B 466-91). Om intrånget skett på uppdrag av annan – exempelvis ett konkurrerande företag – eller om ett konkurrerande företag tar del av de hemliga uppgifterna (och förstår att dessa åtkommits lagstridigt) kan även det konkurrerande företaget (eller rättare sagt dess företrädare) ha gjort sig skyldigt till brott, nämligen olovlig befattning med företagshemlighet (3 § FHL).

Att det tekniska skyddet av nätverket bör ses över efter händelsen är en självklarhet. Med rättsliga åtgärder kan man knappast förebygga eller förhindra ett dylikt intrång. Däremot bör Medytekk polisanmäla händelsen och om möjligt försöka identifiera intrångsgöraren samt fastställa vilken information som denne kommit över. Om förövaren identifieras kan Medytekk väcka skadeståndstalan mot denne, antingen i samband med att åtal väcks eller separat. Skadeståndskrav kan även framställas mot exempelvis ett konkurrerande företag som använder information som härrör från intrånget. De rättsliga åtgärderna förutsätter dock att uppsåt föreligger; förövaren måste inse att informationen inte var allmänt tillgänglig och att det denne gjorde var en olovlig handling. Det tekniska skyddet kan här bidra, inte bara genom att göra det tekniskt sett svårare att få tillgång till skyddsvärd information utan även för att tydligt signalera att den informationen är skyddad - kringgås de tekniska skyddsåtgärderna så föreligger uppsåt.

Vad säger standarden?

- **Kapitel 11** i standarden anger relativt detaljerat olika åtgärder som bör vidtas för att hindra obehörig åtkomst av organisationens information, däribland användning av lösenord, och åtgärder för att i efterhand kunna identifiera intrång.

Appendix 2.1.6 Dokumentering av information

En av de ledande forskarna på Medytekk är en kvinna i 50-årsåldern som är något av en ensamvarg. Hennes idéer och forskning har legat till grund för flera av Medytekks produkter och en stor del av dessa och nya idéer finns enbart i hennes huvud. Den senaste tiden har hon verkat vara lite ur gängorna. Två dagar under en och samma vecka kommer hon kraftigt försenad till arbetet och vid båda tillfällena är hon alkoholpåverkad.

Att uppträda alkoholpåverkad på jobbet är ett brott mot anställningsavtalet, eftersom den anställde inte kan utföra sina arbetsuppgifter på ett korrekt sätt. Medytekk bör skicka hem kvinnan, med uppmaningen att återkomma nykter dagen efter. Därefter bör Medytekk varna henne för att en upprepning av beteendet kan medföra att uppsägning kan aktualiseras. Möjligheterna att säga upp forskaren under åberopande av att hon inte

kan utföra sitt arbete är dock begränsade om hon har alkoholmissbruk, eftersom detta i arbetsrätten jämställs med sjukdom. För de dagar hon inte varit arbetsför har Medytekk rätt att göra löneavdrag.

Den kvinnliga forskaren är utan tvekan att anse som en nyckelperson, eftersom hon sitter inne med mycket väsentlig information om delar av den forskning som bedrivs i företaget. Givetvis bör företaget erbjuda henne det stöd och den hjälp som är möjlig för att hon ska komma till rätta med hennes alkoholproblem. Ur företagets synvinkel är det dock även mycket viktigt att så långt som möjligt se till att den kunskap och information hon besitter dokumenteras så att den inte riskerar att förloras om hon inte kan fortsätta arbeta.

Händelsen aktualiserar även frågan om drogtester av personalen. Lagstiftning saknas f.n., men en utredning arbetar med en översyn (se Utredningsdirektiv 2006:55 ”Personlig integritet i arbetslivet”). Vägledning får tillsvidare hämtas ur AD: s rättspraxis (bl.a. AD: s dom 1991 nr 45 och 1998 nr 97). I korthet kan sägas att arbetsgivaren torde ha rätt att inom sin rätt att leda arbetet på företaget bestämma att drogtester ska ske, men att det förutsätts att de anställda informeras om att tester ska ske och att testerna är adekvata och inte kränker den personliga integriteten mer än nödvändigt.

Vad säger standarden?

- Standarden innehåller i **kapitel 7** föreskrifter om ansvar för, förteckning över och klassificering av information. All väsentlig information ska i enlighet med detta dokumenteras och tilldelas en namngiven ”ägare”. Informationen ska vidare klassificeras samt förtecknas i ett register.
- Standarden innehåller inga föreskrifter om drogtester.

Appendix 2.2 Checklista

Nedan följer en checklista avseende relevant lagstiftning och en förteckning över riktlinjer/föreskrifter med juridisk anknytning som bör antas av organisationen. Checklistan och förteckningen ger inte anspråk på att vara fullständiga; ytterligare relevant lagstiftning kan föreligga och ytterligare riktlinjer/föreskrifter kan behövas.

Appendix 2.2.1 Rättsregler som bör beaktas vid informationsbehandlingen

Regler om sekretess och tystnadsplikt

- Sekretesslagen avgör (exklusivt) vilken information hos myndigheter och andra offentliga organ som är offentlig respektive sekretessbelagd.
- Regler om sekretess- och tystnadsplikt i särskilda verksamheter finns bland annat för sjukvårdsverksamhet, tele- och postverksamhet och advokatverksamhet.

Regler om fysiskt och logiskt skydd

- Säkerhetsskyddslagen
- Lag om skydd för samhällsviktiga anläggningar
- Reglerna om dataintrång, BrB 4:9c
- Lagen om elektroniska signaturer

Regler om förvaring och arkivering

- Arkivregler för myndigheter och andra offentliga organ; bland annat arkivlagen.
- Bokföringslagen: Uppställer bland annat krav på betryggande arkivering av allt räkenskapsmaterial i minst tio år.
- Aktiebolagslagen: Uppställer bland annat krav på att aktiebok och protokoll från styrelsemöten förvaras på betryggande sätt.

Regler om skydd för personlig integritet

- PUL: Innehåller detaljerade bestämmelser om behandling av personuppgifter. Lagen gäller både manuell och automatisk (data) behandling av personuppgifter. Lagen uppställer krav på bland annat
  i) utseende av personuppgiftsombud
  ii) förteckning över organisationens registerbehandlingar
  iii) samtycke från och information till de personer som omfattas av behandling av personuppgifter.

Immaterialrättsliga regler

- Upphovsrättslagen (URL): Innebär att upphovsmannen till exempelvis bilder, texter och datorprogram har ensamrätt att sprida och mångfaldiga dessa. Även databaser skyddas av URL. I princip innebär detta ett förbud för andra att utan tillstånd (licens) från upphovsmannen kopiera bild, text, datorprogram eller databaser. Reglerna i URL och de begränsningar som följer av dessa gäller även på Internet. Förbudet att kopiera är straffbelagt och överträdelse kan dessutom medföra skadeståndsskyldighet. Ensamrätten gäller i 70 år efter upphovsmannens död (för databaser gäller normalt kortare tid).
- Varumärkeslagen (VML) och firmalagen (FL): Dessa lagar innebär att den som inregistrerat eller inarbetat ett varumärke eller en firma (namn på bolag, föreningar och andra organisationer) har ensamrätten till detta

och att andra är förbjudna att utan tillstånd (licens) använda samma eller förväxlingsbart varumärke respektive firma i näringsverksamhet. VML: s respektive FL: s regler och de begränsningar som följer av dessa gäller även på Internet. Förbuden är straffbelagda och överträdelse kan dessutom medföra skadeståndsskyldighet. Ensamrätten gäller så länge varumärket respektive firman används.

- Patentlagen (PL): Innebär att den som erhållit patent på en uppfinning har ensamrätt att yrkesmässigt utnyttja uppfinningen. Detta innebär i princip att ingen utan samtycke (licens) från patenthavaren har rätt att utnyttja uppfinningen. Förbudet är straffbelagt och överträdelse kan dessutom medföra skadeståndsskyldighet. Ensamrätten gäller initialt i 20 år.

Arbetsrättsliga regler

- Medbestämmandelagen (MBL): Förhandlings- och informationsskyldigheten enligt MBL måste iakttas vid införande av riktlinjer för verksamheten i organisationen, exempelvis vid införande av riktlinjer för övervakning av anställdas e-post- och Internetanvändning, och vid införandet av sanktioner för överträdelse av riktlinjerna.

Regler om krypteringsprodukter

- Rådsförordning (EG) nr. 3381/94 och lag (1998:397) om strategiska produkter: Krypteringsprogramvara omfattas generellt av exportkontrollagstiftning – såväl inom EU som i Sverige – varför utgångspunkten är att tillstånd krävs från Inspektionen för strategiska produkter för export och i vissa fall utförsel av sådan programvara. Det finns dock generella undantag för vissa typer av krypteringsprogramvara. Tillgängliggörande via Internet anses normalt innebära export. Sverige har däremot inga importrestriktioner avseende krypteringsprodukter.

Appendix 2.2.2 Riktlinjer/föreskrifter med juridisk anknytning som bör utarbetas

- Behörighetsregler: Behörighetsföreskrifterna bör så långt det är möjligt begränsa tillgången till information (need-to-know-basis). Föreskrifterna bör ange hur information ska klassificeras samt även innehålla ”ordning-och-reda-regler”. Om distansarbete förekommer kan även detta regleras här.
- Sekretessregler: Sekretessreglerna kan utformas som ett separat avtal, som utgör bilaga till anställningsavtalet. Skyldigheten att iaktta sekretess bör omfatta all information som den anställde erhåller genom sin anställning och gälla även efter anställningens upphörande.
- E-post- och Internetanvändning: Riktlinjerna bör så tydligt som möjligt avgränsa vad som utgör tillåten användning och uttryckligen ange att annan användning inte är tillåten. Om övervakning av de anställdas användning ska ske ska detta uttryckligen anges i riktlinjerna.
- Användning och inköp av programvara: Riktlinjerna bör utformas så att användning och inköp av programvara inte medför brott mot upphovsrättsreglerna.
- Hantering av överträdelser: Riktlinjerna bör fastställa vilka åtgärder som vidtas för det fall överträdelse sker av de bestämmelser som gäller inom organisationen. Riktlinjerna bör tas fram tillsammans med den lokala fackliga organisationen.
- Då det är viktigt att säkerställa att de anställda har tagit del av ovan nämnda riktlinjer och regler kan det vara lämpligt att ett kontrakt/avtal upprättas vilket den anställde signerar.

Appendix 3- Riskanalys metoder

Det finns ett stort antal olika metoder för riskanalys. Många av dessa är branschspecifika. Detta appendix beskriver övergripande några vanliga metoder.

Appendix 3.1 Riskanalys – med sannolikhet och konsekvens

En ofta använd metod för analysering av risker är att bedöma risknivån som är sannolikheten multiplicerad med konsekvensen.

Risknivå = Sannolikhet X Konsekvens

Sannolikheten och konsekvensen måste graderas. Det är lämpligt att använda en detaljeringsnivå på graderingen som står i relation till det underlag man har att arbeta med. Konsekvensen kan också uttryckas som kostnader.

Ett exempel på gradering eller kriterierna Sannolikhet, Konsekvenser och Risknivå

Sannolikhet	**Konsekvens**	**Risknivå**
1= Mycket låg	1= Mycket liten	1-4 = Kan accepteras
2= Låg	2= Liten	5-14= Bör åtgärdas
3= Medelstor	3= Medelstor	15-25= Åtgärdas snarast
4= Stor	4= Stor	
5= Mycket stor	5= Mycket stor	

Det är viktigt att ta hänsyn till att det kan finnas krav på verksamheten vilka är tvingande och därför måste åtgärdas med hög prioritet. Exempel på detta är krav från myndigheter och försäkringsbolag.

Nedanstående mall är ett exempel på hur man använder frågor för att analysera säkerhet i en organisation.

Objekt/ Lokal	**Frågelista**	**Aktuell status**	**S**	**K**	**R**	**Åtgärd eller notering**
8	Hur hanteras gods eller handling som besökare vill förvara i reception under ett besök?	Vi har inte några regler eller rutiner för hantering av besökares bagage, värdehandlingar eller annat som lämnas i receptionen!	5	2	10	Anskaffning av ett fackindelat stöldskyddsskåp som placeras inom synhåll från receptionen. Besökaren får kvittera ut facknyckel från receptionen varefter denna hanterar medfört gods själv.

Om vi ser på exemplet objekt 8, förvaring i receptionen hämtat från frågelistan ovan:
S: Sannolikheten för att någon obehörig får tillgång till gods i receptionen bedöms som mycket hög och klassas till 5.
K Konsekvensen om inlämnat gods eller värdehandling försvinner eller skadas? (Här är det konsekvenserna för företaget som skall bedömas 1-5). Vi bedömer konsekvensen som liten och klassar den till 2.

Då risknivån är sannolikheten X konsekvensen ger det nivå 10. Åtgärder bör vidtagas för att reducera risknivån.

Appendix 3.2 Riskanalys med användande av metoder för problemanalys

Nedan beskrivs kortfattat två metoder vilka även kan vara mycket användbara vid felanalys.

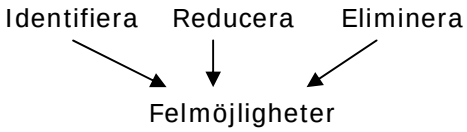
1) FMEA metod, Failure Mode Effect Analysis

- Identifiera potentiella fel och brister, samt följderna av dessa
- Förmå konstruktören/processeknikern att på ett systematiskt sätt pröva sin lösning
- Söka och jämföra alternativa lösningar
- Undvika sena och därmed kostsamma lösningar genom att tidigt finna eventuella svagheter
- Undvika att tidigare fel inte upptäcks
- Påtala områden där kontroll eller kvalitetsstyrning krävs
- Få underlag för planering av testning och underhåll

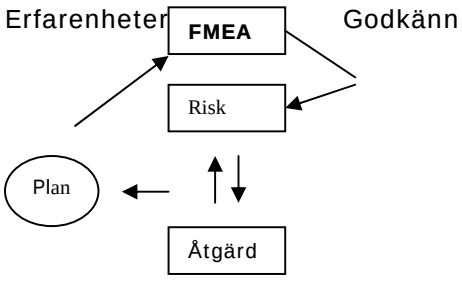
Fördelar med FMEA

- Förutsätter ett systematiskt arbetssätt
- Förutsätter en samtidig värdering av såväl felfenomen som allvarlighetsgrad och sannolikhet för upptäckt.
- Bygger på en objektivkalkylering av ett
- risktal
- Förutsätter samarbete i grupp

Målet av FMEA



Hur FMEA fungerar



FMEA – bedömningstal

• Sannolikheten för fel
• Bedöm allvarlighetsgraden
• Bedöm sannolikheten för upptäckt

Allvarlighetsgrad

1 Ingen påverkan på produktfunktion eller på tillverkningen
2-3 Konsekvenserna av felet bedöms som mindre allvarliga
4-6 Konsekvenserna bedöms som ganska allvarliga
7-8 Konsekvenserna bedöms som allvarliga
9-10 Konsekvenserna bedöms som mycket allvarliga

Sannolikhet för upptäckt

1 Den defekta detaljen kommer nästan helt säkert att upptäckas
2-3 Den defekta detaljen kommer förmodligen att upptäckas
4-6 Den defekta detaljen kommer kanske att upptäckas
7-8 Den defekta detaljen kommer förmodligen inte att upptäckas
9-10 Den defekta detaljen kommer nästan säkert inte att upptäckas

FMEA – Risktalet

(RPN= Risk Priority Number)
RPN = felsannolikhet * allvarlighetsgrad * sannolikhet för upptäckt

2) Ishikawadiagram (Fiskbensdiagram)

Diagrammet används främst för att på ett strukturerat sätt identifiera, sortera och tydligt illustrera tänkbara orsaker till ett problem eller ett tillstånd.
Fiskbensdiagrammet svarar på frågor som:
• Vilka är de tänkbara orsakerna till att…….?
• Vilka orsaker finns bakom……?
• Varför har vi problem med……?

Steg 1. Definiera tydligt problemet (verkan).

Detta får inte vara för allmänt formulerat. Det skall tydligt framgå vad själva problemet är.

Steg 2. Rita en kraftig pil som kommer att bli ryggraden i diagrammet.

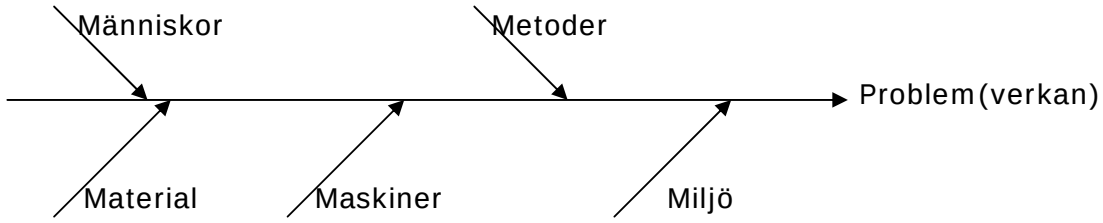
Låt pilen peka åt höger. Skriv problemet (verkan) i en ruta vid pilspetsen.
Rita ut fem fiskben. Fiskbenen utgörs vanligen av fem M: Människor,
Maskiner, Metoder, Material och Miljö. (Se på bifogade exempel)

Steg 3. Sök så många orsaker som möjligt. (Ställ frågan ”varför”)

Använd gärna metoden ”brainstorming”.
Genom att sortera in alla orsakerna under resp. M i fiskbenet får man en klar bild av vilka av de fem M:en som dominerar. Man kan också se vilka orsaker som eventuellt hänger ihop.
Tänk på att en orsaksfaktor kan dyka upp på flera platser i diagrammet.

Steg 4. Efter att ha sammanställt en uppsättning av orsaksteorier är nästa steg att finna vilka de viktigaste grundorsakerna är.

Orsakerna kan rangordnas, dvs. vi måste komma fram till vilka av dem som är väsentligaste. Se bifogade exempel på fiskbensdiagram: Problem (Verkan), Människor, Metoder, Material, Miljö och Maskiner



Appendix 4 – Handledning för LIS planeringsfas

Inledning

Som stöd vid införandet av ett ledningssystem för informationssäkerhet finns en processorienterad handledning som är tillgänglig kostnadsfritt från SIS webb, www.sis.se/projekt/lis. Handledningen finns att ladda hem dels som en rapport i pdf-format och dels som en interaktiv webbtjänst.

Denna handledning kom till för att avdramatisera arbetet med att ha standarden som grund för en organisations informationssäkerhetsarbete. Handledningen visar på ett angreppssätt som inte innebär alltför stor belastning på verksamheten, men ändå leder mot en mera fullständig tillämpning i flera steg. Resultatet ska ses som ett komplement till denna handbok.

Apendix 4.1 Handledningens syfte

Handledningen ska ge vägledning i arbetet med att starta upp och genomföra planeringsfasen i ett ledningssystem för informationssäkerhet enligt SS-ISO/IEC 27001 och med stöd av SS-ISO/IEC 17799. Det skall även ge en grund för fortsatt planering och tillämpning.

Hantering av akuta brister som upptäcks i det inledande stegen (nuläges-, och verksamhetsanalyser) behandlas inte i handledningen. Detta innebär inte att åtgärder av det slaget är mindre viktiga.

Slutprodukten från den fas som handledningen beskriver är ett sammanhållande regelverk där man har tagit hänsyn till resultatet från verksamhets-, nuläges- och riskanalyser.

Appendix 5 Certifiering av ledningssystem för informationssäkerhet – LIS

Appendix 5.1 En beskrivning av certifieringsordningen

5.1.1 Bakgrund

Certifiering av ledningssystem för informationssäkerhet sker mot SS ISO/IEC 27001, Specifikation för ledningssystem för informationssäkerhet, och handlar om att skydda organisationens informationstillgångar och att säkerställa en kontinuerlig verksamhet med marknadens och myndigheters förtroende.
Syftet med denna beskrivning är att enkelt redogöra för hur processen ser ut enligt de regelverk som gäller för ackrediterade certifieringsorgan. För organisationer där det i verksamheten ingår att utfärda elektroniska signaturer tillämpas utöver SS ISO/IEC 27001 kompletterande standarder.

5.1.2 Certifikatens trovärdighet

Certifiering är inget skyddat begrepp. Certifikat kan utfärdas av vem som helst. För att säkerställa trovärdighet finns systemet med ackreditering (kompetensprövning) av certifieringsorgan, dvs. godkännande av att organisationer som utfärdar certifikat har tillräcklig kompetens.
För att få jämförbar nivå på utfärdade certifikat, varigenom trovärdighet säkerställs, finns standarder och riktlinjer för hur certifieringsorgan bör vara organiserade och bedriva verksamhet. Oberoende är här ett viktigt kriterium. I Sverige utfärdas ackrediteringen inom området ledningssystem för informationssäkerhet av myndigheten SWEDAC. Motsvarande system finns i de flesta industriländer.

5.1.3 Grundkraven på certifieringsprocessen

För certifieringsorgan som ackrediteras för att utföra certifieringar av ledningssystem för informationssäkerhet gäller standarden ISO Guide 62 (EN 45 012). Denna standard beskriver både de formella kraven på certifieringsorgan när det gäller oberoende, kompetens, beslutsrutiner etc. samt hur certifieringsprocessen bör se ut. Standarden ger inga tolkningar till SS ISO/IEC 27001..
Ackrediteringsorganen i flera europeiska länder har gemensamt och i samarbete med certifieringsorgan, industriorganisationer och andra intressenter utarbetat ett vägledningsdokument för certifiering av ledningssystem för informationssäkerhet, *EA-7/03,EA Guidelines for the Accreditation of Bodies Operating Certification / Registration of Information Security Management Systems*. Dokumentet finns tillgängligt på Internet <http://www.european-accreditation.org>.
Kraven är inte heltäckande utan ger certifieringsorgan möjlighet att utveckla och anpassa rutinerna utifrån sina och kundernas behov. Certifieringsorganen ska ha en detaljerad beskrivning av sitt revisions- och certifieringsförfarande som är tillgängligt för deras kunder.

Appendix 5.2 Certifieringsordningen – ingående delar

5.2.1 Ansökan/offertbegäran

Företag, myndigheter och andra organisationer som önskar bli certifierade skickar normalt en offertförfrågan till ett eller flera certifieringsorgan. Certifieringsorganen tillhandahåller formulär för detta.
Organisationen förser certifieringsorganet med bland annat basuppgifter om organisationens verksamhet, storlek och lokalisering, information om dess ledningssystem för informationssäkerhet och genomförda riskanalyser samt relevant lagstiftning som organisationen berörs av. Dessutom bör önskad start av certifieringsprocessen anges.
Certifieringsorganet kan på grundval av basuppgifterna, och eventuella kompletteringar, gå igenom handlingarna och försäkra sig om att

- kunden har förstått kraven för certifiering
- den insända dokumentationen är tillräcklig.

Bilagor till offertförfrågan bör vara

- karta som visar hur man kommer till primärorten
- organisationsschema
- beskrivning av ledningssystemet för informationssäkerhet
- riskanalysrapport
- uttalande om tillämplighet
- kopia(or) på ISO 9001, ISO 14001 och/eller andra certifikat som rör verksamheten

Certifieringsorganet har nu att bedöma om man har kompetens inom branschen samt kapacitet att utföra det aktuella uppdraget.
Om organisationens verksamhet bedrivs på flera platser ska certifieringsorganet göra en särskild bedömning enligt regler i ackrediteringsorganens vägledningsdokument. Denna genomgång är nödvändig för att certifieringsorganet ska kunna ge en relevant offert.

5.2.2 Offert

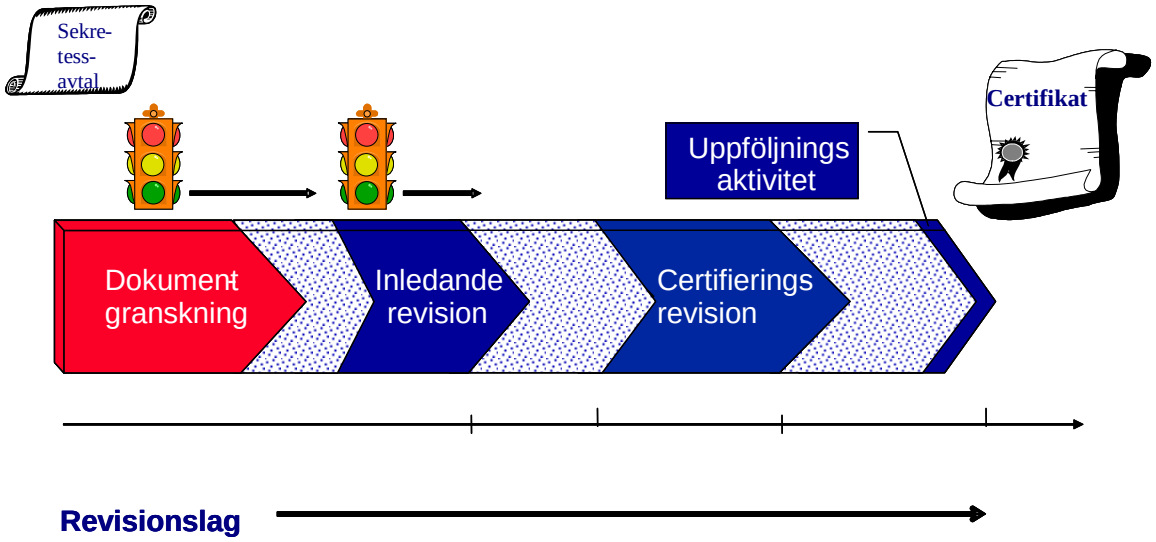
Offerten baseras på information som givits i offertförfrågan och bör bland annat inkludera pris, leveransvillkor, revisionslag, beskrivning av certifieringsprocessen samt uppföljande revisioner.

5.2.3 Planering

När en offert accepterats av kunden planerar certifieringsorganet uppdraget mer i detalj och begär in ytterligare dokumentation från företaget. En bekräftelse på revisionslag som utsetts samt kontaktpersoner skickas. Kunden har möjlighet att komma med invändningar mot personer i laget till exempel av konkurrensskäl.

Appendix 5.3 Revision i två steg på plats

Certifieringsorganet genomför sin granskning på plats i två steg.



Stegindelningen är föranledd av att ledningssystem för informationssäkerhet utgår från ett antal baselement. Dessa är Riskhanteringsprocessen informationssäkerhetspolicy och processen för kontinuitetsplanering.
Riskanalyser och kontinuitetsplaner ska vara utförda utifrån affärsverksamhetens perspektiv. Analyser och planer måste finnas på plats för att det fortsatta arbetet ska vara meningsfullt.

5.3.1 Steg 1

Som minimum ska det första steget bland annat säkerställa att

- informationssäkerhetspolicyn uppfyller standardens krav,
- uttalande om tillämplighet har upprättats,
- informationssäkerhetspolicyn, utfall från genomförda riskanalyser samt validering av kontinuitetsplaner harmoniserar med uttalande om tillämplighet,
- riskanalyser är utförda utifrån ett affärsperspektiv samt att dessa är relevanta med hänsyn till den verksamhet som bedrivs i organisationen och den miljö i vilken verksamheten bedrivs,
- organisationen har rutiner för identifiering av relevant lagstiftning och andra krav som företaget berörs av,
- ledningssystemet är så utformat att organisationens informationssäkerhetspolicy kan uppfyllas,
- systemet är implementerat i sådan utsträckning att en detaljerad granskning kan genomföras i nästa steg,
- interna revisioner av ledningssystemet har ägt rum och att resultatet från revisionerna finns tillgängliga,
- ledningens genomgång har genomförts och att denna omfattat systemets lämplighet och effektivitet,
- kontinuitetsplaner finns utformade utifrån affärsverksamhetens förutsättningar och att deras lämplighet har validerats.

Steg 1 syftar vidare till att

- ge organisationen erfarenhetsåterföring om systemets funktion och revisionsprocessen,
- utgöra underlag för en detaljplanering av steg 2 inkluderande
  - en utvärdering av behov av revisionskompetens, inklusive tekniska experter,
  - avstämning av att planerad tid är tillräcklig,
- samla information inför steg 2 och identifiera områden som ska ägnas särskild uppmärksamhet i detta steg,
- peka på områden där kompletterande information krävs från kunden.

Normalt föranleder steg 1 att justeringar och kompletteringar av systemet krävs före steg 2. Planeringen bör därför vara sådan att tid avsätts till detta. De eventuella avvikelser/förbättringsmöjlighet som identifierats under steg 1 ska ha åtgärdats innan steg 2 inleds.

5.3.2 Steg 2

Det grundläggande syftet med detta steg i revisionen är att säkerställa att

- företaget verkar enligt sin egen policy, sina mål samt enligt sitt ledningssystem för informationssäkerhet
- ledningssystemet uppfyller verksamhetens samt standardens krav

Viktiga områden vid revisionen är

- riskanalysprocessen,
- säkerhetsorganisationen,
- klassificering och kontroll av tillgångar,
- personal och säkerhet,
- styrning av kommunikation och drift,
- styrning av åtkomst,
- systemutveckling och underhåll,
- kontinuitetsplanering,
- efterlevnad.

Revisionen utförs genom stickprov. Den omfattar såväl utvärdering av att systemet är dokumenterat som att det är implementerat, det vill säga att ledningssystemet uppfyller ledningens och standardens krav samt att det används och att det finns ett förtroende för dess fortlevnad och utveckling.

5.3.3 Rapportering

Revisorerna ska på plats, som en avslutning på revisionen, ge företaget och dess ledning en redogörelse för resultatet av revisionen samt lämna över avvikelser och säkerställa att dessa är förstådda. Möjlighet till frågor och förtydliganden ges vid detta tillfälle.

En skriftlig rapport lämnas över eller skickas senare till företaget. De avvikelser från kraven, verksamhetens såväl som standardens, som identifierats ska vara klart angivna. Rapporteringen ska även innehålla mera översiktliga kommentarer kring systemet. Företaget ska ges möjlighet att kommentera rapporten. Revisionsledaren ska beskriva den fortsatta processen och ge besked om rekommendation till certifiering kommer att utfärdas när eventuella avvikelser åtgärdats och verifierats av certifieringsorganet. Om avvikelserna är omfattande eller av allvarlig grad kan en ny revision på plats krävas.

Företaget ska inom avtalad tid vidta åtgärder för att korrigera de avvikelser som konstaterats under revisionen. Om avvikelserna har varit omfattande kan, som ovan nämnts, en ny revision av delar av eller hela systemet erfordras. Revisionsledaren ska utfärda en rekommendation till certifiering när alla avvikelser är stängda.

5.3.4 Beslut om certifiering samt utställande av certifikat

Beslut om certifiering tas av oberoende personal inom certifieringsorganet med motsvarande kompetens. Beslutet föregås av en genomgång av de uppgifter som redovisats av revisionslaget. Vid denna genomgång kan kompletteringar och förtydliganden krävas.

Certifieringsorganet utfärdar därefter ett certifikat där bland annat följande framgår

- Företagets namn
- Standard för certifiering (SS-ISO/IEC 27001)
- Eventuella andra standards och tolkningsdokument som tillämpats vid bedömningen
- Verksamhetens omfattning (scope) – detta kan medföra att bilaga till certifikat erfordras för att med önskvärd tydlighet klargöra verksamhetens omfattning
- Referens till organisationens aktuella uttalande om tillämplighet
- Giltighetstid
- Certifieringsorganets namn
- Ackreditering

I bilagor ges vidare bland annat regler för:

- Uppföljande revisioner, oftast kallad periodiska besök
- Användning av certifierings- och ackrediteringsmärke
- Användning av certifiering i marknadsföring

Dessutom bifogas ofta en periodisk plan där preliminära tider för uppföljande besök anges samt områden som ska revideras vid dessa tas upp. Detta för att säkerställa att hela verksamheten täcks in under den treårsperiod som certifikatet är giltigt.

5.3.5 Uppföljning av certifikat

Certifieringsorgan följer under certifikatets giltighetstid upp att företagets certifierade ledningssystem för informationssäkerhet fortsatt fungerar för verksamheten och uppfyller kraven i standarden. Denna uppföljning ska ske minst en gång per år. Besöken kan omfatta hela eller delar av systemet.
De avvikelser som noteras vid uppföljande revisioner ska åtgärdas för att certifikatet ska fortsätta att gälla. Ytterst handlar det om att förtroendet för organisationens förmåga att skydda sina informationstillgångar hålls levande.

5.3.6 Förnyelse av certifikat

Minst vart tredje år ska en total genomlysning av ledningssystemet göras för att säkerställa dess övergripande överensstämmelse med organisationens ledningssystem för informationssäkerhet och standardens krav och att detta har vidmakthållits korrekt. Denna ska åtminstone säkerställa att

- alla element i ledningssystemet för informationssäkerhet, LIS, harmoniserar,
- övergripande effektivitet hos LIS i sin helhet med hänsyn taget till organisationens verksamhetsförändringar finns,
- företagsledningen visar sitt uttalade stöd för ett effektivt LIS.