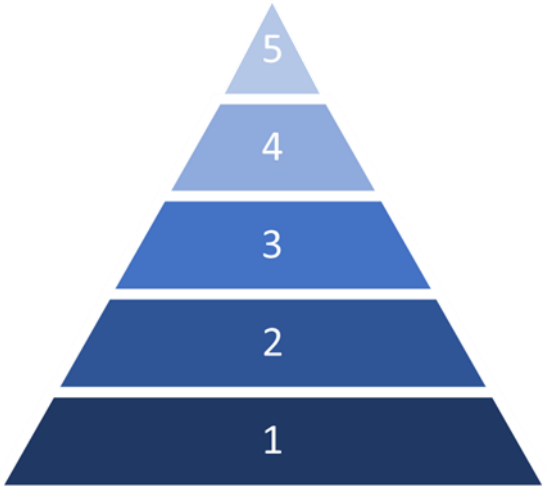
Säker IT-Arkitektur

En säkerhetstrappa



Neha Grundström

Version 27

2022-06-11

Projektarbete inom Dataföreningen Kompetens kurs Certifierad IT-Arkitekt, kurs nr 73

Om uppsatsen

Säkerhet ska genomsyra hela företagets kultur och i denna uppsats presenteras en säkerhetstrappa i fem steg där olika processer och teknologier rekommenderas för att på ett strukturerat sätt arbeta med företagets digitala säkerhet.

Uppsatsen i sammandrag

Digitalt säkerhetsarbete är eller bör vara en del av företagets kontinuerliga arbete. Säkerhet är inte längre bara något som IT ska arbeta med utan ska genomsyra hela företaget och dess policys och processer. I uppsatsen beskrivs teknologier för att göra system säkrare, så som kryptering, brandväggar och VPN, men också processer och steg för hur företag kan arbeta för att öka sin informationssäkerhet med kontinuerlig förbättring, bra lösenordskultur och tydliga policys. Utöver teknik och processer finns det i slutsatsen en säkerhetstrappa där olika steg för att öka säkerheten presenteras. Den är baserad på att det ska finnas tydliga processer gällande policys och informationsspridning kring företagets säkerhetskultur innan avancerad teknik implementeras.

Innehållsförteckning

1 Inledning **5**

1.1 Bakgrund 5
1.2 Problem 5
1.3 Syfte 5
1.4 Avgränsning 5
1.5 Målgrupp 5
1.6 Metodval 6

2 Vad är IT-säkerhet? **7**

2.1 Vad säger svenskt försvar om digital säkerhet? 7
2.2 Varför göra system säkrare? 7
2.3 Etisk och oetisk hackare 8
2.4 Vilka är de vanligaste säkerhetshoten? 8
2.5 Vem har ansvaret? 9
2.6 Kostnader vid cyberattack 9
2.7 Vad kostar säkerhet? 10
2.8 De tio budorden av datoretik 10
2.9 Säkerhetsmodell 10
2.10 Certifiering inom ISO27001 11

3 Policys, standarder och riktlinjer **13**

3.1 Policy 13
3.2 Standard 14
3.3 Riktlinjer 14
3.4 Handlingsplan 14
3.1 Rutiner 14

4 Åtgärder för ökad säkerhet **15**

4.1 Ledningen 15
4.2 Zero-Trust 15
4.3 Anställning 15
4.4 Konton 16
4.5 Behörigheter 17
4.6 Autentisering av användare 18
4.7 Säker utskrift 19
4.8 Vit/svartlistning av applikationer 19
4.9 Rapportering av säkerhetsbrister 20
4.10 Tillgångsägare 20
4.11 Intern utbildning 20
4.12 Antivirusprogram 21
4.13 Nätverk 21
4.14 VPN 22
4.15 Virtuellt skrivbord 22
4.16 Hoppserver 22
4.17 Kryptering 23
4.18 API 25
4.19 Backup 25

4.20 Maximum inloggningsförsök 26
4.21 Sessionstider 26
4.22 Applikationsmiljöer 27
4.23 Loggning och spårbarhet 27
4.24 Penetrationstester 28
5 Upphandling 29
5.1 Förberedelser 29
5.2 Genomförande 29
5.3 Uteslutning 30
5.4 Uppföljning 30
6 Kontinuerlig förbättring 31
6.1 Plan – Planera 31
6.2 Do – Göra 31
6.3 Check – Utvärdera 32
6.4 Act – Agera 32
6.5 Kommunikation 32
7 Identifiera, analysera och värdera risker 33
7.1 Roller 33
7.2 Identifiera 33
8 Kontinuitetshantering 36
8.1 Analysera olika scenarion 36
8.2 Nertid 36
8.3 Responsgrupp och responsplan 36
9 Säker förvaltning- och utvecklingsprocess 38
9.1 DevSecOps 38
9.2 Behovsanalys/kravinsamling 38
9.3 Utveckling 39
9.4 Test 39
9.5 Produktionssättning 39
9.6 Förvaltning 40
10 Slutsatser 41
10.1 Teknisk, strategisk och operativa förändringar 41
10.2 IT budget 41
10.3 Använda ISO27000 eller inte? 41
10.4 Ska företag certifiera sig? 41
11 Rekommendationer 42
11.1 Säkerhetstrappa 42
12 Diskussion 50
13 Referenser 51

1 Inledning

1.1 Bakgrund

Brottsligheten på internet ökar konstant och allt fler företag blir utsatta för det som kallas för cyberattacker. Att ha ett bra skydd är viktigare än någonsin, men det kostar mycket pengar. Samtidigt finns det mycket företag kan göra för att skapa sig ett bra skydd som inte behöver bli dyrt. Det är inte längre bara IT-bolag som blir attackerade utan vem som helst kan bli utsatt. Hur vet företag vad som är viktigt och mindre viktigt att skydda. Vilka steg man ska ta för att öka sin digitala säkerhet, och varför, är det som kommer undersökas och presenteras i projektarbetet.

1.2 Problem

Under de tio åren jag arbetat med IT har jag ofta sett hur säkerhet har blivit eftersatt. Oftast för att det är dyrt. Verksamheterna vill ha så mycket nyutveckling som möjligt för sina pengar, och säkerhet ingår tyvärr inte alltid där. Eftersom det är ”verksamheten” som ofta betalar kommer deras behov och önskningar först. För att då få verksamheten att vilja betala för säkerhet måste man få med dem på tåget. Hur gör man detta på bästa sätt och vilka problem ska man tackla först? Olika företag har olika stor budget för säkerhet så vad ska man koncentrera sig på för att skapa ett bra grundskydd, och vilka steg ska man ta om man därefter vill ha starkare säkerhet?

Säkerhet är inte bara en IT-fråga utan påverkar hela organisationen och är därför viktig att titta på ur ett högre perspektiv mer än bara enskilda system.
Det som kommer undersökas är:

- Hur vet man vika sårbarheter som finns och hur klassificerar man dessa?
- Hur får man ledningen och verksamheten att förstå vikten av säkerhet?
- Vilka standarder finns och hur kan man implementera dessa?
- Vilka olika typer av lösningar finns för att öka säkerheten?

1.3 Syfte

Syftet med projektarbetet är att analysera olika typer av säkerhetsbrister kopplade till IT-system som existerar och undersöka eventuella lösningar. Vilken ordning ska man implementera dessa lösningar? Finns det några lösningar som är mer grundläggande än andra?

1.4 Avgränsning

Säkerhet är ett brett ämne vilket involverar både fysisk och digital säkerhet. Det involverar också många aspekter så som social manipulation, processer och IT-system. I detta projektarbete kommer jag koncentrera mig på digital säkerhet, det vill säga IT-system och dess processer. Vilket också inkluderar generella verksamhets- och organisationsprocesser som är kopplade till ökad IT säkerhet och system.

1.5 Målgrupp

Eftersom kursen har genomförts av eget intresse och inte med ett företag som grund är projekt-arbetet inte företagsspecifikt. Informationen är inte heller koncentrerad till en specifik

företagsstorlek eller verksamhet, utan kan läsas av alla som har ett intresse av IT-säkerhet. Även om det finns förklaringar kring tekniska lösningar är fokuset på administrativa åtgärder och processer, vilket gör att även den som inte har stor teknisk bakgrund kan läsa och förstå stora delar av innehållet.

Företag som innefattas av någon säkerhetslag, myndigheter eller samhällsviktiga tjänster kommer ha liten nytta av detta dokument då den framför allt är skriven för privata aktörer.

1.6 Metodval

För att lära mig mer om ämnet IT-säkerhet, och de sårbarheter som finns, har jag valt att lyssna på poddar, läsa böcker och artiklar. Samtliga har varit inom ämnen som informationssäkerhet och ISO27000. Stora delar av innehållet i uppsatsen är från böckerna i referenslistan. Utöver det har använt egna erfarenheter av digital säkerhet, på de arbetsplatser jag arbetat på, som inspiration på åtgärder för att öka säkerheten. På det sättet attackerar jag problem och lösningar ur både ett praktiskt och teoretiskt perspektiv.

2 Vad är IT-säkerhet?

IT-säkerhet och informationssäkerhet innebär att man skyddar sin hård- och mjukvara samt informationen i system från angrepp. Detta gäller både interna och externa angrepp. Hårdvara innefattar datorer, mobiltelefoner, servrar och andra elektroniska enheter. Mjukvara innefattar system, applikationer, brandväggar och andra programvaror.

2.1 Vad säger svenskt försvar om digital säkerhet?

Personer från Försvarsmakten, Polisen, MUST och Säkerhetspolisen har alla medverkat i Trygghetspodden. De har varierade tips på vad som krävs för privata aktörer att öka säkerheten, och om detta görs har man skapat sig ett bra grundskydd [PODD1-PODD4]. De punkter de gemensamt tagits upp är:

- Personalen måste vara uppdaterade gällande företagets säkerhetskultur
- Uppdaterade system
- Vid en eventuell attack ska daglig verksamhet kunna fortsätta
- Omvärldsbevakning gällande säkerhetshot
- Bra loggning
- Koll på arkitekturen
- Backup
- Bra lösenordskultur
- Kontinuitetsplanering
- Riskanalys

2.2 Varför göra system säkrare?

Alla företag har information som är känslig, som man vill hålla hemlig för utomstående, och ibland även för andra anställda. Hoten mot företag har blivit större de senaste åren. Tidigare skedde de flesta attackerna mot privatpersoner men med tiden har företag blivit mer attraktiva att attackera. Det sker ofta genom att hacka, kryptera data och kräva företaget på pengar. De största riskerna och skadorna för företag kan sammanfattas i tre kategorier:

- Skadat rykte
- Skadad verksamhet
- Legalt brott

2.2.1 Kan system bli helt säkra?

Det enkla svaret är nej, men svaret är mer komplext än så. Om system ändå inte kan bli helt säkra från extern penetration, varför ska man då göra systemen säkra? Oavsett hur säkra vi gör system handlar det främst om hur lång tid det tar för någon obehörig att få åtkomst till känslig information, än om de gör det. Syftet blir då att göra det svårare att få åtkomst. Ju längre tid det tar, desto större chans har man som företag att upptäcka attacken och motverka den.

2.2.2 Kan system bli för säkra?

Är det möjligt att utveckla system och processer så att de blir för säkra? Även om säkerhet är viktigt kan de bli det. Inte ur ett tekniskt perspektiv utan ur användbarhets synvinkel.

Blir stegen att åstadkomma något i ett system för krångligt finns det risk att användare försöker hitta lösningar för att kringgå det, och på det sättet göra system osäkra.

Här krävs en balans mellan säkerhet och användbarhet, något som rollen som arkitekt är en av de stora och viktiga punkterna att jobba med.

2.3 Etisk och oetisk hackare

Hackare som hackare kan man tycka men det finns en skillnad. En väldigt viktig skillnad. Deras intensioner och vad de gör med de säkerhetsbrister de hittar [HACK].

2.3.1 Oetisk hackare

Deras anledning till att hacka är för att stjäla information eller pengar. De som hackar företag och begär en lösensumma för att de ska få tillbaka informationen, är oetiska hackare.

2.3.2 Etisk hackare

En etisk hackare har precis som en oetisk hackare kunskapen att utföra en hackning men skillnaden är hur de gör det och vad de gör med sin kunskap. En etisk hackare är någon som på företags begäran hackar dem för att hitta sårbarheter i deras IT-system, för att rapportera dem och ge tips på möjliga åtgärder. En penetrationstestare är med andra ord en etisk hackare.

Det är möjligt att registrera sig på till exempelvis yeswehack.com eller liknande hemsidor för att få hjälp av etiska hackare att hitta sårbarheter och buggar. Om man anser att sårbarheten anses vara stor nog erbjuder man betalning i gengäld.

2.4 Vilka är de vanligaste säkerhetshoten?

OWASP (Open Web Application Security Project) skapar varje år en lista på de 10 vanligaste hoten för IT-säkerhet [OWSAP]. 2021 var detta topp 10:

1. **Felaktiga behörigheter:** Innefattar fel eller för höga behörigheter. En användare ska inte ha mer behörigheter än som krävs för deras arbetsuppgifter/roll på företaget. Det kan också innebära att konton används av flera personer eller på ett felaktigt sätt.

2. **Trasig/svag kryptering:** Det kan innebära att man helt saknar kryptering eller har svag kryptering, vilket gör det enklare att knäcka. Här innefattas också felaktiga eller utgångna certifikat.

3. **Injektion:** Vanligaste formen är någon typ av SQL-injektion där data kan ändras. Data som matas in valideras inte innan de läses in i databasen eller att felaktig information kan läsas in.

4. **Felaktig/osäker design:** Här räknas dålig kodkvalité in. Koden som skrivits är inte av god kvalité och/eller är inte ordentligt testad. Det kan också innefatta dålig kravhantering, att man med andra ord inte varit tillräckligt tydlig vad systemet ska och inte ska utföra. Även bristande IT-arkitektur inkluderas här.

5. **Felkonfigurering:** Till exempel portkonfigurering, brandväggar, behörighet och liknande. Exempelvis att ett system har för få begränsningar.

6. **Felaktiga eller gamla komponenter:** OS, program, servrar, databaser eller annan mjukvara som är gammal och/eller inte uppdaterade.

7. **Autentisieringsproblem/fel:** Svaga lösenordskriterier. Dåliga processer för glömda lösenord. Visar användarinformation i URL. Möjligt att modifiera URL för att komma åt information som användare inte bör ha behörighet till.

8. **Program och data integritetsproblem:** Data är inte krypterad och/eller kontrolleras inte om det skickas till/från rätt mottagare. Program och plugin från okända och osäkra källor. Dålig segregering av miljöer.

9. **Loggning och monitoreringsfel:** Låg loggningsgrad i system för till exempel transaktioner, inloggningar och händelser. Inga eller dåliga larm vid fel.

10. **Förfrågningsfel:** Saknar segregering och filtrering av nätverk, exempelvis blockering av trafik. En service gör en förfrågan till en annan och kan därför injektera information felaktigt. Kontrollerar inte att en förfrågan kommer från godkänd källa. Mer data presenteras än vad som behövs.

Flera av dessa punkter är knutna till, och påverkas av, varandra. Bara rättning av en punkt kommer inte göra stor skillnad på säkerheten utan det krävs att man arbetar på flera punkter.

2.5 Vem har ansvaret?

Vem har egentligen ansvaret för att se till att ett företag är säkert från intrång? Erfarenheten antyder att många tycker att det är någon annans ansvar. Om det finns en avdelning som enbart arbetar med IT-säkerhet, då tycker majoriteten att det är deras ansvar. Flertalet gånger har jag upplevt att ingen, eller få, bryr sig, eller inte tycker det är viktigt. För en verksamhet kan det tyckas vara IT-avdelningens uppgift, och från IT att verksamheten måste inkludera det i sin kravställning. Det finns inga tydliga krav från ledningen att säkerhet är viktigt och prioriterat, vilket i sin tur visar sig i resten av företaget.

Sanningen är att det är allas ansvar. Många attacker kan motverkas genom att varje enskild anställd tar sitt ansvar. Användarkonton, passerkort, lösenord är exempel på värdehandlingar som ska skyddas av respektive person. Det finns också ett gemensamt ansvar att systemen är säkra.

2.6 Kostnader vid cyberattack

IBM har i deras Data breach report för 2021 beräknat att den genomsnittliga kostnaden för att lösa ett dataintrång var 4,24 miljoner dollar, vilket motsvarar ungefär 41 miljoner kronor. Siffran är baserad på snittkostnaden för ca 500 bolag världen över. Det är en kostnadsökning på ungefär 10 procent jämfört med föregående år. Stor del av detta beror på pandemin då många har arbetat hemifrån under året, vilket i sin tur har medfört nya risker.

För företag utan en riskplan och responsgrupp var snittkostnaden 5,71 miljoner dollar, vilket är ungefär 25 procent mer än genomsnittet. För de företag med en responsgrupp var kostnaden cirka 3,88 miljoner dollar [IBM].

2.7 Vad kostar säkerhet?

I trygghetspodden säger Patrik Ahlgren, chef för cyberförsvarssektionen på Försvarsmakten, ”IT kostar pengar och det är en dyr investering som skrivs av väldigt fort och behöver uppdateras. Säkerhet kostar pengar”.

Hur mycket det kostar att ha säkra system beror helt på vilket typ av företag man bedriver och vilka lagkrav som finns. Företag och leverantörer som tillhandahåller samhällsviktiga tjänster omfattas av NIS-direktivet. Myndigheter har högre krav på informationssäkerhet än andra företag och de avsätter därför större del av sin budget för just det ändamålet.

Ungefär en sjundedel av alla företag spenderar mindre än 1 procent av sin IT budget på säkerhet. Medelbudgeten ligger på strax under 4 procent. Företag med höga krav på sin säkerhet spenderar närmare 13 procent [ITGOV].

Orange Cyberdefens har en mognadstrappa i IT-säkerhet som består av 4 steg. I deras rapport för 2021 kan man avläsa att de företag som ligger i steg 3 lägger ungefär 10 procent av sin IT-budget på säkerhet. De som är på steg 1–2 ligger under 10 procent och steg 4 på mer än 10 procent. Inga exakta siffor har presenterats [ORANGE].

2.8 De tio budorden av datoretik

Computer Ethics institute skapade under tidigt 90-tal en form av moralisk kompass för hur man ska använda en dator.

För den som inte vet var de ska börja sitt säkerhetsarbete, eller hur de ska skriva sin IT-policy, kan använda den som inspiration.

1. Du skall inte använda datorn för att göra skada
2. Du skall inte störa andra i deras datoranvändning
3. Du skall inte söka igenom andras datorer
4. Du skall inte använda datorn för att stjäla
5. Du skall inte använda datorn för att ljuga
6. Du skall inte kopiera eller använda mjukvara du inte betalt för, utan tillåtelse
7. Du skall inte använda andras datorer utan tillåtelse
8. Du skall inte hävda ägarskap för andras arbete
9. Du skall tänka på hur programmet du kodar har för konsekvenser på andra
10. Du skall alltid använda datorn på ett respektfullt sätt.

2.9 Säkerhetsmodell

En säkerhetsmodell hjälper oss att förstå komplexa säkerhetsmekanismer i system. Utöver detta illustrerar en säkerhetsmodell också koncept som kan användas när man designar nytt eller förändrar ett befintligt system. De fundamentala koncepten av samtliga säkerhetsprinciper faller inom tre kategorier.

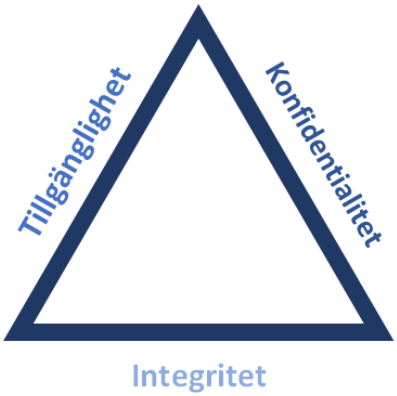


Bild 1 Säkerhetstriangel

2.9.1 Konfidentialitet

- Behörighet och autentisering
- Systemdesign/arkitektur
- Informationshantering
- Sårbarhetsanalys

2.9.2 Tillgänglighet

- Systemarkitektur
- Stabil/hållbar mjukvara
- Stabil/hållbar hårdvara
- Redundans
- Åtgärds- och återställningsplan
- Kontinuerlig förbättring
- Preventiva åtgärder

2.9.3 Integritet

- Autentisering
- Behörighetshantering
- Kontroll in indata
- Kontroll av utdata

2.10 Certifiering inom ISO27001

ISO27000 är en standard för hur företag bör arbeta med informationssäkerhet och det är möjligt för företag att certifiera sig inom ISO27001. Det är möjligt att certifiera enbart delar av organisationen eller hela. Fördelarna med att certifiera sig är:

- **Standard kring hur man arbetar med säkerhet:** ISO27000 är en standard kring hur man arbetar med IT-säkerhet och innefattar till exempel införandet av en IT-policy, hur man utför riskanalyser, åtgärdsplan, krisplan och så vidare.

- **Konkurrensfördel:** Det kan i vissa fall vara en konkurrensfördel att vara certifierade inom ISO 27001. Kunder, eller blivande kunder, till företaget vet då att företaget tar sin IT-säkerhet på allvar och har en plan vid eventuell attack.

För att ett företag ska bli certifierade inom ISO27001 krävs följande [SIS]:

- Organisationen har ett ledningssystem som uppfyller kraven för ISO27001.
- Systemet är en naturlig del av organisationens dagliga verksamhet
- Systemet är beskrivet
- System och beskrivning underhålls löpande
- Att de säkerhetsåtgärder som inkluderas i certifieringen specificeras
- Att verksamheten blir granskad mot kraven i ISO 27001 av ett godkänt certifieringsföretag

Standarden beskriver väl vilka minimumkrav som finns för dokumentation för att man ska uppfylla kraven för att bli certifierad. Det som oftast behöver dokumenteras för att uppnå minimikravet är:

- Informationssäkerhetspolicy
- Omfattningen av Informationssäkerhetsprojektet
- Metoden för hur riskbedömningen ska utföras
- Resultatet av riskbedömningen
- Vilka åtgärder man planerar utföra från ISO27001, bilaga A. Varför/varför inte och hur, samt datum
- Metoden för kontinuerlig förbättring, till exempel PDCA
- Bevis på vilka åtgärder organisationen och ledningen tagit i projektet (till exempel arkitekturmodeller, nätverkskartor) och dokumentation från styrgruppsmöten och dylikt.
- Beskrivning av styrgrupp eller liknande. Kan också vara en organisationskarta vid mindre företag
- Riskhanteringsplan som beskriver vad, hur och när något ska utföras, och av vem
- Tillvägagångssätt för att styra och granska informationssäkerhetsprojektet

Dokumentation som är hemlig, så som riskbedömningen, åtgärdsplan och annan dokumentation som innebär insyn i vad och hur något ska förändras, bör enbart vara tillgängliga för personer i projektet. Eventuella hackers ska inte kunna komma åt informationen för att på det sättet hitta eventuella säkerhetshål.

3 Policys, standarder och riktlinjer

Policys, standarder, riktlinjer, handlingsplaner och rutiner är samtliga viktiga delar i ett företag. Dessa är inte statiska dokument som skrivs och sedan finns tillgängliga i all evighet. Samtliga dokument ska vara levande och revideras med jämna mellanrum eftersom information i dem kan ändras. Om ett företag växer i storlek ändras troligen också hur man behöver arbeta på företaget gällande IT och säkerhet.

3.1 Policy

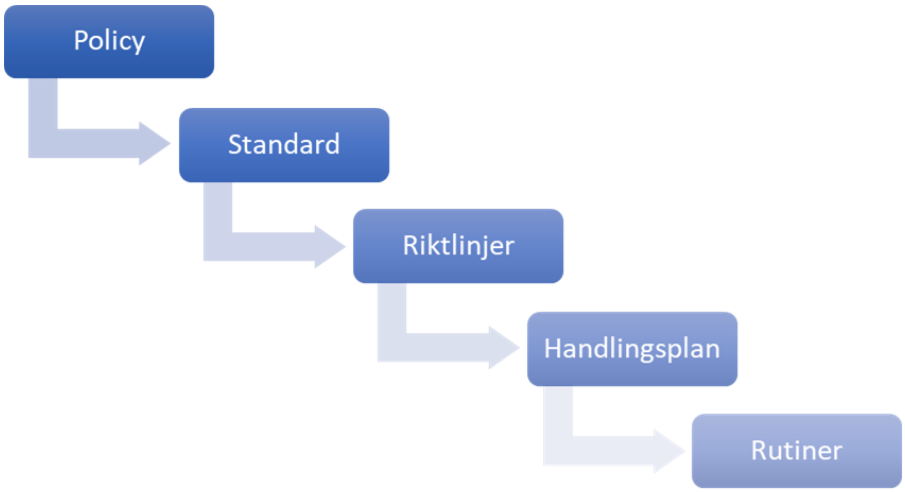


Bild 2 Nedbrytning av policy

Varje företag bör ha policys gällande vilka regler som gäller på företaget. En policy behöver inte enbart vara kopplad till IT utan kan finnas för egentligen vad som helst, exempelvis processer. Det är viktigt att hitta en avvägning av hur många policys man har. För många kan göra det svårhanterat. En del kan i stället bli en standard eller riktlinje.

Det ska alltid vara den senaste versionen som är publicerad offentligt för de anställda. Tidigare och nya versioner ska enbart vara nåbar för de som arbetar med dem.

Det är viktigt att ledningen godkänt policyn och står bakom den. Detta ska också framgå skriftligt i policyn.

3.1.1 IT-policy

En IT-policy kan innehålla allt som har med IT att göra. Både hårda- och mjuka värden. Exempel på vad en IT-policy kan innehålla:

- Syfte
- Lösenordsregler
- Användarkonton
- Behörigheter
- Regler kring användning av intern och extern hårdvara
- Användning av mjukvara/applikationer
- Stöld eller förlust av hårdvara
- Extern kommunikation om företaget
- Användning av e-post och annan intern kommunikation

- Regler kring användning av nätverket
- Hantering av data
- Rapportering av felaktigt beteende/användning
- Missbruk eller felanvändning av policyn
- Ansvarig för policyn

3.1.2 Informationssäkerhetspolicy

ISO27001 har en lista på cirka 114 punkter som ska finnas med i en informationssäkerhetspolicy. I policyn beskrivs hur man arbetar med säkerhet på de olika punkterna. Här beskrivs rubrikerna de olika delarna som ska finnas med i informationspolicyn gällande digital säkerhet:

- Granskning av informationssäkerhetspolicyn
- Roller och ansvar inom informationssäkerhet
- Mobilpolicy
- HR säkerhetspolicy
- Tillgångshantering
- Informationsklassificeringspolicy
- Media hantering
- Behörighetspolicy
- Kryptering
- Operativa processer och ansvar
- Skydd mot skadlig kod

Om certifiering inte är målet utan man enbart vill ha en informationssäkerhetspolicy för att arbeta med digital säkerhet behövs inte samtliga punkter.

3.2 Standard

En standard är gemensamma överenskomna regler för utformning eller beskrivning gällande produkter, tjänster, format, system och så liknande. Exempelvis skulle en standard kunna vara att alla digitala möten ska ske via teams eller att alla integrationer ska ske via API: er. Standarden utgår från innehållet i policyn.

3.3 Riktlinjer

Liknar standarder, men i stället för att vara en gemensam överenskommelse är de rekommendationer eller målsättningar.

3.4 Handlingsplan

En handlingsplan är sammanställning som av uppgifter och aktiviteter som tillsammans ska uppnå ett mål. Handlingsplanen ska även innehålla information om vem som är ansvarig för respektive uppgift.

3.5 Rutiner

Kan vara en instruktion eller en mall. Kan baseras på uppgifter från en handlingsplan

4 Åtgärder för ökad säkerhet

Åtgärderna för att öka sin digitala säkerhet kan vara många. Tekniska lösningar är det första många tänker på men det kräver också administrativa förändringar, så som förändringar i processer. Uttrycket ”En kedja är inte starkare än dess svagaste länk” kan användas även inom säkerhet. Om inte alla i en organisation är medvetna om risker och arbetar med säkerhet är företagets information inte säker.

4.1 Ledningen

ISO27000 lägger stor vikt vid att företagets ledning ska vara delaktig och även ta ansvar för säkerheten på företaget. Det ska vara tydligt att de står bakom de säkerhetsinitiativ som utförs på företaget samt eventuella policys. Precis som för de anställda, är det viktigt att ledningen följer de regler och policys som är uppsatta. I de bästa av världar föregår ledningen med gott exempel och är förebilder.

4.2 Zero-Trust

Med Zero-trust menas att processer och system inte ska lita på någon och konfigurera nätverk och system efter den principen. Ge inte högre behörigheter än som krävs. Kontrollera alltid att det är rätt sändare/mottagare av information. Öppna bara brandväggen för det som behövs, om det behövs.

4.3 Anställning

4.3.1 Nyanställning

Det ska finnas processer och rutiner för vad ska göras när en ny person börjar. Är det någon skillnad om personen är en konsult eller anställd. Hur får den anställde veta vilka policys som finns på företaget? Vilka behörigheter ska den anställde ha och hur får de tillgång till dem? Skapa en checklista på steg som måste göras inför en nyanställning och av vem. Allt ska finnas dokumenterat.

4.3.2 Tillfällig anställning

Det finns anställningar där personen ska vara tillfälligt anställd. Till exempel praktikant, sommarjobbare eller konsulter. Alla dessa anställningar har ett slutdatum. För en konsult kan slutdatumet ändras både framåt och bakåt i tiden. För att säkerställa att de inte kommer åt information efter de avslutat sitt arbete bör de ha ett slutdatum och om personen är tänkt att arbeta längre än först avtalat är det bättre att beställa förlängning av kontot. Om det glöms bort, vilket är vanligt enligt min erfarenhet, är det säkrare att kontot avaktiveras än att det kan användas för att komma in på företagets interna system.

4.3.3 Byte av roll

På större företag är det vanligt att anställda byter roll/tjänst. Gamla behörigheter ska avbeställas och nya beställas. Vem ansvarar för de olika stegen? Det måste finnas en process kring hur det arbetet ska ske och vem som har vilket ansvar. Utöver behörigheter måste det också bestämmas vad som händer med eventuell hårdvara som den anställde har.

4.3.4 Terminera anställning
Det händer sällan, men ibland behöver man kunna terminera en anställd. Om den anställde har misskött sig. Eftersom det ofta sker abrupt är det viktigt att det finns en process som beskriver avaktivering av kontot och andra säkerhetsåtgärder som måste utföras. I dessa lägen finns inte alltid möjligheten att vänta på en avslutningsprocess då den kan ta längre tid och har flera förberedande steg.

4.3.5 Avsluta anställning
När den anställde slutar ska kontot avbeställas. Vems ansvar är det att se till att behörigheter avbeställs? Hur hanteras hårdvara, som telefon och dator när en person slutar? Det behöver finnas en process för hur eventuella mejl ska hanteras.

4.4 Konton
4.4.1 Användarkonton
Samtliga användarkonton som finns i en katalogtjänst, som Active Directory, har ett ”user logon name”. Rekommendationen är att det ska vara baserat på användarens namn, men ska inte vara så enkelt att det är möjligt för någon utomstående att lista ut. Till exempel skulle mitt användar-id kunna vara neg001. På det sättet är inloggningsnamnet svårare att lista ut än om man använder sig av mailadressen. Om någon får tag på lösenordet ska det inte kunna kopplas till användaren baserat på användarens mailadress.

4.4.2 Administrativa konton
Även personer som arbetar som tekniker eller dylikt inom IT är användare av andra system, men när de administrerar servrar, databaser, nätverk eller dylikt behöver de ett annat konto, som enbart ska användas till att administrera. Dessa konton ska ligga segregerade från vanliga användarkonton. Kontona bör inte ha internetaccess eller mailadress för att minska kontonas sårbarhet.

4.4.3 Servicekonton
Servicekonton används på servrar eller databaser för att köra applikationer och utföra ett arbete. Eftersom dessa konton används av en service ska dessa lösenord inte bytas som på ett vanligt användarkonto. Då kommer tjänster, applikationer och system att sluta fungera. För att säkerställa hög säkerhet ska lösenordet vara längre än för andra konton. Se mer information i avsnitt 3.6.1. Olika applikationer och miljöer ska ha olika konton. Det vill säga produktion, test, utveckling ska alla ha separata konton. På det sättet säkerställer man om någon kommer över kontot för test kan de inte komma åt information i produktion. Dessa konton ska också vara segregerade från andra konton och inte heller ha en mailadress.

4.4.4 Återanvändning
Konton ska inte under några omständigheter återanvändas. Risken att det finns behörigheter på kontot från tidigare ägare är stor. Det kan finnas behörigheter till applikationer som registreras i respektive applikation eller lokalt.

4.4.5 Rensning av konton

Minst en gång om året bör konton och behörigheter granskas. ISO27002 rekommenderar två gånger per år, eller vid förändringar. Oanvända konton, låsta konton eller dylikt ska tas bort.

4.5 Behörigheter

För att få åtkomst till filer, system och applikationer behöver en användare bevisa att den är behörig. Oftast finns det flera olika nivåer av behörigheter i system. För att en behörighetsstruktur ska fylla sitt syfte ska en användare bara ha tillgång till det som denne behöver för att utföra sina arbetsuppgifter. Nedanstående punkter är viktigt att tänka på eller åtgärder för att öka säkerheten.

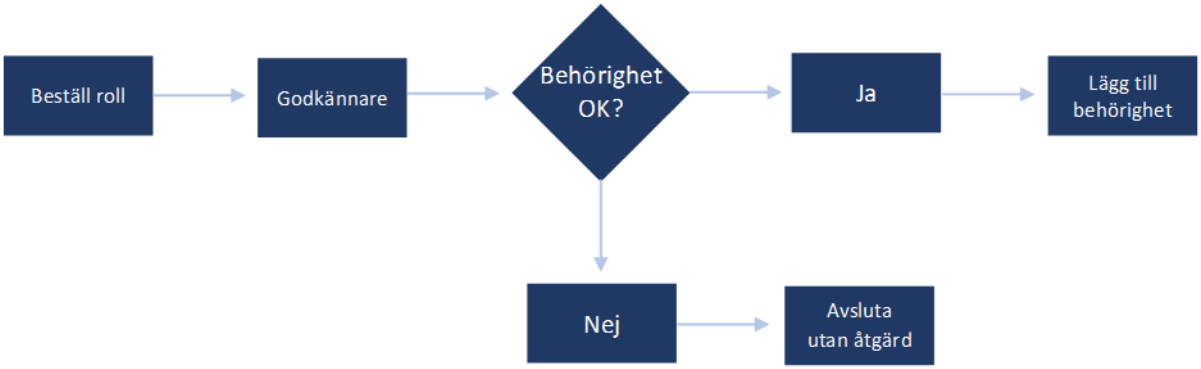


Bild 3 Process för beställning av behörighet

4.5.1 Godkännare

Behörigheter ska godkännas av någon kunnig för att säkerställa att rätt konto får korrekta rättigheter. På mindre företag kan det vara en chef och på större företag kan det till exempelvis vara en organisation eller roll som godkänner användarnas behörigheter. Se process i bild 3.

4.5.2 Avbeställa behörigheter

När en anställd slutar eller byter arbetsuppgifter ska de gamla behörigheterna avbeställas precis som beskrivet i avsnitt 4.3.

4.5.3 Roller

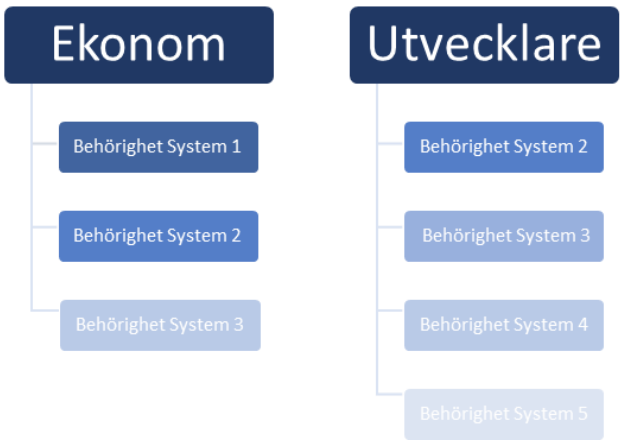


Bild 4 Beställa roller och behörigheter

Sätt upp en behörighetsstruktur baserat på de roller som de anställda kan ha. Då får de bara behörighet till det som behövs för den specifika rollen. Det gäller både behörighetsstrukturer i system och i beställningsformulär.

I stället för att beställa tillgång till system 1,2 och 3 för en ekonom är det lättare att beställa rollen ekonom. De som administrerar behörigheterna ska då ha instruktioner med vilka behörigheter som inkluderas i rollen. I detta fall behörighet till system 1,2 och 3. Se exempel i bild 4. På detta sätt är det enklare att beställa och avbeställa behörigheter. Då avbeställs en roll, inte en behörighet till ett specifikt system, vilket gör att den som lägger beställningen inte behöver veta exakt vad en roll innefattar.

4.5.4 Granskning

Behörigheter bör granskas minst en gång per år. ISO 27002 rekommenderar två gånger per år men beroende på företagets storlek och omsättningen av personal kan det vara bra att ha granskning mer sällan eller oftare [ITGOV].

4.6 Autentisering av användare

Det finns flera olika sätt att autentisera en användare. Nedan beskrivs några vanliga sätt.

4.6.1 Lösenord

När det kommer till lösenord är det viktigt att hitta en avvägning mellan olika lösenordslängder, komplexitet, byten, multi-faktor eller lösenordsfri autentisering. Inte alla varianter är nödvändiga utan man väljer de alternativ man vill implementera på företaget [MSOFT1].

- **Komplexitet:** Lösenord bör innehålla en blandning av versaler, gemener och siffror.

- **Längd:** Ju längre lösenord, desto svårare är de att lista ut eller knäcka. Rekommendationen är minst 8 tecken. För administratörskonton bör längden vara minst 12 tecken. Servicekonton bör ha minst 24 för att säkerställa hög säkerhet.
- **Undvik:** Krav på specialtecken, ääö eller liknande tecken för andra språk då inte alla system kan hantera dessa.

- **Återanvändning:** Implementera begränsning så användare inte kan återanvända lösenord. Detta går att ställa in i Active Directory, men kan behöva implementeras separat i andra system. Det är möjligt att begränsa återanvändning av de senaste x antal lösenord, eller aldrig.

- **Begränsa ord:** Begränsa användningen av vanliga ord och fraser, så som lösenord, password, 1234, qwerty, sommar, vinter, och andra vanliga ord.

- **Byte:** Rekommendationen från Microsoft för lösenordbyte är 30, 60 eller 90 dagar. Det finns även nya direktiv som säger att lösenord hellre ska vara längre och komplexa och inte ska bytas, om inte nödvändigt [MSOFT2].

4.6.1.1 Nytt lösenord

Vid nytt lösenord, ska det genereras med en lösenordsgenerator baserat på de variabler som är satta, och distribueras på ett säkert sätt så inte obehöriga får åtkomst till det.

Utöver detta bör lösenordet för användare och administratörer alltid bytas vid nästa inloggning. Även om ett genererat lösenord är säkert finns det spårbarhet när det skickats till användaren. Om någon kommer över lösenordet ska det inte kunna användas efter första inloggningen. Enbart användaren ska veta sitt lösenord.

4.6.2 MFA

MFA (Multi Factor Authentication) är en tvåstegs autentiseringslösning för inloggning. Användarna måste då verifiera att de är den de utger sig för att vara, utöver att ange lösenord. Det finns olika varianter av multifaktorinloggning. Microsoft authenticator är en app där de ska godkänna åtkomst vid inloggning. SMS med engångskod är också en vanlig lösning.

4.6.3 Lösenordsfri autentisering

Passwordless, även kallat lösenordsfri autentisering, är ett sätt att identifiera sig utan lösenord. Det finns olika typer av hårdvarunycklar eller appar som använder sig av fingeravtryck för identifiering. Microsoft har funktionen Windows Hello som via ansiktsigenkänning loggar in användaren på datorn.

4.6.4 Bank-ID

En annan typ av säker inloggning är BankID. Detta kan användas för inloggning på hemsidor. Genom identifikation av användarens personnummer och BankID-appen, som i sin tur kräver att användaren skriver in sin säkerhetskod.

4.7 Säker utskrift

Beroende på en anställdes roll på företaget har de tillgång till information av varierande klassning av konfidentialitet. För att säkerställa att utskrifter inte hamnar i fel händer finns det tjänster som Secure print. Då är ett kort kopplat till användarens login på datorn (oftast passerkort) så när de skriver ut ett dokument på datorn använder de kortet på en speciell kortläsare på skrivaren för att skriva ut dokumentet. Den andra lösningen är att de på skrivaren loggar in med sitt konto och då får möjlighet att skriva ut dokumentet.

4.8 Vit/svartlistning av applikationer

Det är möjligt att svart/vit-lista applikationer. Man behöver inte båda utan använder bara en av dem.

4.8.1 Vitlista

Precis som med en brandvägg öppnar man för det man vill tillåta, inte blockera, och på samma sätt skapar företaget en vitlista (whitelist på engelska) där man dokumenterar de applikationer som är tillåtna att använda och installera på företagets enheter.

4.8.2 Svartlista

En svartlista (blacklist på engelska) är precis som en vitlista, fast omvänd. Man dokument-erar de applikationer som inte är tillåtna. Det kan liknas med att man blockerar hemsidor man inte vill att de anställde ska komma åt, i stället för de sidor som de anställda får komma åt.

4.9 Rapportering av säkerhetsbrister

Som tidigare förklarat är säkerhet allas ansvar, vilket också betyder att det behöver råda en öppen kultur i att våga påpeka och rapportera eventuella brister. Om det inte är uttalat från ledningen ner i organisationerna kommer anställda antingen inte vilja eller våga rapportera brister. Oavsett var bristen ligger behöver det finnas tydliga tillvägagångssätt för hur dessa ska rapporteras.

Beroende på företagets organisationer kan det antingen rapporteras till respektive ansvarig för den specifika applikationen/tjänsten eller så rapporteras allt till en grupp, som i sin tur rapporterar det vidare till korrekt ansvarig.

4.10 Tillgångsägare

Bild 5 Systemlista med ägare och prioritet

Process	Namn	Prioritet 1-5	Leverantör	Miljö	Kontaktperson leverantör	Ansvarig
Operations	Teams	3	Microsoft	Molnlösning	anna.andersson@msoft.com	Neha Grundström
Marknad	Photoshop	3	Adobe	Lokalt	karl.svensson@adobe.com	Stefan Lind
Inköp	Proceedo	2	Visma	Molnlösning	eva.bjork@visma.com	Ulrika Liljekvist

Alla tillgångar i form av information, data, hårdvara, system och processer ska ha en ägare. En ägare kan exempelvis vara en person eller grupp. För att det inte ska bli konflikter i ett senare skede ska den som blir uttalad ägare förstå ansvaret och godkänna det. Av erfarenhet har jag sett att så inte alltid är fallet, att någon blir ansvarig utan att tycka att det är dennes ansvar, vilket i sin tur skaver i företaget eller organisationen.

Allt ska finnas dokumenterat och vara åtkomliga för samtliga på företaget. Det finns applikationer specifikt för ändamålet men ur kostnadssynpunkt är Excel att föredra för små och medelstora företag. I bild 5 finns ett exempel på hur systemtillgångar kan dokumenteras. Vilka rubriker som är nödvändiga beror helt på företagets behov men system, prioritet och ansvarig bör vara obligatoriskt för att fylla syftet.

4.11 Intern utbildning

Alla företag behöver ha ett sätt att sprida kunskap kring deras IT- och säkerhetspolicy samt skydda sig mot sårbarheter. Ett vanligt sätt att göra detta är att medarbetaren får läsa ett dokument om företagets IT- och säkerhetspolicy när de börjar sin anställning, och sedan aldrig igen. Eftersom informationen i dessa dokument kan förändras är det viktigt att de anställda får en regelbunden uppdatering. Minst en gång om året är att rekommendera.

Andra alternativ till kunskapsspridning är att ha en intern onlineutbildning där den anställde tar del av informationen med kontrollfrågor i slutet för att se att den anställde förstått företagets policy och vilket ansvar de har.

Specifik utbildning behövs för chefer, supportpersonal, säkerhetspersonal och andra som ska hantera säkerhetsincidenter eller risker.

4.12 Antivirusprogram

Antivirusprogram installeras på en dator och är till för att skanna efter virus och skadlig kod. Det finns flera sätt att lösa konfigureringen av programvaran. Antingen installerar och konfigurerar man det på varje enskild dator eller så går det att konfigurera centralt, vilket kan vara enklare för ett företag.

Det finns flera sätt att få in skadlig kod på ett nätverk eller försöka lura användare att ge ut personlig information. Phishing, Malware och Ransomware är tre vanliga sätt att utföra detta.

- **Phishing:** E-postmeddelande där avsändaren utger sig för att vara någon de inte är. Till exempelvis IT-avdelningen eller en tävlingsanordnare som utger sig för att behöva personlig information från användaren.

- **Malware:** Skadlig kod som oftast maskerar som en bifogad fil i ett dokument eller programvara. När man öppnar filen eller programvaran körs en kod som tar över eller hämtar information från datorn.

- **Ransomware:** Malware som krypterar filer på en server, dator eller annan plats som den skadliga koden fått tillgång till. Oftast förknippat med någon/några som sedan kräver pengar för att avkryptera informationen.

Det är viktigt att personalen utbildas i hur de undviker att hamna i dessa fällor, vilket enklast görs i den interna utbildningen. Simulera en phishing attack kan vara ett tillvägagångssätt att mäta de anställdas kunskap kring ämnet. Statistiken från en simulerad attack kan ligga till grund för hur den interna utbildningen utformas.

4.13 Nätverk

4.13.1 Brandvägg

En brandvägg är en barriär som kontrollerar trafik mellan ett internt och externt nätverk och hindrar obehörig trafik. Det finns brandväggar både i form av hårdvara och mjukvara. En blandning av dessa ger det bästa skyddet då de ger olika typer av skydd. Det är viktigt för säkerheten att det finns en brandvägg och att den fungerar för att förhindra intrång. För att den ska fylla sitt syfte, och ge bra säkerhet ska man inte tillåta mer än vad som krävs. Öppna bara de portar som behövs, eller i vissa fall enbart för specifika IP-adresser.

4.13.2 Internt trådlöst nätverk

Trådlöst nätverk finns idag på de flesta arbetsplatser. Eftersom dessa nätverk ger åtkomst till det interna nätverket på företaget ska inte externa datorer, eller obehöriga, inte komma åt det. Ett starkt lösenord är dock att rekommendera.

En annan lösning är att samtliga datorer registreras i Active Directory och att en kontroll sker om datorn finns i företagets Active Directory, eller om datorn är behörig till en specifik behörighetsgrupp.

4.13.3 Gästnätverk

Ett gästnätverk är viktigt för att externa enheter som behöver komma åt nätverket, oavsett om det är för att komma ut på internet eller interna nätverket, inte kommer åt det interna nätverket direkt med en icke företagsgodkänd enhet. Nätverket ska vara segregerat från det interna nätverket för att inte oönskade personer ska komma åt intern information eller kunna sprida virus eller dylikt.

4.14 VPN

VPN (Virtual Private Network) är en anslutning mellan två punkter som är krypterad. På det sättet kan anställda koppla upp sig från en annan plats, till företaget, på ett säkert sätt. Genom att ha en krypterad anslutning minskar man risken för att trafiken kan avlyssnas.

Nätverket på företaget måste också dimensioneras så den kan hantera den trafikmängd som tillkommer. På grund av krypteringen ökar dataanvändningen med cirka 5–15 procent beroende på vilken typ av protokoll tjänsten använder sig av [VPN].

4.15 Virtuellt skrivbord

Det finns flera varianter av virtuella skrivbord, VDI och DaaS, som kan beskrivas som en molnbaserad dator. Största skillnaden är hur de är uppsatta. VDI (Virtual Desktop Infrastructure) är en virtuell dator som är lagrad på en lokal server medan en Daas (Desktop as a Service) är ett molnbaserat skrivbord som tjänst från en leverantör.

Patchning och uppdatering kan ställas in och ske per automatik för samtliga enheter och är inte beroende av att användaren har sin dator påslagen. De är enkla att sätta upp och stänga ner och kan därför användas för en rad olika syften. En tillfällig testmiljö, dator för distansarbetare, säker och isolerad miljö för administratörer/utvecklare.

4.16 Hoppserver

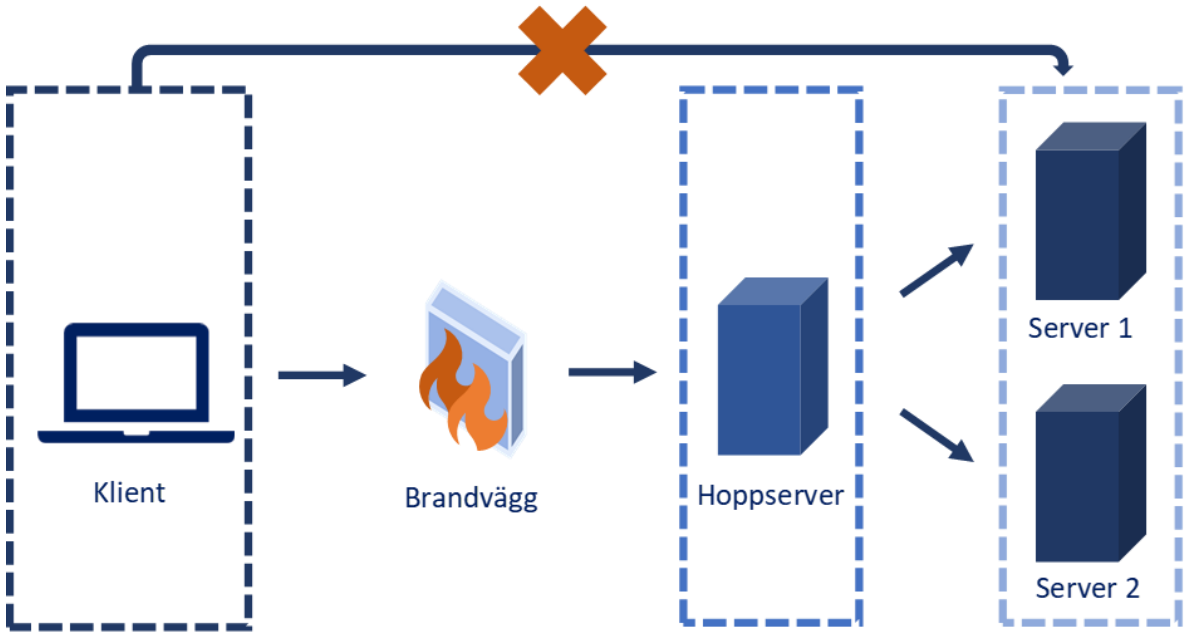


Bild 6 Arkitektur hoppserver

En hoppserver, även kallad jump server eller jump host på engelska, agerar som ett lager mellan företagets nätverk och servrar, som då ligger segregerade. För att komma åt en server måste en administratör först logga in på hoppservern, och sedan därifrån ansluta sig till servern. Som bild 6 visar ska det inte vara möjligt att komma åt en server direkt från en klientdator utan enbart från hoppservern. En hoppserver ska alltid ha MFA för att vara säker att ansluta sig till.

4.17 Kryptering

Information och data som skickas från en punkt till en annan bör vara krypterad för att förhindra att någon obehörig kan läsa eller förstå innehållet. Om texten ”Det var en gång” skickas från ett system till ett annat, utan kryptering, kan vem som helst som avlyssnar eller avbryter kommunikationen se texten, precis som den är.

Om texten i stället krypteras måste texten avkrypteras för att kunna läsas. Kryptering kan ske på flera olika sätt. Med symmetrisk- eller asymmetrisk kryptering, eller en kombination av båda, då de har för och nackdelar.

Komplexiteten av krypteringen varierar beroende på vilken algoritm och längd man väljer. Rekommenderad minsta längd är 128-bit.

Ju högre antal bit, desto svårare är det att knäcka krypteringen. Det blir svårare för att antalet möjliga krypteringsnycklar är fler, vilket i sin tur innebär att det tar längre tid att gå igenom dessa.

4.17.1 Symmetrisk kryptering

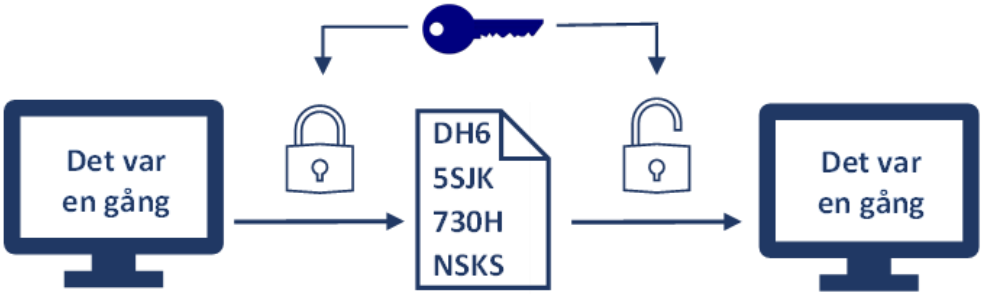


Bild 7 Symmetrisk kryptering

Med symmetrisk kryptering krypteras enbart informationen som sänds, inte från var eller till informationen ska. Meddelandet krypteras av sändaren och avkrypteras av mottagaren, med samma nyckel.

Fördelen är att det är enkelt och snabbt att kryptera informationen men mindre säkert än asymmetrisk kryptering.

4.17.2 Asymmetrisk kryptering

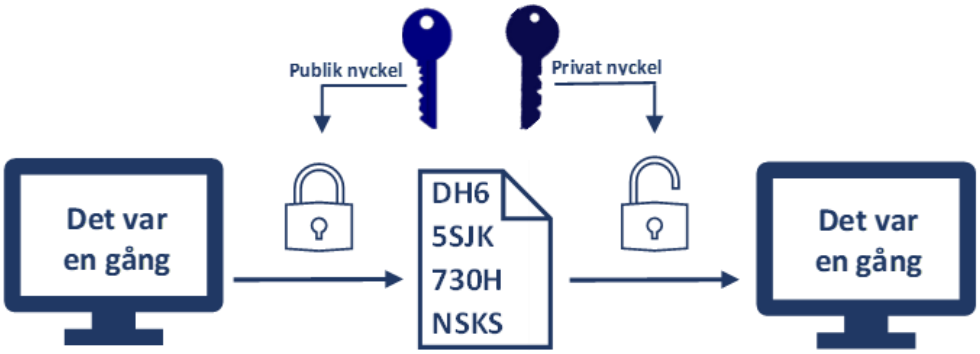


Bild 8 Asymmetrisk kryptering

Asymmetrisk kryptering kräver att varje instans som ska ta del av ett meddelande har en egen nyckel. Sändaren har en nyckel som krypterar och mottagaren har en annan för att avkryptera. Detta kan ske på flera olika sätt:

- **Kryptering:** Avsändare krypterar meddelandet med mottagarnas publika nyckel och mottagaren avkrypterar det med sin privata nyckel. Det är inte möjligt att avkryptera med den publika nyckeln utan enbart med den privata. Detta gör att om publika nyckeln hamnar i fel händer kan denne inte avkryptera meddelandet.

- **Kryptering och signering:** Avsändaren krypterar meddelandet med sin privata nyckel. Mottagaren verifierar sändaren av meddelandet med avsändarens publika nyckel och sedan med sin privata nyckel. På det sättet konfirmerar systemet att meddelandet kommer från korrekt avsändare.

Nackdelen är att det är långsamt, men höjer säkerheten och minskar sårbarheten jämfört med symmetrisk kryptering.

4.17.3 SSL/TSL

SSL (Secure Sockets Layer) och TLS (Transport Layer Security) är båda protokoll för att anslutningen och informationen på en webbplats är krypterad. Detta är extra viktigt om känslig eller personliga uppgifter från användaren behövs.

4.17.4 Hash

Hash är en form av algoritm som omvandlar data till en annan form av data. Det är vanligt att man använder en form av hashalgoritm för att spara lösenord i en databas eller vid digital signering. I stället för att orden står i klartext hashar man den. Om man använder samma algoritm får ett meddelande samma hash. ”Lösenord” skulle få hash ”88FC757BB99-A74998A3C7DE1B8181C20” med krypteringen MD5.

4.17.5 Informationssaltning

Att salta information innebär att man lägger till information innan man krypterar den. Det kan vara ett sätt att förhindra att en knäckt hash inte ger korrekt värde utan att veta vad informationen är saltad med.

Det är bra att salta lösenord innan man hashar dem. Om man saltar ordet Lösenord med 123, får Lösenord123 hashen ”AA4E6DF556B22B1D21E927A84D27EC16” med MD5 kryptering. Om någon obehörig får tillgång till hashen kan de trots det inte använda lösenordet för inloggning.

4.18 API

API (Application Programming Interface) fungerar som en bro mellan system eller system och dator för kommunikation. Information skickas i stor utsträckning från ett system till ett annat och då är API ett sätt att göra det. FTP (File Transfer Protocol) är en gammal metod för att skicka filer eller för två system att kommunicera och detta är till stor del ersatt med API: er. Det är möjligt att ha specifika stängda API:er som enbart ska kunna användas mellan system för säkert transportera data men också det som kallas för öppna API:er. Det kan vara information som man kan hämta och använda. Kollektivtrafiken kan exempelvis ha öppna API: er för att andra tjänster ska kunna använda informationen.

4.19 Backup

En kopia (backup) på data är nödvändigt för samtliga företag, oavsett storlek. Om all data sparas på samma ställe blir den sårbar. Om information blir komprimerad eller det blir något annat fel på den data som finns, är det enkelt att hämta en gammal kopia om man har en backup.

Hur ofta en kopia behöver tas beror helt på organisationen, men att ta en kopia per dag är att rekommendera. Detta är en del av riskanalysen (som presenteras i avsnitt 6) då det inte är säkert att alla system behöver ha daglig backup. Utöver att granska verksamheten och deras behov är det också bra att fundera på följande:

- Tiden det tar att göra en backup.
- Tiden det tar att återställa en backup.
- Jämförelsen med andra typer av återställning av data

4.19.1 Personlig backup

Varje anställd bör ha en plats, som inte är lokalt på datorn, där deras data är lagrad. Microsoft har sin OneDrive-tjänst där allt som sparas i dokument, bilder och så vidare på datorn synkroniseras till molnet. Det finns även andra tjänster som kan användas. Om användarens dator går sönder eller byts ut ska användarna inte bli av med sin data. Det är också möjligt att aktivera säkerhetskopiering för vissa av dessa tjänster, för andra kan det vara en tilläggstjänst. Då är det möjligt att återställa tidigare versioner av filerna om så behövs.

4.19.2 RAID

RAID (Redundant Array of Independent Disks) är en metod för att skapa redundans för hårddiskar. Det finns flera olika typer av varianter av RAID. 1,5,6 är de vanligaste. Samtliga innebär att man speglar information på en eller fler diskar. RAID 1 speglar en disk med en annan, vilket innebär att om en hårddisk går sönder kan den enkelt ersättas med en annan och informationen är fortfarande intakt. RAID 5 och 6 innebär spegling på flera diskar, men har till skillnad från RAID 1, felkorrigeringsdata. Det är det vanligaste alternativet för servrar.

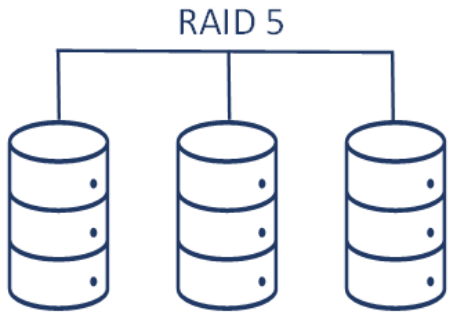


Bild 9 RAID 5 med tre hårddiskar

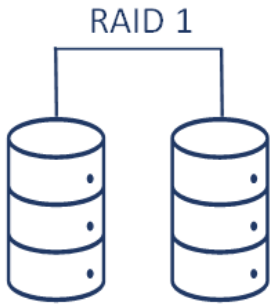


Bild 10 RAID 1 med två hårddiskar

4.19.3 Molnlösningar

Molnlösningar har ofta någon form av säkerhetskopiering, eller så är det en tjänst som enkelt går att koppla på. Om informationen ligger på en server som är placerad i Irland ligger kopian också där.

4.19.4 Extern kopia

Att ha en kopia på sin data är viktigt för att säkra att den finns kvar om det oväntade händer. Om företaget har egna serverhallar är det av yttersta vikt att det finns redundans, helst i samma stad så den är enkel att komma åt. Vid en kris ska man inte behöva besöka en annan stad.

Om man har en molnlösning som ligger i AWS, Azure eller liknande kan det i stället vara bra att ha en kopia på en annan plats. Antingen lokalt, eller i ett annat land

4.19.5 Lokal kopia

En lokal kopia, det vill säga en kopia som inte finns på företagets nätverk, är viktigt utifall det värsta händer. Syftet är att om företaget blir hackat och man blir utslängd från sin egen miljö, eller den interna miljön inte är tillgänglig ska det finnas en kopia någon annanstans som är möjlig att använda för att kunna fortsätta verksamheten.

4.20 Maximum inloggningsförsök

Varje system bör ha en gräns på maximalt antal felaktiga inloggningsförsök. När gränsen är nådd låses kontot under en viss period, Exempelvis 20 minuter. Genom detta säkrar man ett system för intrångsförsök om det sker genom att testa en användares lösenord.

4.21 Sessionstider

Sessionstider kan låta som en värdslig sak att bry sig om, och som användare kan man lätt bli irriterad när en ruta kommer upp och säger att man blir utloggad om x antal minuter om ingen aktivitet sker, men det har ett bra syfte ur säkerhetssynpunkt. Fördelen med detta, förutom att det inte finns öppna sessioner i en databas, är att om användarna glömmer logga ut eller stänga ner fönstret ska det inte vara möjligt att komma åt systemet med användarens inloggning.

Det ska alltid vara möjligt för en användare att logga ut och avsluta sin session om denne vill eller behöver.

4.22 Applikationsmiljöer

Produktion, test, och andra applikationsmiljöer ska alltid vara separerade. De ska ligga på separata servrar och data ska sparas i olika databaser. Det ska dessutom vara separata inloggningar till de olika miljöerna. Det ska inte vara möjligt att komma åt produktion om man enbart har behörighet till testmiljön, utan varje miljö ska vara separerade både ”fysiskt” och med behörighetsstyrning. De miljöer som inte behöver finnas online på det interna nätverket, till exempel utvecklingsmiljöer, bör inte vara det. Det är för att förhindra attacker och skadlig kod.

4.23 Loggning och spårbarhet

Det tar det i snitt 200 dagar innan ett företag upptäcker att de blivit utsatta för en cyberattack och i snitt 87 dagar att lösa problemet [IBM]. Med tydliga processer och bra loggning kan det upptäckas och åtgärdas snabbare. Det görs genom att logga händelser. Vem som gjort vad och när. Det kan ske på en rad olika detaljnivåer. Spårbarhet är viktigt dels för att lösa eventuella problem, dels som bevis.

4.23.1 In- och utloggning

In- och utloggning i ett system är viktigt att kunna spåra, så är även misslyckade inloggningsförsök. Då finns det spårning av ett eventuellt hackningsförsök eller om någon försökt logga in med någon annans användaruppgifter.

4.23.2 Konton och behörigheter

När en användare och/eller behörigheter läggs till, ändras eller tas bort ska detta loggas. När, vad som ändrats och av vem måste vara tydligt.

Beställningar av behörigheter ska finnas spårbara för att säkerställa att processen följts och vid eventuell kontroll.

4.23.3 Informationsförändring

När data läggs till, ändras eller tas bort ska detta loggas. När, vad, var och av vem. Det är för att supporten ska kunna felsöka men också för spårbarhet om något händer. Förändringar ska alltid kunna härledas tillbaka till en fysisk person.

4.23.4 NIDS

Network Intrusion Detection System (NIDS) är en programvara som skannar aktivitet på nätverket för att hitta potentiella sårbarheter eller möjliga attacker mot nätverket. Det finns både aktiva och passiva varianter.

4.23.4.1 Passiv

Passiv NIDS monitorerar och analyserar nätverkstrafiken och genererar larm om något suspekt hittas. Det är förhållandevis lätt att sätta upp en passiv NIDS vilket gör att det är enkelt även för mindre företag att installera en.

4.23.4.2 Aktiv

En aktiv NIDS är konfigurerad för att automatiskt stoppa trafik som är felaktig eller farlig. En nackdel med aktiv NIDS är att den kan stoppa även godkänd trafik vilket kan leda till att användare blir blockerade till sådant de har behörighet till.

4.23.5 SIEM

Security Information and Event Management (SIEM) är ett realtidssystem för att hämta, analysera, kontrollera och presentera loggar och larm genererade av olika nätverksdelar, så som routrar, NIDS, servrar och dylikt. Då systemet behöver mycket konfiguration för att fungera, och också någon som kan kontrollera loggarna och larmen är det inget man börjar med, men är ett bra verktyg att ha då det kan analysera en stor mängd trafik.

4.24 Penetrationstester

Penetrationstester kan göras på flera olika typer av IT-lösningar. Exempelvis nätverk och applikationer. Det innebär att någon, oftast utomstående, identifierarar och hittar sårbarheter i IT-miljön genom att på ett säkert och kontrollerat sätt simulera en attack. Eftersom den som utför testet ska vara opartisk kommer det sannolikt rapporteras fel och åtgärder som intern personal inte sett eller reflekterat över.

5 Upphandling

Som företag är det viktigt att inkludera säkerhet redan i upphandlingsfasen av ett nytt system. Det görs via en analys av det faktiska behovet innan upphandlingen genomförs. Om det finns ett krav på att data inte får sparas på servrar i ett specifikt land eller att det måste vara MFA-inloggning till applikationen, ska detta framgå i kravställnigen. Detta ska då också gälla för samtliga av leverantörens underleverantörer [UPPMYH].

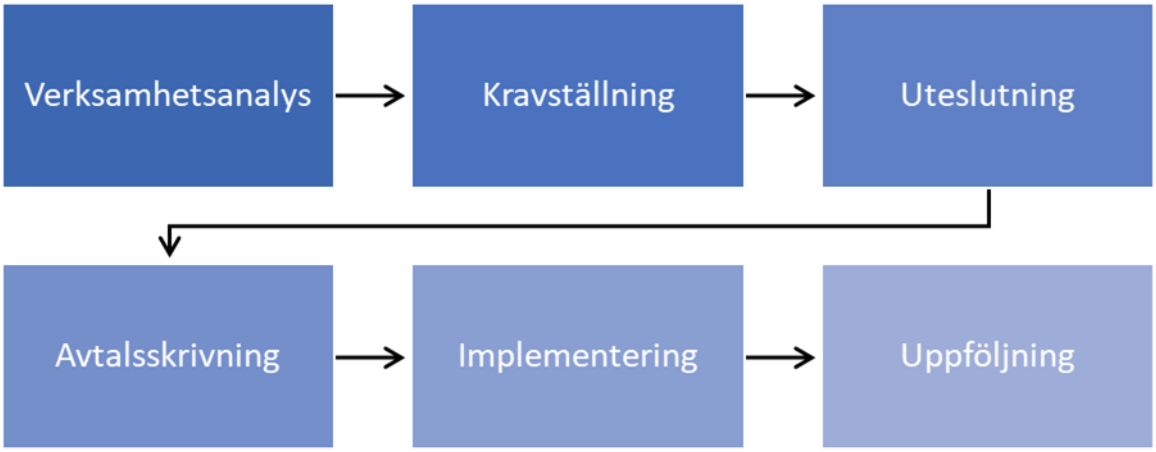


Bild 11 Upphandlingsprocess

5.1 Förberedelser

För att en upphandling ska bli så bra som möjligt är det viktigt med förberedelserna. I det här steget analyseras behoven och om en upphandling verkligen behövs, eller om det går att lösa på annat sätt. För att göra detta behöver man sätta samman en arbetsgrupp där alla på något sätt har en åsikt eller användning av det som ska upphandlas. Det som är viktigt att ta med i analysen är:

- Mål och syfte
- Värde och behov
- Nuläge
- Kostnader

Utöver att analysera behoven är det också viktigt att analysera riskerna. Exempel att undersöka är:

- Finansiella risker
- Verksamhetspåverkan
- Konsekvenser
- Sannolikhet

5.2 Genomförande

Genomförandefasen är högt beroende av att en grundlig analys av behovet är utfört. Säkerhet ska vara en del av processen vid en upphandling och kravställning. Kraven kan vara både funktionella och icke funktionella.

- **Detaljkrav:** Detaljerade krav på hur tjänsten ska utföras.

- **Funktionskrav:** Krav på funktionalitet. Vad som ska utföras för att nå önskat resultat, inte hur något ska uppnås.
- **Standarder:** Standarder kan användas vid upphandling för att det ska bli tydligt för både företaget och leverantören vad en tjänst ska innehålla.

5.3 Uteslutning

När inkomna anbud inkommit är det dags att utesluta leverantörer. Det är vitalt att jämföra anbuden mot de krav som är ställda i genomförandefasen. Här får inte nya krav ställas utan uteslutningen får enbart ske med de krav som redan är satta i tidigare skede.

5.4 Uppföljning

När leverantören är vald och avtalet är skrivet är det dags för uppföljning, så man säkerställer att leverantören kan leverera det som är avtalat. Det bör också genomföras regelbundna uppföljningar efter implementationen, så att de fortsatt levererar det som är avtalat.

6 Kontinuerlig förbättring

ISO27001 låter företag själva bestämma hur och i vilken ordning de ska utforma och implementera kontinuerlig förbättring. Enda kravet är att arbetet är strukturerat och dokumenteras. I tidigare versioner av ISO27001 rekommenderades ett processbaserat tillvägagångssätt för att utföra detta. Denna modell kallas PDCA (Plan-Do-Check-Act). Modellen liknar DEVOPS, metoden som används för utveckling och drift, det vill säga att man kontinuerligt planerar, testar, implementerar förändringar, utvärderar resultatet/får återkoppling och sedan börjar om cykeln. Se bild 12 för visuell representation.

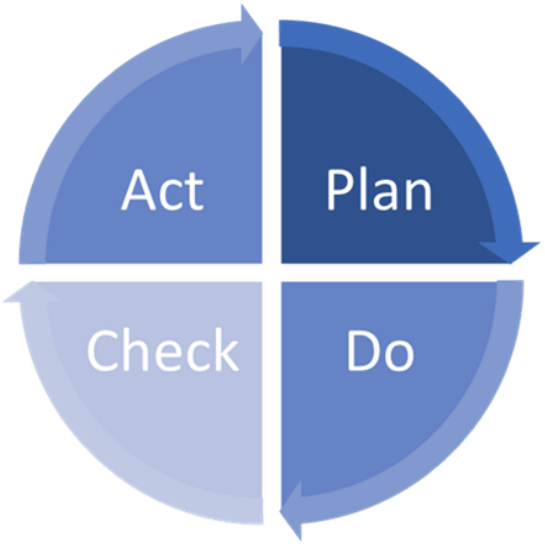


Bild 12 PDCA cykel

6.1 Plan – Planera

- Skapa ett ramverk för vad som ingår i projektet och dess omfattning
- Definiera företagets organisation, både intern och extern
- Identifiera behoven
- Skapa en plan för kontinuerlig förbättring
- Beskriv vad och hur arbetet ska dokumenteras
- Definiera resurser, roller och ansvar
- Gör en riskbedömning av företagets information och data och värdera dem
- Identifiera och utvärdera lösningar för objekten i riskbedömningen
- Gör en plan för vad som ska implementeras och när baserat på riskbedömningen
- Kommunicera risk- och implementationsplanen med berörande organisationer.

6.2 Do – Göra

- Säkerställ att riskbedömningen och implementationsplanen är korrekt och görbar
- Färdigställ dokumentationen
- Påbörja implementeringen av åtgärderna i riskbedömningen
- Säkerställ resursers tillgänglighet
- Implementera hantering och processer kring säkerhetsincidenter
- Uppdatera policys

6.3 Check – Utvärdera

- Övervaka
- Inspektera
- Testa
- Granska

6.4 Act – Agera

- Utkomsten av testningen och granskningen bör granskas av ledningen
- Om något behöver förändras, så som risker, miljöer, teknologi, implementation och/eller dokumentation ska detta göras i detta steg, för att sedan gå tillbaka till planeringsfasen och påbörja en ny cykel med PDCA.

6.5 Kommunikation

Utöver att planera, göra, utvärdera och agera, måste också kommunikation ske inom företaget. Rekommendationen för ISO27001 ser ut så här:

- Kommunikationen ska avge en vision av säkerhetsarbetet. Varför det är viktigt, vad de legala åtagandena är, hur det kommer påverka företagets verksamhet och hur det ska fungera när projektet är klart.

- Kommunikationen ska ske med regelbundna intervaller från ledningen och nedåt i organisationen. Den här typen av kommunikation bör bli en del av de redan existerande processer för informationsspridning, så som gruppmöten.

- Hitta tillvägagångssätt och forum för att få snabb återkoppling på eventuella fel och brister. Beroende på företag kan detta innefatta både från interna och externa personer.

- Viktiga händelser och annan typ av information bör gå ut i någon form av offentlig kanal på företaget. Till exempel ett intranät.

7 Identifiera, analysera och värdera risker

Det här är planeringsfasen i PDCA. I det här steget analyseras risker och sårbarheter för att sedan fortsätta med göra, utvärdera och agera. Det är av yttersta vikt att arbetet dokumenteras och distribueras till berörda personer.

7.1 Roller

För att kunna identifiera, analysera och värdera risker och sårbarheter är det viktigt att ha rätt personer med sig i arbetet. Ett effektivt sätt att göra detta är att skapa en grupp med personer från olika delar av organisationen på företaget, och på olika nivåer. På stora företag kan detta dock bli svårt och många inblandade och då kan det vara lättare att ta det organisation för organisation. Det är viktigt att ta med även de delar som inte har ett specifikt system eller processansvar men som ändå kommer bli påverkade. Till exempel supportpersonal. Av egen erfarenhet är det en grupp som lätt kan glömmas bort i den här typen av arbete, men som alla vänder sig till och förlitar sig på.

7.2 Identifiera

Det finns många aspekter att titta på när man analyserar och identifierar risker. Här har jag beskrivit vad ISO27001 rekommenderar.

7.2.1 Verksamhetsanalys

- Informationssäkerhetsarbetet innefattar hela företaget och dess organisationer. I verksamhetsanalysen granskar man de faktorer som kan påverka säkerheten. Utöver att granska verksamheten måste man också titta på de mål man har, hur infrastrukturen ser ut och vilka risker som finns. De tre punkterna som ska ligga för grund i arbetet är:

- Interna intressenter: Vem eller vilka påverkas av informationen och dess tillgångar. Vilka krav de har på informationssäkerhetsarbetet. Kan vara alla från VD, systemägare, projektledare, supportpersonal eller specifika grupper inom företaget.

- Interna förutsättningar: Kan vara nästintill vad som helst inom företaget som påverkar eller påverkas. Exempelvis policys, standarder, processer och system.

- Informationstillgångar: hård- och mjukvara, hemsidor och dokument som påverkas av förändringen.

7.2.2 Omvärldsanalys

I omvärldsanalysen granskas faktorer utanför företaget som kan påverka företagets kontroll. I analysen är det framför allt tre punkter att titta på.

- Externa intressenter: Personer, grupper eller företag som påverkas eller har krav på informationen som hanteras eller utför säkerhetsarbetet.

- Externa förutsättningar: Tekniska, exempelvis molntjänster, samhället, ekonomiska, politiska och miljömässiga förutsättningar.

- Rättsliga krav: Lagar och förordningar, myndigheters krav och lokala kommunala regler.

7.2.3 Risk och sårbarhetsanalyser

Riskanalyser utförs på system eller processer. Riskerna hittas genom en kreativ men strukturerad process, där riskerna och potentiella händelser som kan leda till negativa konsekvenser beskrivs. Det kan vara exakt vad som helst. Redan från start bör ledningen vara med för att identifiera särskilt prioriterade risker som påverkar utformningen av arbetet och särskilt vilka delar som behöver finnas på plats omgående.

7.2.4 Acceptanskriterier

Ibland kan förlusten av en säkerhetsrisk vara mindre än kostnaden att åtgärda den och i det läget är det viktigt att ha acceptanskriterier. Om det blir en dyr utveckling eller man inte ser att det är en risk om det inte ger en viss påverkan på verksamheten. Det kan vara om det kostar mindre att underhålla än att bygga till/bygga nytt. Ett acceptanskriterium kan vara att risken är okej om det kostar företaget under en viss summa pengar.

7.2.5 Riskbedömning

När riskerna och sårbarheterna är hittade ska man riskbedöma dem. Utifrån analysen får man en lista på prioriterade åtgärder. Riskbedömningen görs oftast med två utgångspunkter. Sannolikheten för att händelsen inträffar och hur stor konsekvensen blir. Det är viktigt att komma ihåg att det inte är en absolut sanning utan enbart en estimering.

Konsekvens	
1	< 50 000 kr
2	50 001 - 100 000 kr
3	100 001 - 200 000 kr
4	200 001 - 400 000 kr Skadat rykte
5	> 400 001 kr Skadat rykte

Bild 13 Konsekvensbedömning

Konsekvensen kan vara mer än direkt ekonomisk förlust. Det kan också innebära minskat förtroende från kunder och leverantörer eller eventuell kostnad för vite om man inte uppfyller lagkrav. Bild 13 förklarar ekonomisk förlust för de olika konsekvenserna.

Riskbedömningen ska utifrån kriterierna konsekvens och sannolikhet och värderas med hjälp av en matris. Samtliga kriterier ska vara tydligt definierade så samtliga risker behövs likvärdigt. I bild 14 nedan finns det fem steg i både konsekvens och sannolikhet. Om både konsekvens och sannolikhet är hög får den en hög siffra och anses därför vara kritisk att åtgärda. Om siffran blir låg bör åtgärden hamna långt ner på prioritetslistan.

Hur många kriterier som behövs beror helt på hur stort företaget är. För ett litet företag kan det räcka med tre steg, låg, mellan och hög, medan för medelstort eller stort företag kan de behöva sju steg.

		Konsekvens				
		1 Mycket låg	2 Låg	3 Medium	4 Hög	5 Mycket hög
Sannolikhet	5 Mycket hög	5	10	15	20	25
	4 Hög	4	8	12	16	20
	3 Medium	3	6	9	12	15
	2 Låg	2	4	6	8	10
	1 Mycket låg	1	2	3	4	5

Bild 14 Riskmatris

7.2.6 GAP-analys

En GAP-analys görs för att analysera skillnaden mellan hur säkerheten ser ut nu och det önskade läget. Gapet kan vara både stort och litet. Det i sin tur skapar en åtgärdslista med punkter som behöver förbättras.

7.2.7 Åtgärdslista och åtgärdsplan

Efter analysen och värderingen av risker är utförda och GAP-analysen är gjord är det dags att skapa en åtgärdslista och åtgärdsplan.

En åtgärdslista är utfallet av vad som behöver göras i det man kommer fram till i GAP-analysen. Vad behöver företaget göra för att gå från nuvarande situation till önskad situation. Åtgärderna skrivs ner i en lista med prioritet, datum för utförande och vem som är ansvarig.

Åtgärdsplanen är som en detaljerad projektplan som visar på vad som ska utföras när och av vem. Det är viktigt att allokera resurserna som behövs innan implementeringen påbörjas.

8 Kontinuitetshantering

Under en attack eller annan typ av kris är det viktigt att ha en plan för hur man ska hålla verksamheten fungerande under tiden man löser problemet. Det är inte alltid nödvändigt att hela verksamheten ska vara fungerande i dessa lägen utan bara de kritiska delarna. Vilka de kritiska systemen och processerna är, ska vara framtagna i identifikations- och analysfasen. Det är mycket viktigt att allt dokumenteras så det är nåbart för samtliga inblandade. Responsgruppens kontaktuppgifter måste dokumenteras och vara nåbar även utanför företagets nätverk då det är de personer som ska kontaktas vid en eventuell kris.

8.1 Analysera olika scenarion

En kris eller katastrof kan ha flera orsaker och det är viktigt att man analyserar olika scenarion som kan uppstå och göra en riskanalys baserat på dessa scenarion. Det kan vara om man får ransomware, virus eller något annat som anses vara ett rimligt scenario. Här är det bara att spotta ut sig tankar och scenarion, även om de kan tänka sig vara orimliga. Beroende på företagets storlek kan det behöva finnas en eller flera planer för olika delar av organisationen.

8.2 Nertid

Eftersom alla verksamheter ser annorlunda ut kan olika system ha olika lång nertid innan det skapar tillräcklig stor förlust för företaget för att anses som kritiskt. Det är viktigt att veta hur länge ett system kan vara otillgängligt då det har påverkan på både kontinuitets- och krisplanen. Ett system som kan ligga nere en dag behöver inte ha en lika snabb responsplan som ett system som enbart kan vara otillgängligt i en timme. Det har en påverkan på hur systemen ska konfigureras och vilken nivå av säkerhet de behöver.

8.3 Responsgrupp och responsplan

Alla system som klassas som kritiska enligt kontinuitetsplanen måste också ha en responsgrupp om någonting händer. Om det finns en extern leverantör som har hela eller delar av den tekniska kompetensen är det viktigt att även de är delaktiga i arbetet.

8.3.1 Responsgrupp

Gruppen innefattar alla de som har en roll för att få systemet att fungera och granska informationen. Det vill säga att det är inte enbart tekniker som ska finnas med i en responsgrupp utan också personal från verksamheten och en eller flera ledare som kan leda gruppen under krisen och se till att arbetet flyter på och att samtliga har det de behöver för att utföra sitt arbete. Det är också viktigt att ha eventuella reservpersoner med som antingen kan ta över stafettpinnen vid vila eller om någon av ordinarie tekniker inte är tillgängliga.

8.3.2 Responsplan

När en responsgrupp finns måste en plan för hur man ska hantera en kris skapas. Vem ska göra vad och i vilken ordning. Eftersom det inte är möjligt att förutspå hur länge arbetet kommer fortgå måste man också planera för raster och vila. Det måste skapas handlingsplaner och rutiner med en checklista.

Det måste finnas en plan för både hur man får en fortsatt fungerande verksamhet och hur man under tiden ska lösa den riktiga krisen. Det kan vara att temporärt sätta upp en hemsida medan man återställer miljön som blivit påverkad. Resultatet av accepterad nertid kommer ha påverkan på responsplanen.

8.3.3 Bevishantering

Det är viktigt att det finns loggar och annat för att hitta bevis på att en attack faktiskt har hänt, vad som hänt och när. Det ska sedan ligga som grund för eventuell incidentrapport och framtida åtgärder. Om en polisanmälan leder till rättegång måste bevis finnas för att styrka händelsen.

8.3.4 Intern kommunikation

Om ett företag blir utsatt för en attack och delar eller hela verksamheten blir påverkad på ett sådant sätt att systemen blir obrukbara måste detta kommuniceras. Oberoende på hur en attack sker och hur stor påverkan det har finns det en vikt av att ha en kommunikationsväg som är utanför företagets interna kommunikationsvägar. Vid en eventuell attack kan de interna kommunikationerna möjligen vara avlyssnade eller obrukbara.

Om en leverantör är ansvarig för hela eller delar av systemet inkluderas de här.

8.3.5 Extern kommunikation

Det är viktigt att eventuella kunder, leverantörer och liknande får veta hur situationen ser ut vid en kris. Ärlighet och transparens är viktigt och bidrar ofta till ökat förtroende.

8.3.6 Testa responsplanen

Det är också viktigt att både teoretiskt och praktiskt testa planen på riktigt och se att den fungerar. Att testa planen i teorin bör göras först för att sedan utvärdera resultatet. Efter det bör man göra en praktisk övning där man testar allt från kommunikation till slutförande av handlingsplanen.

Det rekommenderas att ha en krisövning minst en gång per år för att uppdatera kunskaperna och även lära ny personal vad som ska ske vid en kris.

I de fall man har en extern leverantör är det viktigt att testa krisplanen även med dem för att säkerställa att de förstår sin roll.

9 Säker förvaltning- och utvecklingsprocess

Som nämnt tidigare är säkerhet allas ansvar, vilket betyder att alla i en förvaltning och utvecklingsprocessen måste tänka säkerhet. Det är inte hållbart att enbart mjukvaruarkitekten och/eller systemförvaltaren har det i åtanke utan det ska genomsyra hela processen.

9.1 DevSecOps

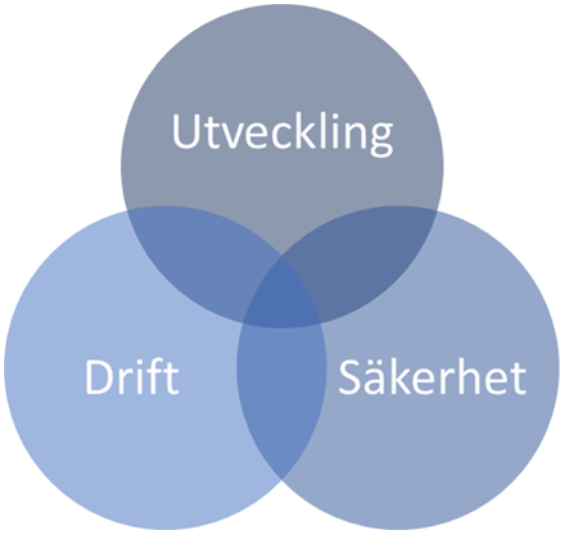


Bild 15 DevSecOps samarbete

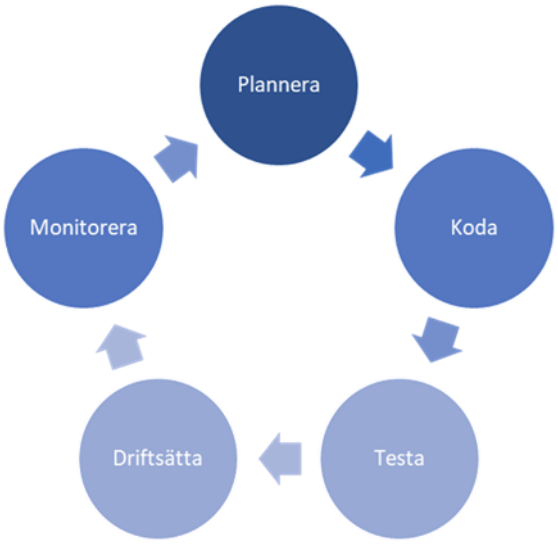


Bild 16 DevOps flöde

DevSecOps är Devops, men med genomgående säkerhetstänk. DevOps är en förkortning för Development Operations och DevSecOps står för Development Security Operations. Det är en metod för att utveckling och drift ska arbeta tillsammans i hela livscykeln med förvaltning och utveckling. Utöver detta ska det skapa effektivare processer och snabbare driftsättning av funktionalitet. Kopplat till säkerhet så ska säkerheten vara en del av hela processen och inte något som enbart kontrolleras efter produktionssättningen.

En av de stora fördelarna med Dev(Sec)Ops jämfört med andra agila metoder är att det handlar om kontinuerligt arbete, och att det ska kunna utföras med automatik. Det finns olika programvaror för att stora delar av flödet ska kunna automatiseras men väldigt få företag är där idag, men det bör vara ett mål att sträva efter för att göra processen snabbare och enklare.

9.2 Behovsanalys/kravinsamling

Utveckling, oavsett om det är nyutveckling eller förändring av en befintlig funktion, börjar oftast med ett behov hos verksamheten. Redan i behovsanalysen ska man tänka på säkerhet. Vad vill användaren göra och varför? Finns det sårbarheter som måste undersökas innan utvecklingen påbörjas.

9.3 Utveckling

9.3.1 Lösningsförslag

Innan utvecklingen påbörjas ska behovsanalysen vara klar. Personligen är jag en förespråkare för lösningsförslag som ett sätt att ge ett eller flera förslag på lösning på behovet. Dels för att utvecklarna ska fundera på en eller flera lösningar, dels som ett sätt att visa på de faktiskt förstått behovet. Säkerhet ska vara en del av förslaget.

Lösningsförslaget ska revideras och/eller godkännas av någon med övergripande ansvar för att se att alla aspekter är genomtänkta och inget glömts bort.

9.3.2 Kodgranskning

När koden är skriven är det dags för kodgranskning. Det kräver att det finns minst två personer som kan skriva/läsa koden då det ska göras av någon annan än den som skrivit den. I det läget är det möjligt att se om något missats eller implementerats felaktigt och åtgärda dem innan de sätts i produktion och skapar riktiga sårbarheter.

9.4 Test

Efter utvecklingen och kodgranskningen är slutförd är det dags för systemtestning. I den bästa av världar ska systemet testas från början till slut. Vad som ska testas och hur mycket måste bestämmas gemensamt av förvaltningen/projektet. Oavsett omfattningen måste förändringen som gjorts testas.

9.4.1 Systemtest

För att säkerställa att det inte går att göra fel, eller utföra arbetet på ett felaktigt sätt, ska även sådant som inte förväntas fungera testas. Om det finns flera roller i behörighetsstrukturen, kan användarna enbart se och göra det de behöver eller kan de även göra sådant de inte ska ha behörighet till.

Flödestester eller liknande kan med olika programvaror automatiseras. Det är tester som kan behöva köras för att säkerställa att de redan befintliga funktionerna i systemet fortfarande fungerar som de ska.

9.4.2 Användartest

För att säkerställa att utvecklingen faktiskt överensstämmer med behovet behöver även användarna testa funktionaliteten. Även här behöver användarna testa att utföra uppgifter eller knapptryckningar som de inte ska kunna göra, för att säkerställa att de inte kan utföra mer än bestämt.

9.5 Produktionssättning

När kravinsamlingen, utvecklingen och testningen är gjort är det dags för att produktionssätta. Om man valt att använda CI/CD i utvecklingssteget behöver ingen manuellt flytta koden från en miljö till en annan. Det är sätt att minska antalet fel och snabbare kunna produktionssätta sin kod. Annars sker detta oftast manuellt av en eller flera utvecklare. Om så är fallet måste funktioner testas igen efter de är satta i produktion för att säkerställa funktionaliteten.

9.6 Förvaltning

Även i en förvaltning är det viktigt att tänka på säkerhet men kan enkelt glömmas bort då mycket handlar om att lösa befintliga problem och det kan i vissa fall behöva gå snabbt.

9.6.1 Behörigheter

Som supporttekniker behöver man behörighet till att utföra allt i ett system för att hjälpa sina kunder vid fel och problem. Det man kan göra är att bara ge sig själv den behörighet man behöver för att göra det specifika testet eller kontrollera en specifik funktion, och sedan ta bort dem.

Den som inte behöver ha tillgång till en viss miljö för sitt arbete, bör inte ha det. Till exempel behöver inte en testare tillgång till produktionsmiljön om deras arbete inte innebär att de behöver arbeta i den miljön.

9.6.2 Temporära lösningar

Temporära lösningar, även kallat workarounds, är en lösning man antingen implementerar för att tillfälligt lösa ett problem, medan man undersöker och hittar en lösning på det faktiska felet. Temporära lösningar har en dålig vana att bli permanenta. Eftersom dessa lösningar ofta är hastigt implementerade är de sällan genomtänkta. Det är därför viktigt att antingen utveckla en riktig lösning som är säker, eller förbättra säkerheten på den temporära lösningen om den blir permanent. Annars kan det bli en sårbarhetspunkt att lösa senare.

9.6.3 Systemuppgraderingar

Systemuppgraderingar och patchningar kan lätt bli eftersatta i förvaltningsarbetet eftersom det tar tid och kostar pengar att testa och produktionssätta nya systemversioner. Av erfarenhet sker det oftast när det löser ett tekniskt problem och är inte en naturlig del av förvaltningsarbetet, vilket det borde vara. Att hålla system uppdaterade är ett sätt att säkerställa att systemen är säkra.

10 Slutsatser

Syftet med projektarbetet har varit att undersöka hur företag kan öka sin säkerhet. Vilka steg de behöver ta och vad de behöver ha i åtanke när de sätter upp eller uppdaterar system. Jag har i denna uppsats lyckas hitta lösningar på de flesta problemen i listan med de vanligaste sårbarheterna. Baserat på informationen i det här dokumentet har jag skapat en säkerhetstrappa med olika steg för att öka säkerheten, som presenteras under rubriken rekommendationer.

10.1 Teknisk, strategisk och operativa förändringar

Som presenterats flertalet gånger tidigare är tekniska lösningar inte det enda som är viktigt för att öka sin IT-säkerhet. Det spelar nästintill ingen roll hur säkra system är ur en teknisk synvinkel för om användarna inte följer de regler och processer som finns, kommer ett säkert system snabbt bli osäkert.

Säkerhet är inte något som fixas en gång, och inte igen om några år, utan för att det ska ge ett värde måste det finnas en långsiktig plan, tydliga processer och operativ support.

Om ett större säkerhetsarbete utförs tar det lång tid att utföra och är inget som görs i en handvändning utan kan ta allt från några månader till flera år.

10.2 IT budget

Hur mycket av IT budgeten som ska vigas till IT-säkerhet beror helt på företagets verksamhet och hur stort företaget är. Baserat på siffror presenterade tidigare kan cirka 4–10 procent vara ett riktmärke att hålla sig till. All kostnad är inte ren teknisk kostnad utan också strategiska kostnader, som långsiktig planering och operationella kostnader så som analyser, intern utbildning och upprätthålla redan befintliga lösningar.

10.3 Använda ISO27000 eller inte?

Fördelen med att använda sig av ISO27000 för sitt säkerhetsarbete är att man får en färdig process att följa, i stället för att skapa en egen. Standarden är framtagen för att företag på ett systematiskt sätt ska kunna arbeta med säkerhet. Det är inte ett krav utan finner man att ett annat sätt, som fungerar lika bra eller bättre, så använd det.

10.4 Ska företag certifiera sig?

Om företag ska välja att certifiera sig inom ISO27001 är upp till dem själva. Det är inte nödvändigt men det finns fördelar med att göra det. Beroende på företagets verksamhet kan det vara en konkurrensfördel. En form av kvalitetsstämpel på att företaget tar sitt, och sina kunders säkerhet på allvar.

11 Rekommendationer

11.1 Säkerhetstrappa

Just för att förbättringar bör göras i steg har jag skapat en säkerhetstrappa i fem steg med rekommendationer på åtgärder för att arbeta med säkerhet, och vilka åtgärder man kan utföra. bild 17 visar de fem stegen och vad det i stora drag fokuserar på. Börja på steg ett och när det är utfört, fortsätt med steg två och arbeta er uppåt i trappan. Vissa steg kan behöva repeteras en eller flera gånger över tid för att kontinuerligt arbeta med säkerhet.

Vad som behöver implementeras eller inte beror helt på hur företagets verksamhet och storlek. Det som presenteras i detta kapitel är enbart rekommendationer baserat på informationen som presenterats tidigare, från referenserna och egna erfarenheter.

De förslagen jag gett är till stor del processbaserade men också några tekniska. Även om system och tekniska förändringar är viktiga har jag valt att inte fokusera på dessa i säkerhetstrappan. Anledningen är att jag har tagit en generell approach och gett förslag som kommer påverka hela företaget, inte specifika system.

Företag har olika behov och det är därför inte nödvändigt för samtliga företag att gå igenom alla fem stegen. Det är möjligt att stanna på vilket steg som helst.

Min rekommendation är att välja vilket steg man strävar efter att stanna på då det finns förslag på lösningar för ”samma problem” i de olika stegen. Förslag i steg 3 kan bli redundant eller meningslös då lösningar i steg 4 kan ersätta dessa lösningar med säkrare teknik, eller process.

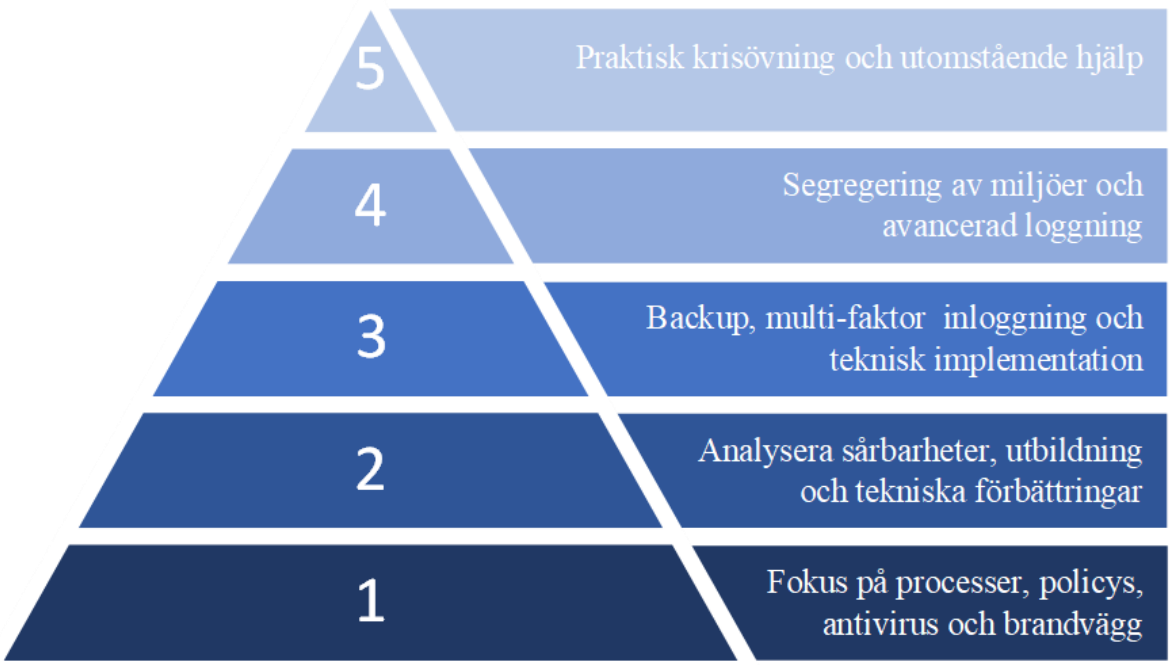


Bild 17 Säkerhetstrappa steg 1–5

11.1.1 Steg 1

Bild 18 Säkerhetstrappa steg 1

11.1.1.1 Policys

Med en policy vet alla på företaget vilka regler som gäller. Vilka krav som finns gällande IT, säkerhet och andra policys som behövs för organisationen. Men för att de anställda ska veta detta behöver man bestämma vilka typer av policys som ska finnas och dokumentera dessa och göra dem tillgänglig för samtliga på företaget.

11.1.1.2 Standarder och riktlinjer

När policys finns på plats är det dags att skapa standarder och riktlinjer. Beroende på företagets storlek kan dessa vara få eller många. Är det bestämt att man ska använda vissa typer av tjänster eller att man rekommenderar viss typ av programvara för vissa ändamål. Skriv ner dem så de är tillgängliga för samtliga som de berör.

11.1.1.3 Anställning

Att ha tydliga processer vid nyanställning, byte av roll och avslutning. Det ska vara enkelt att starta upp en nyanställd med hård- och mjukvara. När någon byter roll inom företaget, vem ansvarar för att personen inte har kvar de gamla behörigheterna och får tillgång till de nya. När någon slutar, vilka steg behövs ta för att avsluta ett konto och dess behörigheter. Denna punkt kan bli en stor sårbarhet om den inte utförs och kontrolleras med jämna intervaller.

11.1.1.4 Konton och behörigheter

- **Användarkonto:** Alla användare som ska in på det interna nätverket och ska använda företagets datorer ska ha ett användarkonto. För att en användare inte direkt ska kunna knytas till ett användarkonto ska mailadress och användar-id inte vara densamma.

- **Administratörskonto:** Samtliga administratörer ska ha ett separat konto som enbart används för att administrera med. Kontot ska inte användas för inloggning på datorer eller liknande.

- **Servicekonto:** Varje server och miljö ska ha varsitt servicekonto. Det vill säga att produktion ska ha ett konto och test ett annat och så vidare.

- **Behörigheter:** Behörigheter tilldelas enbart till personer som behöver dem, efter godkännande av ansvarig. Beroende på företagets storlek är det bra om behörigheterna är kopplade till roller. I stället för att beställa 5 olika behörigheter till en ny anställd med en specifik roll, beställer man en roll, som i sin tur har 5 behörigheter kopplade till sig. När en ny person börjar, byter tjänst eller slutar är det bara att beställa/avbeställa rollen. På det sättet är det enklare att säkerställa att rätt behörigheter blir beställda/avbeställda, och att en anställd inte tar med sig gamla behörigheter till en ny roll inom företaget.

- **Rensning:** ISO27002 rekommenderar att rensning av konton och behörigheter ska ske minst 2 gånger per år.

11.1.1.5 Lösenord

- Starka lösenord: Skapa en bra lösenordskultur där användare ska ha minst 8 tecken i sitt lösenord. Administratörskonton och servicekonton bör ha längre lösenord än vanliga användarkonton för att säkerställa att dessa är svårare att knäcka.

- Lösenordsbyte: Lösenordsbyte bör inte ske oftare än 90 dagar för att ta hänsyn till den mänskliga faktorn. Om lösenordet behöver bytas för ofta kan det vara svårt för de anställda att komma ihåg dem, eller de väljer enkla lösenord, eller det värsta av allt, de skriver ner dem. Om man väljer att ha lösenordskrav på 12 tecken är det bra att inte ha kortare än 90 dagar då det kan bli svårt att komma ihåg långa och komplexa lösenord.

- Generering av lösenord: Vid skapande av nytt konto eller om en användare glömt lösenordet ska ett nytt lösenord genereras. Lösenordet ska alltid bytas vid nästa inloggning. Ingen förutom användaren ska veta lösenordet för att minska sårbarheten om någon kommer över informationen.

11.1.1.6 Datakopia

- Personlig kopia: Allt som sparas på datorn ska säkerhetskopieras till en annan plats. Molntjänster som kopplas till användarens inloggning är vanliga för att säkerställa att om datorn går sönder ska ingen data gå förlorad.

- Server/databaskopia: Data som finns på servrar och databaser behöver säkerhetskopieras för att säkerställa företagets funktion även om ordinarie hårddiskar går sönder eller blir påverkade av en attack. Då är det möjligt att återställa informationen om så behövs.

11.1.1.7 Brandvägg

En brandvägg ska hålla oönskad trafik borta. För bästa säkerhet ska man bara öppna för de portar och IP-adresser man vill tillåta. Här är det bättre att tänka Zero-trust, det vill säga stäng ute allt du inte vill ska komma in eller som du inte litar på. Det är bättre än tvärtom, för det kan vara svårt att blockera något du inte känner till.

11.1.1.8 Antivirus
Samtliga av företagets datorer bör ha antivirusprogram installerat för att skydda datorn från skadlig kod.

11.1.1.9 Vitlista applikationer
Att ha en vitlista på godkända applikationer är ett måste. På det sättet vet de anställda vilka applikationer som är godkända att beställa/installera. Anledningen varför man ska ha en vitlista i stället för en svartlista är för att det är svårare att ha kontroll om man skriver ner de applikationer som inte är tillåtna, än omvänt.

11.1.1.10 Dokumentera tillgångar och ansvar
Tillgångar som system, processer, information ska finnas dokumenterade och ska vara åtkomlig för samtliga. Det ska finnas som stöd för att veta vilken prioritet olika system och processer har och vem som har ansvaret. I riskanalysen som finns i steg 2 kommer dokumentet till nytta.

Tydliga roller och ansvar är viktigt oavsett om det är i projekt, förvaltning eller daglig verksamhet för att processer ska fungera så felfritt som möjligt och minska antalet fel som kan leda till säkerhetsbrister eller konflikter.

11.1.1.11 Rapportering av brister
Det är viktigt att personalen förstår sitt ansvar, och det är därför väsentligt att ha en öppen kultur gällande att se och rapportera säkerhetsbrister. För att påvisa att det är något som tas på allvar är det en fördel om företaget har ett sätt för användare att kunna rapportera säkerhetsbrister.

11.1.1.12 Loggning
Loggning innebär spårbarhet av behörigheter, in- och utloggning, system eller annat som måste kunna spåras. Oavsett om det gäller att samla bevis vid en attack, se felaktiga inloggningar, kontrollera spårbarhet av behörigheter eller vid felsökning är loggning viktigt. Med bra loggning är det lätt att se om någon gjort något felaktigt.

11.1.2 Steg 2

Bild 19 Säkerhetstrappa Steg 2

11.1.2.1 Simulerad Phishing
Att man inte ska trycka på okända länkar eller öppna dokument från okända avsändare kan tyckas är känt för alla men trots det kan det vara en bra idé att ha en simulerad phishing-attack. Då får man statistik på hur många som faktiskt trycker på länkar och/eller öppnar dokument. Det kan då användas för hur man strukturerar interna säkerhetsutbildningar.

11.1.2.2 Intern utbildning
Utöver att ha en policy som beskriver vilka regler man har på företaget gällande IT och säkerhet är det också viktigt att ha någon form av intern utbildning som går mer in på djupet gällande specifika delar av säkerhet, så som cybersäkerhet. Denna utbildning ska vara obligatorisk för samtliga. Upprepning av utbildningen är ett måste av flera anledningar. Dels för att fräscha upp minnet på de anställda, dels för att säkerhetsstrategier kan ha ändrats.

11.1.2.3 Kontinuerlig uppdatering
För att säkerställa att system, servrar och databaser är säkra är det viktigt att uppgradera och uppdatera systemen.

11.1.2.4 Identifiera och analysera risker
Innan förbättring eller implementering av säkerhetsåtgärder kan påbörjas måste en riskanalys göras. I det här steget analysers vilken typ av information och data som är viktig för företaget och hur stor risk det är att de blir stulna. Om riskanalysen inte utförs kommer det bli svårt att veta vad som är viktigt för företaget och var man ska börja sina säkerhetsåtgärder.

Acceptanskriterierna är också viktiga att sätta. Med det hittar man nivåer för vad som är acceptabelt och inte. Det används som grund för att veta hur mycket tid, pengar och vilken teknologi man ska använda för att öka säkerheten.

GAP-analysen behöver också göras i detta steg för att hitta vilka åtgärder för att gå från nuvarande läge till önskat läge.

11.1.2.5 Penetrationstest
Utöver att göra en riskanalys kan det vara bra att göra penetrationstest för att hitta fler sårbarheter. Eftersom detta kan göras på både nätverk och applikationer kan det vara bra att koncentrera sig på nätverket och/eller kritiska system. Resultatet kan sedan användas som en del i riskanalysen.

11.1.2.6 VPN
Nu när hemarbete är vanligare är en VPN viktigare än någonsin. På hemmaplan har de flesta dåligt skydd. De flesta har inte ett långt och krångligt lösenord till sitt nätverk eller ännu mindre, en bra brandvägg. Om hemarbete ska godkännas i större utsträckning än innan pandemin bör det vara krav på VPN. Informationen mellan hemmet och företaget är då krypterad och det blir svårare att avlyssna trafiken. Detta är extra viktigt om de anställda hanterar känslig information, servrar eller nätverk.

11.1.2.7 Kryptering
För att säkra att information, oavsett om det är lösenord eller data som sparas eller transporteras från ett system till ett annat är det viktigt att den är säkrad med kryptering för att ingen ska kunna använda sig av informationen, om den kommer i orätta händer.

11.1.2.8 Multi-faktorinloggning för administratörer
Administratörer som har ett administratörskonto bör ha någon form av multi-faktorinloggning på dessa för att säkerställa att rätt person använder kontot. Administratörskonton är känsliga då de kan göra stor skada på företaget.

11.1.2.9 NIDS
För att få en grundläggande analys och monitorering av nätverket är NIDS ett bra och kostnadseffektivt alternativ. Det är enkelt att sätta upp och ger larm vid suspekt trafik.

11.1.3 Steg 3

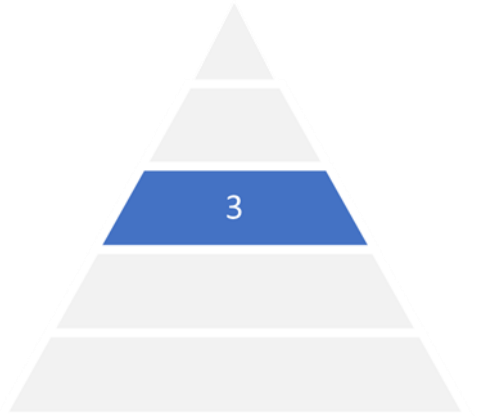


Bild 20 Säkerhetstrappa Steg 3

11.1.3.1 Extern datakopia
Utöver att ha en säkerhetskopia på sin data är det också viktigt att ha data sparad på annan plats. Helst lokal så den inte kan kommas åt från interna nätverket. Om företaget använder en molnlösning och inte har möjlighet att lagra en lokal kopia kan de via sin leverantör ha en kopia lagrad på annan ort så den inte är åtkomlig från samma plats som den första kopian om det blir några problem på den fysiska platsen eller informationen blir krypterad.

11.1.3.2 Multi-faktor inloggning för användare
Utöver att ha lösenord till datorn är det bra med någon form av multi-faktor inloggning för att den anställde på något sätt ska verifiera att användaren är den som den utger sig för att vara. Det är en utökning från steg 2 där det enbart implementeras för administratörskonton.

11.1.3.3 Virtuellt skrivbord
Virtuellt skrivbord har som förklarat tidigare fler användningsområden och i det här steget är det framför allt tänkt som en miljö för utvecklare och andra administratörer att arbeta från i stället för att ha administrativa programvaror på datorn. Den ska enbart vara nåbar med användarens administratörskonto.

11.1.3.4 Åtgärdslista och -plan
När risker och sårbarheter är analyserade är det dags att göra en åtgärdsplan. Den ska vara baserad på åtgärdslistan. Åtgärdsplanen ska innehålla allt från listan men här ska allt finnas i form av vad som ska göras av vem och datum när det beräknas vara klart.

11.1.3.5 Implementera åtgärder
Hur mycket som behöver åtgärdas beror helt på företagets mognadsgrad när det gäller säkerhet men det är viktigt att så snart som möjligt påbörja arbetet med att implementera åtgärder. Det finns ingen anledning att vänta till nästa årsskifte eller budgetarbete för då är risken stor att arbetet inte tas upp igen. Däremot kan detta steg ta lång tid beroende på hur många och komplicerade åtgärder som måste åtgärdas.

11.1.3.6 Kontinuitetsplan
Samtliga kritiska processer behöver en kontinuitetsplan om olyckan är framme och systemen går ner eller blir obrukbara. Kontinuitetsplanen måste analyseras, definieras och dokumenteras Det ska göras både en analys av verksamheten, och en krisplan om det värsta händer.

11.1.4 Steg 4

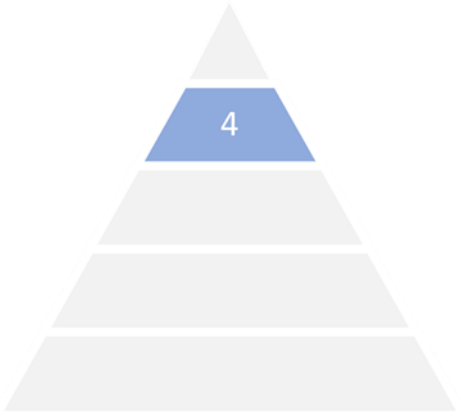


Bild 21 Säkerhetstrappa Steg 4

11.1.4.1 Teoretisk krisövning
Inget företag önskar att de ska bli utsatt för en cyberattack, men sannolikheten att man någonsin blir utsatt för ett försök är stort. Att vara förberedd är viktigt. Krisplanen beskriver hur och vem som ska göra vad, vid en eventuell attack och det är viktigt att öva för att se om krisplanen håller. Vem som har vilken roll och hur detta ska gå till väga i teorin ska vara planerat redan i säkerhetsarbetet i steg 3.

11.1.4.2 Hoppserver
För att få åtkomst till servrar bör man sätta upp en hoppserver som administratörer ansluter till, för att därifrån ansluta till den server man vill ansluta till. Det är ett säkrare sätt att ansluta sig till servrar då det ligger segregerat från servrarna och agerar som ett mellanlager.

11.1.4.3 SIEM
För att få bra loggning på hela nätverket och dess delar är SIEM ett bra verktyg. Det är mer avancerat att sätta upp än NIDS men har bra monitorering för att upptäcka felaktigheter och eventuella attacker.

11.1.5 Steg 5

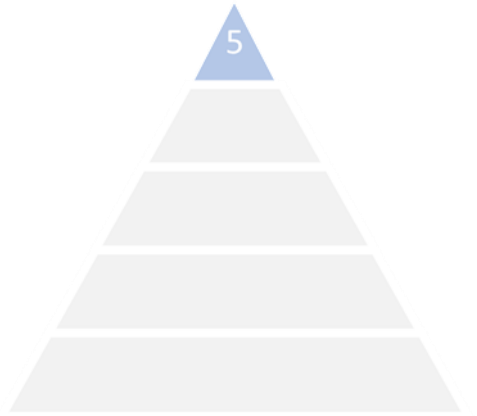


Bild 22 Säkerhetstrappa Steg 5

11.1.5.1 Praktisk krisövning

Alla som arbetat med kritiska incidenter vet att det sällan är kontrollerat för det finns ingen plan för hur det ska gå till när det händer. För att inte alla ska virra runt som yra höns när det blir skarpt läge är en krisövning ett måste. Vem som har vilken roll och hur detta ska gå till väga i teorin ska vara planerat redan i säkerhetsarbetet i steg 3 och testat i steg 4. Nu ska det testas på riktigt, i praktiken.

11.1.5.2 Ta hjälp av etiska hackare

I steg 2 rekommenderade jag att ha hjälp av en penetrationstestare för att hitta sårbarheter i IT-systemen. Det finns också andra sätt att få hjälp av etiska hackare. Allt fler företag annonserar ut att etiska hackare får försöka hacka dem och om de hittar sårbarheter och rapporterar dem får de en viss ersättning. Det kan vara ett bra sätt att få kunniga hackares hjälp utan att anställa någon.

12 Diskussion

Innan uppsatsen påbörjades hade jag en hyfsat tydlig bild av hur säkerhetstrappan skulle se ut, men när jag kom till den delen av uppsatsen blev det svårare än jag först trott. Konkurrensen om vad som skulle komma på steg 1 och 2 blev större än jag först trott och steg 3,4,5 blev svårare att värdera jämte varandra.

Från början var tanken att den skulle innehålla ungefär 60 procent teknik och 40 procent processer. Efter att ha läst om ISO27000 och läst om informationssäkerhet på internet och i böcker insåg jag att processer stod för merparten av arbetet. Så i stället blev utfallet ungefär 30 procent teknik och 70 procent processer.

Planen var att intervjua personer som arbetar med säkerhet men det visade sig vara svårare än jag trott att få personer att ställa upp. Däremot är jag övertygad att det hade varit ett bra sätt att få mer insikt i arbetet.

En förhoppning jag hade när jag började arbetet var att ha fler exempel på tillvägagångssätt men på grund av tidsbrist och bortfall av intervjuer blev utfallet inte så.

Uppsatsen blev ungefär 30 procent längre än jag först beräknat men då det var flera delar jag insåg behövdes, för att uppsatsen skulle bli komplett, valde jag att skriva allt jag tyckte var viktigt. Fler ord innebar också mer tid som behövdes för att slutföra arbetet, vilket förhoppningsvis inte har sänkt kvalitén på arbetet i sin helhet.

Det finns delar så som riskanalys, kontinuitetsplan och responsplan som jag velat undersöka mer men efter att ha läst flertalet böcker och artiklar om ämnena insåg jag att enda sättet att faktiskt få bättre förståelse för det är genom att praktiskt göra arbetet.

I slutänden är jag nöjd med det resultat jag åstadkommit på den tid jag haft och med den kunskapsnivå jag hade när arbetet påbörjades.

13 Referenser

Böcker:

[ITGOV] Calder, Alan; Watkins Steve. 2020. IT-Governance. 7. uppl. Storbritannien: Kogan Page Limited.

[CISSP] Miller, Lawrence C; Gregory, Peter H. 2018. CISSP. 3. uppl. New Jersey: JohnWiley & Sons, inc.

Hemsidor:

[OWASP] OWASP top10: https://owasp.org/Top10/

[IBM] IBM data breach report: https://www.ibm.com/security/data-breach

[ORANGE] Rapport cybersäkerhet 2021: https://orangecyberdefense.com/se/rapport-om-svensk-cybersakerhet-2021/

[SIS] ISO27000: https://www.sis.se/iso27000/dettariso27000/

[MSOFT1] Microsoft lösenordsregler: https://docs.microsoft.com/sv-se/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide

[MSOFT2] Lösenordsfri autentisering: https://www.microsoft.com/sv-se/security/business/identity-access-management/passwordless-authentication

[PASS] Vanliga lösenord: https://cybernews.com/best-password-managers/most-common-passwords/

[UPPMYH] Upphandlingsmyndigheten: https://www.upphandlingsmyndigheten.se/inkopsprocessen/

[VPN] VPN dataanvändning: https://www.security.org/vpn/does-vpn-use-data/

[HACK] Hackers: https://us.norton.com/internetsecurity-emerging-threats-black-white-and-gray-hat-hackers.html

Poddar:

[PODD1]Trygghetspodden Försvarsmakten: https://trygghetspodden-b2696783.simplecast.com/episodes/podd-78-it-sakerhet-och-cyberhotet-forsvarsmakten

[PODD2]Trygghetspodden säkerhetspolisen: https://trygghetspodden-b2696783.simplecast.com/episodes/podd-79-it-sakerhet-och-cyberhotet-sakerhetspolisen

[PODD3]Trygghetspodden polisen: https://trygghetspodden-b2696783.simplecast.com/episodes/podd-80-it-sakerhet-och-cyberhotet-polisen

[PODD4]Trygghetspodden must: https://trygghetspodden-b2696783.simplecast.com/episodes/podd-84-it-sakerhet-och-cyberhotet-must