Handbok Säkerhetsskydd för IT

Innehållsförteckning

Denna version av dokumentet skapades: 2025-02-19 15:55:41 +0100

Kapitel 1. Inledning

Handboken och relaterat material är ett projekt som skapats av projektgruppen.

Projektgruppen består av:
Tomas Carlsson LinkedIN
Joel Selinder, Selution AB
Tomas Uddenberg, Castra AB
Samt övriga deltagare som valt att inte vara namngivna.

Syftet med denna handbok (PDF och webbsida) är att underlätta för personer som arbetar med IT, IT-Säkerhet, Informationssäkerhet och projektledning genom att på ett IT nära språk beskriva vad varje "informationssäkerhetsrelaterad paragraf" i PMFS 2022:1 innebär. Målsättningen är att beskrivningarna skall vara mer konkreta än Säkerhetspolisens vägledningar och innehålla referenser till publika ramverk och dylikt som används inom IT (ISO27002, NIST, CIS etc). Det finns även en mappning mot de preliminära säkerhetsåtgärderna i NIS2 (NISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION).

Tänkt arbetssätt att man för varje paragraf i PMFS 2022:1 Kapitel 4 skall kunna få effektiv information om vad som är det huvudsakliga syftet/målet, samt hänvisning till relevanta källor för fördjupad kunskap. I t.ex. ISO27002 och NIS2 (ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION) finns en uppsjö av förslag på möjligheter att analysera fram relevanta säkerhetsåtgärder.

Det finns även referenser till fördjupad läsning i Säkerhetsskydd - En introduktion av Kim Hakkarainen Utgåva 3.

Målgruppen är primärt civil IT-intensiv verksamhet.

Frågor och feedback välkomnas.

- Maila säkerhetsguiden
- Signal

Den senaste versionen finns på http://säkerhetsguiden.se

Kapitel 2. Säkerhetsskydd

2.1. Säkerhetskänslig verksamhet

Förenklat kan man tänka att säkerhetskänslig verksamhet i huvudsak består av,

- Verksamhet som hanterar säkerhetsskyddsklassificerade uppgifter
- Säkerhetskänslig verksamhet i övrigt

Nedan följer en förenklad beskrivning av delarna, det är en **stark rekommendation** att läsa den fördjupade dokumentationen i Säkerhetspolisens vägledning och PM samt Kim Hakkarainens bok enligt referenserna sist i kapitlet.

2.2. Säkerhetsskyddsklassificerade uppgifter

Uppgifter som rör säkerhetskänslig verksamhet och därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), OSL. Uppgiftens röjande skall ha en påverkan på Sveriges säkerhet.

I verksamhet som inte omfattas av offentlighets- och sekretesslagen (2009:400) så måste man göra en fiktiv sekretessbedömning som om man ofattades av OSL. Detta är mycket svårt att göra rätt, lämpligen så görs denna sekretessbedömning av en jurist eller någon annan utbildad.

Om en uppgift blir säkerhetsskyddsklassificerad så träder omedelbart ett omfattande regelverk för hantering av uppgiften i kraft, straffen för felaktig hantering av en säkerhetsskyddsklassificerad uppgift kan vara mycket kännbara.

Säkerhetsskyddklassificerade uppgifter delas in i fyra nivåer Begränsat Hemlig, Konfidentiell, Hemlig och Kvalificerat Hemlig, där Kvalificerat Hemlig är den högsta.

Det kan finnas annan sekretess (t.ex. företagshemligheter) denna sekretess är dock inte kvalificerande för att en uppgift skall bli säkerhetsskyddsklassificerad.

2.3. Säkerhetskänslig verksamhet

> Avgörande för om en verksamhet kan anses röra Sveriges säkerhet bör vara om en antagonistisk handling (exempelvis spionerі, sabotage eller terroristbrott) skulle kunna medföra skadekonsekvenser på **nationell** nivå.
>
> — Säkerhetspolisen, Vägledning i säkerhetsskydd - Introduktion

Säkerhetskänslig verksamhet i övrigt är sådan verksamhet som kan medföra skador på nationall nivå och hota Sveriges säkerhet. En verksamhet måste genomföra en säkerhetsskyddsanalys (SSA) för att genomlysa vilka säkerhetsskyddsvärden som kan finnas och på så sätt komma fram till om verksamheten är säkerhetskänslig eller inte.

Säkerhetskänslig verksamhet i övrigt indelas i fyra konsekvensnivåer A - D, där A är den högsta.

Nivåer

Säkerhetsskyddsklassificerad uppgift och säkerhetskänslig verksamhet i övrigt indelas i olika nivåer. Dessa nivåer kan anses ungefärligen motsvara varandra enligt nedan.

Konsekvensnivå A	Kvalificerat hemlig	Synnerligen allvarlig skada för Sveriges säkerhet
Konsekvensnivå B	Hemlig	Allvarlig skada för Sveriges säkerhet
Konsekvensnivå C	Konfidentiell	Inte obetydlig skada för Sveriges säkerhet
Konsekvensnivå D	Begränsat hemlig	Endast ringa skada för Sveriges säkerhet

Referenser

Säkerhetspolisens Vägledning i säkerhetsskydd - Introduktion	5 Säkerhetskänslig verksamhet 6 Skyddsvärda uppgifter och säkerhetsskyddsklassificerade uppgifter
Säkerhetspolisens PM 2024-03-05	Vad är säkerhetskänslig verksamhet
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	1.5 Säkerherhetskänslig verksamhet 1.6 Säkerhetsskyddsklassificerad uppgift

Kapitel 3. PMFS 2022:1 4 kap. Informationssäkerhet i och kring informationssystem

3.1. Granskning vid utveckling och anskaffning

3.1.1. Granskning av egenutvecklad programvara

```
1 § Verksamhetsutövaren ska se till att egenutvecklad programvara i informationssystem
som har betydelse för säkerhetskänslig verksamhet granskas för att upptäcka och
åtgärda säkerhetsbrister och sårbarheter.
```

Syfte

Egenutvecklad programvara ska vara av hög kvalitet och vara fri från sårbarheter och säkerhetsbrister.

Vägledning

Arbetssätt för utveckling av programvara av hög kvalitet sammanfaller ofta med utveckling av säker programvara.

Utveckling av programvara som ska användas i säkerhetskänslig verksamhet medför ett stort ansvar och kan medföra stora kostnader. Egenutvecklad programvara är vanligtvis specialskriven och anpassad till verksamheten på ett sätt som gör programvaran (programkoden) känslig och som vanligtvis kräver att de personer och aktörer som deltar i utvecklingen är säkerhetsprövade.

Innan utveckling påbörjas bör man upprätta ett regelverk för säker utveckling (eng. Secure Software Development Lifercycle (SDL/SDLC/SSDLC)) som är grunden för hur programvara ska utvecklas och hur det ska ske på ett säkert sätt. Regelverket bör minst styra följande:

Bemanning och resurser

Oavsett om utveckling sker med egna anställda eller andra resurser så måste dessa personer säkerhetsprövas på ett sätt som motsvarar det deltagande i den säkerhetskänsliga verksamheten som förväntas. Användandet av andra resurser än egna anställda (t.ex. konsulter) kräver med stor sannolikhet att ett säkerhetsskyddsavtal tecknas med den externa parten (t.ex. konsultbolag). Detta kräver god planering och framförhållning då säkerhetsskyddsavtal och säkerhetsprövning är tids- och resurskrävande.

Separation av utvecklings-, test- och produktionsmiljöer är av stor betydelse. Vanligtvis så kan säkerhetsskyddsvärden (konfidentialitet, riktighet, tillgänglighet) påverkas direkt i produktionsmiljön, med separation av miljöerna så blir möjligheterna att direkt påverka säkerhetsskyddsvärdena mindre. Separationen ska vara både teknisk och administrativ, den administrativa separationen är särskilt viktig för att kunna vidta de nödvändiga åtgärderna vid driftsättning av programvaran/informationssystemet.

Teknisk separation av miljöer för säkerhetskänslig verksamhet och annan verksamhet ska som huvudregel ske genom fysisk separation (eng. air gapped). Det finns omständigheter när logisk separation är tillåten baserat på nivån av skyddsvärden. I de fall logisk separation är tillåten krävs en noggrann analys av de risker, hot och sårbarheter som uppkommer genom att använda den svagare (logiska) separationen (Se Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)

4.9.2 Separation).

Utvecklingsmiljö

Vid val av programmeringsspråk och verktyg är det viktigt att tänka på att dessa är väl etablerade och kommer att finnas tillgängliga under informationssystemets förväntade livstid. I säkerhetskänslig verksamhet är det tidskrävande och kostsamt att säkerhetspröva personal, det kan var väldigt svårt att låta externa aktörer utveckla och administrera informationssystem med betydelse för säkerhetskänslig verksamhet. Inför driftsättning måste det bedömas vilka resurser och kompetenser som behövs för att vidmakthålla beslutat säkerhetsskydd under informationssystemets förväntade livstid. Tillgång till kompetenta utvecklare är ett exempel på en sådan resurs Se PMFS 2022:1 4 Kap 4 §.

Den tekniska utvecklingsmiljön bör innehålla en så stor bredd som möjligt av relevanta säkerhetsfunktioner och användandet av dessa ska vara automatiserat och tvingande. Byggandet av programkod med kända säkerhetsbrister och risker ska automatiskt stoppas.

Modern mjukvaruutveckling kräver vanligtvis ett stort antal externa programvarubibliotek, ett flertal av dessa brukar vara öppen källkod och hämtas från Internet. Utvecklingsmiljön bör innehålla tekniska stöd och processer för att kontinuerligt riskbedöma och analysera externa programvarubibliotek. Ett första steg är att göra en förteckning av vilka externa programvarubibliotek som används (eng. SCA - Software Composition Analysis, SBOM - Software Bill of Materials, Software supply chain). Från denna förteckning kan analyser av risker och sårbarheter ske, det finns verktyg som automatiserar detta.

Det bör även finnas verktyg och processer för att tillse att funktioner i programvara används på ett korrekt sätt, detta bör automatiseras i största möjliga mån och byggandet av programkod med felaktigt nyttjande av funktioner stoppas.

Granskning

Granskning innebär att man verifierar att rutiner och regelverk för säker utveckling är definierade och har följts. Det innebär också att man testar/verifierar den tekniska säkerheten i programvaran som har utvecklats.

Granskning bör ske löpande och särskilt inför driftsättning av ny programvara eller informationssystem. Den löpande granskningen kan med fördel vara inbyggd i utvecklingsmiljön och ske så automatiserat som möjligt. En automatiserad granskning bör vara tvingande och stoppa byggandet av programvaran om fel upptäcks. Inför driftsättning bör systemet som helhet granskas och testas, rapporten från granskningen bör ingå i underlaget för beslutet om driftsättning.

Om fel och brister upptäcks vid granskning så måste en ny granskning genomföras efter att fel och brister rättats. Inför driftsättning så ska alla säkerhetsskyddsåtgärder testas och en eventuell Särskild Säkerhetsskyddsbedömning (SSB) ska uppdateras med eventuellt tillkommande (mitigerande) skyddsåtgärder.

En granskning kan även vara en granskning av programkoden (kodgranskning) eller ett penetrationstest av hela informationssystemet. Båda dessa moment kan med fördel automatiseras och vid behov genomföras av en extern kompetenspartner.

Nya säkerhetsgranskningar bör genomföras regelbundet vid varje release/driftsättning

Exempel på aktiviteter

- Teknisk säkerhetsgranskning av den egenutvecklade programvaran
- Ta fram en policy för hur organisationen hanterar säker utveckling av system och mjukvara. Baserad på relevanta standards och best practice
- Genomför hotmodellering
- Genomför riskanalys

Exempel på säkerhetsåtgärder

- Automatiserad sårbarhetsscanning av egenutvecklad programvara och tredjepartsbibliotek
- Använd OWASP Application Security Verification Standard (ASVS)
- Statisk och Dynamisk Applikationssäkerhetsanalys (SAST ,DAST ,IAST)
- OWASP Top10

Exempel på bevis

- Dokumenterade rutiner för säker utveckling
- Resultat från kontinuerlig sårbarhetsscanning
- Dokumenterad process (runbook) för hantering av upptäckta sårbarheter
- Dokumentation från driftsättning av varje version av programkoden, som ska innehålla vem som tog beslutet och vilka underlag beslutet baserade sig. Samt en bedömning om driftsättningen var samrådspliktig eller inte
- Granskningsrapporter (Administrativ, Teknisk, Extern)
- Dokumenterad hotmodellering
- Dokumenterad riskanalys
- Mappning av egna funktionella och icke funktionella krav mot välkänt ramverk (t.ex. CIS, OWASP) för att lättare kunna påvisa kravefterlevnad

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.1.1 Egenutvecklad mjukvara och säkerhetsgranskning

SS-EN ISO/IEC 27002:2022	8.25 Säker Utvecklingscykel 8.26 Säkerhetskrav för applikationer 8.27 Säker systemarkitektur och tekniska principer 8.28 Säker kodning 8.29 Säkerhetstestning i utveckling och acceptans 8.30 Utkontrakterad utveckling 8.31 Separation av utvecklings-, test- och produktionsmiljöer
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	6.2 SECURE DEVELOPMENT LIFE CYCLE
	6.5 SECURE TESTING
OWASP Application Security Verification Standard (ASVS)	https://owasp.org/www-project-application-security-verification-standard/
NIST SP 800-218 - Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities	https://csrc.nist.gov/pubs/sp/800/218/final
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.8 Programvaror och hårdvaror ska granskas

3.1.2. Hårdvara och programvara

```
2 § Verksamhetsutövaren ska se till att hårdvara och tredjepartsprogramvara i
informationssystem som har betydelse för säkerhetskänslig verksamhet granskas för att
upptäcka och åtgärda säkerhetsbrister och sårbarheter, eller att hårdvaran och
programvaran på annat sätt bedöms vara tillförlitlig från säkerhetsskyddssynpunkt.
```

Syfte

Säkerställa att anskaffad hårdvara och programvara är så säker som möjligt.

Vägledning

I säkerhetskänslig verksamhet är det viktigt att den hårdvara och programvara som används i sig själv är så säker som möjligt. Anskaffning av hårdvara och programvara måste ske på ett strukturerat sätt och följa definierade processer

Normalt så finns det styrande dokument och processer för hur inköp hanteras, det gäller att det finns en definierad säker leveranskedja (Engelska: Supply Chain). Ett av syftena med en säker leveranskedja är att det ska finnas en spårbarhet i dels vilka produkter som används men även var dessa kom från. Ursprunget och hanteringen av produkterna är av stor betydelse vid en bedömning av dessa samt ovärderlig information vid eventuella incidenter.

För att kunna upprätthålla säkerheten i produkter så behöver dessa förvaltas och livscykelhanteras, detta för att undvika att det finns produkter som inte är uppdaterade eller underhållna.

Programvara som inte är egenutvecklad är generellt sett mindre anpassad till den säkerhetskänsliga verksamheten. Den har på så sätt mindre möjlighet att påverka den säkerhetskänsliga verksamheten ju mer generell den är. Exempelvis så kan det vara svårt att granska en ordbehandlare på ett effektivt sätt, men en sådan programvara borde inte vara en kritiskt del av säkerhetskänslig verksamhet.

Om en tillverkare av programvara själva har granskat programvaran så kan man överväga om man behöver göra ytterligare säkerhetsgranskningar eller inte. Det handlar om att bedöma hur tillförlitlig leverantören och deras metoder är. Man behöver också säkerställa att programvaran är korrekt konfigurerad när man implementerar den jämfört med när leverantörens granskning gjordes. Det är alltid den säkerhetskänsliga verksamheten som är slutligt ansvarig för att granskning är gjord och dokumenterad.

Syftet med granskning är bland annat att upptäcka:

- oönskad funktionalitet
- skadlig kod
- dold kommunikation

Vid anskaffning av programvara och uppdatering är det av största vikt att dessa hämtas från betrodda källor. Det bör vara en definierad del av en säker leveranskedja att beskriva var hämtning

kan ske och vilka rutiner som ska följas. Man bör endast använda programvara och uppdateringar som är kryptografiskt signerade.

Hårdvara behöver granskas så att eventuell fysisk manipulation och oönskad funktionalitet upptäcks.

Fysisk granskning av hårdvara för att säkerställa att den inte blivit manipulerad är väldigt svårt, det kan finnas variationer i komponenter vid tillverkning som gör att olika exemplar av hårdvara ser olika ut. Det kan även vara så att tillverkarens garantier upphör om hårdvaran öppnas för inspektion. Ett kostnadseffektivt sätt kan vara att utföra stickprov där frekvensen beror på hur känslig hårdvaran är för den säkerhetskänsliga verksamheten. Frekvensen kan bestämmas baserat på en riskanalys och/eller kopplas till klassificeringen av informationen eller informationssystemet.

Vid inköp av hårdvara minskar riskerna för riktade angrepp om man köper lagerhållen hårdvara jämfört med beställningar där hårdvara skickas direkt från tillverkare i utlandet till den säkerhetskänsliga verksamheten. Vissa tillverkare och återförsäljare tillhandahåller möjligheten att försegla kartonger och produkter som ett transportskydd. Som en del i den säkra leveranskedjan bör hårdvara hanteras på ett dokumenterat sätt redan från leverans, det kan till exempel innebära att hårdvaran inte lämnas utan kravställt fysiskt skydd och att den förseglas och registreras i samband med leverans.

I praktiken så behöver man själv granska hårdvara till en nivå som är rimlig och sedan kontinuerligt analysera och bedöma tillverkare, leverantörer och leveranskedjan. - Alla uppdateringar av hårdvara och programvara (inkl. hårdvarunära programvara) bör testas innan den införs i produktionsmiljön. Det kan vara utmanande om utveckling, test och produktion endast är logiskt separerade i samma hårdvara. Uppdatering bör ske snarast möjligt, ju mer exponering ett informationssystem har ju viktigare är det.

Exempel på aktiviteter

- Besluta rutiner för inköp som fastställer en säker leveranskedja
- Definiera en rutin för hämtning och kontroll av programvara

Exempel på säkerhetsåtgärder

- Granskning av hårdvara
- Granskning av programvara

Exempel på bevis

- Beskriven och beslutad säker leveranskedja som omfattar både hårdvara och programvara
- Inventarieregister som innehåller all hårdvara och information om hårdvaran
- Icke överskrivbart programvarubibliotek som innehåller all programvara som används
- Kvittenser från överlämning
- Dokumenterad spårbarhet i plomberingar, serienummer m.m.

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.1.2 Granskning av tredjepartsprogramvara och hårdvara
SS-EN ISO/IEC 27002:2022	5.21 Hantering av informationssäkerhet i IKT-leveranskedjan
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	6.1 SECURITY IN ACQUISITION OF ICT SERVICES, ICT SYSTEMS OR ICT PRODUCTS
Indispensable baseline security requirements for the procurement of secure ICT products and services	https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.8 Programvaror och hårdvaror ska granskas

3.2. Åtgärder inför driftsättning eller förändring

3.2.1. Test av skyddsåtgärder

```
3 § Verksamhetsutövaren ska, innan ett informationssystem som har betydelse för
säkerhetskänslig verksamhet tas i drift, genomföra tester av skyddsåtgärderna.
Resultatet ska jämföras med de säkerhetskrav som gäller för informationssystemet. Den
särskilda säkerhetsskyddsbedömningen ska uppdateras med eventuella avvikelser och de
kompensatoriska åtgärder som måste vidtas
```

Syfte

Säkerställa att informationssystemet uppfyller alla säkerhetskrav och att säkerhetsskyddsåtgärder fungerar och har avsedd effekt.

Vägledning

Vid utveckling och införande av informationssystem med betydelse för säkerhetskänslig verksamhet bör man genomföra en Särskild Säkerhetsskyddsbedömning (SSB) för att fastställa vilka skyddsvärden som hanteras och vilka säkerhetsskyddsåtgärder som behöver vidtas. En SSB gör det möjligt att analysera vilka krav som ska gälla för informationssystemet. Den Särskilda Säkerhetsskyddsbedömningen (SSB) blir därmed ett viktigt styrande dokument för utvecklingen av informationssystemet.

Inför driftsättning måste informationssystemet testas för att se att kraven uppfylls och att säkerhetsskyddsåtgärderna är effektiva och fungerar som tänkt. Om kraven inte uppfylls eller säkerhetsskyddsåtgärderna inte fungerar som tänkt så måste SSB uppdateras med resultaten och vilka nya säkerhetsskyddsåtgärder som behöver vidtas. Dessa nya säkerhetsskyddsåtgärder ska testas innan driftsättning.

Själva beslutet att genomföra driftsättningen behöver vara väl dokumenterat och det ska framgå vem (person, funktion) som fattat beslutet. Det är även viktigt att beslutet tar ställning till om driftsättningen (ändringen) är samrådspliktig. Rent generellt krävs en högre nivå av dokumentation vid en driftsättning i säkerhetskänslig verksamhet än vid till exempel ITIL Change eller DevOps.

Exempel på aktiviteter

- Tester av kraven på informationssystemet
- Genomför samråd med Säkerhetspolisen vid behov (Konfidentiell/Konsekvensnivå C eller högre)
- Särskild Säkerhetsskyddsbedömning (SSB)

Exempel på säkerhetsåtgärder

Exempel på bevis

- Särskild Säkerhetsskyddsbedömning (SSB)
- Testrapporter
- En förändringsprocess (ex. ITIL Change) där driftsättningsbeslut och samrådsbeslut ingår
- En rollbeskrivning för den person eller funktion som beslutar om driftsättning

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.2.1 Verifiering av funktions- och säkerhetskrav
SS-EN ISO/IEC 27002:2022	8.29 Säkerhetstestning i utveckling och acceptans 8.32 Ändringshantering
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	6.4 CHANGE MANAGEMENT, REPAIRS AND MAINTENANCE
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.9 Skyddsåtgärderna ska testas före driftsättning

3.2.2. Resurser och kompetenser i förvaltning

```
4 § Verksamhetsutövaren ska innan ett informationssystem som har betydelse för
säkerhetskänsligverksamhet tas i drift, bedöma vilka resurser och kompetenser som
krävs för att bibehålla fastställt säkerhetsskydd under informationssystemets
förväntade livstid
```

Syfte

Säkerställa att kompetenser och resurser finns under informationssystemets förväntade livstid.

Vägledning

Utveckling och drift av informationssystem och programvara kräver tillgång till kompetens och resurser över tid. Innan driftsättning av ett informationssystem måste en plan finnas för hur kompetens och resurser ska säkerställas för att vidmakthålla säkerhetsskyddet under systemets förväntade livstid.

I många fall finns det en projektmodell som knyter an till en förvaltningsmodell, dessa brukar ha inslag av resursplanering och kompetensförsörjning. Om detta inte finns i tillräcklig omfattning måste man skapa en dokumenterad plan för detta separat.

Deltagande personal måste ha kompetens för de IT-komponenter som ingår och även hur man använder dessa på ett säkert sätt, exempelvis genom att känna till sårbarheter och kunna omhänderta dessa.

Val av teknik bör styras av tillgången på kompetens, att kunna få tag på resurser med rätt kompetens som kan säkerhetsprövas över lång tid är avgörande för att bibehålla säkerhetsskyddet. Lika viktigt är val av leverantörer.

Med resurser menas även separata miljöer för test, utveckling och drift, samt datahallar som lever upp till kraven på fysiskt skydd och kontinuitet.

Exempel på aktiviteter

- Skapa en förvaltningsplan för informationssystemet inkluderande bemanning och övriga resurser
- En arkitektur för systemet inklusive separerade miljöer för utveckling, test och produktion
- Datahallar som uppfyller kraven (från SSA/SSB)

Exempel på säkerhetsåtgärder

Exempel på bevis

- Bemanningsplanering inklusive kompetenser
- Resursplanering inklusive separerade miljöer och datahallar

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.2.2 Bedömning av behov av kompetenser och resurser
SS-EN ISO/IEC 27002:2022	8.31 Separation av utvecklings-, test- och produktionsmiljöer
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	1.1 POLICY ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS (e)
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.10 Resurser och kompetenser som krävs under informationssystemets livstid 6.2.2 Utbildningsplan

3.3. Rutiner för hantering av informationssystem

3.3.1. Fastställda rutiner

```
5 § Verksamhetsutövaren ska fastställa rutiner för hanteringen av informationssystem
som har betydelse för säkerhetskänslig verksamhet under systemets förväntade livstid.
```

Syfte

Säkerställa att rutiner för hantering av informationssystemet finns.

Vägledning

Det ska finnas beslutade rutiner för hanteringen av informationssystemet under systemets förväntade livstid.

Med hantering menas drift, underhåll, incidenter och livscykelhantering.

Styrning av hanteringen kan baseras på standardramverk så som exempelvis PM3 och ITIL, dessa måste dock anpassas till den specifika organisationen och informationssystemet för att säkerställa säkerheten under systemets förväntade livstid.

Styrningen ska vara fastställd och dokumenteras skriftligen. Det ska även finnas en beskrivning av vilka roller som finns och vilket ansvar och befogenheter respektive roll har.

Vid förändringar i informationssystemet är det viktigt att säkerhetsfunktioner inte påverkas negativt. Det är även viktigt att testa ändringar i en miljö som är separat från produktionsmiljön.

Ramverket ITIL används flitigt inom it och är en bra grund för att strukturera och definiera rutiner för hantering av informationssystemet.

- Felhantering: Problem management (ITIL) https://wiki.en.it-processmaps.com/index.php/Problem_Management
- Förändringshantering: Change Management (ITIL) https://wiki.en.it-processmaps.com/index.php/Change_Management
- Uppdateringar: Release and Deployment Management (ITIL) https://wiki.en.it-processmaps.com/index.php/Release_and_Deployment_Management
- Incidenthantering: Incident management (ITIL) https://wiki.en.it-processmaps.com/index.php/Incident_Management
- Kontinuitetshantering: IT-Service Continuity Management (ITIL) https://wiki.en.it-processmaps.com/index.php/IT_Service_Continuity_Management
- Livscykelhantering: IT-Service Lifecycle management (ITIL)

Exempel på aktiviteter

- Skapa styrning för att hantera drift och underhåll (Exempelvis, Felhantering, Förändringshantering, Livscykelhantering inkl. uppdateringar, kontinuitetshantering)

Exempel på säkerhetsåtgärder

Exempel på bevis

- Bemanningsplanering inklusive kompetenser
- Rollbeskrivningar inkluderande ansvar och kompetenser
- Processer och rutiner för felhantering
- Processer och rutiner för förändringshantering
- Processer och rutiner för uppdateringar
- Processer och rutiner för incidenthantering
- Processer och rutiner för kontinuitetshantering
- Processer och rutiner för livscykelhantering

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.3 Rutiner för hantering av informationssystem
SS-EN ISO/IEC 27002:2022	5.37 Dokumenterade driftsrutiner 7.13 Underhåll av utrustning 7.14 Säker Avveckling eller återanvändning av utrustning 8.31 Separation av utvecklings-, test- och produktionsmiljöer 8.32 Ändringshantering
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	6.4 CHANGE MANAGEMENT, REPAIRS AND MAINTENANCE
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.11 Rutiner för hantering av informationssystemet

3.4. Granskning av säkerheten

3.4.1. Årlig granskning

```
6 § Verksamhetsutövaren ska årligen granska säkerheten i ett informationssystem som är
avsett för att behandla säkerhetsskyddsklassificerade uppgifter i
säkerhetsskyddsklassen hemlig eller kvalificerat hemlig eller i informationssystem som
är av motsvarande betydelse för Sveriges säkerhet.
```

Syfte

Säkerställa att säkerheten upprätthålls och att krav efterlevs över tid.

Vägledning

I granskning så ingår uppföljning och kontroll, såväl administrativ som teknisk, av att system hålls uppdaterade och att styrning för hantering av systemet följs.

Systemets säkerhetsfunktioner och säkerhetskonfigurationer ska verifieras genom exempelvis säkerhetsgranskning, sårbarhetsscanning och penetrationstester. Syftet är att säkerställa att de säkerhetskrav som fastställts i den särskilda säkerhetsskyddsbedömningen (SSB) uppfylls över tid.

Över tid kan nya hot och sårbarheter uppstå, det kräver en kontinuerlig granskning och uppdatering av säkerhetskrav och säkerhetsåtgärder.

För att uppnå oberoende i uppföljning och kontroll så bör denna genomföras av en intern kontrollfunktion eller extern part.

Exempel på aktiviteter

- Kontrollera efterlevnad av fastställda hanteringsrutiner Se hanteringsrutiner
- Kontrollera användarnas efterlevnad av de regler och rutiner som reglerar hur informationssystemet får användas
- Sårbarhetsscanning av systemet för att upptäcka sårbarheter
- Omvärldsbevakning för att upptäcka nya hot

Exempel på säkerhetsåtgärder

Exempel på bevis

- Granskingsrapporter av användares efterlevnad
- Rapporter från säkerhetsgranskning, sårbarhetsscanning och penetrationstester
- Uppdateringar av SSB/SSA

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.4 Granskning av säkerheten
SS-EN ISO/IEC 27002:2022	5.35 Oberoende granskning av informationssäkerhet 5.36 Efterlevnad av policyer, regler och standarder för informationssäkerhet
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	2.2 COMPLIANCE MONITORING 2.3 INDEPENDENT REVIEW OF INFORMATION AND NETWORK SECURITY
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.13 Årlig granskning av säkerheten

3.5. Unika identiteter och spårbarhet

3.5.1. Unika och spårbara identiteter

```
7 § Alla utställda identiteter i ett informationssystem som har betydelse för
säkerhetskänslig verksamhet ska vara unika över tid. Åtkomsten ska vara spårbar till
individ, system eller resurs.
```

Syfte

Identiteter ska vara unika över informationssystemets hela livstid för att säkerställa spårbarhet.

Vägledning

I ett informationssystem kan det finnas många olika typer av identiteter. Det kan vara fysisk person, servicekonton, systemkonton, lokala eller domänanslutna. Alla identiteter ska vara unika över informationssystemets hela livstid.

Delade konton som exempelvis funktions- och gruppkonton och lokala systemkonton ska kompletteras med säkerhetsåtgärder för att säkerställa vilken fysisk individ som använt kontot.

Spårbarhet till individ är speciellt viktig vid incident- och brottsutredningar. Se Säkerhetsloggning

Det är viktigt att behörigheter tilldelas strikt enligt dokumenterade processer och rutiner. Tilldelningen av behörigheter måste vara spårbar och tillförlitlig.

Stödsystem som används för tilldelning av identiteter och behörigheter måste uppfylla höga krav på riktighet och tillgänglighet under informationssystemets hela livstid.

Exempel på aktiviteter

- Kontrollera efterlevnad av fastställda processer, rutiner, regler för hantering av identiteter

Exempel på säkerhetsåtgärder

- Återanvänd inte konton
- Radera inte konton (Inaktivera)
- Kontinuerlig uppföljning av tilldelade konton och behörigheter
- Rutiner för offboarding

Exempel på bevis

- Styrande dokument för hantering av identiteter i informationssystemet
- Granskningsrapporter för identitets- och behörighetshantering

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.5 Unika identiteter och spårbarhet
SS-EN ISO/IEC 27002:2022	5.15 Åtkomstkontroll 5.16 Identitetshantering 5.18 Åtkomsträttigheter
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	11.4 ADMINISTRATION SYSTEMS 11.5 IDENTIFICATION
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.14 Behörigheter och autentisering

3.6. Behörighetsstyrning

3.6.1. Restriktiv tilldelning och årlig uppföljning

```
8 § Verksamhetsutövaren ska tilldela behörigheter som ger systemadministrativ åtkomst
eller annan särskild tillgång till informationssystem som har betydelse för
säkerhetskänsligverksamhet restriktivt. Beslut om sådana behörigheter ska fattas av
säkerhetsskyddschefen eller den han eller hon bestämmer.
Behörigheterna ska vara tidsbegränsade, följas upp och omprövas löpande, minst
årligen.
```

Syfte

Användning av höga behörigheter ska vara under strikt kontroll och minimeras.

Vägledning

Inga konton ska ha systemadministrativ behörighet som inte uttryckligen behövs.

> Tilldelning av behörigheter med systemadministrativa rättigheter ska ske restriktivt och behörigheterna vara tidsbegränsade, följas upp samt omprövas löpande, minst årligen.
>
> — Säkerhetspolisen, Vägledning informationssäkerhet Okt 2023

Se även Säkerhetsloggning

Det är viktigt att tillse att en individ inte kan erhålla behörigheter för att utföra arbetsuppgifter som är kontroll- eller säkerhetsfunktioner till varandra, exempelvis skapa logg/granska logg, storage/backup. Om organisationen har för få individer för att uppnå separation av arbetsuppgifter kan det behövas ytterligare säkerhetsfunktioner så som tvåhandsfattning.

Där det är möjligt så är det att föredra att använda ett system (exempelvis PAM, Privileged access management) som endast tilldelar höga behörigheter precis vid behov. Ett sådant system måste ha full spårbarhet på vilken individ som hade behörigheten vid vilket tillfälle under informationssystemets hela livstid.

Konton med systemadministrativa rättigheter kan finnas i windowsmiljöer, Linux/Unix, nätverksutrustning, applikationer, databaser med mera.

För att ta del av säkerhetsskyddsklassificerad uppgift eller på annat sätt delta i säkerhetskänslig verksamhet så behöver man vara behörig, se Behörig att deltaga - Säkerhetsskyddsförordning (2021:955) 2 Kap 2 §

Höga behörigheter bör ej tilldelas ordinarie användarkonton, systemadministratörer bör ha separata konton och arbetsstationen för utförandet av arbete med förhöjda behörigheter. Konton med förhöjda rättigheter och arbetsstationer avsedda för systemadministration bör ej ha åtkomst till Internet eller e-post.

Exempel på aktiviteter

- Utveckla processer och rutiner för tilldelning av systemadministrativa behörigheter
- Utbilda systemadministratörer - behörighet inte är detsamma som befogenhet
- Detaljerad genomgång av maskin/service konton
- Dokumentera hur säkerhetsskyddschefen ska besluta om behörigheter

Exempel på säkerhetsåtgärder

- Tekniskt stöd för uppföljning av tilldelning av systemadministrativa behörigheter
- System för tillfällig behörighetstilldelning (PAM)

Exempel på bevis

- En förteckning över konton med förhöjda rättigheter, vem som beslutat om dom och när omprövning senast skedde

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.6 Behörighetsstyrning
SS-EN ISO/IEC 27002:2022	8.2 Privilegierade åtkomsträttigheter
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	11.3 PRIVILEGED ACCOUNTS AND SYSTEM ADMINISTRATION ACCOUNTS
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.14 Behörigheter och autentisering

3.7. Autentisering m.m.

3.7.1. Flerfaktorsutentisering

```
9 § Verksamhetsutövaren ska se till att autentisering vid åtkomst till
informationssystem som har betydelse för säkerhetskänslig verksamhet baseras på flera
faktorer, om det inte är uppenbart obehövligt.
```

Syfte

Flerfaktorautentisiering ska användas

Vägledning

Flerfaktorautentisiering minskar risken för att obehöriga får tillgång till ett informationssystem och ska alltid tillämpas för informationssystem med betydelse för säkerhetskänslig verksamhet.

De faktorer som användaren vet eller har måste omgärdas av säkerhetskrav för att förhindra att dessa kopieras, förkommer eller sprids.

För exempelvis servicekonton och fristående datorer kan det vara svårt att implementera flerfaktorsautentisering, dessa måste skyddas genom kompletterande säkerhetsåtgärder (inlåst i säkerhetsskåp, starka lösenord, lägsta möjliga behörigheter etc.)

Om inte flerfaktorsautentisering kan användas så måste detta tydligt dokumenteras och motiveras i den särskilda säkerhetsskyddsbedömningen (SSB).

Se även Förvaring av lösenord

Exempel på aktiviteter

- Implementera flerfaktorsautentisering

Exempel på säkerhetsåtgärder

- Förvaring av fristående datorer
- Certifikatsbaserad autentisering för servicekonton och liknande

Exempel på bevis

- SSB med motivering
- Loggar som visar att MFA används vid alla inloggningar

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.7.1 Flerfaktorsautentisering

SS-EN ISO/IEC 27002:2022	8.5 Säker autentisering
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	11.7 MULTI-FACTOR AUTHENTICATION
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.14 Behörigheter och autentisering

3.7.2. Regler för lösenord

```
10 § Verksamhetsutövaren ska fastställa tekniska eller administrativa regler för
utformning, byte och hantering av lösenord, där sådana används för att ge åtkomst till
informationssystem som har betydelse för säkerhetskänslig verksamhet.
```

Syfte

Det ska finnas regler för utformning, byte och hantering av lösenord.

Vägledning

Lösenord är en relativt svag form av autentisering och det behöver finnas regler för utformning, byte och hantering av lösenord.

Regler bör innehålla minst följande

- Lösenord får inte återanvändas
- Hur och var lösenord får nedtecknas (exempelvis password manager)
- Lösenords längd och komplexitet (15 tecken eller längre)
- Standardlösenord från tillverkare måste bytas ut
- Inte återanvända lösenord i olika system eller olika säkerhetszoner
- Lösenord bör skapas med programvara som skapar slumpade lösenord av rätt längd och komplexitet

Se även Förvaring av lösenord

Exempel på aktiviteter

- Skapa standard för lösenord. Längd, komplexitet, bytesfrekvens

Exempel på säkerhetsåtgärder

- System för lösenordshantering
- Tvingande byte av lösenord
- Tvingande regler för lösenordskvalitet (längd, komplexitet, kända ord)
- Regelbunden kontroll av svaga, publicerade eller läckta lösenord

Exempel på bevis

- Loggar som visar att byte av lösenord skett

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.7.2 Autentisering med lösenord

SS-EN ISO/IEC 27002:2022	5.17 Autentiseringsinformation
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	11.6.2 AUTHENTICATION
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.14 Behörigheter och autentisering

3.7.3. Uppgifter om lösenord

```
11 § En anteckning med uppgift om lösenord som ger tillgång till informationssystem
som har betydelse för säkerhetskänslig verksamhet ska vara under kontroll eller
förvaras i ett förvaringsutrymme som verksamhetsutövaren enligt 5 kap. 10 § har
godkänt för förvaring av säkerhetsskyddsklassificerade handlingar.
```

Syfte

Lösenord ska vara under kontroll eller förvaras på ett kontrollerat sätt

Vägledning

Lösenord måste förvaras på ett sätt som gör att en antagonist inte får åtkomst till det. Om någon får åtkomst till ett lösenord så spelar det ingen roll hur starkt det är.

Lösenordet ska vara under kontroll och när det inte används så ska det förvaras i ett utrymme som godkänt för den nivå som systemet har. Under kontroll kan tolkas som inom armlängds avstånd under kontinuerlig uppsikt.

Konsekvensnivå A	Kvalificerat hemlig
Konsekvensnivå B	Hemlig
Konsekvensnivå C	Konfidentiell
Konsekvensnivå D	Begränsat hemlig

Även om lösenord förvaras krypterat så ska de förvaras i ett godkänt utrymme.

Se PMFS 2022:1 5 kap. 10 § för mer information om godkända utrymmen.

Exempel på aktiviteter

- Skapa styrande dokument för förvaring av lösenord

Exempel på säkerhetsåtgärder

Exempel på bevis

- Ett beslut på godkänt utrymme för förvaring av lösenord
- Protokoll från egenkontroller av förvaring

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.7.2 Autentisering med lösenord
Säkerhetspolisen Vägledning fysisk säkerhet (Dec 2023)	6.1.3 Förvaringsutrymmen

PMFS 2022:1	5 kap. 10 § Förvaring
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	11.6.2 AUTHENTICATION
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.14 Behörigheter och autentisering 5.6.1 Förvaringsutrymmen

3.7.4. Centrala funktioner

```
12 § Vid användning av en central funktion för identifiering eller
behörighetskontroll, ska verksamhetsutövaren se till att denna funktion ges ett
säkerhetsskydd som svarar upp mot det säkerhetsskydd som de anslutna
informationssystemen ska ha.
```

Syfte

En central funktion för identifiering eller behörighetskontroll (t.ex. Exempelvis Microsoft AD) måste skyddas

Vägledning

En central funktion för identifiering eller behörighetskontroll (t.ex. Microsoft Active Directory) måste ges samma säkerhetsskydd som de informationssystem som är anslutna till den. Anledningen är att den kan påverka autentisering och behörigheter i det säkerhetskänsliga informationssystemet.

Om en central funktion för identifiering eller behörighetskontroll faller under säkerhetsskydd så finns det en överhängande risk att allt som är anslutet till den centrala funktionen faller under säkerhetsskydd. Man behöver vara mycket vaksam på hur säkerhetsskydd kan "spridas".

Användandet av molnbaserade tjänster eller hybrider för identifiering eller behörighetskontroll till informationssystem med betydelse för säkerhetskänslig verksamhet är inte lämpligt och oftast inte möjligt. Om man använder tjänster utanför sina lokaler eller sin kontroll måste ett säkerhetsskyddsavtal upprättas med motparten.

Den centrala funktionen ska ha ett säkerhetsskydd som är i nivå med det anslutna informationssystem som har högst krav, och ska omfatta både tekniska och administrativa åtgärder.

Se även Förvaring av lösenord

Exempel på aktiviteter

- Skapa en arkitektur för säkerhet runt system för autentisering och behörighetskontroll
- Skapa en zonmodell med olika säkerhetszoner
- Dela upp funktionen för identifiering och behörighetskontroll i de olika säkerhetszonerna (blanda inte säkerhetskänslig med annan verksamhet)

Exempel på säkerhetsåtgärder

- Kontrollerad kommunikation

Exempel på bevis

- Arkitekturbeskrivning

- Zonmodell

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.7.3 Central funktion för identifiering eller behörighetskontroll
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.14 Behörigheter och autentisering

3.8. Skydd mot röjande signaler

3.8.1. Röjande signaler

```
13 § Verksamhetsutövaren ska för ett informationssystem som är avsett för att behandla
säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller
högre vidta åtgärder för att försvåra obehörig inhämtning av röjande signaler utifrån
identifierade säkerhetshot och en beskrivning av dimensionerande antagonistiska
förmågor, om Säkerhetspolisen tillhandahållit en sådan.
```

Syfte

Skydd mot röjande signaler (RÖS)

Vägledning

För informationssystem som behandlar säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre behöver man beakta förekomsten av röjande signaler. Åtgärder för att försvåra inhämtningen av röjande signaler styrs av analyser i särskilda säkerhetsskyddsbedömningen (SSB) eller i dimensionerande antagonistiska förmågor (DAF) om säkerhetsskyddsavdelningen har erhållit en sådan.

Se även,

- Säkerhetspolisens Vägledning i säkerhetsskydd – Fysisk säkerhet
- Säkerhetspolisens Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys

Skydd mot röjande signaler handlar i huvudsak om skydd av byggnader och utrymmen, i mindre omfattning utformning av informationssystem.

Exempel på aktiviteter

- Rådgör med säkerhetsskyddsavdelning

Exempel på säkerhetsåtgärder

Exempel på bevis

- En särskild säkerhetsskyddsbedömning som klargör kraven och åtgärderna

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.8 Skydd mot röjande signaler
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.15 Skydd mot röjande signaler

3.9. Kommunikationssäkerhet

3.9.1. Kontrollerad kommunikation

```
14 § Verksamhetsutövaren ska se till att informationssystem som har betydelse för
säkerhetskänslig verksamhet
1. kommunicerar på ett kontrollerat sätt med komponenter eller delsystem inom samma
informationssystem, och
2. kommunicerar på ett kontrollerat sätt med informationssystem eller nätverk som inte
omfattas av krav på säkerhetsskydd.
```

Syfte

Ha gjort ett medvetet ställningstagande till varje möjlig kommunikationsväg.

Vägledning

Kontrollerad kommunikation innebär att man först fastställer hur kommunikation ska får ske och sedan inför säkerhetsåtgärder för att säkerställa att ingen annan kommunikation sker.

Kontrollerad kommunikation kan t.ex. uppnås genom en zonmodell med olika zoner där informationssystem placeras baserat på sin klassificering och behov av kommunikation. Man kan sedan använda exempelvis brandväggar och behörighetskontrollsystem för att säkerställa att regler i zonmodellen efterföljs.

> Med begreppet "kommunicerar på ett kontrollerat sätt" avses att verksamhetsutövaren har gjort ett medvetet ställningstagande till varje möjlig kommunikationsväg.
>
> — Säkerhetspolisen, Vägledning informationssäkerhet Okt 2023

Endast definierad och nödvändig kommunikation ska tillåtas, all annan kommunikation ska förhindras. Nätverk ska segmenteras så att ingen onödig eller otillåten kommunikation kan ske, metoder som brandväggar och VLAN kan användas.

Gemensamma funktioner som exempelvis administration, loggning eller säkerhetskopiering bör finnas i egna särskilt skyddade nätverkssegment.

Där det är möjligt utan att påverka tillgängligheten t.ex. genom att begränsa felsökningsmöjligheter bör kryptering användas.

Exempel på aktiviteter

- Tillse att ändringshantering (ITIL Change) innehåller ett specifikt steg för att uppdatera dokumentationen
- Gör det till en del av incident- och krisövningar att tillse att dokumentationen är uppdaterad och finns tillgänglig

Exempel på säkerhetsåtgärder

- En brandvägg för varje nätsegment
- Ett behörighetskontrollsystem

Exempel på bevis

- Uppdaterad dokumentation av nätverk och kommunikationsvägar
- Dokumenterade ställningstaganden rörande kommunikationsvägar
- Process för att uppdatera dokumentation

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.9 Kommunikationssäkerhet
SS-EN ISO/IEC 27002:2022	5.37 Dokumenterade driftsrutiner 8.32 Ändringshantering
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	1.1 POLICY ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS - (h)
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.16 Kontrollerad kommunikation

3.9.2. Logisk separation

```
15 § Verksamhetsutövaren ska se till att informationssystem som är avsett för att
behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen begränsat
hemlig eller konfidentiell, logiskt separeras från informationssystem eller nätverk
som inte omfattas av motsvarande krav på säkerhetsskydd.
```

Syfte

Det är möjligt att logiskt separera informationssystem och nätverk.

Vägledning

Logisk separation innebär att informationssystem och nätverk separeras genom logik i stället för genom att ha separat hårdvara för varje informationssystem och nätverk. Separationen ska även gälla administrationen, om ett logiskt separerat system som inte omfattas av säkerhetsskydd i en delad hårdvara/it-miljö ska administreras utanför den säkerhetsskyddade zonen måste administrationen vara helt separat från administrationen i den säkerhetskänsliga zonen.

Separationen måste alltså finnas på alla lager i informationssystemet och måste gälla såväl informationsflöden som administration.

Även i en logiskt separerad it-miljö måste kommunikationen vara kontrollerad PMFS 2022:1 Kap4 P14 - Kontrollerad kommunikation.

Tecken på tillräcklig separation

- En mixad miljö har separat hårdvara för administration i varje säkerhetszon
- Varje virtualiserad (logiskt separerad) miljö har sin egen konfigurationsfil/databas
- Varje säkerhetszon har ett separat ingress- och/eller egressinterface

Tecken på otillräcklig separation

- Konfiguration för informationssystem eller infrastruktur i olika säkerhetszoner blandas i samma fil eller databas
- Gränssnittet (WEBB GUI, GUI-klient) för olika säkerhetszoner ansluter till samma nätverksinterface i en säkerhetszon
- En infrastrukturkomponent som kräver att alla instanser uppgraderas med samma programvara vid samma tillfälle
- Separationen styrs av ett attribut, exempelvis en användare tillhör en grupp
- Administrationsgränssnitt är åtkomliga utanför verksamhetens lokaler

Observera att detta uttryckligen gäller för säkerhetsskyddsklassificerade uppgifter, det finns inget omnämnande av motsvarande konsekvensnivå för skador på Sveriges säkerhet.

Exempel på aktiviteter

- En arkitektur som stödjer och visar hur separationen ska realiseras
- Tillse och dokumentera Kontrollerad kommunikation PMFS 2022:1 Kap4 P14 - Kontrollerad kommunikation

Exempel på säkerhetsåtgärder

Exempel på bevis

- Dokumenterad kontrollerad kommunikation PMFS 2022:1 Kap4 P14 - Kontrollerad kommunikation
- Dokumentation som beskriver hur separationen är genomförd (teknisk nivå) per komponent i informationssystemet/infrastrukturen

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.9.2 Separation
SS-EN ISO/IEC 27002:2022	8.22 Separation av nätverk 8.31 Separation av utvecklings-, test- och produktionsmiljöer
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	6.8 NETWORK SEGMENTATION
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.17 Logisk och fysisk separation

3.9.3. Fysisk separation

```
16 § Verksamhetsutövaren ska se till att informationssystem som är avsett för att
behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskydds klassen hemlig
eller kvalificerat hemlig, fysiskt separeras från informationssystem eller nätverk som
inte omfattas av motsvarande krav på säkerhetsskydd.
```

Syfte

Högre nivåer av säkerhetsskyddsklassificering tillåter inte logisk separation informationssystem och nätverk.

Vägledning

Vid nivåerna Hemlig/Kvalificerat Hemlig krävs att informationssystem och nätverk fysiskt separeras från system som inte har like höga krav på säkerhetsskydd.

Observera att detta uttryckligen gäller för säkerhetsskyddsklassificerade uppgifter, det finns inget omnämnande av motsvarande konsekvensnivå för skador på Sveriges säkerhet.

Även i en fysiskt separerad it-miljö måste kommunikationen vara kontrollerad PMFS 2022:1 Kap4 P14 - Kontrollerad kommunikation.

Kontrollerad kommunikation i en fysiskt separerad miljö kan innebära att det finns en galvanisk separation (air gap) där information förs över manuellt (band, USB minnen etc.) eller genom envägs kommunikation (Diod).

Exempel på aktiviteter

- Tillse och dokumentera Kontrollerad kommunikation PMFS 2022:1 Kap4 P14 - Kontrollerad kommunikation
- En tydligt dokumenterad arkitektur och design där det med lätthet går att förstå var separationen finns

Exempel på säkerhetsåtgärder

Exempel på bevis

- Dokumenterad kontrollerad kommunikation PMFS 2022:1 Kap4 P14 - Kontrollerad kommunikation
- Dokumentation som beskriver hur separationen är genomförd (teknisk nivå) per komponent i informationssystemet/infrastrukturen

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.9.2 Separation
SS-EN ISO/IEC 27002:2022	8.22 Separation av nätverk 8.31 Separation av utvecklings-, test- och produktionsmiljöer
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	6.8 NETWORK SEGMENTATION
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.17 Logisk och fysisk separation

3.9.4. Envägskommunikation

```
17 § Informationssystem som är separerade från andra informationssystem enligt 15
eller 16 § får genom envägskommunikation överföra data för export till eller import
från andra informationssystem.
```

Syfte

Det är tillåtet att överföra information genom envägskommunikation (till eller från)

Vägledning

Informationssystem som är separerade enligt PMFS 2022:1 Kap4 P15 - Logisk separation eller PMFS 2022:1 Kap4 P16 - Fysisk separation får överföra information till **eller** från andra informationssystem.

Det är tillåtet att föra in **eller** ut information från ett informationssystem med säkerhetsskydd till ett annat system genom en funktion för envägskommunikation oavsett om det är ett säkerhetsskyddat system eller inte. Observera ordet eller, det är inte tillåtet att föra in och ut information genom två envägsfunktioner.

Med envägsfunktioner menar man oftast en så kallad diod, en teknisk anordning som genom sin konstruktion omöjliggör att nätverkskopplingar och information kan flöda i mer än en riktning. Det är möjligt att använda andra tekniska lösningar.

Det är viktigt att envägskommunikationen beskrivs enligt PMFS 2022:1 Kap4 P14 - Kontrollerad kommunikation samt att funktionen testas. Det krävs även att den övergripande designen tillser att inte information kan flöda i två riktningar när avsikten var att ha en envägsfunktion.

En datadiod kan användas för att förhindra dubbelriktad kommunikation, samma resultat kan uppnås genom andra tekniska lösningar, exempelvis brandväggar. En datadiod kan också användas för att säkerställa att inga nätverkssessionen kan kopplas upp, i det användningsfallet borde två datadioder kunna användas för att få ett dubberiktat informationsflöde utan möjligheter till att nätverkssessioner skapas. I sammanhanget används även andra begrepp så som datasluss, datatrappa och datapump för att beskriva tekniska lösningar med liknande egenskaper.

Exempel på aktiviteter

- Tillse och dokumentera Kontrollerad kommunikation PMFS 2022:1 Kap4 P14 - Kontrollerad kommunikation

Exempel på säkerhetsåtgärder

Exempel på bevis

- Dokumenterad kontrollerad kommunikation PMFS 2022:1 Kap4 P14 - Kontrollerad kommunikation
- Dokumentation som beskriver hur envägsfunktionen är genomförd (teknisk nivå) per komponent i informationssystemet/infrastrukturen

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.9.2 Separation
SS-EN ISO/IEC 27002:2022	8.22 Separation av nätverk 8.31 Separation av utvecklings-, test- och produktionsmiljöer
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	6.8 NETWORK SEGMENTATION
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.17.3 Envägskommunikation för import och export

3.10. Konfiguration, uppdatering och dokumentering

3.10.1. Konfiguration

```
18 § Verksamhetsutövaren ska för informationssystem som har betydelse för
säkerhetskänslig verksamhet tillämpa konfiguration som använder lämpliga
säkerhetsfunktioner, stänger av funktioner som inte används och även i övrigt
reducerar sårbarheter.
```

Syfte

Informationssystem ska vara konfigurerade (inkl. säkerhetsfunktioner) på ett sätt som höjer säkerheten genom att försvåra attacker, hindra skadlig kod och upprätthålla kontrollerad kommunikation.

Vägledning

Säkerhetskonfigurering (härdning) kan bland annat innebära,
- Åtkomsträttigheter begränsas
- Möjlighet till hantering med förhöjda rättigheter begränsas
- Åtkomstmöjligheter genom infrastruktur (nätverk, virtualisering, lagring etc.) begränsas
- Exponering mot andra informationssystem eller nätverk begränsas
- Exponering mot annan säkerhetskänslig verksamhet begränsas
- Onödiga funktioner slås av eller tas bort
- Ändra autentiseringsinformation som är satt som standardkonfiguration
- Ta bort identiteter och behörigheter som inte behövs eller är osäkra

Härdningen måste anpassas till den exponering av informationssystemet och den hotbild mot verksamheten som finns. Härdning får inte inverka negativt på systemets stabilitet. Lämpligen automatiseras standardkonfiguration och härdning så långt som möjligt.

Informationssystemets exponering och hotbilden kan med fördel beskrivas i en Särskild Säkerhetsskyddsbedömning (SSB).

Härdning av ett informationssystem bör utföras enligt tillverkarens rekommendationer eller enligt något välkänt ramverk som exempelvis CIS Benchmarks eller DISA STIGs. Vid utveckling av egen programvara kan till exempel OWASP Top Ten eller OWASP Application Security Verification Standard (ASVS) användas som grund.

Först bör inbyggda säkerhetsfunktioner användas om de ger ett effektivt skydd, man bör även använda säkerhetsfunktioner i flera lager. För ett system kan man exempelvis skydda hårdvara (Fysisk säkerhet, plombering etc.), skyddad uppstartsprocess, kryptering, vitlistning av hårdvara med mera. Ett skydd i flera lager blir ett bättre skydd.

Användarvänligheten får inte medföra sårbarheter i informationssystemet. Ur ett användarperspektiv bör det vara ”lätt att göra rätt”.

Exempel på aktiviteter

- Utveckla en härdningsprocess anpassad efter verksamhetens behov, exponering och hotbild
- Skapa härdade standardkonfigurationer

Exempel på säkerhetsåtgärder

- Granskning av konfigurationer
- Funktioner för att övervaka konfigurationer
- Funktioner för att hantera konfigurationsavvikelser

Exempel på bevis

- Dokumenterad och uppdaterad härdningsprocess
- Audit rapporter

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.10 Konfiguration, uppdatering och dokumentering
SS-EN ISO/IEC 27002:2022	8.9 Konfigurationshantering
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	6.3 CONFIGURATION MANAGEMENT
Center for Internet Security® - Benchmarks	https://www.cisecurity.org/cis-benchmarks
Defense Information Systems Agency (DISA) - Security Technical Implementation Guides (STIGs)	https://public.cyber.mil/stigs/
National Security Agency - Network Infrastructure Security Guide	https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF
National Security Agency - Hardening Network Devices	https://media.defense.gov/2020/Aug/18/2002479461/-1/-1/0/HARDENING_NETWORK_DEVICES.PDF
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.19 Konfiguration för ökad säkerhet

3.10.2. Uppdatering

```
19 § Verksamhetsutövaren ska se till att programvara i informationssystem som har
betydelse för säkerhetskänslig verksamhet hålls uppdaterad så att
säkerhetsbrister och sårbarheter motverkas.
Om det finns särskilda skäl får verksamhetsutövaren besluta om undantag från kravet i
första stycket.
```

Syfte

Programvara ska vara uppdaterad för att motverka sårbarheter och säkerhetsbrister.

Vägledning

Säkerhetsuppdateringar (säkerhetspatchar) publiceras oftast av tillverkare efter att en sårbarhet blivit känd för tillverkaren, en säkerhetsuppdatering åtgärdar en eller flera sårbarheter. Oftast tillförs ingen ny funktionalitet förutom åtgärden mot sårbarheten. Regelbundna säkerhetsuppdatering ger ett grundläggande skydd mot att kända sårbarheter utnyttjas.

En bra förvaltning och livscykelhantering av programvaran gör att man undviker problem när tillverkare slutar publicera uppdateringar till en föråldrad version av programvaran. En god kontakt med tillverkaren behövs för att i god tid kunna uppgradera programvara eller avveckla denna om ingen support eller uppdatering finns längre.

Undantagsvis kan man besluta om att säkerhetsuppdatering inte behöver göras. Det beslutet kan göras efter noggrann analys av sårbarhet och exponering, det kan vara så att sårbarheten inte har någon betydelse i det specifika fallet. Det kan också vara så att det är teknisk omöjligt att installera uppdateringen. Undantaget måste dokumenteras och omprövas regelbundet.

Säkerhetsuppdateringar behövs även i hårdvara så som nätverksinfrastruktur, servrar, lagringssystem.

Exempel på aktiviteter

- Utveckla en plan för att kontinuerligt bedöma och spåra sårbarheter på alla tillgångar i den infrastruktur verksamheten nyttjar, för att åtgärda och minimera möjligheten för angripare. (Vulnerability Management)

Exempel på säkerhetsåtgärder

- Omvärldsbevakning för att få information om nya sårbarheter och hot relevanta för verksamheten och de produkter som används
- Inventarieförteckning för att kunna utföra relevant omvärldsbevakning
- Rutiner för test och verifiering av uppdateringar
- Rutiner för distribution av säkerhetsuppdateringar
- Gör kontinuerliga sårbarhetsscanningar

Exempel på bevis

- Uppdaterad inventarieförteckning
- Resultat från sårbarhetsscanningar

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.10.4 Uppdateringar
SS-EN ISO/IEC 27002:2022	8.8 Hantering av tekniska sårbarheter 8.25 Säker utvecklingscykel 8.31 Separation av utvecklings-, test- och produktionsmiljöer 8.32 Ändringshantering
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	6.6 SECURITY PATCH MANAGEMENT
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.20 Kontinuerlig uppdatering för att motverka sårbarheter

3.10.3. Dokumentation

```
20 § Verksamhetsutövaren ska ha dokumentation som visar logiska samband och inbördes
beroenden mellan komponenter som används i informationssystem som har betydelse för
säkerhetskänslig verksamhet.
```

Syfte

En komplett och uppdaterad dokumentation som är tillgänglig vid incidenter, drift, uppdateringar.

Vägledning

En bra dokumentation:

- Ger en god översikt av hela informationssystemet
- Är en förutsättning för att snabbt och effektivt kunna hantera driftrelaterade problem
- Underlättar hantering av incidenter
- Ger stöd vid uppdatering av informationsystemet
- Kan användas vid utbildning av ny personal
- Är uppdaterad
- Skapas innan driftsättning av informationssystemet
- Finns tillgänglig även vid katastrofala driftstörningar (exempelvis på papper)

Innan ett informationssystem driftsätts måste driftsorganisation upprättas, dokumentation behöver vara anpassad till deras arbetssätt.

Exempel på aktiviteter

- Tillse att ändringshantering (ITIL Change) innehåller ett specifikt steg för att uppdatera dokumentationen
- Gör det till en del i incident- och krisövningar att tillse att dokumentationen är uppdaterad och finns tillgänglig

Exempel på säkerhetsåtgärder

- Stickprov som visar om dokumentationen är uppdaterad
- Ett dokumentationssystem där dokument har ett "uppdateras senast" datum

Exempel på bevis

- Uppdaterad dokumentation
- Process för att uppdatera dokumentation

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.10.5 Dokumentation
SS-EN ISO/IEC 27002:2022	5.37 Dokumenterade driftsrutiner 8.32 Ändringshantering
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	1.1 POLICY ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS - (h)
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.21 Dokumenterade system är lättare att granska, uppdatera och incidenthantera

3.10.4. Dokumentation (Kvalificerat Hemlig)

```
21 § Verksamhetsutövaren ska för informationssystem som är avsett för att behandla
säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen kvalificerat hemlig,
dokumentera vilken hård- och mjukvara som används i informationssystemet och deras
inbördes beroenden.
Kraven i första stycket gäller även informationssystem som är av motsvarande betydelse
för Sveriges säkerhet.
```

3.10.5. Syfte

En komplett och uppdaterad dokumentation som är tillgänglig vid incidenter, drift, uppdateringar.

3.10.6. Vägledning

Gäller nivå Kvalificerat Hemlig och Konsekvensnivå A

Förutom det som beskrivs i PMFS 2022:1 Kap4 P20 - Dokumentation så gäller följande:

- All hårdvara som används ska vara dokumenterad
- All mjukvara som används ska vara dokumenterad
- Alla inbördes beroenden (hårdvara, mjukvara) ska vara dokumenterad

3.10.7. Exempel på aktiviteter

- Dokumentera hårdvara och mjukvara
- Dokumentera alla inbördes beroenden

3.10.8. Exempel på säkerhetsåtgärder

- Stickprov som visar om dokumentationen är uppdaterad
- Ett dokumentationssystem där dokument har ett "uppdateras senast" datum

3.10.9. Exempel på bevis

- Uppdaterad dokumentation
- Process för att uppdatera dokumentation

3.10.10. Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.10.5 Dokumentation

Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.21 Dokumenterade system är lättare att granska, uppdatera och incidenthantera

3.11. Skydd mot skadlig kod

3.11.1. Behov och funktioner

```
22 § Verksamhetsutövaren ska för informationssystem som har betydelse för
säkerhetskänsligverksamhet analysera behovet av och i förekommande fall besluta att
använda de funktioner för skydd mot skadlig kod som är nödvändiga från
säkerhetsskyddssynpunkt.
```

Syfte

Ett försvar i djupled mot skadlig kod

Vägledning

Informationssystemet måste analyseras och skyddas som en helhet på alla lager. Skydd införs enligt principen försvar i djupled och anpassat till informationssystemets uppbyggnad.

Skydd mot skadlig kod,

- Kontrollerad kommunikation
- Antivirusprogramvara
- System för att upptäcka och förhindra att otillåten programvara körs (Vitlistning)
- Härdning av system och applikationer
- System för att upptäcka och hindra otillåten kommunikation (IDS/IDP)
- System för att skydda klientsystem (EDR/XDR)
- Använda betrodda källor
- Alltid ha möjlighet att återställa system och information
- Strikt behörighetsstyrning
- Härdning/loggning av standardverktyg i miljön som t.ex. Powershell (som kan användas för exploatering (LOTL-attacker))

Exempel på aktiviteter

- Ta fram rutiner för att kontrollera att skyddet mot skadlig kod är fungerar

Exempel på säkerhetsåtgärder

- Testa att skyddet mot skadlig kod fungerar

Exempel på bevis

- Uppdaterad dokumentation
- Testrapporter som visar att skyddet mot skadlig kod fungerar

- Incidentrapporter

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.11 Skydd mot skadlig kod
SS-EN ISO/IEC 27002:2022	8.7 Skydd mot skadlig kod
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	6.9 PROTECTION AGAINST MALICIOUS AND UNAUTHORISED SOFTWARE
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.22 Skydd mot skadlig kod

3.12. Skydd mot obehörig förändring av informationssystem

3.12.1. Försvåra och upptäcka

```
23 § Verksamhetsutövaren ska för informationssystem som har betydelse för
säkerhetskänslig verksamhet vidta skyddsåtgärder som ger förmåga att försvåra och
upptäcka obehörig förändring av informationssystemet och dess säkerhetsskydd.
```

Syfte

Stoppa, försvåra och upptäcka obehöriga förändringar

Vägledning

Skydd mot obehörig förändring ryms inom informationssäkerhetsbegreppet riktighet (eng. Integrity).

I ett informationssystem med betydelse för säkerhetskänslig verksamhet är det av stor betydelse att inga obehöriga förändringar görs då dessa kan påverka systemets funktionalitet och säkerhetsskydd.

Det är av stor vikt att obehöriga förändringar stoppas, försvåras och upptäcks. Detta behöver ske på alla nivåer i systemet och med en blandning av teknik och processer.

Se även,

- PMFS 2022:1 Kap4 P18 - Konfiguration, uppdatering och dokumentering
- PMFS 2022:1 Kap4 P26 - Säkerhetsloggning
- PMFS 2022:1 Kap4 P30 - Säkerhetsövervakning

Exempel på aktiviteter

- Ta fram styrande dokument för behörig förändring
- Ta fram tester för skyddet mot obehörig förändring
- Se till att konfigurationsändringar loggas

Exempel på säkerhetsåtgärder

- Följ upp loggar rörande ändringar

Exempel på bevis

- Uppdaterad dokumentation
- Testrapporter som visar att skyddet obehörig förändring fungerar
- Loggrapporter

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.12 Skydd mot obehörig förändring av informationssystem
SS-EN ISO/IEC 27002:2022	8.9 Konfigurationshantering 8.32 Ändringshantering
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	6.3 CONFIGURATION MANAGEMENT
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.23 Skydd mot obehörig förändring av informationssystem

3.13. Intrångsdetektering och intrångsskydd

3.13.1. Funktioner för intrångsdetektering och intrångsskydd

```
24 § Verksamhetsutövaren ska förse ett informationssystem som har betydelse för
säkerhetskänslig verksamhet och som kommunicerar med andra informationssystem, med
funktioner för intrångsdetektering och intrångsskydd.
```

Syfte

Upptäcka, identifiera och uppmärksamma oönskade aktiviteter

Vägledning

Intrångsdetektering (IDS) och intrångsskydd (IDP) kan finnas på olika lager och punkter i ett informationssystem. Vanligtvis finns dessa funktioner i nätverket (NIDS/NIPS) eller på ett delsystem/komponent (HIDS/HIPS). Det är viktigt att man anpassar funktionerna till informationssystemet och att man bygger ett skydd i djupled bestående av skydd på flera ställen och lager. På system kan man också använda funktioner som skyddar mot olika typer av attacker mot systemminnet (EDR, XDR etc.)

Det effektivaste skyddet får man om funktionerna man använder till så stor del som möjligt kan avkoda och förstå normalt beteende. Skydden behöver vara anpassad till den förväntade nyttotrafiken och förstå de protokoll som används. Skyddet blir effektivare om dom appliceras på okrypterad kommunikation (där det är möjligt och lämpligt)

Det är oerhört viktigt att ha en säkerhetsövervakning som reagerar på de larm som skyddsfunktionerna genererar.

Exempel på aktiviteter

- Skapa en arkitektur som visar var intrångsdetektering (IDS) och intrångsskydd (IDP) finns
- Skapa larmöverföring till säkerhetsövervakning
- Skapa rutiner för hantering av larm
- Kontinuerligt testa funktionerna

Exempel på säkerhetsåtgärder

- Kontrollerad kommunikation

Exempel på bevis

- Uppdaterad dokumentation
- Rapporter från tester av funktioner
- Rapporter över larm och vidtagna åtgärder

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.13 Intrångsdetektering och intrångsskydd
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.24 Intrångsdetektering och intrångsskydd

3.14. Säkerhetsloggning

3.14.1. Loggning av händelser

```
25 § Verksamhetsutövaren ska logga händelser som kan påverka säkerheten i
informationssystem som har betydelse för säkerhetskänslig verksamhet.
```

Syfte

Upptäcka och reagera oönskade aktiviteter, samt att kunna utreda incidenter och brott.

Vägledning

Loggning av händelser i informationssystemet ska ske, loggar bör minst omfatta vad, när och hur en händelse inträffade samt vem som utförde den.

Ett syfte med loggarna är att kunna bevisa vem som gjort vad vid ett givet tillfälle i ett informationssystem, exempelvis tagit del av eller haft åtkomst till säkerhetsskyddsklassificerade uppgifter. Ett annat exempel kan vara vem som utfört systemadministrativa åtgärder med privilegierade konton.

Loggarna ska bland annat kunna användas till,

- Utredning av incidenter
- Upptäckt och utredning av obehörig åtkomst
- Utredning av brott
- Upptäcka oönskade händelser
- Möjliggöra spårbarhet

För att loggarna ska vara användbara krävs korrekt systemtid och tidszon i hela informationssystemet samt att tidsformatet är det samma (Z-time, ISO, Epoch) .

Exempel på aktiviteter

- Konfigurera loggning av relevanta säkerhetshändelser
- Använda loggformat som organisationen kan hantera
- Skapa unika ID för sessioner/transaktioner så att dessa kan följas genom systemet (Correlation ID)

Exempel på säkerhetsåtgärder

- Tidssynkronisering

Exempel på bevis

- Loggrapporter

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.14 Säkerhetsloggning
SS-EN ISO/IEC 27002:2022	8.15 Loggning 8.17 Synkronisering av tid
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	3.2 MONITORING AND LOGGING
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.25 Säkerhetsloggning

3.14.2. Rutiner för loggning

```
26 § Verksamhetsutövaren ska ha rutiner för loggning av händelser som kan påverka
säkerheten i informationssystem som har betydelse för säkerhetskäns
lig verksamhet. Rutinerna ska omfatta hur verksamhetsutövaren ska kunna upptäcka
skadlig inverkan, obehörig åtkomst eller påverkan, och funktions
störningar. Rutinerna ska även omfatta vilka åtgärder som ska vidtas vid upptäckta
händelser.
```

Syfte

Att bara logga räcker inte, åtgärder för att upptäcka och hantera skadlig inverkan, obehörig åtkomst eller påverkan, och funktionsstörningar krävs.

Vägledning

Loggar måste följas upp, det kan ske mer eller mindre automatiserat och kontinuerligt som en del av Säkerhetsövervakning i en SOC. Det kan även ske vid intervaller, stickprov eller på förekommen anledning.

Loggning bör ske i hela informationssystemet och kringliggande infrastruktur. Loggning från skyddsfunktioner (Skydd mot skadlig kod, IDP/IDS mm) och användaraktiviteter (systemadministrativ åtkomst, privilegierade konton) samt ändringar i konton, rättigheter och behörigheter är extra viktiga att logga.

Rutiner ska finnas för hantering av utfall av logguppföljning, till exempel eskalering och incidenthantering.

Om loggar hanteras av extern part så bör ett SLA för tillgång till loggar definieras och troligen även ett säkerhetsskyddsavtal tecknas med den externa parten.

Exempel på aktiviteter

- Definiera syftet med logguppföljning
- Ta fram process och rutiner som beskriver vem som ska utföra logguppföljning och vilket sätt det ska ske på
- Skapa process för kontinuerlig utvärdering och förbättring av loggning (behov, anpassning etc.)
- Ta fram process och rutiner för att hantera utfall i logguppföljningen

Exempel på säkerhetsåtgärder

Exempel på bevis

- Dokumenterade processer
- Dokumenterade rutiner
- Rapporter som visar hur logguppföljningen skett

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.14 Säkerhetsloggning
SS-EN ISO/IEC 27002:2022	8.15 Loggning 8.16 Övervakning
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	3.2 MONITORING AND LOGGING
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.25 Säkerhetsloggning

3.14.3. Loggning av högre behörigheter

```
27 § För informationssystem som är avsett för att behandla
säkerhetsskyddsklassificerade uppgifter ska loggningen omfatta användning och ändring
av behörigheter med systemadministrativ åtkomst och av roller med särskild behörighet
till informationssystemet.
```

Syfte

Informationssystem som används för behandling av säkerhetsskyddsklassificerade uppgifter ska logga användning av och förändring i högre behörigheter

Vägledning

I informationssystem som behandlar säkerhetsskyddsklassificerade uppgifter är det extra viktigt att ha en loggning som ger spårbarhet användning och ändring i behörigheter.

Om ett informationssystem faller under denna paragraf så bör man separat redovisa hur loggningen som sker uppfyller paragrafen.

Exempel på aktiviteter

- Definiera loggning för användning av behörigheter med systemadministrativ åtkomst och annan särskild behörighet
- Definiera loggning för ändring av behörigheter med systemadministrativ åtkomst och annan särskild behörighet
- Loggning av alla kommandon/åtgärder som utförs med behörigheter med systemadministrativ åtkomst och annan särskild behörighet
- Se Logguppföljning

Exempel på säkerhetsåtgärder

Exempel på bevis

- Dokumenterade processer
- Dokumenterade rutiner
- Rapporter som visar hur logguppföljningen skett

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.14 Säkerhetsloggning
SS-EN ISO/IEC 27002:2022	8.2 Privilegierade åtkomsträttigheter 8.15 Loggning 8.16 Övervakning

ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	3.2 MONITORING AND LOGGING
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.25 Säkerhetsloggning

3.14.4. Bevarande av säkerhetsloggar

```
28 § Verksamhetsutövaren ska bevara säkerhetsloggar i minst tio år. För ett
informationssystem som är avsett för att behandla säkerhetsskyddsklassificerade
uppgifter i säkerhetsskyddsklassen kvalificerat hemlig ska säkerhetsloggar bevaras i
minst 25 år. I det allmännas verksamhet tillämpas i stället bestämmelserna om gallring
i arkivlagen (1990:782) och föreskrifter som har meddelats med stöd av den lagen.
```

Syfte

Loggar ska bevaras under 10 resp. 25 år för att tillgodose krav på att bland annat kunna göra brottsutredningar

Vägledning

Loggar behöver bevaras i minst 10 år och i vissa fall i minst 25 år, lagringslängden är knuten till skyddsvärdet på informationen och under vilken tid man kan förväntas kunna göra brottsutredningar.

För verksamhet som lyder under arkivlagen (1190:782) ska tillämpa denna och de föreskrifter som meddelats.

Säkerhetsloggar ska bevaras i **minst** tio år, eller för system som behandlar kvalificerat hemlig information i **minst** 25 år.

Exempel på aktiviteter

- Definiera hur loggar ska kunna bevaras i 10 resp. 25 år

Exempel på säkerhetsåtgärder

- Åtgärder för att säkerställa riktighet 10/25 år
- Åtgärder för att säkerställa läsbarhet 10/25 år

Exempel på bevis

- Dokumenterade processer
- Dokumenterade rutiner
- Rapporter som visar att loggar lagras

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.14 Säkerhetsloggning
SS-EN ISO/IEC 27002:2022	8.15 Loggning

ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	3.2 MONITORING AND LOGGING
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.25 Säkerhetsloggning

3.14.5. Skydd av säkerhetsloggar

```
29 § Verksamhetsutövaren ska vidta åtgärder för att skydda säkerhetsloggar mot
obehörig åtkomst, ändring eller förstöring.
```

Syfte

Riktighet och spårbarhet i loggning och loggar är av stor vikt

Vägledning

Att riktigheten i upprätthålls är avgörande för att kunna skydda informationssystem, utreda brott och i förlängningen skydda Sveriges säkerhet.

Loggar måste också skyddas från obehörig åtkomst, speciellt om loggarna innehåller säkerhetsskyddsklassificerade uppgifter (vilket de vanligtvis inte gör).

Loggar kan exempelvis skyddas genom,

- Strikt behörighetshantering
- Signering av loggar
- Centralt loggarkiv (Med minst samma säkerhetsskydd som loggkällor)
- Separat administration (teknik, personal) av det centrala loggarkivet (immutable)

Exempel på aktiviteter

- Definiera hur loggar ska kunna bevaras i 10 resp. 25 år
- Arkitektur/teknisk lösning av säker logglagring

Exempel på säkerhetsåtgärder

- Kontrollerad kommunikation

Exempel på bevis

- Dokumenterade processer
- Dokumenterade rutiner
- Rapporter som visar att loggar lagras

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.14 Säkerhetsloggning
SS-EN ISO/IEC 27002:2022	8.15 Loggning

ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	3.2 MONITORING AND LOGGING
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.25 Säkerhetsloggning

3.15. Säkerhetsövervakning

3.15.1. Funktioner för säkerhetsövervakning

```
30 § Verksamhetsutövaren ska använda funktioner för säkerhetsövervakning av
informationssystem som är avsedda för att behandla säkerhetsskyddsklassificerade
uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig.
Kraven i första stycket gäller även informationssystem av motsvarande betydelse för
Sveriges säkerhet.
```

Syfte

Att kunna upptäcka, försvåra och hantera intrångsförsök/säkerhetshändelser

Vägledning

Med säkerhetsövervakning menas en funktion som,

- Utför säkerhetsövervakning
- Kan upptäcka, försvåra och hantera intrångsförsök/säkerhetshändelser
- Förhindrar obehörig avlyssning och åtkomst
- Har kompetent personal som med tekniska hjälpmedel aktivt söker efter oönskade säkerhetshändelser
- Förhindrar intrångsförsök
- Utreder incidenter i informationssystemet

Exempel på aktiviteter

- Definiera syftet och målet med övervakningen
- Definiera vilka som ska utföra säkerhetsövervakningen och under vilka former (24x7 ?)
- Testa att säkerhetsövervakning fungerar med hjälp av exempelvis penetrationstester

Exempel på säkerhetsåtgärder

- SIEM (eng. Security Information and Event Management)
- Öva incidenthantering

Exempel på bevis

- Dokumenterade rutiner för säkerhetsövervakning
- Bemanningsplaner för säkerhetsövervakning

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.15 Säkerhetsövervakning
SS-EN ISO/IEC 27002:2022	5.28 Insamling av bevis 8.16 Övervakning
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	3.2 MONITORING AND LOGGING
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.26 Säkerhetsövervakning

3.15.2. Rutiner för säkerhetsövervakning

```
31 § Verksamhetsutövaren ska ha rutiner för säkerhetsövervakning enligt 30 §.
Rutinerna ska omfatta vad som ska övervakas och vilken funktion som ansvarar för
övervakningen. Rutinerna ska även omfatta vad som behövs i övrigt samt vilka åtgärder
som ska vidtas vid upptäckta händelser.
```

Syfte

Att kunna upptäcka, försvåra och hantera intrångsförsök/säkerhetshändelser

Vägledning

Vid upptäckt av intrångsförsök/säkerhetshändelser behöver det finnas en dokumenterad och tydlig instruktion för hur incidenter ska hanteras. Dokumenterade rutiner, checklistor och processer med mera.

Även rutiner för fördjupad analys av loggar i loggkällor och andra it-forensiska åtgärder (minnesdumpar, nätverkstrafik, analys av skadlig kod) ska finnas.

Exempel på aktiviteter

- Definiera syftet och målet med övervakningen
- Definiera vilka som ska utföra säkerhetsövervakningen och under vilka former (24x7 ?)
- Testa att säkerhetsövervakning fungerar med hjälp av exempelvis penetrationstester
- Definiera roller med kunskap och tydligt mandat att agera omedelbart vid en incident.

Exempel på säkerhetsåtgärder

- SIEM (eng. Security Information and Event Management)
- Öva incidenthantering

Exempel på bevis

- Dokumenterade rutiner för säkerhetsövervakning
- Bemanningsplaner för säkerhetsövervakning
- Erfarenhetsåterkoppling från upptäckta händelser (lessons learned)
- Kontroller av att inträffade incidenter upptäcks
- Dokumenterade roller med kunskap och tydligt mandat att agera omedelbart vid en incident.

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.15 Säkerhetsövervakning

SS-EN ISO/IEC 27002:2022	5.28 Insamling av bevis+ 8.16 Övervakning
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	3.2 MONITORING AND LOGGING
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.26 Säkerhetsövervakning

3.16. Åtgärder för att upprätthålla kontinuitet

3.16.1. Rutiner och funktioner för kontinuitet

```
32 § Verksamhetsutövaren ska för informationssystem som är skyddsvärda utifrån
perspektiven riktighet eller tillgänglighet ha de rutiner och funktioner som krävs för
att upprätthålla kontinuitet i den säkerhetskänsliga verksamheten. Verksamhetsutövaren
ska för sådana informationssystem vidta åtgärder som säkerställer att
informationssystemet kan återställas.
```

Syfte

Upprätthålla kontinuiteten

Vägledning

Att information och informationssystem med betydelse för säkerhetskänslig verksamhet blir otillgängliga kommer nästan alltid att medföra att en skada för Sveriges säkerhet uppstår. I den övergripande Säkerhetsskyddsanalysen (SSA) eller i den Särskilda Säkerhetsskyddsbedömningen (SSB) så bör det framgå vilken skada som kan uppstå och vilka tidsrymder som är relevanta.

Verksamheten behöver göra en kontinuitetsplanering för informationssystemet, den ska inkludera tillgång till kompetens och resurser som behövs för att återställa systemet.

It-funktionen hos verksamheten ska ha en återställningsrutin för informationssystemet, systemet ska gå att återställa på samma plats eller annan plats.

Den sammantagna planeringen bör inkludera, - Kompetensförsörjning - Resurser - Driftsplatser - Redundans - Test av återställning - Övning

De bedömningar som gjorts vid framtagande av kontinuitetsplan och återhämtningsplan bör redovisas i den Särskilda Säkerhetsskyddsbedömning (SSB) för informationssystemet.

Kontinuitetsplaner och återställning bör övas flera gånger per år

Exempel på aktiviteter

- Utveckla en kontinuitetsplan
- Utveckla återställningsrutiner
- Definiera roller för kontinuitetsscenarion
- Tröskelvärden för aktivering av kontinuitetsplan
- Reservmetoder för upprätthållandet av verksamheten

Exempel på säkerhetsåtgärder

- Öva kontinuitetsplanen

- Testa återställningsrutiner

Exempel på bevis

- Dokumenterad och uppdaterad kontinuitetsplan
- Dokumenterad och uppdaterad återställningsrutin
- Rapporter från genomförda övningar (resultat, lessons learned)

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.16 Åtgärder för att upprätthålla kontinuitet
Säkerhetspolisens Vägledning i säkerhetsskydd Säkerhetsskyddsanalys (Jan 2023)	3.4 Perspektiven konfidentialitet, riktighet och tillgänglighet
SS-EN ISO/IEC 27002:2022	5.30 Kontinuitetsberedskap inom IKT 8.6 Kapacitetshantering 8.14 Redundans för informationsbehandlingsresurser
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	4.1 BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.27 Upprätthålla kontinuitet

3.17. Kontroll av säkerhetskopior

3.17.1. Kontroll av säkerhetskopior

```
33 § När säkerhetskopiering av säkerhetsskyddsklassificerade uppgifter eller uppgifter
i övrigt som har betydelse för säkerhetskänslig verksamhet genomförs, ska
verksamhetsutövaren regelbundet, minst en gång per år, kontrollera att uppgifterna på
säkerhetskopiorna går att återskapa
```

Syfte

Verifiera att återställning från säkerhetskopior är möjlig

Vägledning

Säkerhetskopiering är viktig för att säkerställa att ingen information går förlorad och att det är möjligt att återställa informationen och informationssystemen. Bortfall av information och informationssystem i säkerhetskänslig verksamhet kan i många fall leda till en skada för Sveriges säkerhet.

All information bör klassificeras för att förstå vilken betydelse den har för verksamheten och vilket behov av säkerhetskopiering som finns.

Behov av säkerhetskopior och återställning kan uppstå efter tekniska fel, angrepp med skadlig kod, naturkatastrofer och andra skäl, hantering och förvaring av säkerhetskopior behöver ta hänsyn till alla eventualiteter. Behoven och åtgärderna kan beskriva i t.ex. en Särskild Säkerhetsskyddsbedömning (SSB).

För information och informationssystem bör man fastställa inom vilken maximal tidsrymd man vill att systemet är återställt (RTO, Recovery Time Objective) och vilken informationsförlust som eventuellt kan vara acceptabel (RPO, Recovery Point Objective). Säkerhetskopior som innehåller säkerhetsskyddsklassificerade uppgifter måste hanteras och förvaras enligt den högsta säkerhetsskyddsklassen som finns på säkerhetskopiorna. Sammantaget kan det betyda omfattande kostnader för återställning och hantering om man genom logisk separation blandat system och information med olika RTO, RPO och säkerhetsskyddsklasser på samma hårdvara och backuplösning.

Säkerhetskopior måste förvaras inom verksamhetens lokaler och vara under kontroll. Om säkerhetskopiorna innehåller säkerhetsskyddsklassificerade uppgifter eller annan sekretessbelagd information så måste även dessa regelverk följas.

Säkerhetskopior måste skyddas från angrepp som leder till att de blir obrukbara för sitt syfte, det innebär i princip alltid att det måste finnas säkerhetskopior som är offline. Om det bara finns säkerhetskopior som är nåbara (online) så är risken överhängande att en antagonist angriper dessa och omöjliggör återställning.

Testa att säkerhetskopior går att återläsa och att det är möjligt att återställa informationssystemet ofta. Dock minst en gång per år.

Exempel på aktiviteter

- Klassificera **all** information för att få fram RPO, RTO och skyddsvärde
- Ta fram ett backupschema som stödjer RPO och RTO

Exempel på säkerhetsåtgärder

- Testa återläsning av säkerhetskopior ofta, minst en gång per år
- Kontrollera förvaringen årligen

Exempel på bevis

- Informationsklassificering
- Backupschema
- Dokumenterade återläsningar
- Dokumenterade rutin för säkerhetskopiering
- Loggar från säkerhetskopieringssystemet

Referenser

Säkerhetspolisens Vägledning Informationssäkerhet (Okt 2023)	4.17 Kontroll av säkerhetskopior
SS-EN ISO/IEC 27002:2022	8.13 Säkerhetskopiering av information
ENISA IMPLEMENTING GUIDANCE On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 - DRAFT FOR PUBLIC CONSULTATION	4.2 BACKUP MANAGEMENT
Säkerhetsskydd - En introduktion Utg 3 - Kim Hakkarainen	4.2.28 Säkerhetskopior kontrolleras minst varje år

Kapitel 4. Säkerhetsskyddsförordning (2021:955)

4.1. Grundläggande bestämmelser om säkerhetsskydd (2 Kap)

4.1.1. Behörighet att medverka i säkerhetskänslig verksamhet

```
2 §   Behörig att få del av säkerhetsskyddsklassificerade uppgifter eller tillgång
till säkerhetskänslig verksamhet i övrigt är, om inte något annat följer av
bestämmelser i lag, endast den som
   1. har bedömts pålitlig från säkerhetssynpunkt,
   2. har tillräckliga kunskaper om säkerhetsskydd, och
   3. behöver uppgifterna eller annan tillgång till verksamheten för att kunna utföra
sitt arbete eller på annat sätt medverka i den säkerhetskänsliga verksamheten.
```

4.1.2. Vägledning

Pålitlighet bedöms som en del av personalsäkerhet.

Tillräckliga kunskaper och behov är kopplat till roll/arbetsuppgifter och varierar över tid.

Den som hanterar säkerhetsskyddsklassificerade uppgifter i informationssystem eller är systemadministratör för ett informationssystem med betydelse för säkerhetskänslig verksamhet behöver omfattande utbildning och kunskaper i säkerhetsskydd.

4.2. Informationssäkerhet (3 Kap)

4.2.1. Förberedande åtgärder inför driftsättning av ett informationssystem

```
2 §   Innan ett informationssystem som kan förutses komma att behandla
säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller
högre tas i drift, eller i väsentliga avseenden förändras, ska verksamhetsutövaren
skriftligen samråda med Säkerhetspolisen. Om verksamhetsutövaren hör till
Försvarsmaktens eller Försvarets materielverks tillsynsområde ska denne i stället
samråda med Försvarsmakten.
Samrådsskyldigheten gäller även i fråga om andra informationssystem än sådana som
anges i första stycket, om obehörig åtkomst till systemen kan medföra en skada för
Sveriges säkerhet som inte är obetydlig.
Säkerhetspolisen och Försvarsmakten ska underrätta verksamhetsutövarens
tillsynsmyndighet om samråd som skett enligt första stycket.
```

4.2.2. Vägledning

Samrådsskyldigheten gäller för informationssystem som behandlar säkerhetsskyddsklassificerade uppgifter i nivå Konfidentiellt/Hemlig/Kvalificerat Hemlig samt för system vars konsekvensnivå är C/B/A.

Se PMFS 2022:1 4 Kap 3 § - driftsättning

Index