Vägledning i säkerhetsskydd

Informationssäkerhet

Säkerhetspolisen

För dig som läser en nedladdad eller utskriven kopia av denna vägledning
Kontrollera att du har den senaste versionen på Säkerhetspolisens webbplats.
Där finns även andra vägledningar inom området säkerhetsskydd.
Version Oktober 2023

Denna vägledning riktar sig till dig som på något sätt arbetar med att styra, leda eller utforma informationssäkerheten i en säkerhetskänslig verksamhet eller som ska genomföra samråd inför driftsättning av informationssystem i enlighet med säkerhetsskyddsförordningen (2021:955).

Denna vägledning beskriver innebörden av säkerhetsskyddsåtgärden informationssäkerhet samt ger vägledning i tillämpning av vissa för informationssäkerhet relevanta bestämmelser i säkerhetsskyddslagen (2018:585), säkerhetsskyddsförordningen och Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1). Syftet med vägledningen är framför allt att tydliggöra bestämmelser i tredje och fjärde kapitlen i Säkerhetspolisens föreskrifter om säkerhetsskydd.

Vägledningen utgör ett komplement till författningstexterna. Den tar inte upp säkerhetsskyddslagstiftningens alla bestämmelser och krav med bäring på informationssäkerhet, utan innehåller förtydliganden och tolkningshjälp endast i valda delar. Vägledningen redogör sällan i detalj för innehållet i relevanta bestämmelser, utan är avsedd att läsas parallellt med dessa.

För riksdagen och dess myndigheter finns bestämmelser om informationssäkerhet i 5–6 §§ lagen (2019:109) om säkerhetsskydd i riksdagen och dess myndigheter.

För att kunna tillgodogöra sig innehållet i denna vägledning rekommenderas att läsaren har tagit del av Säkerhetspolisens övriga vägledningar i säkerhetsskydd – Introduktion till säkerhetsskydd och Säkerhetsskyddsanalys. Även vissa förkunskaper om informationssäkerhet behövs.

Innehåll


För att förhindra skada
på såväl verksamheten som Sveriges
säkerhet behöver verksamhetsutövaren
identifiera vilka uppgifter som är
säkerhetsskyddsklassificerade och
kan ge konsekvenser för Sverige om
uppgifterna skulle röjas.

1 Introduktion

1.1 Informationssäkerhet inom säkerhetsskydd

§ *2 kap. 2 § säkerhetsskyddslagen*

Uppgifter (information) är av avgörande betydelse i alla typer av verksamheter. För säkerhetskänslig verksamhet är tillgång till tillförlitliga uppgifter avgörande för att verksamheten ska fungera. Därför är det viktigt att verksamhetsutövare identifierar vilka uppgifter den säkerhetskänsliga verksamheten på olika sätt är beroende av. För att förhindra skada på såväl verksamheten som Sveriges säkerhet behöver verksamhetsutövaren även identifiera vilka uppgifter som är säkerhetsskyddsklassificerade med anledning av konsekvenser förknippade med uppgifternas röjande.

Informationssäkerhet inom säkerhetsskydd syftar till:

- att förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, och
- att förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet.

Notera:
En verksamhet har i allmänhet stora mängder information som av olika anledningar kan vara skyddsvärd. En förutsättning för effektiv och säker informationshantering är att informationssäkerhetsarbetet bedrivs systematiskt.

+ *För stöd i hur ett systematiskt informationssäkerhetsarbete kan bedrivas, se www.informationssakerhet.se som förvaltas av Myndigheten för samhällsskydd och beredskap.*

Informationssäkerhet handlar om att skydda information ur olika aspekter. Även om det i olika kontexter finns skiftande definitioner av begreppet informationssäkerhet återkommer alltid följande tre centrala perspektiv eller egenskaper:

- **Konfidentialitet:** Att förhindra att obehöriga får tillgång till information.
- **Riktighet:** Att det går att lita på att den information som används i verksamheten är korrekt och inte manipulerad.
- **Tillgänglighet:** Att säkerställa att informationen är tillgänglig när den behövs.

Vid sidan av de tre aspekterna ovan nämns ofta spårbarhet, det vill säga entydig härledning av utförda aktiviteter till en identifierad användare (individ, system eller resurs). Spårbarhet ses som ett viktigt sätt att upprätthålla de tre informationssäkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet.

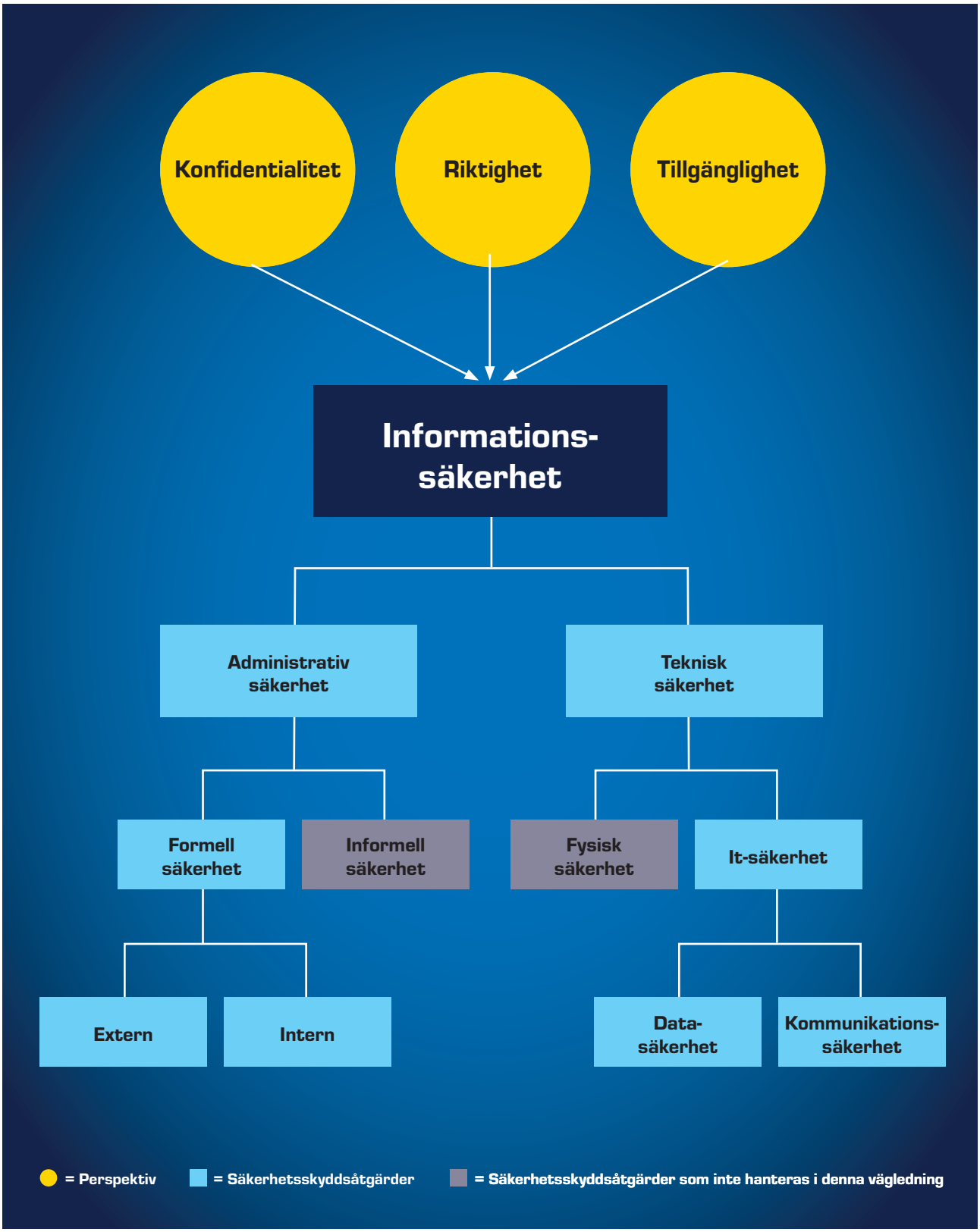
Denna vägledning är avgränsad till säkerhetsskyddsåtgärden informationssäkerhet. För majoriteten av verksamhetsutövare omfattas endast delar av verksamheten av säkerhetsskyddslagen och dess krav på säkerhetsskyddsåtgärder. För sådana verksamhetsutövare är det viktigt att säkerhetsskyddsarbete som avser informationssäkerhet bedrivs i samklang med verksamhetens övriga informationssäkerhetsarbete.

1.2 Begrepp

Ord och uttryck i vägledningen har samma innebörd som i säkerhetsskyddslagstiftningen, om inte annat framgår särskilt.

- **Informationssystem:** Definitionen i 1 kap. 3 § säkerhetsskyddsförordningen lyder: *"Med informationssystem avses ett system av sammansatt mjuk- och hårdvara som behandlar information."* Detta innebär att även en fristående dator som inte kommunicerar med andra system ska betraktas som ett informationssystem. Därför innebär det också att en fristående dator med av Försvarsmakten godkänt filkrypto såsom signalskyddsystem PGBI eller MGS/MGSI är ett informationssystem enligt säkerhetsskyddsförordningen.
- **Ackumulering:** För denna vägledning, se särskild definition i avsnitt 2.4.
- **Aggregering:** För denna vägledning, se särskild definition i avsnitt 2.4.
- **Hotmodellering:** Systematisk sammanställning och bedömning av tänkbara hot.
- **Kompensatoriska åtgärder:** Med kompensatoriska åtgärder, avses ytterligare åtgärder, som efter konstaterade brister i planerade säkerhetsskyddsåtgärder, behöver vidtas för att säkerhetskrav ska uppnås inför driftsättning eller förändring.
- **Process:** En process är en serie aktiviteter som främjar ett avsett resultat.
- **Rutin:** En rutin är ett bestämt tillvägagångssätt för hur en aktivitet ska utföras.

Ett sätt att visualisera vad informationssäkerhet omfattar.



Säkerhetsskyddsklassificerade uppgifter avser uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) (OSL) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.

2 Indelning och bedömning av uppgifter

Den som bedriver säkerhetskänslig verksamhet kan ha uppgifter som är skyddsvärda ur perspektiven konfidentialitet, riktighet och tillgänglighet.

Informationssystem som är skyddsvärda utifrån perspektiven riktighet eller tillgänglighet kan utgöra exempel på sådana andra tillgångar som enligt 2 kap. 3 § andra stycket och 2 kap. 5 § Säkerhetspolisens föreskrifter om säkerhetsskydd ska delas in i konsekvensnivåer. Denna indelning ska göras oberoende av om informationssystemet hanterar säkerhetsskyddsklassificerade uppgifter eller inte.

I Säkerhetspolisens Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys finns stöd för bedömning av skyddsvärden och indelning i konsekvensnivå.

2.1 Säkerhetsskyddsklassificerade uppgifter

1 kap. 2 § andra stycket säkerhetsskyddslagen

Begreppet säkerhetsskyddsklassificerade uppgifter avser uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) (OSL) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.

Sekretessbedömning kan utgöra ett vägledande moment i bedömningen av vilka uppgifter som är säkerhetsskyddsklassificerade. Det är dock alltid risken för skada för Sveriges säkerhet vid ett röjande som är avgörande för om en uppgift är att bedöma som säkerhetsskyddsklassificerad.

Särskilt relevant för vägledning i fråga om vilka uppgifter som till sin natur medför krav på säkerhetsskydd är den så kallade försvarssekretessen i 15 kap. 2 § OSL. En uppgift som omfattas av försvarssekretess kommer alltid vara säkerhetsskyddsklassificerad. Även andra sekretessbestämmelser som delvis överlappar försvarssekretessen kan tjäna som vägledning till vilka förhållanden som är av betydelse för Sveriges säkerhet. Det är samtidigt viktigt att komma ihåg att det finns många uppgifter som omfattas av sekretess utan att dess röjande skulle innebära skada för Sveriges säkerhet.

Notera:
Några vanligt förekommande bestämmelser om sekretess i OSL som kan vara av relevans för säkerhetsskyddsklassificering är:

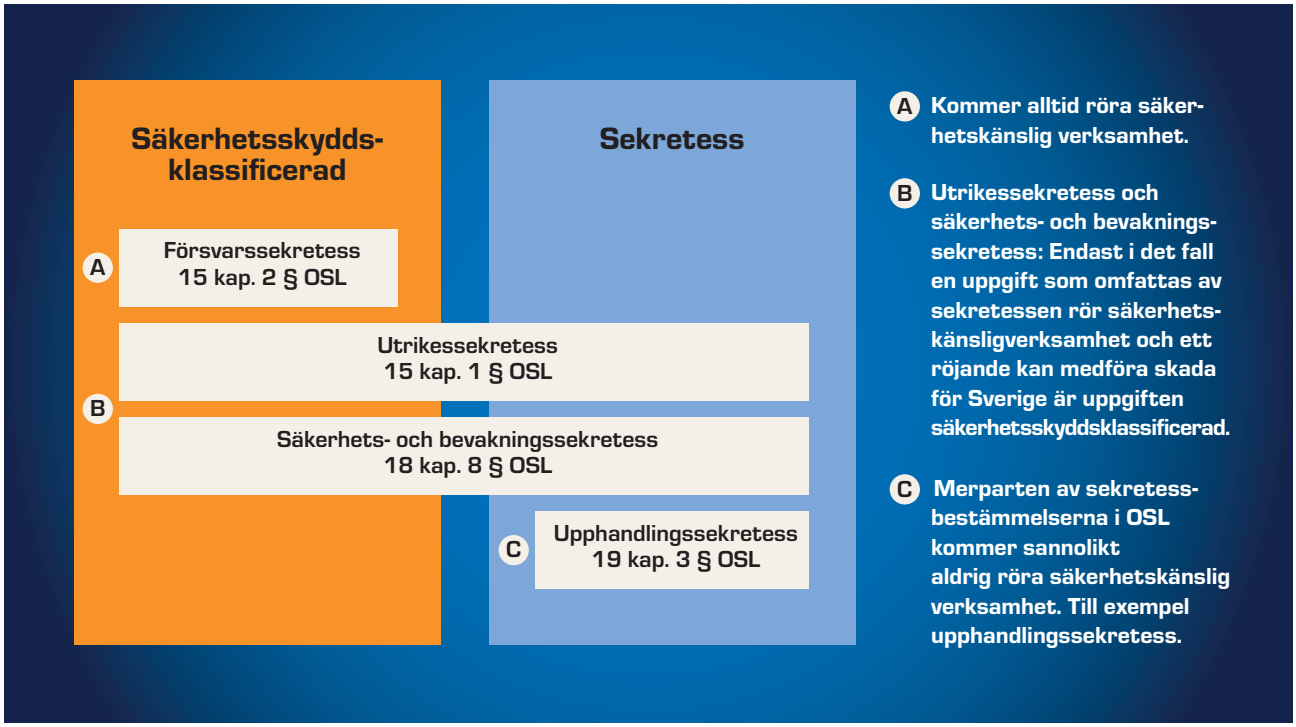
- 15 kap. 1 § om utrikessekretess
- 15 kap. 2 § om försvarssekretess
- 18 kap. 1 § om förundersökningar m.m.
- 18 kap. 2 § om underrättelseverksamhet
- 18 kap. 8 § om säkerhets- eller bevakningsåtgärd
- 18 kap. 13 § om risk- och sårbarhetsanalyser m.m.

Listan ovan är inte heltäckande. Det är endast sekretessbestämmelser till skydd för allmänna, inte enskilda intressen som kan vara av relevans för säkerhetsskyddsklassificering.

Huruvida en uppgift omfattas av sekretess prövas i regel först i samband med en begäran om utlämnande av allmän handling från en myndighet, eller när en myndighet har behov av att dela med sig av uppgiften till någon utomstående. Här skiljer sig OSL och säkerhetsskyddslagstiftningen markant. För alla som bedriver säkerhetskänslig verksamhet, såväl myndigheter som enskilda, ska bedömningen av huruvida en uppgift är säkerhetsskyddsklassificerad, och vilken säkerhetsskyddsklass uppgiften i sådant fall har, göras redan när uppgiften skapas eller på annat sätt först hanteras. Syftet med säkerhetsskyddsklassificeringen är att kunna vidta rätt säkerhetsskyddsåtgärder. Om uppgiften i ett senare skede avses att lämnas ut eller inte, eller om handlingen som innehåller uppgiften enligt OSL kan anses upprättad eller inte, saknar betydelse.

Notera:
Kravet på säkerhetsskyddsklassificering gäller även minnesanteckningar, arbetsmaterial och liknande handlingar.

Figur 1. Hur fyra sekretessbestämmelser i OSL förhåller sig till säkerhetsskyddslagstiftningen.



2.2 Indelning i säkerhetsskyddsklasser

§ *2 kap. 5 § första stycket säkerhetsskyddslagen*

§ *3 kap. 7 § säkerhetsskyddsförordningen*

Syftet med indelning av uppgifter i säkerhetsskyddsklasser är att fastställa en korrekt skyddsnivå för uppgifterna. Vilka säkerhetsskyddsåtgärder som ska vidtas beror på vilken säkerhetsskyddsklass de aktuella uppgifterna har. Det är därför viktigt med tydliga rutiner för klassificering av uppgifter. Felaktigt klassificerade uppgifter riskerar att leda till antingen ett för dåligt skydd, det vill säga en risk för att uppgifterna röjs, eller ett alltför omfattande skydd, vilket såväl kan medföra onödiga kostnader som försvåra för verksamheten att verka effektivt.

Vid indelning av uppgifter i säkerhetsskyddsklasser bör eventuella konsekvenser av ett röjande som framstår som orimliga inte beaktas. I stället för att utgå från det värsta tänkbara scenariot bör bedömningen ske utifrån det värsta rimliga scenariot, om uppgifterna röjs. Enligt samma princip bör inte heller beaktas vad som skulle hända om andra uppgifter skulle röjas vid samma tidpunkt.

2.3 Uppgifter som omfattas av internationella åtaganden om säkerhetsskydd

§ *2 kap. 5 § andra stycket säkerhetsskyddslagen*

Hur säkerhetsskyddsklasser benämns varierar mellan olika länder. Det saknas enhetlig internationell nomenklatur. Varje internationell överenskommelse om säkerhetsskydd innehåller därför bestämmelser där de nationella säkerhetsskyddsklasserna framgår och hur dessa förhåller sig till varandra.

I det internationella samarbetet kan det förekomma säkerhetsskyddsklassificerade handlingar. Det kan till exempel handla om en handling som inkommer från en EU-stat och som är märkt EU SECRET. Eftersom handlingen redan har klassificerats av en annan stat ska den enligt den aktuella överenskommelsen delas in i säkerhetsskyddsklass hemlig. Med överenskommelse i detta sammanhang avses i typfallet ett GSA (eng. *general security agreement*). När det kommer till EU regleras detta i en särskild överenskommelse mellan Europeiska unionens medlemsstater, församlade i rådet, om skydd av säkerhetsskyddsklassificerade uppgifter som utbyts i Europeiska unionens intresse (2011/C 202/05). Majoriteten av GSA och andra typer av internationella överenskommelser om säkerhetsskydd finns publicerade på regeringens webbplats under Sveriges internationella överenskommelser (SÖ).

Ett exempel är de olika säkerhetsskyddsklasserna inom EU, i det följande på franska respektive engelska, med de svenska motsvarigheterna inom parentes.

Franska	Engelska	Svenska
TRÈS SECRET UE	EU TOP SECRET	KVALIFICERAT HEMLIG
SECRET UE	EU SECRET	HEMLIG
CONFIDENTIEL UE	EU CONFIDENTIAL	KONFIDENTIELL
RESTREINT UE	EU RESTRICTED	BEGRÄNSAT HEMLIG

2.4 Samling av uppgifter

Informationssystem kan innehålla stora mängder uppgifter av samma natur. Därtill finns olika funktioner för att kunna sammanställa och kombinera olika uppgifter.

Även en enskild handling kan innehålla uppgifter som går att kombinera.

Ovanstående innebär att det i ett informationssystem eller i en handling kan vara möjligt att utläsa ”nya” uppgifter i betydelsen uppgifter som inte uttryckligen framgår, men som följer av övriga uppgifter.

- **Ackumulering:** Med ackumulering avses häri en större samling av många liknande uppgifter, till exempel ett register över anställda. Ackumulering av uppgifter leder i normalfallet inte till några konsekvenser för säkerhetsskyddsklassificeringen av uppgifterna eller uppgiftssamlingen.
- **Aggregering:** En samling av uppgifter kan i vissa fall leda till så kallad aggregering. Med aggregering avses häri att det genom att kombinera uppgifterna i samlingen går att härleda ny information, till exempel genom nyttjande av uteslutningsmetoden eller av så kallad motsatstolkning. Det innebär att en eller flera nya uppgifter skapas genom aggregeringen.

Notera:
En aggregering kan uppstå när uppgifter ackumuleras.

De nya uppgifter som går att härleda genom aggregering ska säkerhetsskyddsklassificeras, precis som alla andra uppgifter i verksamheten. Observeras bör att den nya uppgiften kan bedömas ha högre säkerhetsskyddsklass än de enskilda uppgifterna i uppgiftssamlingen. Den nya uppgiften blir då dimensionerande för de säkerhetsskyddsåtgärder som behöver vidtas. Nya uppgifter som identifieras vid en aggregering behöver vara konkreta och formulerbara. Det bör finnas spårbarhet i ställningstagandena om varför de uppstår.

Aggregering av uppgifter behöver beaktas även för samlingar av uppgifter som inte bedöms säkerhetsskyddsklassificerade, eftersom eventuella nya uppgifter som kan härledas ur samlingen skulle kunna vara säkerhetsskyddsklassificerade.

Notera:
Att nya uppgifter uppstår kan även bero på att ny funktionalitet tillförs ett informationssystem, vilken ger möjlighet till nya slags sammanställningar, eller att andra typer av uppgifter tillförs ett informationssystem.

+ *Se även avsnitt 5.3.2 Samråd vid väsentlig förändring av ett informationssystem.*

2.5 Stöd i bedömning vid indelning i säkerhetsskyddsklass

I förarbetena till den nya säkerhetsskyddslagen ges ingen närmare förklaring till vad som avses med respektive säkerhetsskyddsklass. Nedanstående värdeord kan tjäna som viss vägledning när det gäller indelning i säkerhetsskyddsklass.

Med nationell förmåga kan till exempel avses den nationella försvarsförmågan, den nationella elförsörjningsförmågan eller den nationella betalningsförmågan.

Notera:
Värdeorden i tabell 1 ska inte blandas ihop med beskrivningarna av de olika konsekvensnivåerna som återfinns i Säkerhetspolisens Vägledning i säkerhetsskydd: Säkerhetsskyddsanalys.

En handling ska förses med en anteckning om vilken högsta säkerhetsskyddsklass uppgifterna i handlingen har.

Tabell 1. Vägledning för indelning i säkerhetsskyddsklass

Säkerhetsskydds-klass	Den skada som ett röjande av uppgifterna kan medföra för Sveriges säkerhet	Värdeord till stöd för bedömningen om en viss typ av skada föreligger
Kvalificerat hemlig	Ett röjande kan medföra en synnerligen allvarlig skada.	Synnerligen allvarliga negativa konsekvenser av stor omfattning, under lång tid, som utgör ett direkt hot mot den nationella förmågan. Konsekvenserna är inte begränsade till enstaka funktioner. Mycket svårt att återställa.
Hemlig	Ett röjande kan medföra en allvarlig skada.	Allvarliga/betydande negativa konsekvenser, av stor omfattning eller av väsentlig art, som innebär ett direkt hot mot den nationella förmågan, om än mot avgränsade funktioner. Svårt att återställa.
Konfidentiell	Ett röjande kan medföra en inte obetydlig skada.	Påtagliga negativa konsekvenser för den nationella förmågan, om än i begränsad omfattning, som äventyrar, vållar skada, hindrar, underlättar för en antagonist eller innebär större avbrott.
Begränsat hemlig	Ett röjande kan medföra endast ringa skada.	Ringa negativa konsekvenser som är begränsade till att påverka, försvåra eller störa den nationella förmågan i mindre omfattning.

2.5.1 Mottagande av säkerhetsskyddsklassificerade handlingar

En verksamhetsutövare som tar emot en säkerhetsskyddsklassificerad handling av en annan (svensk) verksamhetsutövare är inte i formell mening bunden av den tidigare säkerhetsskyddsklassificeringen av uppgifterna i handlingen. Utgångspunkten bör dock vara att den ursprungliga säkerhetsskyddsklassificeringen ska respekteras av mottagaren, om det inte tillkommit några nya omständigheter sedan indelningen i säkerhetsskyddsklass gjordes. För detta talar att det är den verksamhetsutövare som upprättat handlingen som också borde ha bäst möjlighet att bedöma vilken skada ett röjande skulle medföra för Sveriges säkerhet, särskilt om uppgifterna rör verksamhetsutövarens egen verksamhet.

Se även avsnitt 2.5.2 Klassificering av uppgifter som omfattas av internationellt åtagande om handlingar som kommer från en annan stat eller en mellanstatlig organisation med vilken Sverige har ingått överenskommelse om säkerhetsskydd.

För uppgifter i säkerhetsskyddsklassen kvalificerat hemlig finns särskilda krav. Se avsnitt 3.4 Anteckning om samråd vid sänkning av säkerhetsskyddsklass.

2.5.2 Klassificering av uppgifter som omfattas av internationellt åtagande

I internationella överenskommelser om säkerhetsskydd som Sverige har ingått med andra stater och mellanfolkliga organisationer, framgår vanligtvis att säkerhetsskyddsklassificerade uppgifter som har klassificerats av den andra staten eller mellanfolkliga organisationen inte får ändras utan skriftligt tillstånd från den som har klassificerat uppgifterna.

Om det finns behov av att ändra säkerhetsskyddsklass på en säkerhetsskyddsklassificerad handling som har inkommit från en annan stat eller mellanfolklig organisation, måste den överenskommelsen som gäller för samarbetet undersökas i syfte att utröna om det är tillåtet att ändra säkerhetsskyddsklassificeringen eller om det först krävs ett skriftligt tillstånd från avsändaren.

Frågan om utlämnande till enskild av allmän handling som är av synnerlig betydelse för rikets säkerhet ska enligt 1 § offentlighets- och sekretessförordningen (2009:641) (OSF) prövas av statsministern eller chefen för Justitiedepartementet, Utrikesdepartementet eller Försvarsdepartementet, allt beroende på vad uppgifterna i handlingen rör och var handlingen förvaras.

Krav på internationellt säkerhetsskyddsåtagande

§ 3 kap 9 § säkerhetsskyddsförordningen (2021:955)

När en verksamhetsutövare i Sverige lämnar säkerhetsskyddsklassificerade uppgifter till någon i utlandet måste det enligt denna bestämmelse finnas ett internationellt säkerhetsskyddsåtagande (GSA, eng. *general security agreement*) med den andra staten eller mellanfolkliga organisationen. Kravet gäller även när säkerhetsskyddsklassificerade uppgifter ska lämnas till en utländsk leverantör. Vid publiceringen av denna vägledning har dock bestämmelsen ännu inte trätt i kraft, jfr säkerhetsskyddsförordningens ikraftträdande- och övergångsbestämmelser punkten 6.

2.6 Stöd i bedömning av tillgänglighet och riktighet av informationssystem

§ 2 kap. 3–5 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd

I verksamhetsutövarens säkerhetsskyddsanalys kan informationssystem identifieras som skyddsvärden. Utifrån tillgänglighet och riktighet kan informationssystemet placeras i en konsekvensnivå.

Ett viktigt skyddsvärde från säkerhetsskyddsanalysen är också den tid det tar innan skada för Sveriges uppstår om verksamheten avbryts. Tidsspannet utgör ett viktigt underlag för utformning av säkerhetskrav (säkerhetskyddsåtgärder) för att kunna upprätthålla tillgänglighet och riktighet.

När det gäller frågan om tillgänglighet, se vidare i avsnitt 4.16 Åtgärder för att upprätthålla kontinuitet.

Säkerhetsskyddsklassificerade uppgifter ska förstöras på ett sätt som omöjliggör återskapande av uppgifterna. Metoder för förstöring är till exempel dokumentförstörare eller bränning.

3 Hantering av säkerhetsskyddsklassificerade uppgifter och handlingar

3.1 Krav på godkännande av informationssystem

§ *3 kap. 3 § säkerhetskyddsförordningen*

§ *3 kap. 1 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Bestämmelsen i 3 kap. 3 § säkerhetsskyddsförordningen om krav på godkännande från säkerhetsskyddssynpunkt inför driftsättning omfattar nya informationssystem som har betydelse för säkerhetskänslig verksamhet. En motsvarande bestämmelse fanns i 3 kap. 3 § i den numera upphävda säkerhetsskyddsförordningen (2018:658). Enligt tillhörande ikraftträdande- och övergångsbestämmelser omfattar detta krav på godkännande inte informationssystem som togs i drift innan den 1 april 2019. Detta betyder dock inte att sådana äldre informationssystem inte behöver vara godkända från säkerhetsskyddssynpunkt av verksamhetsutövaren.

Godkännandekravet i 3 kap. 1 § Säkerhetspolisens föreskrifter är, till skillnad från ovanstående bestämmelser, av löpande karaktär och omfattar således alla informationssystem (och lagringsmedium) som hanterar säkerhetsskyddsklassificerade uppgifter, oberoende av när informationssystemet togs i drift.

Säkerhetsskyddsklassificerade uppgifter får således endast behandlas i informationssystem eller på lagringsmedium som verksamhetsutövaren godkänt för lägst den säkerhetsskyddsklass uppgifterna har. Av godkännandet ska framgå den högsta säkerhetsskyddsklass som får behandlas i informationssystemet eller på lagringsmediet.

+ *Se vidare i avsnitt 5 om behövligt underlag för beslut om godkännande och avsnitt 6 om vad som gäller informationssystem som driftsattes före den 1 april 2019.*

3.2 Krav på att uppmärksamma mottagaren på säkerhetsskyddsklassificeringar

§ *3 kap. 2 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

För att säkerställa rätt hantering av säkerhetsskyddsklassificerade uppgifter ska mottagaren uppmärksammas på att uppgifterna är säkerhetsskyddsklassificerade och vilken säkerhetsskyddsklass de har. Kravet gäller även inom en verksamhetsutövares egen verksamhet, till exempel då en anställd delar säkerhetsskyddsklassificerade uppgifter i ett internt e-postmeddelande.

Notera:
En anteckning om säkerhetsskyddsklass som syns för mottagaren vid mottagandet är tillräcklig för att avsändaren ska anses ha uppmärksammat mottagaren.

3.3 Rutiner

§ *3 kap. 3 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Bestämmelsen innefattar krav på rutiner för behandling av säkerhetsskyddsklassificerade uppgifter genom hela deras livscykel. Rutinerna ska minst reglera vad som gäller för *spårbarhet, upprättande, kopiering, utskrift, utdrag, kvittering, distribution, medförande, inventering och förstöring*.

Beroende på vilken säkerhetsskyddsklass en uppgift har finns olika miniminivåer för säkerhetsskyddsåtgärderna.

+ *Se sammanställningarna i tabellerna 2–4 nedan.*

Kraven ska betraktas som minimikrav; verksamhetsutövaren behöver analysera huruvida det finns behov av att komplettera dessa kravställningar.

Tabell 2. Anteckningar, märkning, medgivande och kvittering.

Anteckning, märkning, medgivande och kvittering	Begränsat hemlig	Konfidentiell	Hemlig	Kvalificerat hemlig
Anteckning om säkerhetsskyddsklass och i förekommande fall:	Ja	Ja	Ja	Ja
Anteckning om handlingens beteckning	Nej	Ja	Ja	Ja
Antal sidor	Nej	Ja	Ja	Ja
Uppgift om bilagor	Nej	Ja	Ja	Ja
Exemplarnummer (fysisk handling)*	Nej	Ja	Ja	Ja
Anteckning om ursprungsland för handling som kan komma att lämnas över till en utländsk myndighet, mellanfolklig organisation eller utländsk leverantör (om det inte är olämpligt)	Ja	Ja	Ja	Ja
Märkning av lagringsmedium med säkerhetsskyddsklass och identifieringsnummer**	Ja	Ja	Ja	Ja
Antecknande om mottagning av elektronisk handling	Nej	Nej	Nej	Ja
Anteckning vid/efter muntlig delgivning eller visning	Nej	Nej	Nej	Ja
Krav på medgivande från högsta chef eller motsvarande organ vid kopia eller utdrag (får delegeras)	Nej	Nej	Nej	Ja
Kvittering av fysisk handling i register, liggare eller på ett kvitto*	Nej	Ja	Ja	Ja
Kvittens ska bevaras***	–	Minst 10 år	Minst 10 år	Minst 25 år

** I offentlig verksamhet gäller dessa krav enbart för allmänna handlingar.*
*** Om lagringsmediet är fastmonterat i annan utrustning ska i stället utrustningen märkas.*
**** I offentlig verksamhet tillämpas i stället bestämmelserna om gallring i arkivlagen (1990:782) och föreskrifter som har meddelats med stöd av den lagen.*

Tabell 3. Förvaring, medförande och distribution.

Förvaring, medföra och distribution	Begränsat hemlig	Konfidentiell	Hemlig	Kvalificerat hemlig
En säkerhetsskyddsklassificerad handling ska vara under kontroll eller förvaras i ett utrymme som verksamhetsutövaren har godkänt enligt 5 kap. 10 § PMFS 2022:1 * såvida inte handlingen skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten	Ja	Ja	Ja	Ja * *
I ett register över säkerhetsskyddsklassificerade handlingar ska handlingens beteckning, säkerhetsskyddsklass, antal exemplar och mottagare av respektive exemplar framgå. För varje exemplar som förvaras hos verksamhetsutövaren ska det framgå vem som kvitterat exemplaret, när exemplaret inventerats och om exemplaret återlämnats, förkommit, arkiverats eller förstörts	Nej	Ja	Ja	Ja
Får endast sändas med en godkänd distributör	Nej	Ja	Ja	Ja
Ska skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten vid kommunicering till ett informationssystem utanför verksamhetsutövarens kontroll	Ja	Ja	Ja	Ja
Tillstånd från högsta chef eller motsvarande organ att medföra handling utanför verksamhetsutövarens lokaler (får delegeras)	Nej	Nej	Nej	Ja
Vid försändelser till och från utlandet ska Utrikesdepartementets kurirförbindelse användas. Tillsynsmyndigheterna får i ett enskilt fall medge undantag från detta krav	Ja, såvida inte handlingen skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten	Ja, såvida inte handlingen skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten	Ja, såvida inte handlingen skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten	Ja, såvida inte handlingen skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten
Medföra en försändelse med en säkerhetsskyddsklassificerad handling i till utlandet	Ja i enskilt fall efter beslut av säkerhetsskyddschef för behörig personal	Ja i enskilt fall efter beslut av säkerhetsskyddschef för behörig personal	Ja i enskilt fall efter beslut av säkerhetsskyddschef för behörig personal	Efter beslut av verksamhetsutövarens högsta chef

** Notera att kravet på att sådana utrymmen endast får godkännas om de är försedda med eller omges av åtgärder för att upptäcka, försvåra och hantera obehörigt tillträde utifrån identifierade säkerhetshot och en beskrivning av dimensionerande antagonistiska förmågor, om Säkerhetspolisen tillhandahållit en sådan, fortfarande gäller.*

** * Beslut att godkänna ett förvaringsutrymme avsett för förvaring av säkerhetsskyddsklassificerade handlingar i säkerhetsskyddsklassen kvalificerat hemlig ska fattas av verksamhetsutövarens högsta chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer.*

Tabell 4. Inventering och förstöring.

Inventering och förstöring	Begränsat hemlig	Konfidentiell	Hemlig	Kvalificerat hemlig
Årlig inventering av handlingar*	Nej	Ja (endast fysiska)	Ja (endast fysiska)	Ja (även elektroniska)
Årlig inventering av lagringsmedier	Nej	Ja	Ja	Ja
Ska förstöras så att återskapande omöjliggörs	Ja	Ja	Ja	Ja
Dokumentering av förstöring av fysisk handling	Nej	Ja	Ja	Ja

**För offentliga verksamhetsutövare gäller kravet enbart för allmänna handlingar*

3.4 Anteckning

§ *3 kap. 7 § säkerhetsskyddsförordningen*

§ *3 kap. 4–7 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd*

En säkerhetsskyddsklassificerad handling ska förses med en anteckning om vilken säkerhetsskyddsklass uppgifterna i handlingen har, i syfte att klargöra vilka hanteringsregler som gäller för handlingen. Kravet på anteckning gäller både för fysiska och elektroniska handlingar som innehåller säkerhetsskyddsklassificerade uppgifter.

Uppgifter upp till och med säkerhetsskyddsklassen hemlig bör ha en anteckning som är röd och omgärdas av en enkel ram. För uppgifter i säkerhetsskyddsklassen kvalificerat hemlig bör anteckningen omgärdas av en dubbel ram.

Anteckningen bör även innehålla hänvisning till tillämplig sekretessbestämmelse i OSL, datum då anteckningen gjordes, samt vilken verksamhetsutövare som har gjort anteckningen. På så sätt uppfyller även anteckningen kriterierna för en sekretessmarkering.

Även enskilda verksamhetsutövare bör, trots att de inte omfattas av OSL, hänvisa till tillämplig sekretessbestämmelse i OSL. Detta i syfte att underlätta hanteringen av handlingar som distribueras mellan enskilda och offentliga verksamhetsutövare och för att åstadkomma transparens i säkerhetsskyddsklassificeringen.

För allmänna handlingar i säkerhetsskyddsklassen kvalificerat hemlig ska det på anteckningen även framgå om det är chefen för Justitie-, Utrikes-, eller Försvarsdepartementet som prövar om handlingen efter begäran kan utlämnas till en enskild.

+ *Se figurerna 2 och 3 nedan för exempel på hur anteckningarna kan utformas.*

För elektroniska handlingar eller samlingar av uppgifter där formatet inte stödjer en anteckning kan uppgift om säkerhetsskyddsklass i stället anges i filnamnet eller liknande. Exempelvis kan en ordbehandlingsfil ha stöd för hantering av anteckningar enligt ovan medan en logg-fil saknar den möjligheten.

Om en handling i säkerhetsskyddsklass konfidentiell eller högre består av flera sidor eller har bilagor, ska även antalet sidor och bilagor anges på första sidan. Efterföljande sidor i handlingen bör innehålla en anteckning om säkerhetsskyddsklass och i övrigt hänvisa till anteckningen på första sidan.

Vidare ska fysiska handlingar i säkerhetsskyddsklasserna konfidentiell eller högre förses med en anteckning om handlingens exemplarnummer. Detta gäller även om det endast finns ett fysiskt exemplar av handlingen. Notera att detta krav även gäller för handlingar som skickas via kryptofax. I offentlig verksamhet gäller detta krav endast för allmänna handlingar.

Om det kan antas att en säkerhetsskyddsklassificerad

handling kan komma att lämnas över till utländska myndigheter eller leverantörer, ska den, om det inte är olämpligt, förses med en anteckning om ursprungsland.

Om en säkerhetsskyddsklassificerad handling inte längre ska vara indelad i säkerhetsskyddsklass, eller ska delas in i annan säkerhetsskyddsklass än vad som anges på handlingen, ska detta antecknas på handlingen eller i ett register. Det ska av anteckningen framgå vem som har fattat beslut om att ändra säkerhetsskyddsklass och datum för beslutet. Om beslutet innebär att en säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen kvalificerat hemlig inte längre ska vara indelad i den säkerhetsskyddsklassen, ska beslutet fattas av verksamhetsutövarens högsta chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer. Om handlingen upprättats av någon annan än verksamhetsutövaren ska samråd ske med den som upprättat handlingen innan beslutet fattas. Anteckning om samrådet ska göras på handlingen.

Figur 2. Exempel på hur anteckningar om säkerhetsskyddsklass kan se ut för offentliga verksamhetsutövare. Den nedre anteckningen används på efterföljande sidor, när handlingen innehåller flera sidor.

Figur 3. Exempel på hur anteckningar om säkerhetsskyddsklass kan se ut för enskilda verksamhetsutövare. Den nedre anteckningen används på efterföljande sidor, när handlingen innehåller flera sidor.

3.5 Förvaring

§ *3 kap. 9 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

En säkerhetsskyddsklassificerad handling ska vara under kontroll eller förvaras i ett förvaringsutrymme som verksamhetsutövaren har godkänt enligt 5 kap. 10 § Säkerhetspolisens föreskrifter om säkerhetsskydd.

+ *Se avsnitt 3.8, för exempel på vad kontroll innebär.*

Förvaringsutrymmen som är avsedda för förvaring av säkerhetsskyddsklassificerade uppgifter får endast godkännas om de är försedda med eller omges av åtgärder för att upptäcka, försvåra och hantera obehörigt tillträde. Åtgärderna ska vara gjorda utifrån identifierade säkerhetshot och en beskrivning av dimensionerande antagonistiska förmågor, om Säkerhetspolisen tillhandahållit en sådan.

+ *Se Vägledning i säkerhetsskydd – Fysisk säkerhet för mer information om förvaring.*

När det gäller förvaringsutrymmen avsedda för förvaring av säkerhetsskyddsklassificerade handlingar i säkerhetsskyddsklassen kvalificerat hemlig ska dessa godkännas av verksamhetsutövarens högsta chef eller motsvarande organ, eller den som sådan chef eller sådant organ bestämmer.

För en handling som skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten gäller inte kravet på godkänt förvaringsutrymme.

3.6 Märkning av lagringsmedium

§ *3 kap. 11 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Märkning med identifieringsuppgift syftar till att fastställa en specifik identitet för ett lagringsmedium som innehåller säkerhetsskyddsklassificerade uppgifter. Verksamhetsutövaren bör upprätta en förteckning över de lagringsmedier som finns i verksamheten för att underlätta vid den årliga inventeringen.

+ *För exempel på anteckning som kan användas som utgångspunkt vid märkning, se figur 2 och 3.*

Om ett lagringsmedium, som är fastmonterat i en utrustning (vilken i sådant fall ska vara märkt), avlägsnas från utrustningen ska lagringsmediet märkas.

3.7 Distribution inom och utom verksamheten

§ *3 kap. 3 och 12 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd*

Rutiner för distribution ska omfatta både intern och extern distribution av säkerhetsskyddsklassificerade uppgifter.

Verksamhetsutövaren bör analysera verksamhetens behov av distribution av säkerhetsskyddsklassificerade uppgifter. Analysen bör som minst omfatta aktuella säkerhetsskyddsklasser för uppgifterna och hos aktuella mottagare, i syfte att få underlag för att kunna bedöma vilka säkerhetsskyddsåtgärder och rutiner som är nödvändiga. Verksamhetsutövaren ska godkänna den eller de distributörer som får användas för försändelser av säkerhetsskyddsklassificerade fysiska handlingar i säkerhetsskyddsklassen konfidentiell eller högre eller lagringsmedium som innehåller handlingar i motsvarande nivå.

Verifiering av att en försändelse nått rätt mottagare utan obehörig åtkomst är en viktig säkerhetsskyddsåtgärd vid distribution. Det är också viktigt att, innan distribution sker, säkerställa att mottagaren är medveten om sitt ansvar att verifiera att ingen obehörig åtkomst skett.

Notera:
En metod för verifiering kan vara att använda säkerhetsförslutet engångsemballage. Det förutsätter att avsändaren granskar att emballaget är oskadat och försluter emballaget enligt tillverkarens instruktioner samt sparar eller noterar emballagets unika serienummer. Mottagaren undersöker okulärt att emballaget inte uppvisar spår av manipulation samt verifierar emballagets unika serienummer med avsändaren.

Om spår av manipulation upptäcks, eller om serienumret på försändelsen inte överensstämmer med det nummer som angivits av avsändaren, ska det utredas som en möjlig säkerhetshotande händelse. Händelsen ska skyndsamt anmälas till Säkerhetspolisen enligt 2 kap. 4 § första stycket säkerhetsskyddsförordningen.

Rutiner för handlingar som skyddas av kryptografiska funktioner som har godkänts av Försvarsmakten ser annorlunda ut. Det kan finnas behov av ytterligare säkerhetshetsskyddsåtgärder, exempelvis för spårbarhet i distributionen.

3.8 Medförande utanför verksamhetsutövarens lokaler

§ *1 kap. 4 §, 3 kap. 18 och 20 §§ samt 5 kap. 10 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Med verksamhetsutövarens lokaler avses alla områden, byggnader och andra anläggningar eller objekt där verksamhetsutövaren har ansvar för, och kontroll över, säkerhetsskyddet.

En säkerhetsskyddsklassificerad handling som medförs utanför verksamhetsutövarens lokaler ska vara under kontroll eller förvaras i ett förvaringsutrymme som verksamhetsutövaren har godkänt enligt 5 kap. 10 § Säkerhetspolisens föreskrifter om säkerhetsskydd.

En säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen kvalificerat hemlig får medföras från verksamhetsutövarens lokaler efter beslut från verksamhetsutövarens högsta chef eller motsvarande organ, eller den som sådan chef eller sådant organ bestämmer.

Ett sådant beslut ska dokumenteras.

Några exempel på när säkerhetsskyddsklassificerade fysiska handlingar eller lagringsmedier är under kontroll är:

- Handlingarna eller lagringsmedierna läggs i en väska, portfölj eller liknande som personen bär med sig överallt under hela medförandet.
- Under övernattning på hotell eller i bostad hålls väskan eller portföljen låst. Dessutom låses väskan eller portföljen fast med en vajer i nära anslutning till sängen, så att ett eventuellt tillgrepp under natten försvåras och lättare kan upptäckas.
- Den person som medför handlingar och lagringsmedier stannar kvar i hotellrummet eller bostaden under hela den tid som väskan eller portföljen är fastlåst med vajern.
- På flygplan tas väskan eller portföljen med som handbagage och hålls under uppsikt

3.9 Distribution till och från utlandet

§ *3 kap. 10 § säkerhetsskyddsförordningen, 3 kap. 13 och 19–20 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd*

För försändelser av säkerhetsskyddsklassificerade handlingar till och från utlandet ska Utrikesdepartementets kurirförbindelser anlitas, såvida handlingarna inte skyddas av kryptografiska funktioner som har godkänts av Försvarsmakten. Tillsynsmyndigheterna får i enskilda fall medge undantag från detta krav. Notera att säkerhetsskyddsåtgärder behöver vidtas även för säkerhetsskyddsklassificerade handlingar som skickas med Utrikesdepartementets kurirförbindelser.

Säkerhetsskyddschefen får i ett enskilt fall besluta att personal, som är behörig enligt 2 kap. 2 § säkerhetsskyddsförordningen, till utlandet får medföra en försändelse med säkerhetsskyddsklassificerad handling i säkerhetsskyddsklassen hemlig eller lägre. När det gäller handlingar i säkerhetsskyddsklassen kvalificerat hemligt ska verksamhetsutövarens högste chef eller motsvarande organ eller den som sådan chef eller sådant organ bestämmer, lämna motsvarande tillstånd.

3.10 Förstöring

§ *3 kap. 22–23 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd*

Säkerhetsskyddsklassificerade uppgifter ska förstöras på ett sätt som omöjliggör återskapande av uppgifterna. Metoder för förstöring är till exempel dokumentförstörare eller bränning. Vid användning av dokumentförstörare ska verksamhetsutövaren säkerställa att resterna inte går att utläsa någonting av och således inte kan användas för att återskapa den förstörda handlingen.

Förstöring av en säkerhetsskyddsklassificerad fysisk handling i säkerhetsskyddsklassen konfidentiell eller högre ska dokumenteras.

Förstöring av säkerhetsskyddsklassificerade uppgifter kan även utföras av en leverantör. Verksamhetsutövaren behöver då säkerställa säkerhetsskyddet för uppgifterna till dess att de är förstörda.

+ *Se vidare i Vägledning i säkerhetsskydd – Skyldigheter vid exponering av säkerhetskänslig verksamhet.*

3.11 Avveckling eller återanvändning av lagringsmedium

§ *3 kap. 24 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Det är svårt att radera information på lagringsmedier så att återskapning omöjliggörs. Därför bör lagringsmedier återanvändas restriktivt.

- Personliga, bärbara lagringsmedier, till exempel USB-stickor, bör endast återanvändas för lagring av uppgifter med samma eller högre säkerhetsskyddsklass än tidigare lagrade uppgifter och av samma användare eller av annan användare som är behörig till samma uppgifter som tidigare lagrats på lagringsmediet.
- Andra lagringsmedier bör endast återanvändas i informationssystem godkänt för behandling av säkerhetsskyddsklassificerade uppgifter i samma eller högre säkerhetsskyddsklass än tidigare lagrade uppgifter.

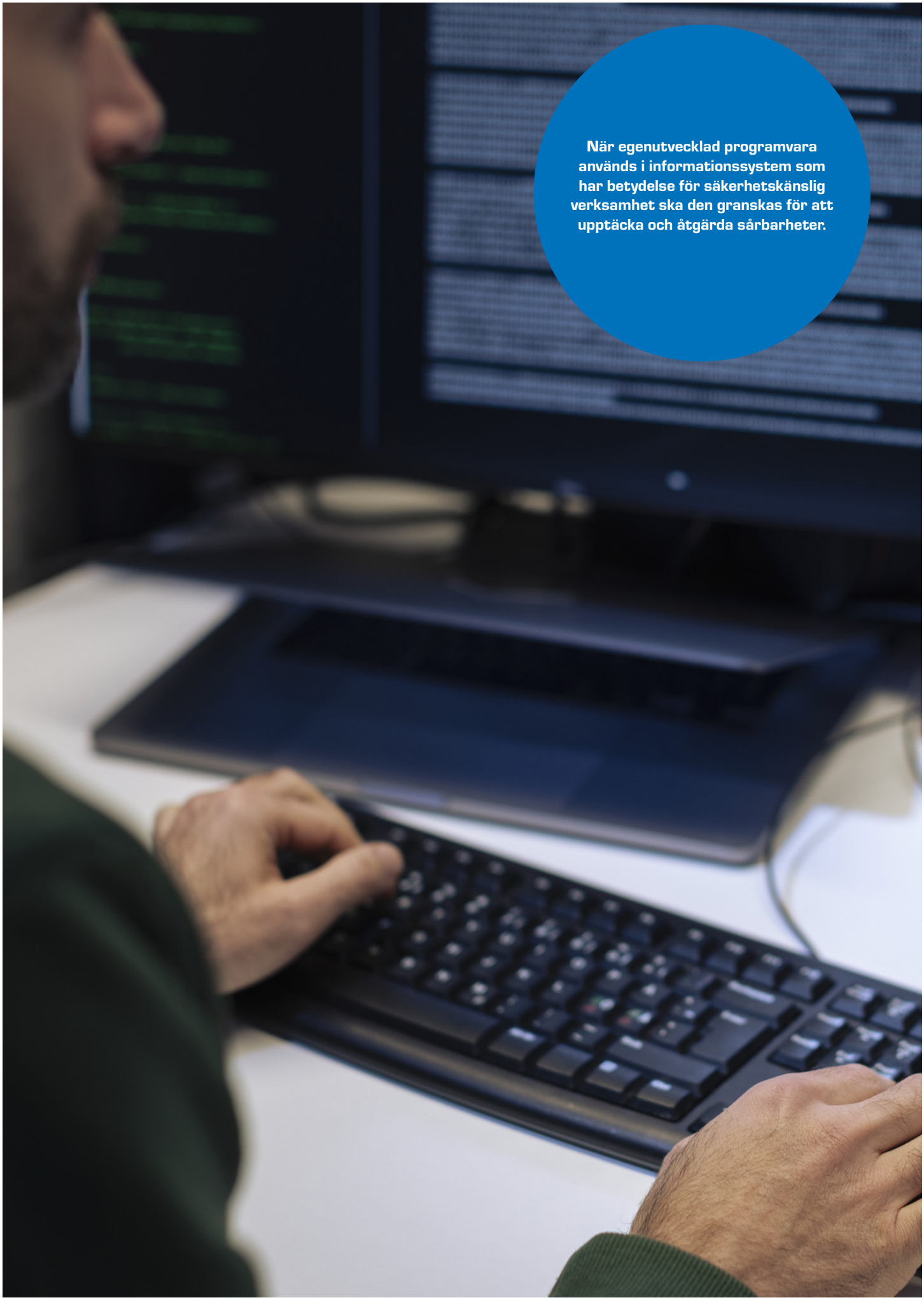
Verksamhetsutövaren ska ha rutiner för avveckling och återanvändning av lagringsmedier som använts i säkerhetskänslig verksamhet. Ett lagringsmedium som inte ska återanvändas av verksamhetsutövaren bör avvecklas genom fysisk destruktion.

Vid distribution bör alltid ett nytt lagringsmedium användas.

Notera:
En vanlig metod för att försöka förhindra möjligheten att återskapa information på ett lagringsmedium är överskrivning av data. Detta innebär att befintliga data vid upprepade tillfällen skrivs över och ersätts av annan, obetydlig data. En annan metod är att förstöra nyckeln till ett krypterat lagringsmedium. Båda dessa metoder har visat sig innehålla sårbarheter som inneburit att en person som har tillgång till lagringsmediet kan återskapa delar av informationen.

3.12 Lokaler godkända för samtal som behandlar säkerhetsskyddsklassificerade uppgifter

För närmare vägledning såvitt avser lokaler, se Vägledning i säkerhetsskydd – Fysisk säkerhet och Vägledning i säkerhetsskydd – Avlyssningsskyddade utrymmen.


När egenutvecklad programvara används i informationssystem som har betydelse för säkerhetskänslig verksamhet ska den granskas för att upptäcka och åtgärda sårbarheter.

4 Informationssäkerhet i och kring informationssystem

I detta kapitel berörs olika krav som följer av fjärde kapitlet i Säkerhetspolisens föreskrifter om säkerhetsskydd.

4.1 Granskning vid utveckling och anskaffning

4.1.1 Egenutvecklad mjukvara och säkerhetsgranskning

§ *4 kap. 1 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

När egenutvecklad programvara används i informationssystem som har betydelse för säkerhetskänslig verksamhet ska den granskas för att upptäcka och åtgärda sårbarheter. Granskning bör ske strukturerat utifrån upprättade rutiner och checklistor. Resultatet av granskningen ska dokumenteras.

Vid utveckling av informationssystem bör standardiserade och välbeprövade programvarubibliotek användas. Det är viktigt att noggrant följa originaldokumentation avseende hur funktioner i sådana bibliotek ska användas.

Säkerhetsgranskning kan grovt indelas i två typer:

- granskning av styrning i fråga om rutiner och regelverk och
- teknisk granskning, som syftar till att verifiera säkerheten i olika tekniska implementationer i ett informationssystem.

Vid utveckling av egen programvara bör tekniska säkerhetsgranskningar genomföras löpande under utvecklingsprocessen för att enklare kunna upptäcka och åtgärda säkerhetsproblem i ett tidigt skede. Verksamhetsutövaren bör ta fram rutiner och metodstöd för detta ändamål, så att tekniska säkerhetsgranskningar blir en naturlig del av utvecklingsprocessen.

Även om granskning av delkomponenter genomförs under en utvecklingsprocess bör en sammantagen säkerhetsgranskning genomföras, där alla komponenter i den egenutvecklade programvaran granskas tillsammans. Detta kan lämpligen ske i slutskedet av utvecklingsprocessen, exempelvis genom ett så kallat penetrationstest. Efter att eventuella upptäckta brister och sårbarheter har åtgärdats bör ytterligare en granskning ske för att verifiera att sårbarheterna faktiskt är åtgärdade eller på annat sätt motverkats.

Nya säkerhetsgranskningar bör genomföras regelbundet efter driftsättning.

4.1.2 Granskning av tredjepartsprogramvara och hårdvara

§ *4 kap. 2 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Vid användning av programvara som inte utvecklats av verksamhetsutövaren, så kallad tredjepartsprogramvara, är det viktigt att verksamhetsutövaren undersöker om programvaran har någon oönskad funktionalitet som kan påverka säkerheten i informationssystemet negativt.

Om tredjepartsprogramvaran inte har granskats av en part som verksamhetsutövaren bedömer som tillförlitlig behöver verksamhetsutövaren själv säkerhetsgranska programvaran innan den implementeras i informationssystemet. Syftet med granskningen är att upptäcka oönskad funktionalitet samt skydda informationssystemet mot exempelvis dolda kanaler och skadlig kod som kan finnas i tredjepartsprogramvaran. Där det är lämpligt ska även säkerhetskonfigurationen granskas så att produkten implementeras på ett korrekt sätt.

+ *Se vidare i avsnitt 4.10.*

Att tänka på när tillförlitlighet ska bedömas

- Finns det tredjepartsmoduler i den programvaran du ska bedöma? Granska dessa.
- Är programvaran rätt konfigurerad? Granska säkerhetskonfigurationen.
- Finns det en aktiv förvaltning av programvaran? Granska att det finns en fungerande förvaltning.
- Är programvara hämtad från en betrodd källa? Gratisprogramvara och öppen källkod finns ofta att ladda ner på många olika ställen.
- Behöver programvaran uppdateras? Hämta uppdateringen från en betrodd källa.
- Om möjligt testa programvara och uppdateringar. Detta gäller även hårdvarunära programvara (eng. *firmware*).

Det är viktigt att informationssystemets hårdvara granskas på motsvarande sätt som tredjepartsprogramvara i syfte att upptäcka oönskad funktionalitet. Hårdvaran ska därtill undersökas fysiskt i syfte att upptäcka eventuell manipulation. Fysisk undersökning kan bestå i att kontrollera garantiförseglingar och skruvar.

Manipulation av hårdvara kan ske på flera olika sätt. Det kan exempelvis handla om att placera en avlyssningsenhet i en hårdvarudetalj eller att lägga till någon komponent som kan vidarebefordra knapptryckningar, inloggningsuppgifter eller liknande till den som introducerat avlyssningen. Ett annat sätt kan vara att introducera en komponent som skapar en datakommunikationsbaserad bakdörr för en angripare. Även behovet av uppdatering av hårdvarunära program (eng. *firmware*) är en attackvektor som antagonister kan utnyttja. Det handlar ytterst om att försäkra sig om att inte hårdvaran är manipulerad, genom antingen granskning av hårdvaran eller en bedömning av att en tillverkare, som har kontroll över hela leveranskedjan, är tillförlitlig.

All uppdatering, till såväl applikationer som komponenter och hårdvara, bör testas innan uppdatering sker i driftmiljö. För informationssystem som är separerade från andra nät eller system finns det ofta mer tid för testning av uppdateringen, eftersom det är svårare för obehörig att utnyttja eventuella sårbarheter som uppdateringen avser åtgärda. I miljöer exponerade mot andra nät, till exempel internet, kan verksamhetsutövare behöva ta ställning till om en omedelbar uppdatering utan föregående testning bör göras eller inte. Har inte uppdateringen utvärderats innan den driftsattes bör detta ske så snart möjligt efter driftsättningen, i syfte att säkerställa att inte någon annan sårbarhet eller oönskad funktionalitet följt med.

Se även avsnitt 4.10.4 Uppdateringar.

4.2 Åtgärder inför driftsättning eller förändring

4.2.1 Verifiering av funktions- och säkerhetskrav

4 kap. 3 § Säkerhetspolisens föreskrifter om säkerhetsskydd

Verksamhetsutövaren ska, innan ett informationssystem som har betydelse för säkerhetskänslig verksamhet tas i drift, genomföra test av säkerhetsskyddsåtgärderna som vidtagits. Syftet är att säkerställa att ett informationssystem som har betydelse för säkerhetskänslig verksamhet uppfyller säkerhetskraven och att de säkerhetskyddsåtgärder som identifierats som behövliga i den särskilda säkerhetsskyddsbedömningen ger önskad effekt.

Resultatet av testerna ska jämföras med verksamhetsutövarens funktionella och säkerhetsrelaterade krav för informationssystemet. Detta är ett sätt att verifiera att informationssystemet uppfyller de säkerhetskrav som verksamhetsutövaren fastställt. Kraven identifieras och fastställs av verksamhetsutövaren i den särskilda säkerhetsskyddsbedömningen. Den särskilda säkerhetsskyddsbedömningen ska uppdateras efter testningen med eventuella avvikelser och säkerhetsskyddsåtgärder som måste vidtas för att säkerhetskraven ska uppfyllas.

Den särskilda säkerhetsskyddsbedömningen utgör därmed ett styrande dokument för alla delar i utvecklingen av ett informationssystem som ska användas i säkerhetskänslig verksamhet, och då särskilt såvitt avser tester och säkerhetsgranskningar.

4.2.2 Bedömning av behov av kompetenser och resurser

4 kap. 4 § Säkerhetspolisens föreskrifter om säkerhetsskydd

Verksamhetsutövaren ska bedöma vilka resurser och kompetenser som behövs för att bibehålla det fastställda säkerhetsskyddet under systemets förväntade livstid.

Utveckling av informationssystem eller mjukvara i ett informationssystem bedrivs ofta i projektform. Inte sällan är den personal som utvecklar informationssystemet inhyrd eller i övrigt organisatoriskt frånskild från den personal som ska arbeta med drift och förvaltning av informationssystemet. Utvecklingsarbetet kan ske i olika plattformar och baseras på en

mängd olika programmeringsspråk. Var och en av dessa it-plattformar kan ha inneboende sårbarheter som både kan nyttjas av en antagonist vid ett angrepp och påverka driftsäkerheten i informationssystemet. Den som deltar i utveckling av informationssystem måste därför ha adekvat och aktuell kompetens om de sårbarheter som finns i de plattformar där utveckling sker för att sårbarheter ska kunna omhändertas. Samtidigt får inte den framtida driftorganisationens resurs- och kompetensbehov komma i skymundan.

Verksamhetsutövaren bör planera för drift och förvaltning av informationssystemet i god tid innan det tas i drift. I detta ligger att fastställa vilka resurser och kompetenser som kommer att behövas. Att utbilda och nyrekrytera personal tar tid och är ofta resurskrävande. Att rätt kompetenser och resurser finns på plats innan driftsättning är avgörande för att verksamhetsutövarens driftorganisation ska kunna upprätthålla god funktionalitet och fastställt säkerhetsskydd för informationssystemet, från början och över tid.

Bedömningar som görs ska dokumenteras. Så sker lämpligen i informationssystemets förvaltningsplan.

4.3 Rutiner för hantering av informationssystem

§ *4 kap. 5 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Verksamhetsutövaren ska fastställa rutiner för hantering av informationssystemet som har betydelse för säkerhetskänslig verksamhet under systemets förväntade livstid.

Arbetet med drift och underhåll av informationssystem handlar om att dels hantera olika driftrelaterade problem som kan uppstå i vardagen, dels tillse att säkerheten i informationssystemet upprätthålls över tid. Viktiga delar i detta arbete är att tillse att informationssystemet hålls uppdaterat, att föråldrad programvara byts ut samt att förändringar och avveckling genomförs på ett kontrollerat sätt.

I detta avsnitt beskrivs bland annat ett antal principer som en verksamhetsutövare bör beakta vid drift, underhåll och avveckling av informationssystem som har betydelse för säkerhetskänslig verksamhet.

4.3.1 Styrning av drift och underhåll

För att tillgodose att säkerheten i ett informationssystem upprätthålls över tid är det viktigt att en verksamhetsutövare har tydlig styrning av hur drift och underhåll av informationssystemet ska hanteras.

Om drift och underhåll av ett informationssystem inte hanteras på ett medvetet och strukturerat sätt av behörig personal, kan det leda till att systemets tillförlitlighet påverkas, exempelvis på grund av tillgänglighetsrelaterade problem eller andra sårbarheter i informationssystemet.

Vanligen styrs drift och underhåll av ett informationssystem med stöd av ett skriftligt ramverk som innehåller både övergripande principer och anvisningar om hur olika driftrelaterade frågor ska hanteras i praktiken. Oavsett styrmodell är det viktigt att styrdokumenten anpassas utifrån den egna verksamhetens förutsättningar samt informationssystemets komplexitet och omfattning. En alltför detaljreglerad styrning kan i vissa fall medföra att driften blir svårhanterlig, medan en alltför svag reglering kan medföra att kontrollen över informationssystemet blir bristfällig.

Vid framtagande av styrdokument för drift och underhåll av informationssystem bör verksamhetsutövaren företrädesevis beakta följande perspektiv.

- **Felhantering:** Hur ska uppkomna fel i systemet hanteras?
- **Förändringshantering:** Hur ska förändringar i systemet hanteras?
- **Uppdateringar:** Hur ska uppdateringar av mjuk- respektive hårdvara i systemet hanteras?
- **Incidenthantering:** Hur ska personalen agera vid incidenter?
- **Kontinuitetshantering:** Hur ska personalen arbeta för att upprätthålla informationssystemets tillgänglighet över tid?

Det är av stor vikt att verksamhetsutövaren etablerar tydliga roller med beskrivningar av vem som gör vad, vem som har vilket ansvar och vem som har vilka befogenheter och att detta dokumenteras i de hanteringsrutiner som verksamhetsutövaren har att fastställa. I övrigt bör förändringar i styrdokument för drift och underhåll endast genomföras efter att de har godkänts av en specifikt utpekad person eller funktion hos verksamhetsutövaren.

4.3.2 Förändringshantering

Förändringar i ett informationssystem, särskilt när ny programvara implementeras, kan påverka konfidentialitet, riktighet och tillgänglighet. Förändringar av befintlig programvara eller implementering av ny programvara som kan komma att påverka informationssystemet ska därför ske under kontrollerade

former. Det är viktigt att förändringar inte genomförs på ett sätt som åsidosätter säkerhetsfunktioner i informationssystemet, antingen tillfälligt eller permanent.

Om möjligt bör ny programvara testas i ett informationssystem som är separerat från informationssystem i skarp drift där programvaran avses installeras och användas. Detta ger verksamhetsutövaren möjlighet att testa och granska hur den nya programvaran beter sig, utan att det kan påverka informationssystemet som är i drift. Motsvarande testförfarande bör tillämpas vid uppdatering och utbyte av befintlig programvara. I facklitteratur åtskiljs ofta de informationssystem som beskrivs ovan genom benämningarna utvecklingsmiljö, testmiljö respektive driftsmiljö.

Notera:
Förändringshantering som sker enligt en verksamhetsutövares ordinarie rutiner för hantering av informationssystem behöver inte vara väsentliga förändringar som avses i 3 kap. 2 § säkerhetsskyddsförordningen.

Se avsnitt 5 Förberedande åtgärder innan driftsättning av ett informationssystem.

4.4 Granskning av säkerheten

§ *4 kap. 6 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

4.4.1 Allmänt om uppföljning och kontroll

Uppföljning och kontroll är viktiga verktyg för att kunna säkerhetsställa att säkerhetsskyddet för ett informationssystem upprätthålls över tid och ger avsedd effekt. Granskningar av säkerheten i informationssystem bör utföras av någon annan än den som utför drift, förändringar och underhåll i det systemet. Detta i syfte att uppföljning och kontroll ska kunna ske med en tillräcklig grad av oberoende.

Uppföljning och kontroll av säkerheten i ett informationssystem bör vara av såväl administrativ som tekniskt karaktär.

En administrativ säkerhetsgranskning bör ta sikte på exempelvis:

- att identifiera brister i verksamhetens efterlevnad av fastställda hanteringsrutiner, inklusive de styrdokument som reglerar drift, förändring och underhåll av informationssystemet, och
- att identifiera brister i användarnas efterlevnad av de regler och rutiner som reglerar hur informationssystemet får användas.

En teknisk säkerhetsgranskning bör ta sikte på exempelvis:

- att identifiera generella brister och sårbarheter i funktioner i och kring informationssystemet,
- att granska om informationssystemet är skyddat mot sådana sårbarheter som är allmänt kända och borde vara omhändertagna inom ramen för verksamhetsutövarens omvärldsbevakning samt att identifiera brister i efterlevnaden av de styrdokument som reglerar drift och underhåll av informationssystemet, exempelvis gällande hantering av tjänstekonton och användarkonton med systemadministrativ åtkomst.

4.4.2 Efterlevnad av kravställning

Att de säkerhetskrav som identifierats i den särskilda säkerhetsskyddsbedömningen uppfylls bör följas upp regelbundet genom exempelvis säkerhetsgranskningar, sårbarhetsskanningar och penetrationstester. Syftet är att verifiera att de säkerhetsfunktioner och den säkerhetskonfiguration som initialt applicerades vid driftsättning upprätthålls över tid.

Säkerhetsarbetet är i behov av kontinuerlig revidering; skyddet blir i regel mest effektivt om det iterativt anpassas och uppdateras. Nya attackvägar och sårbarheter kräver att skyddet anpassas och det är inte ovanligt att säkerhetsåtgärder avaktiveras eller av andra orsaker blir ineffektiva med tiden. Detta kan ske till exempel för att ny funktionalitet förs in, vilket kan både introducera nya sårbarheter och ändra hur verksamheten använder systemet. Därför är det en fördel om granskningar genomförs systematiskt och på regelbunden basis, till exempel årligen.

Notera:
Såvitt avser informationssystem som är avsedda att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig eller som av annan anledning har motsvarande betydelse för Sveriges säkerhet, ska säkerheten granskas årligen.

4.5 Unika identiteter och spårbarhet

§ *4 kap. 7 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Den vanligaste formen av digital identitet i ett informationssystem är ett användarkonto skapat åt en fysisk person (individ). Därtill finns emellertid ofta konton i informationssystem som inte kan kopplas till en individ. Sådana konton kan kallas för tjänstekonton eller systemkonton. Tjänstekonton används av systemet för att hantera olika funktioner i systemet eller de tjänster som en användare kan använda. Systemkonton finns i två versioner, lokala eller domänanslutna. Domänanslutna konton fungerar som ett användarkonto för till exempel en dator. Lokala systemkonton finns bland annat på olika it-komponenter för konfigurering och hantering. I dessa fall behövs kompletterande åtgärder för att säkerställa vilken fysisk individ som har gjort en konfiguration eller andra åtgärder i komponenten.

I ett informationssystem som har betydelse för säkerhetskänslig verksamhet ska alla utställda identiteter vara unika över tid, det vill säga över hela informationssystemets livstid. Att ett visst konto med säkerhet kan knytas till en viss fysisk person eller tjänst i systemet är viktigt när det kommer till spårbarhet. En identitet får aldrig återanvändas för annan fysisk person eller tjänst.

Vid utställandet av en ny identitet, i betydelsen skapandet av ett användar-, tjänste- eller systemkonto, tilldelas kontot behörigheter som ger olika typer av åtkomst i informationssystemet.

Åtkomst i ett informationssystem ska vara spårbar till antingen individ, system eller resurs. Funktions- och gruppkonton ska undvikas att användas men om sådana konton måste användas då behövs kompletterande åtgärder för att säkerställa vilken fysisk individ som har disponerat kontot vid alla tillfällen kontot använts.

Spårbarheten till individ är viktigt vid brottsutredningar samt för att kunna upptäcka och utreda incidenter.

+ *Beskrivs mer utförligt i avsnitt 4.14 Säkerhetsloggning.*

Även om tjänstekonton inte går att koppla till en fysisk individ, är det lika viktigt att dessa identiteter är och förblir unika över tid.

Identiteter kan ställas ut på många sätt och i olika former. När verksamhetsutövare tar fram processer, rutiner och regler för sin behörighetsstyrning är det viktigt att säkerställa:

- att användarkonton inte återanvänds,
- att användarkonton aldrig tas bort från ett informationssystem, utan i stället inaktiveras om de inte används eller bevaras på annat sätt samt
- att det sker kontinuerlig uppföljning av tilldelade användarkonton och deras respektive behörighet.

Det är även viktigt att verksamhetsutövaren har processer som säkerställer att alla identiteter i ett informationssystem har ställts ut och tilldelats behörigheter på ett tillförlitligt sätt.

4.6 Behörighetsstyrning

§ *4 kap. 8 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Alla konton i ett informationssystem – användarkonton, systemkonton och tjänstekonton – som har tilldelats systemadministrativ åtkomst eller annan särskild tillgång (ofta kallat privilegierade rättigheter) ska hanteras med särskild försiktighet. Anledningen är att sådana konton ofta direkt eller indirekt kan ha fullständig åtkomst att såväl läsa som förändra funktioner och information som finns i systemet.

Tilldelning av behörigheter med systemadministrativa rättigheter ska ske restriktivt och behörigheterna vara tidsbegränsade, följas upp samt omprövas löpande, minst årligen. Med restriktiv tilldelning menas att inget konto ska ha någon form av systemadministrativ behörighet som inte behövs. Det ska finnas processer och rutiner, gärna med tekniskt stöd, för relevant uppföljning och kontroll av behörigheterna.

+ *Se vidare i avsnitt 4.14 Säkerhetsloggning.*

En separation av roller behövs för att till exempel skilja den som granskar loggar från den som utför åtgärderna som genererar loggarna. För vissa roller som hanterar åtgärder som kräver omfattande tillgång och behörighet kan det behövas dualitet, det vill säga att en enskild person inte själv får utföra arbetet utan att det ska ske av två personer i samverkan. Ett annat sätt att åstadkomma bättre säkerhet är att vissa behörigheter tilldelas temporärt, i betydelsen endast när ett visst arbetsmoment ska genomföras, för att omedelbart därefter återtas. Det är viktigt att det finns full spårbarhet över behörigheter och förändringar av dessa.

Notera:
Det är vanligt förekommande att tjänstekonton tilldelas onödigt höga behörigheter. Tjänstekonton ska, precis som alla andra konton, tilldelas endast de behörigheter som krävs för den uppgift som kontot ska utföra.

Exempel på konton med systemadministrativa rättigheter är:

- domän- och lokala administratörer i Windowsmiljöer,
- administratörskonton (root) i Linux/Unix-system,
- systemkonton med högre behörighet i nätverksutrustning,
- användarkonton med högre behörighet i applikationer eller databaser,
- delade konton med högre behörighet i tekniska ”24/7-funktioner” såsom driftövervakning (eng. *Network Operations Center, NOC*) och säkerhetsövervakning (eng. *Security Operations Center, SOC*),
- tjänstekonton med särskild behörighet för till exempel säkerhetskopiering, överföringar och batchkörningar samt
- användarkonton med högre behörighet (eng. *power users*).

Åtkomst med privilegierade rättigheter är som regel en förutsättning för att en systemadministratör ska kunna förändra grundläggande funktionalitet och säkerhetsfunktioner i ett informationssystem. En verksamhetsutövare bör därför utbilda sina systemadministratörer i hur användarkonton med sådan åtkomst får användas. Det är viktigt att förmedla att behörighet inte är detsamma som befogenhet. Att en systemadministratör kan läsa innehållet i en databas på grund av teknisk behörighet medför inte per automatik att administratören har rätt att göra det. Behörig att få del av en säkerhetsskyddsklassificerad uppgift är enligt 2 kap. 2 § säkerhetsskyddsförordningen endast den som behöver uppgiften för att kunna utföra sitt arbete eller på annat sätt medverka i den säkerhetskänsliga verksamheten.

Systemadministratörer bör i övrigt, vid sidan av sina ordinarie arbetskonton, ha såväl separata administratörskonton som särskilda klienter för systemadministrativt arbete och som bara får användas när de utför sådant arbete. Administrativa konton bör aldrig ha åtkomst till internetanslutna tjänster, såsom e-post och webbsurf. Verksamhetsutövaren ska tillse att tilldelning, förändring och användning av användarkonton med systemadministrativ åtkomst loggas och följs upp.

4.7 Autentisering med mera

4.7.1 Flerfaktorsautentisering

§ *4 kap. 9 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Autentisering som baseras på flera faktorer kallas vanligen flerfaktorsautentisering (eng. *multifactor authentication, MFA*) och refereras ibland även till som stark autentisering.

Flerfaktorsautentisering är en åtgärd som minskar riskerna att en obehörig person får åtkomst till ett informationssystem. Flerfaktorsautentisering ska alltid tillämpas för autentisering vid åtkomst till informationssystem av betydelse för säkerhetskänslig verksamhet, om det inte är uppenbart obehövligt.

Faktorerna som autentiseringen ska baseras på utgörs vanligen av en kombination av minst två av följande:

- något kontoinnehavaren *har,* exempelvis ett smart kort,
- något kontoinnehavaren *vet*, exempelvis ett lösenord eller en kod, eller
- något kontoinnehavaren *är* (biometri, till exempel fingeravtryck eller ansiktsigenkänning).

Den faktor som kontoinnehavaren har behöver omges av skyddsåtgärder som förhindrar att den kopieras. En vanlig lösning är att använda så kallade smarta kort som har försetts med funktioner som förhindrar att kortet kan klonas.

Den faktor som kontoinnehavaren vet behöver också omgärdas av säkerhetskrav,

+ *Se vidare i avsnitt 4.7.2 Autentisering med lösenord.*

Ibland är flerfaktorsautentisering inte möjligt. Ett exempel på detta är tjänstekonton. I dessa fall kommer ett lösenord ensamt att ge tillgång till vissa funktioner i informationssystemet. I sådant fall blir användandet av svårgissade, så kallade starka lösenord, extra viktigt.

Notera:
Flerfaktorsautentisering i ett informationssystem som har betydelse för säkerhetskänslig verksamhet som är beroende av externa tredjepartstjänster, exempelvis sms, kan vara en sårbarhet. Anledningen är att verifieringen av kontoinnehavarens identitet då sker utanför verksamhetsutövarens kontroll.

För fristående datorer kan flerfaktorsautentisering vara svårt att implementera. Detta samtidigt som betydelsen av det skydd flerfaktorsautentisering ger är svagare mot bakgrund av att tillgången till själva datorn ofta utgör en större sårbarhet än svagheter i autentiseringen. För att uppnå ett skydd för dessa informationssystem behöver tydliga hanteringsregler, som omfattar inlåsning eller kontroll över datorn, etableras.

+ *Se även avsnitt 3.5 Förvaring.*

Om verksamhetsutövaren vidtar andra tillräckliga säkerhetsskyddsåtgärder kan flerfaktorsautentisering vara uppenbart obehövligt. I dessa fall är det viktigt att verksamhetsutövaren i den särskilda säkerhetsskyddsbedömningen tydligt motiverar sitt ställningstagande att inte använda flerfaktorsautentisering. Ett exempel kan vara ett informationssystem i form av en fristående dator som används av endast en användare och annars förvaras avstängd och inlåst i ett säkerhetsskåp.

4.7.2 Autentisering med lösenord

§ *4 kap. 10–11 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd*

Lösenord, koder eller motsvarande är det vanligaste sättet att autentisera användare. När ett lösenord i kombination med användarnamn eller liknande ensamt ger åtkomst till ett informationssystem utgör förfarandet en så kallad enfaktorsautentisering.

Ett problem med lösenord är att de med enkelhet kan delas och spridas, vilket medför att tilliten ofta bör anses låg för denna typ av autentisering. Lättgissade, så kallade svaga lösenord, samt användare som använder samma lösenord på flera ställen, är en vanlig brist som kan utnyttjas av en antagonist för att få tillgång till ett informationssystem. En antagonist som kommer över en användares lösenord kan pröva att använda lösenordet på andra ställen i ett informationssystem och i värsta fall tillskansa sig privilegierade rättigheter. En typisk måltavla för ett sådant angrepp är systemadministratörer, som ofta har både ett vanligt användarkonto och ett konto med systemadministrativ åtkomst. Denna angreppsmetodik är ett exempel på vad som i engelsk facklitteratur kallas *privilege escalation*.

Om ett lösenord förvaras på sådant sätt att en antagonist enkelt kan få åtkomst till det spelar det ingen roll om lösenordet är starkt eller inte. Säkerhetspolisen förskrifter om säkerhetsskydd innehåller därför krav på hur nedtecknade koder eller lösenord som ger tillgång till informationssystem som har betydelse för säkerhetskänslig verksamhet ska förvaras. När lösenord antecknas ska anteckningen eller likande antingen vara under kontroll eller förvaras i utrymme som verksamhetsutövaren har godkänt för förvaring av säkerhetsskyddsklassificerade handlingar. Nivån på skyddet ska motsvara den konsekevensnivå som ett skadligt icke-behörigt användande av behörigheten kan medföra. Exempelvis om konsekvensnivån är B så ska förvaringen vara godkänd för säkerhetsskyddsklassen hemlig.
För att tillse att hanteringen av lösenord inte blir bristfällig är det viktigt att verksamhetsutövaren har

rutiner för hur lösenord ska hanteras. Verksamhetsutövaren ska fastställa tekniska eller administrativa regler för utformning, byte och hantering av lösenord, om sådana används för att ge tillgång till informationssystem som har betydelse för säkerhetskänslig verksamhet. Reglerna bör bland annat innehålla bestämmelser gällande förbud mot återanvändning av lösenord, förbud mot nedteckning av lösenord i privat lösenordsapplikation eller liknande samt krav på lösenordens längd och komplexitet.

Ett antal viktiga aspekter som en verksamhetsutövare behöver beakta i fråga om lösenordshantering är följande.

- Standardlösenord bör alltid bytas ut eftersom de utgör en sårbarhet som lätt kan utnyttjas av en antagonist.
- Lösenord bör vara unika mellan system och inte återanvändas.
- Begreppet ”lösenordsfras” bör användas i stället för ”lösenord” för att uppmuntra användning av en sammansatt mening snarare än ett enskilt ord.
- Lösenordens längd är viktigare än deras komplexitet (de bör helst vara 15 tecken eller längre).
- Nedtecknade lösenord ska förvaras säkert, till exempel i ett godkänt säkerhetsskåp och i enlighet med de rutiner verksamhetsutövaren fastställt.
- Använd hellre långa nedskrivna lösenord som förvaras enligt ovan, än enkla lösenord som hålls i minnet.
- Lösenord till tjänstekonton (eller andra konton som inte en fysisk person ska använda) bör, om de skapas manuellt, skapas med hjälp av program för att skapa lösenord.

4.7.3 Central funktion för identifiering eller behörighetskontroll

§ *4 kap. 12 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

En teknisk funktion som styr användarnas åtkomst i ett informationssystem, eller mellan informationssystem, benämns behörighetskontrollsystem. Ett sådant system baseras ofta på olika roller som kan tilldelas användarna. Dessa roller styr användarnas skriv- och läsrättigheter till den information som finns i systemet. För att förenkla hantering och uppföljning av behörigheter hanteras dessa många gånger i en central funktion, ofta benämnd centralt behörighetskontrollsystem. Ett exempel på en sådan funktion är Microsoft Active Directory.

Ett centralt behörighetskontrollsystem utgör ett typiskt intressant angreppsmål för en antagonist. Det är därför viktigt att verksamhetsutövaren vidtar adekvata säkerhetsskyddsåtgärder för att förhindra att systemet utgör den svagaste länken i kedjan, i fråga om kontroll av åtkomst till information. Ett centralt behörighetskontrollsystem ska ges ett säkerhetsskydd som svarar upp mot det säkerhetsskydd som de anslutna informationssystemen ska ha. Vid val av skyddsåtgärder för ett centralt behörighetskontrollsystem blir därför säkerhetsskyddsklassificeringen av informationen i de anslutna informationssystemen ett viktigt ingångsvärde. Skyddsåtgärderna behöver omfatta såväl tekniska som administrativa säkerhetsåtgärder.

4.8 Skydd mot röjande signaler

§ *3 kap. 4 § säkerhetsskyddsförordningen*

§ *4 kap. 13 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Verksamhetsutövare som ansvarar för ett informationssystem som ska användas i säkerhetskänslig verksamhet ska beakta förekomsten av röjande signaler (RÖS) och vidta lämpliga säkerhetsskyddsåtgärder om informationssystemet avses behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre.

RÖS är oavsiktliga elektromagnetiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehöriga, kan bidra till att information röjs. Signalerna kan vara ledningsburna (metalliska ledare) eller ha en strålad vågutbredning (antenner).

Vanliga typer av RÖS är:

- Radio-RÖS som kan förekomma i elektroniska komponenter med radiosändare.
- Elektromagnetisk överhörning som kan uppstå när signaler överförs med hjälp av en elektromagnetisk koppling.
- Tecken-RÖS som kan uppstå när information överförs exempelvis vid utskrift.
- Video-RÖS som kan uppstå när information överförs från exempelvis en dator till en bildskärm.

Skydd mot elektromagnetisk RÖS kan uppnås genom att använda RÖS-inmätt utrustning i kombination med tillräckligt avstånd mellan verksamhetsutövarens yttre och inre delar av den så kallade skyddslöken.

+ *Se vidare i Säkerhetspolisens Vägledning i säkerhetsskydd – Fysisk säkerhet.*

Utöver avståndet kan även hänsyn tas till hur mycket de röjande signalerna dämpas av byggnadstekniska egenskaper. Byggnadens material och läge har stor inverkan på hur de röjande signalerna kan sprida sig från den signalerande utrustningen. På motsvarande sätt påverkar byggnadens anslutning till elnätet hur ledningsburna signaler sprider sig till omgivningen.

Skydd mot RÖS kan även uppnås genom att använda ett så kallat RÖS-skyddat utrymme. Ett sådant utrymme omges av ett sammanhängande metallhölje, med särskilda genomföringar för ledningar, vilket förebygger att röjande signaler når ut från utrymmet. RÖS-skyddade utrymmen kan också upprättas i mindre skala för särskild utrustning, så kallade RÖS-kabinett.

Säkerhetsskyddsåtgärder mot RÖS ska försvåra obehörig inhämtning av röjande signaler utifrån de säkerhetshot som identifierats i den särskilda säkerhetsskyddsbedömningen och utifrån erhållen beskrivning av dimensionerande antagonistiska förmågor.

+ *Se vidare i Säkerhetspolisens Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys.*

4.9 Kommunikationssäkerhet

Regler om kommunikationssäkerhet syftar till att minska ett informationssystems exponering och möjliga angreppsytor.

Ett informationssystem innehåller i regel både kända och okända sårbarheter som under vissa omständigheter kan nyttjas av en antagonist. Vilken insats som krävs av en antagonist för att utnyttja en sådan sårbarhet är till stor del beroende av hur informationssystemet exponeras.

Notera::
Informationssystem som är avsett för behandling av säkerhetsskyddsklassificerade uppgifter får inte kommunicera med andra informationssystem och nätverk som inte omfattas av motsvarande krav på säkerhetsskydd.

+ *Se vidare i avsnitt 4.9.2 Separation.*

4.9.1 Kontrollerad kommunikation

§ *4 kap. 14 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Ett sätt att minska exponeringen av ett informationssystem är att säkerställa att det kommunicerar på ett kontrollerat sätt.

Alla informationssystem av betydelse för säkerhetskänslig verksamhet ska utformas enligt principen om kontrollerad kommunikation. Med detta avses att verksamhetsutövaren först fastställer hur och på vilket sätt ett sådant informationssystem får kommunicera. Därefter ska verksamhetsutövaren införa lämpliga säkerhetskyddsåtgärder som säkerhetsställer att informationssystem endast tillåts kommunicera på ett kontrollerat sätt.

I detta avsnitt beskrivs viktiga principer som en verksamhetsutövare har att beakta.

Säkerhetszoner

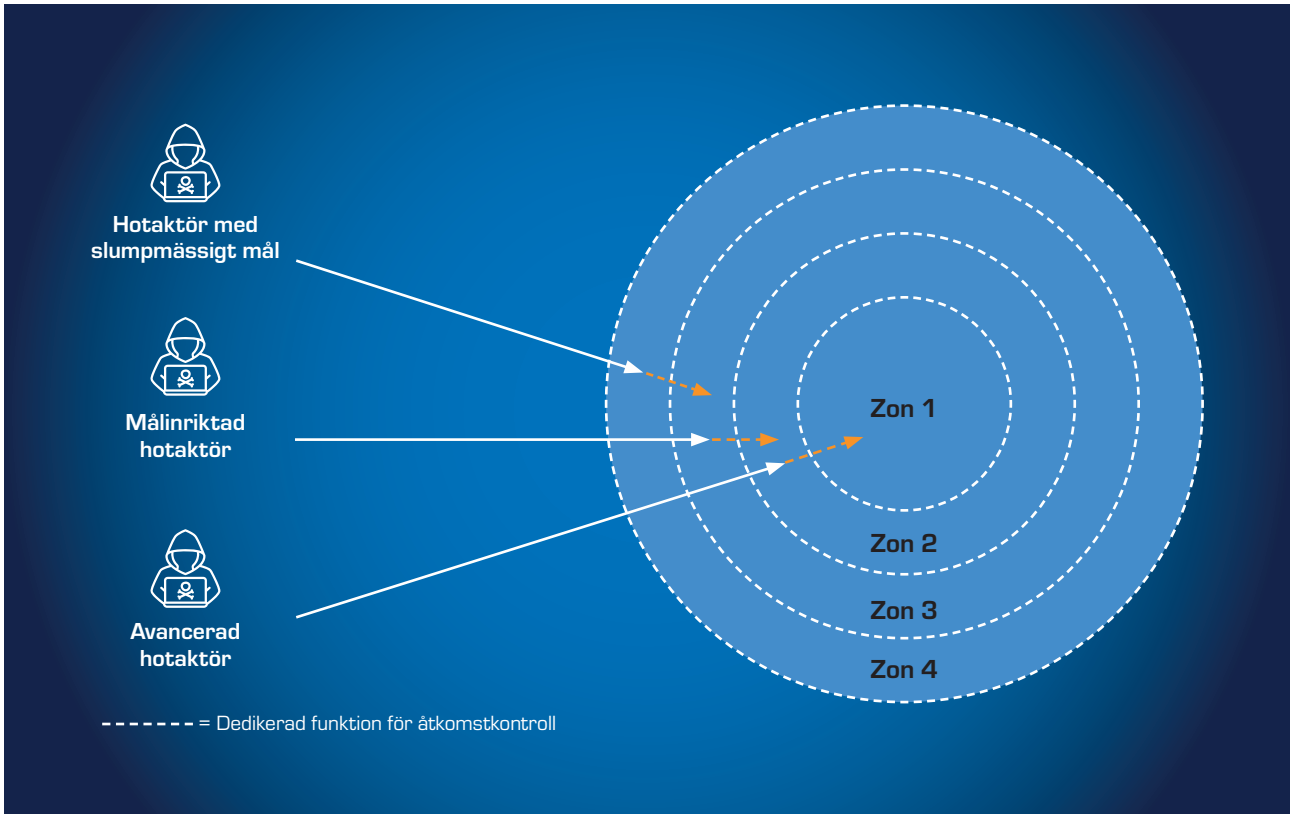
Ett teoretiskt koncept som kan användas för att åskådliggöra olika principer för att minska exponeringen av ett informationssystem är att modellera olika säkerhetszoner. I denna kontext placeras ett informationssystem i en säkerhetszon baserat på hur skyddsvärt det är.

Med utgångspunkt i illustrationen i figur 4 kan lämpliga säkerhetskyddsåtgärder tillse att endast tillåten kommunikation kan ske från en zon till en nästliggande zon. Det bör exempelvis inte vara möjligt att upprätta kommunikation direkt från zon 4 till zon 2 eller 1, utan att passera mellanliggande zon(er) där datatrafiken verifieras att den är behörig innan den skickas vidare. Informationssystem som omfattas av motsvarande krav på säkerhetsskydd kan placeras i samma säkerhetszon.

Som illustreras i figur 4 har en antagonist med ett slumpmässigt mål oftast inte de resurser, den kunskap eller den uthållighet som krävs för att få åtkomst till de mest skyddsvärda zonerna. En målinriktad antagonist med mer omfattande resurser och uthållighet kan försöka komma åt mer skyddsvärda informationssystem. En avancerad antagonist (eng. *advanced persistent threat, APT*) arbetar långsiktigt och förfogar över stora resurser, vilket kan möjliggöra kompromettering även av de mest skyddsvärda informationssystemen.

I figur 5 ges ett exempel på hur informationssystem placerade inom samma säkerhetszon kan kommunicera direkt med varandra och dela infrastrukturkomponenter. Kommunikation mellan dessa system ska dock ske på ett kontrollerat sätt, exempelvis med hjälp av brandväggar och behörighetskontrollsystem.

Figur 4. Exempel på indelning i säkerhetszoner.



Kommunikation på ett kontrollerat sätt
Ett informationssystem innehåller flera olika entiteter (komponenter, tjänster, funktioner osv.) som utbyter information med varandra. Så snart en entitet tillåts att kommunicera med en annan entitet öppnas möjliga vägar till angrepp som kan nyttjas av en antagonist. Ett annat sätt att beskriva detta är att entiteterna exponerar angreppsytor.

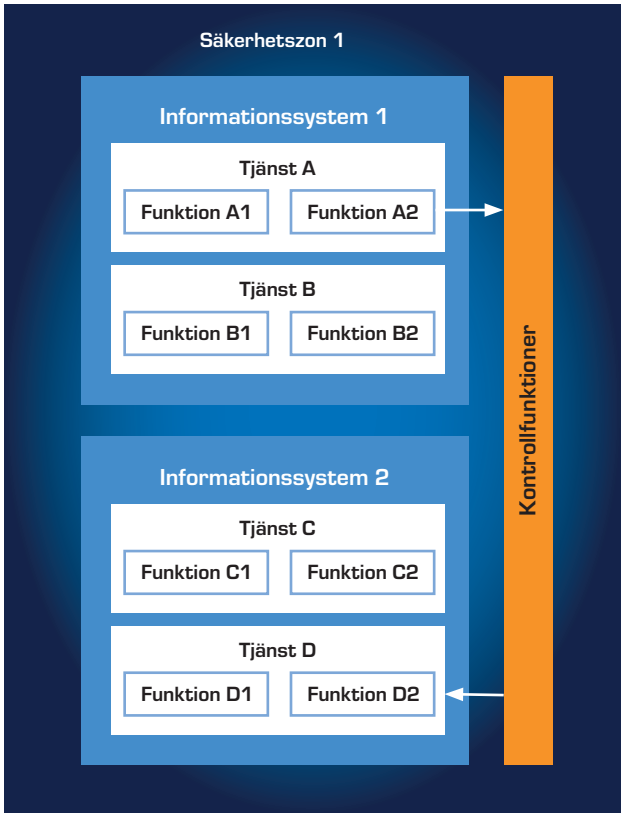
För att minska exponering av angreppsytor ska verksamhetsutövaren tillse att informationssystem som har betydelse för säkerhetskänslig verksamhet endast kommunicerar på ett kontrollerat sätt med såväl komponenter och delsystem inom samma informationssystem som med andra system.

Med begreppet kommunicerar på ett kontrollerat sätt avses att verksamhetsutövaren har gjort ett medvetet ställningstagande till varje möjlig kommunikationsväg. Verksamhetsutövaren behöver även införa säkerhetsskyddsåtgärder som förhindrar kommunikation som inte är tillåten. En viktig princip att beakta för att kunna uppnå kontrollerad kommunikation är att endast nödvändig kommunikation mellan entiteter ska tillåtas medan övrig kommunikation ska förhindras. Att kontrollera kommunikation på det sätt som beskrivs ovan kallas ofta för segmentering.

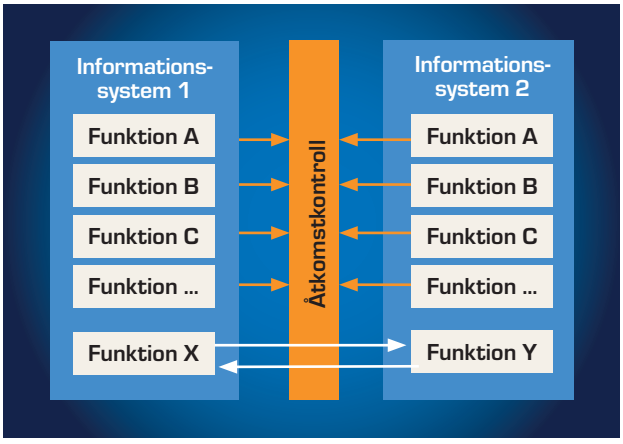
I figur 6 ses två informationssystem där åtkomstkontroll har implementerats. Åtkomstkontrollen avgör vilka funktioner som får kommunicera med varandra, vilket medför att möjliga vägar till angrepp kraftigt reduceras. Endast specifikt utpekade funktioner, benämnda funktion X och funktion Y, kan kommunicera med varandra.

Kommunikation mellan entiteter kan även begränsas genom exempelvis VLAN (eng. V*irtual Local Area Network*) och brandväggar som endast tillåter godkänd kommunikation mellan olika nätsegment. Stödjande eller säkerhetsrelaterade funktioner i ett informationssystem såsom exempelvis administration, loggning eller säkerhetskopiering bör utföras och hanteras i avskilda nätsegment. Syftet med detta är att minska exponering av angreppsytor och begränsa möjligheterna för en antagonist att få åtkomst till känsliga resurser som kan ge administrativa behörigheter eller påverka spårbarheten. Vidare bör kommunikation till sådana avskilda nätsegment om möjligt krypteras för att förhindra obehörig insyn och påverkan.

Figur 5. Informationssystem inom en och samma säkerhetszon.
Exempel på hur informationssystem placerade inom samma säkerhetszon kan kommunicera direkt med varandra och dela infrastrukturkomponenter. Kommunikationen mellan dessa system ska dock ske på ett kontrollerat sätt, exempelvis med hjälp av brandväggar och behörighetskontrollsystem.



Figur 6. Två informationssystem där åtkomstkontroll har implementerats.
Åtkomstkontrollen avgör vilka funktioner som får kommunicera med varandra, vilket medför att möjliga vägar till angrepp kraftigt reduceras. Endast specifikt utpekade funktioner, benämnda funktion X och funktion Y, kan kommunicera med varandra.



4.9.2 Separation

Ett informationssystem som inte kommunicerar med något annat informationssystem har en låg grad av exponering mot externa antagonister. Ett informationssystem som kommunicerar med ett eller flera andra informationssystem har en högre exponering, i betydelsen att det finns fler möjliga vägar till angrepp.

För att minska exponering av informationssystem som innehåller säkerhetsskyddsklassificerade uppgifter är separation mellan informationssystem en viktig säkerhetsskyddsåtgärd.

Logisk separation

§ *4 kap. 15 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

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

Med logisk separation avses att möjligheten till kommunikation mellan ett sådant informationssystem och andra system förhindras med stöd av mjuk- eller hårdvara. Ett informationssystem avsett för behandling av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen begränsat hemlig eller konfidentiell kan i vissa fall dela infrastrukturkomponenter med ett informationssystem som inte omfattas av säkerhetsskydd.

De tekniska lösningar som finns tillgängliga för att dela infrastruktur medför dock en rad sårbarheter som en verksamhetsutövare behöver hantera.

+ *Se exempel i tabell 5.*

Tabell 5. Risker kopplade till olika tekniska lösningar för logisk separation.

Område	Teknik	Sårbarhet
Nätverk	Nätverksvirtualisering (VLAN) Brandväggar Mjukvarudefinierade nätverk (eng. *Software Defined Networks, SDN*)	Otillåten kommunikation mellan entiteter i nätverket som kan öppna upp möjliga vägar för angrepp.
Lagring	Lagringsvirtualisering (lagringsmedia delas genom virtuella zoner/pooler)	Att servrar som inte omfattas av säkerhetsskydd kan kommunicera med servrar som omfattas av säkerhetsskydd och den information som hanteras där.
Operativsystem	Servervirtualisering (resurser såsom processor och arbetsminne delas mellan virtuella maskiner)	Att integriteten mellan virtualiserade maskiner inte upprätthålls. En virtualiserad maskin får åtkomst till en annan virtualiserad maskin och den information som hanteras där.
Programvara	Applikationsvirtualisering (operativsystem delas mellan processer)	Att integriteten mellan virtualiserade processer inte upprätthålls. En virtualiserad process får åtkomst till en annan virtualiserad process och den information som hanteras där.

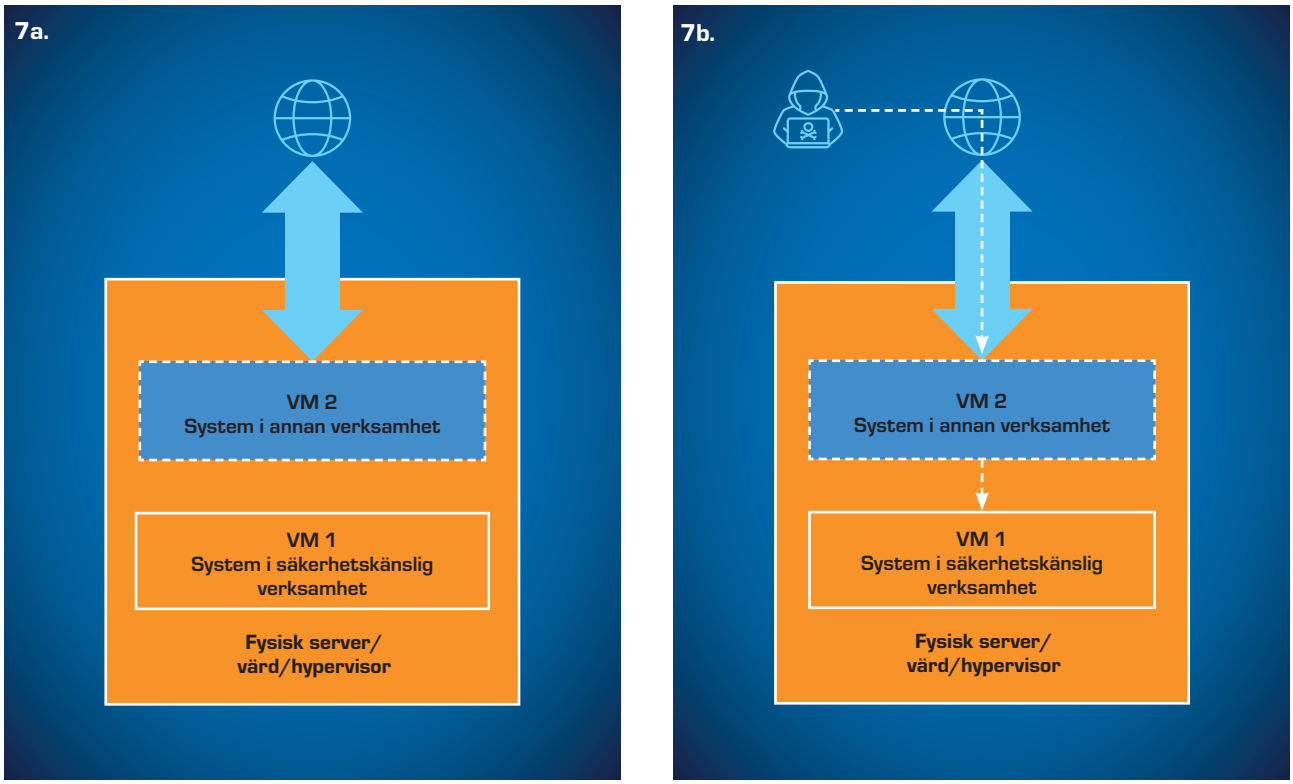
I figur 7a illustreras en sårbarhet som delning av infrastrukturkomponenter mellan informationssystem kan medföra. I figuren ses en virtuell server där den virtuella infrastrukturen delas mellan ett informationssystem som behandlar säkerhetsskyddsklassificerade uppgifter och ett informationssystem som inte omfattas av säkerhetsskydd. Med hjälp av en sårbarhet i det senare informationssystemet angriper antagonisten den virtuella infrastrukturen och får åtkomst till det säkerhetskänsliga informationssystemet (figur 7b). För att kravet på separation i 4 kap. 15 § Säkerhetspolisens föreskrifter om säkerhetsskydd ska anses uppfyllt måste virtualiseringsmiljön, inklusive den administrativa och tekniska delen, ha minst samma säkerhetsskyddsnivå (begränsat hemlig eller konfidentiell) som den virtuella miljön som har högst säkerhetsskyddsnivå.

Fysisk separation

§ *4 kap. 16 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Verksamhetsutövaren ska se till att informationssystem som är avsett att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen hemlig eller kvalificerat hemlig fysiskt separeras från informationssystem eller nätverk som inte omfattas av motsvarande krav på säkerhetsskydd. Med fysisk separation avses att ett informationssystem inte har några fysiska sammankopplingar med andra informationssystem (eng. *air gapped*).

Figur 7 Illustration av hur sårbarhet kan uppstå vid delning av infrastrukturkomponenter mellan informationssystem.



Import och export av data

§ *4 kap. 15–17 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd*

Om data ska importeras från ett informationssystem som inte omfattas av säkerhetsskydd till ett informationssystem avsett att behandla säkerhetsskyddsklassificerade uppgifter, behöver verksamhetsutövaren tillse att importen görs på ett sådant sätt att informationssystemen inte kan kommunicera med varandra. För informationssystem avsedda att behandla säkerhetsskyddsklassificerade uppgifter ska kommunikation för import eller export av data endast ske via envägskommunikation, alltså att information enbart kan flöda åt ett håll.

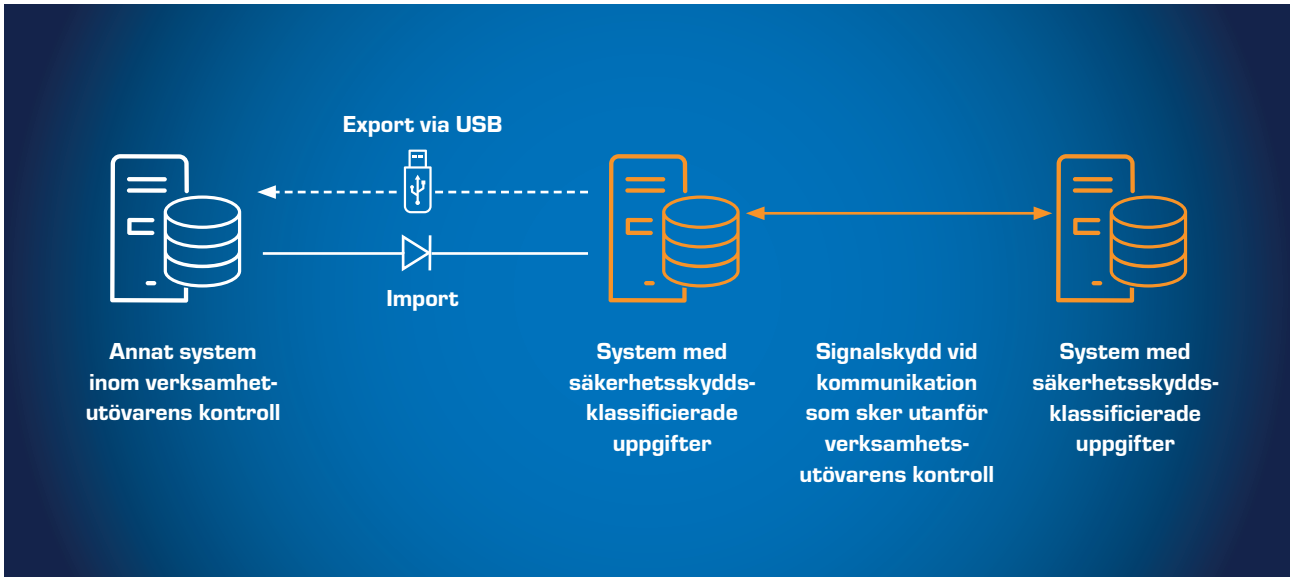
Det är således tillåtet att i sådana system använda datakommunikation för import ***eller*** export. Ett enkelriktat dataflöde för import får inte existera i ett informationssystem som också har ett enkelriktat dataflöde för export. En av import- eller exportvägarna måste vara manuell, vilket exempelvis kan åstadkommas med hjälp av ett flyttbart datamedium. Ett sådant förfarande behöver omgärdas av administrativa och tekniska kontroller, exempelvis rutiner som en genomsökningsstation för flyttbara datamedier som detekterar skadlig kod och kvittenslistor, eller på annat sätt verifiera integriteten i data som importeras. Ett tillvägagångsätt kan vara att exekvera data i ett fristående informationssystem, en så kallad sandlåda (eng. *sandbox*). Med denna metod kan verksamhetsutövaren kontrollera innehållet och i förekommande fall ”tvätta” filerna eller förhindra filerna från att importeras.

I figur 8, visas att en verksamhetsutövare valt att implementera en envägs importfunktion till ett system med säkerhetsskyddsklassificerade uppgifter upp till nivån hemlig. Eventuellt behov av export får då lösas på annat sätt än via nätverk, exempelvis en flyttbar lagringsenhet.

För att koppla ihop två delar av informationssystemet med säkerhetsskyddsklassificerade uppgifter över nätverk eller platser som är utanför verksamhetsutövarens kontroll krävs kryptografiska funktioner som har godkänts av Försvarsmakten.

Figur 8 Fysisk separation.

Figuren visar att en verksamhetsutövaren valt att implementera en envägs importfunktion till ett informationssystem med säkerhetsskyddsklassificerade uppgifter upp till nivån hemlig. Eventuellt behov av export får då lösas på annat sätt än via nätverk, exempelvis en flyttbar lagringsenhet. För att koppla ihop två delar av informationssystemet med säkerhetsskyddsklassificerade uppgifter över nätverk eller platser som är utanför verskamhetsutövarens kontroll krävs kryptografiska funktioner som har godkänts av Försvarsmakten.



4.10 Konfiguration, uppdatering och dokumentering

§ *4 kap. 18 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Informationssystem som har betydelse för säkerhetskänslig verksamhet ska tillämpa konfiguration som använder lämpliga säkerhetsfunktioner, stänga av funktioner som inte används och i övrigt reducera sårbarheter.

4.10.1 Säkerhetskonfigurering

Säkerhetskonfigurering, eller härdning som det kallas i facklitteratur, innebär att komponenter, operativsystem, inbyggda programvaror, nätverkskomponenter, databaser och andra applikationer som ingår i ett informationssystem konfigureras på ett så säkert sätt som möjligt. Till exempel kan åtkomsträttigheterna i systemet och de delar som ingår begränsas, möjliga vägar till angrepp via sårbara funktioner i infrastrukturkomponenter och applikationer skäras av och exponering mot andra informationssystem eller externa enheter förhindras.

Härdning utgår från principen att det som inte behövs för informationssystemets definierade funktion ska vara åtkomstbegränsat, avstängt eller borttaget ur informationssystemet. Därvid ska särskilt beaktas hur informationssystemet exponeras samt vilken hotbild verksamhetsutövaren har att förhålla sig till. Härdning måste ske utan att informationssystemets stabilitet påverkas. Därutöver kan användarvänligheten vara en aspekt att beakta, förutsatt att säkerhetsskyddet inte påverkas negativt. Härdning kan vara en del av en standardkonfiguration, och automatiseras så långt det är möjligt för att minimera risken för felkonfigurationer.

4.10.2 Systemintegritet

För att säkerställa att en antagonist inte ska kunna påverka ett informationssystem behöver säkerhetsskyddsåtgärderna utformas så att de kompletterar och överlappar varandra. Ett sätt att åstadkomma detta är att säkerhetsskyddsåtgärderna byggs i flera lager. Lämpliga säkerhetsskyddåtgärder att implementera utifrån ett sådant resonemang kan till exempel vara följande:

- Fysisk plombering för att upptäcka eventuell manipulation av hårdvara
- Secure Boot för verifiering av uppstartsprocess
- Hårddiskkryptering
- Skydd av systemfiler (åtkomstkontroll)
- Vitlistning av godkända hårdvaruenheter (USB, Thunderbolt, etc.)
- Vitlistning och signering av godkända applikationer
- Användning av lokal brandvägg
- Skydd mot skadlig kod
- Detektering och skydd mot skadliga aktiviteter (intrångsdetektering/intrångsskydd)

4.10.3 Inbyggda funktioner

Informationssystemets inbyggda säkerhetsfunktioner bör användas så långt det är möjligt och så länge de tillför ett faktiskt skydd. I vissa fall kan det vara lämpligt att ta hänsyn till användarvänlighet, så att funktionen inte tillför allt för stora hinder för användaren i arbetet. Användarvänligheten får inte medföra sårbarheter i informationssystemet. Ur ett användarperspektiv bör det vara ”lätt att göra rätt”.

För att härda ett informationssystem finns det en mängd olika rekommendationer från både tillverkare och andra aktörer på marknaden. Kvaliteten på rekommendationerna kan dock vara svår att bedöma, och varierar från tillverkare till tillverkare. Som alternativ till dessa finns olika standarder utgivna av oberoende organisationer. Dessa är ofta mer konceptuella och omfattar de vanligaste delarna i ett informationssystem. Tillverkarspecifika rekommendationer eller andra allmänt kända och verifierade inställningar bör i första hand användas, om sådana finns.

4.10.4 Uppdateringar

§ *4 kap. 19 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Säkerhetsuppdateringar

Sårbarheter i programvaror identifieras löpande och blir ibland publikt kända redan innan tillverkaren av programvaran hunnit åtgärda sårbarheten och publicerat en säkerhetsuppdatering.

Regelbunden uppdatering av programvara genom säkerhetsuppdateringar (även kallade säkerhetspatchar) är en åtgärd som utgör en del av det grundläggande skyddet av ett informationssystem. Syftet med säkerhetsuppdateringar är att användaren ska ha en möjlighet att åtgärda publikt kända sårbarheter i programvaran och på så sätt minska risker för att drabbas av ett angrepp via dessa.

Hur en känd sårbarhet i en programvara kan nyttjas av en antagonist skiljer sig åt och beror till stor del på hur programvaran är implementerad och konfigurerad av användaren.

Notera:
Säkerhetsuppdateringar publiceras inte bara för mjukvara såsom applikationer och operativsystem, utan även för hårdvara i infrastruktur såsom exempelvis switchar, routrar och servrar.

Utbyte av föråldrad programvara
När en tillverkare släpper en ny version eller utgåva av en programvara upphör ofta publiceringen av säkerhetsuppdateringar till äldre versioner av programvaran. I de flesta fall sker detta inte över en natt, utan äldre versioner av programvaran kan ha support under en övergångsperiod som fastställs av tillverkaren. Det är av vikt att verksamhetsutövaren har kännedom om när tillverkarens support för en programvara upphör (eng. *end-of-life*) och har en plan för när och hur avveckling av den föråldrade programvaran ska ske. Programvara som inte längre erhåller säkerhetsuppdateringar från tillverkaren bör avvecklas och ersättas omgående.

Beslut om undantag och praktisk hantering av säkerhetsuppdateringar
En grundläggande princip är att informationssystem som används i säkerhetskänslig verksamhet ska hållas uppdaterade så att säkerhetsbrister och sårbarheter motverkas. I praktiken innebär detta att verksamhetsutövaren ska förse både mjuk- och hårdvaran i informationssystemet med de säkerhetsuppdateringar som publiceras av tillverkaren, samt i övrigt byta ut äldre versioner av programvara som inte längre kan förses med säkerhetsuppdateringar.

Om det finns särskilda skäl får en verksamhetsutövare besluta om undantag från kravet att programvara i ett informationssystem som har betydelse för säkerhetskänslig verksamhet hålls uppdaterad. Så kan vara fallet om det inte är tekniskt möjligt att installera säkerhetsuppdateringarna eller i det fall verksamhetsutövaren konstaterat att det uppenbarligen är obehövligt med hänsyn till andra säkerhetsskyddsåtgärder som har vidtagits.

Ett informationssystem som hanterar säkerhetsskyddsklassificerade uppgifter får inte anslutas direkt mot internet för hämtning av uppdateringar. Säkerhetsuppdateringar behöver därför hämtas till ett separat informationssystem och därefter, på ett kontrollerat sätt, föras över till informationssystemet som hanterar de säkerhetsskyddsklassificerade uppgifterna. För att arbetet med uppdatering och utbyte av programvara ska fungera tillfredställande bör verksamhetsutövaren ta fram och etablera följande i sin organisation:

- **Omvärldsbevakning** – i syfte att information om nya sårbarheter uppmärksammas och värderas.
- **Inventarieförteckning** – i syfte att omvärldsbevakning sker för rätt hårdvara, mjukvara och versioner samt att kunna bedöma vilka system som behöver åtgärdas efter att en sårbarhet har identifieras.
- **Rutiner för test och verifiering** – i syfte att kontrollera att uppdateringen överensstämmer med den av leverantören publicerade uppdateringen och att inga kompatibilitetsproblem eller andra problem uppstår vid installation av säkerhetsuppdateringar eller nya programvaruversioner i driftmiljön. Test bör göras i en separat testmiljö eller i en begränsad del av driftmiljön (exempelvis i vissa datorer).
- **System och rutiner för distribution** – i syfte att säkerhetsuppdateringar effektivt och snabbt ska kunna distribueras till alla berörda enheter.
- **System och rutiner för uppföljning** – i syfte att möjliggöra kontroll av att alla sårbara enheter har fått en säkerhetsuppdatering installerad och är omstartade om detta krävs.

4.10.5 Dokumentation

§ *4 kap. 20–21 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd*

En väl genomarbetad systemdokumentation är en förutsättning för att få en god översikt över ett informationssystem. Det är också en förutsättning för att snabbt och effektivt kunna hantera driftrelaterade problem i vardagen samt incidenter.

Systemdokumentationen är ett viktigt hjälpmedel för att identifiera vilka delar av informationssystemet som berörs av en säkerhetsuppdatering som ska installeras, vilka delar som berörs av en inträffad incident, samt i övrigt för att kunna identifiera beroenden mellan olika komponenter i ett informationssystem.

När ett informationssystem har driftsatts överlämnas ansvaret i regel till personal som ska hantera drift och underhåll av informationssystemet. Systemdokumentationen är en viktig förutsättning för att dessa personer ska kunna utföra sina arbetsuppgifter utan att äventyra säkerheten i informationssystemet. Det är därför viktigt att verksamhetsutövaren har upprättat systemdokumentation för informationssystemet innan det driftsätts.

Innan systemdokumentationen upprättas bör avsedd mottagare kartläggas och fastslås. Systemdokumentation kan behövas i olika delar av en organisation och behöver utformas på ett sådant sätt att den är till nytta för de olika avsedda mottagarna.

Exempel på vad systemdokumentation kan innehålla är:

- beskrivningar av informationssystemets arkitektur med ingående hård- och mjukvara, exempelvis genom ett SAD (eng. *Solution Architecture Document*),
- förklaringar av hur varje komponent inom systemet fungerar, samt
- beskrivningar av hur systemet ska underhållas och vad som ska göras vid vissa kända problem.

En kopia av systemdokumentationen bör finnas i pappersform, så att den är möjlig att ta del av även i det fall den elektroniskt lagrade dokumentationen är otillgänglig, exempelvis vid större störningar i nätverket.

4.11 Skydd mot skadlig kod

4 kap. 22 § Säkerhetspolisens föreskrifter om säkerhetsskydd

Skydd mot skadlig kod syftar till att skydda informationssystemet mot programkod som är tänkt att användas för att otillbörligt ändra, röja (exfiltrera/avlyssna) eller förstöra uppgifter, filer eller programvara som lagras på eller kommuniceras till eller från ett informationssystem.

En verksamhetsutövare som har ett informationssystem som är av betydelse för säkerhetskänslig verksamhet behöver i första hand göra en analys av vilka funktioner för skydd mot skadlig kod som är lämpliga utifrån hur informationssystemet ska användas. Därefter ska verksamhetsutövaren besluta vilka funktioner som ska användas, och slutligen införa dessa funktioner för att skydda informationssystemet.

Ett effektivt skydd mot skadlig kod kan bestå av följande:

- Programexekveringskontroll (så kallad vitlistning), så att enbart godkända program kan exekveras
- Behörighetsstyrning (inklusive begränsning av administratörsrättigheter)
- Begränsning av möjlighet att exekvera scriptkod inom olika dokumenttyper såsom exempelvis Microsoft Office-dokument och PDF-filer
- Lokala brandväggar som hindrar skadlig programvara från att sprida sig vidare till andra komponenter och system
- Funktioner som försvårar utnyttjande av sårbarheter, exempelvis buffertöverskridning
- Antivirusprogramvara

Det vanligaste skyddet mot skadlig kod är antivirusprogramvara, som med hjälp av signaturer söker efter hela eller delar av filer som kan ha ett skadligt beteende. Det är dock relativt enkelt för en antagonist att skapa nya versioner av skadlig kod som inte upptäcks av antivirusprogramvaran. Antivirusprogramvara kan därför vara ett svagt skydd mot en kvalificerad aktör, men ska ändå ses som ett viktigt grundläggande skydd av informationssystem.

Utöver antivirusprogramvaror finns en uppsjö av säkerhetsprodukter som ytterligare kan stärka skyddet. Vidare ska rutiner för att kontrollera att skyddet mot skadlig kod är aktivt tas fram och dokumenteras.

4.12 Skydd mot obehörig förändring av informationssystem

4 kap. 23 § Säkerhetspolisens föreskrifter om säkerhetsskydd

Verksamhetsutövaren måste vidta åtgärder som ger förmåga att försvåra och upptäcka obehörig förändring av informationssystemet.

Metoder för att bibehålla systemintegritet beskrivs i avsnitt 4.10.2 Systemintegritet.

Andra åtgärder för att uppnå kravet på upptäckt är logguppföljning och säkerhetsövervakning.

4.13 Intrångsdetektering och intrångsskydd

§ *4 kap. 24 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Intrångsskydd (eng. *intrusion prevention*) har som funktion att stoppa eller blockera oönskade aktiviteter som pågår i ett nätverk eller informationssystem. Syftet är att identifiera och göra verksamhetsutövaren uppmärksam på oönskade aktiviteter som pågår i ett nätverk eller i ett informationssystem.

Funktioner för intrångsdetektering och intrångsskydd kan se ut på olika sätt, och omfatta till exempel såväl nätverksbaserade produkter som programvara som installeras i någon del av informationssystemet. Nätverksbaserade produkter tar oftast sikte på att upptäcka skadliga aktiviteter i nätverkstrafik och kallas NIDS (eng. *Network Intrusion Detection System*). Produkter som även förhindrar skadliga aktiviteter i nätverkstrafik kallas NIPS (eng. *Network Intrusion Prevention System*). Operativsystemnära mekanismer för detektion eller prevention kallas HIDS (eng. *Host Intrustion Detection System*), respektive HIPS (eng. *Host Intrusion Prevention System*). Utöver dessa finns även applikationsnära skydd som är specialiserade på vissa nätverksprotokoll, exempelvis WAF (eng. *Web Application Firewalls*) för webbaserad kommunikation.

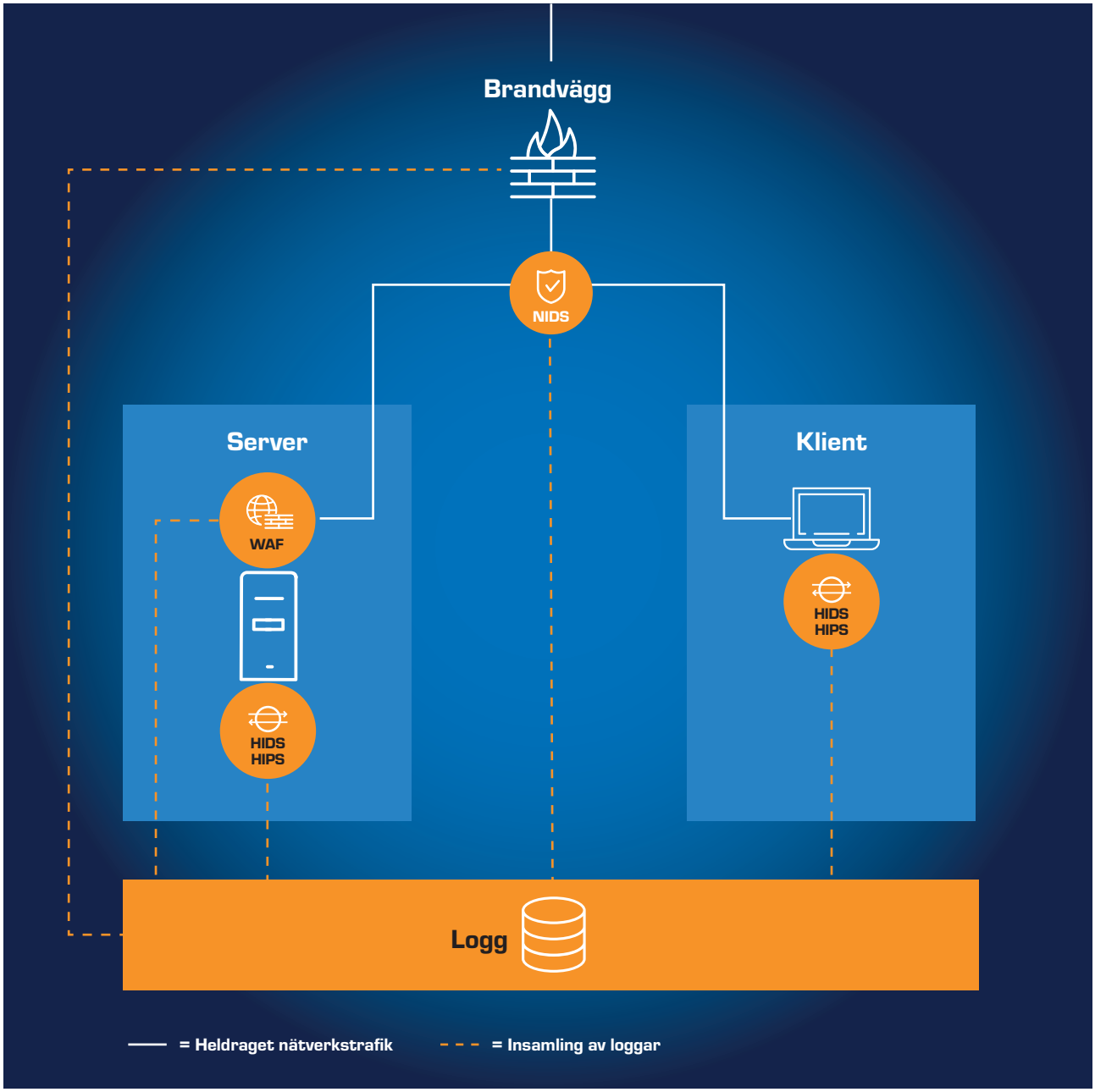
Det är viktigt att IDS- och IPS-system som avses användas verkligen kan analysera de protokoll som används inom systemet och identifiera angrepp på dessa protokoll eller tjänster. Verksamhetsutövare måste analysera var informationssystemet är exponerat och var sådana säkerhetsfunktioner ska implementeras.

I tabell 6 beskrivs ett antal exempel på skyddsmekanismer.

Tabell 6 Skyddsmekanismer

Område	Exempel på övervakningspunkter	Skyddsmekanism
Nätverk	Kända attackmönster i nätverkstrafik. Nätverksflöden som avviker från normala nivåer	Nätverksbaserad intrångsdetektering/ skydd (NIDS/NIPS)
Applikation	Anrop utanför protokollstandarden Felmeddelanden från applikation	Applikationsbrandvägg (WAF)
Operativsystem	Skadliga anrop mot OS-API Suspekta anrop mot systemfiler	Systembaserad intrångsdetektering/skydd (HIDS/ HIPS)

Figur 9. Olika typer av intrångsdetektering.
En illustration av olika typer av intrångsdetektering, se tabell 6 för beskrivning av de olika skyddsmekanismerna



Effektiviteten hos nätverksbaserade produkter för intrångsdetektering och intrångsskydd påverkas negativt av att allt mer nätverkstrafik är krypterad och därmed svårare att inspektera. I vissa fall är det dock möjligt att till exempel placera servertjänster bakom en lastbalanserare som handhar kryptering gentemot klienter. Dekryptering sker då innan nätverkstrafiken skickas vidare till servern, vilket möjliggör inspektion av densamma.

Systemnära intrångsskydd och intrångsdetektering ger ofta bättre skydds- och detekteringsförmåga än nätverksbaserade motsvarigheter, eftersom de ligger närmare systemet där händelsen sker. Det är dock av vikt att även implementera säkerhetsövervakning som kan agera på larm. Detta eftersom en antagonist i de flesta fall kan ta sig runt dessa skydd, om tid ges.

4.14 Säkerhetsloggning

§ *4 kap. 25 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

En logg kan beskrivas som insamlad information om en händelse i ett informationssystem. Informationen brukar som minst omfatta vad som hänt, när det hände och vem som utförde handlingen i systemet. Loggar är ett bra hjälpmedel för att kunna veta vad som hänt i ett informationssystem vid ett givet tillfälle. Därför är säkerställande av en korrekt systemtid genom hela informationssystemet viktigt. I fackspråk används ofta begreppet spårbarhet, där loggar är en förutsättning för att en verksamhetsutövare ska kunna uppnå spårbarhet till olika händelser som inträffar i ett informationssystem.

Spårbarhet är i sin tur en förutsättning för att en verksamhetsutövare ska kunna leda i bevis vem som har gjort vad i ett informationssystem vid ett givet tillfälle, exempelvis vem som haft åtkomst till säkerhetsskyddsklassificerade uppgifter. Detta är viktigt i synnerhet vid misstanke om brott. I övrigt är loggar ett bra hjälpmedel för att i efterhand kunna identifiera orsaken till varför incidenter av olika slag har inträffat. Loggar kan även vara till hjälp vid återställandet av systemet.

En verksamhetsutövare som är ansvarig för ett informationssystem av betydelse för säkerhetskänslig verksamhet ska logga händelser som kan påverka säkerheten i systemet. Detta i syfte att kunna upptäcka och utreda skadlig inverkan, obehörig åtkomst eller påverkan och funktionsstörningar.

I detta avsnitt beskrivs viktiga principer som en verksamhetsutövare ska beakta i fråga om säkerhetsloggning och logguppföljning i ett informationssystem som har betydelse för säkerhetskänslig verksamhet.

4.14.1 Logguppföljning och åtgärder vid upptäckta händelser

§ *4 kap. 26—27 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Verksamhetsutövaren ska kunna upptäcka skadlig inverkan.

Logguppföljning är en viktig åtgärd för att kunna upptäcka händelser som kan påverka säkerheten i informationssystem som har betydelse för säkerhetskänslig verksamhet.

För att arbetet med logguppföljning ska ge önskad effekt behöver verksamhetsutövaren ta fram en process med olika rutiner som beskriver hur verksamhetsutövarens personal ska arbeta med logguppföljning. Sådana rutiner bör ge svar på följande frågor:

- Varför ska logguppföljning genomföras (vad är syftet och målet med logguppföljningen)?
- Vem eller vilka ska utföra logguppföljningen?
- När ska logguppföljning genomföras (löpande, jämna intervaller, stickprovskontroller, på förekommen anledning, etc.)?
- Hur ska logguppföljning genomföras och vilka åtgärder ska vidtas när verksamhetsutövaren upptäckt en potentiellt oönskad händelse (checklistor, rutinbeskrivningar, etc.)?
- Med vilka tekniska hjälpmedel ska logguppföljningen genomföras?

Rutinerna bör också innehålla en tydligt beskriven eskaleringsordning som stöd i beslut om åtgärd vid en upptäckt händelse, till exempel att incidenthantering ska påbörjas.

Vad som ska loggas i ett informationssystem är en komplex fråga. Svaret är beroende av flera olika faktorer såsom syften med loggningen, hur informationssystemet ska användas, av vilka det ska användas och hur det exponeras.

Rutinerna ska omfatta hur verksamhetsutövaren ska kunna upptäcka skadlig inverkan, obehörig åtkomst eller påverkan och funktionsstörningar. För informationssystem som behandlar säkerhetsskyddsklassificerade uppgifter ska det även omfatta användning och ändringar av behörigheter med systemadministrativ åtkomst och av roller med särskild behörighet till informationssystemet.

Loggar kan generas från olika typer av källor, så kallade loggkällor. Loggning kan exempelvis ske i en programvara, i ett operativsystem eller i olika komponenter i infrastrukturen för ett informationssystem. Vad som ska loggas och vilka loggkällor som ska användas behöver verksamhetsutövaren fastställa innan ett informationssystem tas i drift. Loggning i programvara bör ske av användaraktiviteter såsom lyckade och misslyckade inloggningar, objektåtkomst samt hantering av informationsobjekt (exempelvis förändring, radering och skapande av nya informationsobjekt).

Loggning i operativsystem bör ske av systemhändelser såsom systemstart och -stopp, processer kopplade till uppstart av programvara samt larm som genererats av olika skyddsfunktioner (till exempel antivirusprogram).

Loggning i infrastrukturkomponenter bör ske av åtkomst till, och förändringar av, systemkonfiguration i exempelvis switchar, routrar, brandväggar, VPN-koncentratorer, m.m.. Loggning bör även ske av larm som genererats av skyddsfunktioner i samma komponenter (exempelvis intrångsdetektering, innehållsfiltrering, m.m.).

Gemensamt i alla ovanstående fall är att loggning av aktiviteter kopplade till användare och konton med systemadministrativ åtkomst eller annan särskild tillgång

till informationssystem bör ägnas extra uppmärksamhet. I övrigt bör verksamhetsutövaren kontinuerligt utvärdera behovet av loggning och därefter göra anpassningar, exempelvis genom att etablera nya loggkällor eller förändra kriterier i befintliga loggkällor.

4.14.2 Hantering av säkerhetsloggar

§ *4 kap. 28–29 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd*

Att upprätthålla tillförlitligheten hos de loggar som genereras är en mycket viktig aspekt som en verksamhetsutövare behöver beakta. En av anledningarna till detta är att loggar ofta används som underlag i internutredningar som kan leda till disciplinära åtgärder och användas som bevis i brottmål.

Om riktigheten i loggarna kan ifrågasättas kan det leda till att ansvar inte kan utkrävas av den som gjort sig skyldig till brott. En annan aspekt som en verksamhetsutövare behöver beakta är att loggar kan innehålla säkerhetsskyddsklassificerade uppgifter och att konfidentialitet för loggarna därmed behöver upprätthållas.

Loggar kan skyddas på flera olika sätt. En grundläggande åtgärd för att skydda riktigheten i loggarna och samtidigt upprätthålla konfidentialitet är att begränsa åtkomsten till loggarna genom en strikt behörighetshantering. Tillförlitligheten kan stärkas ytterligare med hjälp av kryptografiska funktioner, exempelvis genom så kallad elektronisk signering.

För att kunna skydda och bevara loggar, upprätthålla tillförlitlighet hos innehållet i loggarna samt genomföra logguppföljning, kan loggarna samlas i en centraliserad teknisk funktion, såsom en central loggserver. Vid användning av en central loggfunktion är det viktigt att denna ges minst samma säkerhetsskydd som de informationssystem i vilka loggarna genererats. Ett antal skyddsåtgärder att särskilt beakta för en sådan funktion är strikt behörighets- och åtkomstkontroll, kryptering av nätverkstrafik vid överföring av logghändelser samt kryptering av loggdata i vila. Personal med systemadministrativ åtkomst i informationssystemet bör inte ha tillgång till den centrala loggservern eftersom de då kan förvanska loggposter för att dölja skadlig aktivitetSäkerhetsloggar ska bevaras i minst tio år, eller för system som behandlar kvalificerat hemlig information i 25 år.

4.15 Säkerhetsövervakning

§ *4 kap. 30–31 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd*

Med säkerhetsövervakning avses en funktion som arbetar med aktiv övervakning av ett informationssystem i syfte att kunna upptäcka, försvåra och hantera skadlig inverkan på informationssystemet samt obehörig avlyssning av eller åtkomst till informationssystemet.

Enkelt beskrivet är säkerhetsövervakning en funktion där personal med hjälp av olika tekniska hjälpmedel aktivt söker efter oönskade händelser i ett informationssystem.

Vid upptäckt agerar funktionen genom att försöka förhindra exempelvis ett intrångsförsök. Skulle ett intrångsförsök lyckas utreder funktionen hur, var och varför intrånget skedde samt vad som behövs för att förhindra framtida intrång.

Notera:
För informationssystem som är avsett för behandling av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass hemlig eller kvalificerat hemlig, eller som är av motsvarande betydelse för Sveriges säkerhet, är verksamhetsutövaren skyldig att använda funktioner för säkerhetsövervakning och ha rutiner som omfattar bland annat ansvarsutpekande och åtgärder vid upptäckta händelser/incidenter.

4.15.1 Genomförande

En funktion för säkerhetsövervakning är beroende av både en teknisk plattform och kompetent personal. Personal som arbetar med säkerhetsövervakning tillhör ofta en del i en verksamhet som organiseras som SOC (eng. *Security Operations Center*). Vid sidan av en SOC finns ofta även en funktion för driftövervakning som benämns NOC (eng. *Network Operations Center*). En NOC fokuserar oftast på övervakning av informationssystem med syfte att upprätthålla tillgänglighet och prestanda. Dessa båda funktioner kompletterar varandra och utgör sammantaget en viktig funktion för att upprätthålla säkerheten i ett informationssystem.

Hur arbetet med säkerhetsövervakning ska genomföras behöver verksamhetsutövaren fastställa och därefter reglera i dokumenterade rutiner. Dessa bör ge svar på följande frågor:

- Varför ska säkerhetsövervakning genomföras (vad är syftet och målet med övervakningen)?
- Vem eller vilka ska utföra säkerhetsövervakningen (exempelvis en SOC-funktion)?
- När ska säkerhetsövervakning genomföras (under vilka tider)?

- Hur ska logguppföljning genomföras och vilka åtgärder ska vidtas när verksamhetsutövaren upptäckt en potentiellt oönskad händelse (rutiner, checklistor, processbeskrivningar, etc.)?
- Med vilka tekniska hjälpmedel ska säkerhetsövervakning genomföras (exempelvis ett SIEM, jfr avsnitt 4.15.3)?

4.15.2 Åtgärder vid upptäckta händelser

När funktionen för säkerhetsövervakning upptäcker ett potentiellt intrång eller en annan oönskad händelse i ett informationssystem bör det även finnas en tydligt beskriven eskaleringsordning att ta stöd av. Utifrån denna kan de som arbetar med säkerhetsövervakning fatta beslut om vidare åtgärd. Exempel på fortsatta åtgärder kan vara att inleda fördjupad analys av händelsen och incidenthantering.

En fördjupad analys kan bestå av granskning av loggar direkt i en loggkälla såsom ett operativsystem, en programvara eller i infrastrukturkomponenter. Fördjupad analys kan även göras i switchar, routrar, brandväggar, VPN-koncentratorer och i de inbyggda skyddsfunktionerna i sådana komponenter, exempelvis intrångsdetektering eller innehållsfiltrering. Även analys av minnesavbilder, nätverkstrafik och eventuell skadlig kod kan vara en del av den fördjupade analysen.

4.15.3 Tekniska hjälpmedel

Som ett stöd i arbetet med säkerhetsövervakning finns en mängd olika programvaror anpassade för ändamålet. SIEM (eng. *Security Information and Event Management*) är en vanlig benämning på en programvara som kan vara ett stöd vid säkerhetsövervakning av skyddsvärda system.

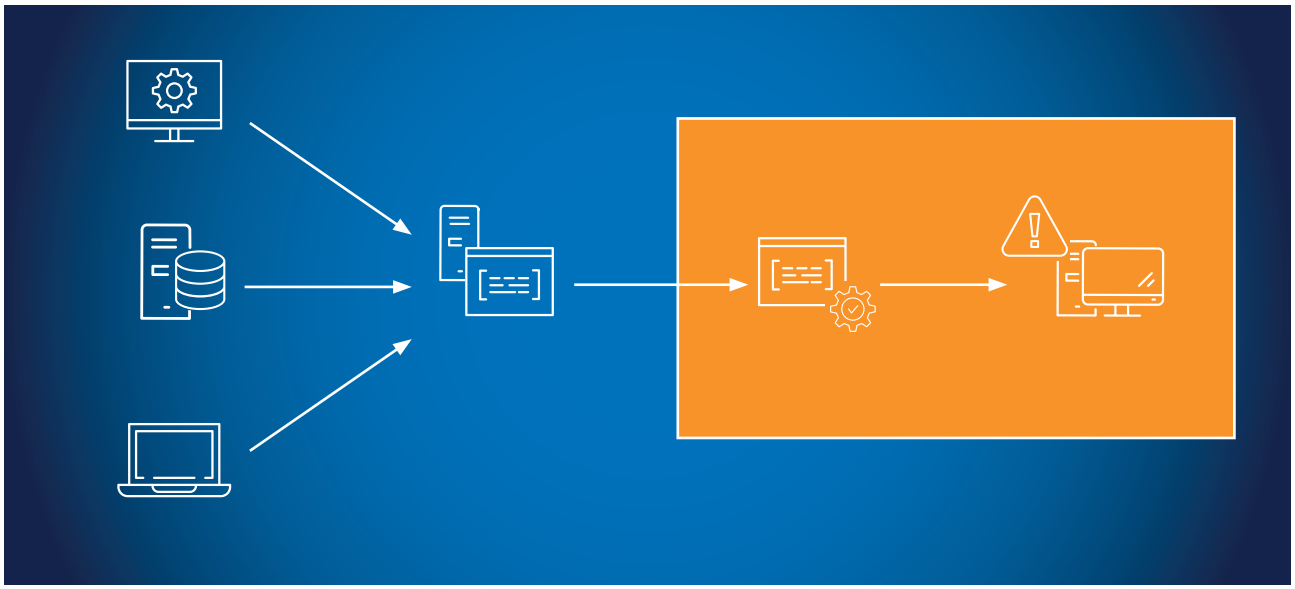
SIEM sköter insamling och aggregering av loggar som genererats av olika loggkällor i ett informationssystem. Baserat på innehållet i loggarna identifierar och kategoriserar SIEM möjliga incidenter och händelser som skett i informationssystemet och gör sedan en automatisk analys av dem. SIEM har därefter två syften:

1. Tillhandahålla rapporter gällande säkerhetsrelaterade incidenter och händelser såsom förekomst av skadlig kod, misslyckade inloggningsförsök, avaktiverade användarkonton som återaktiveras och andra potentiellt skadliga aktiviteter i informationssystemet.
2. Generera larm, om det under den automatiska analysen visar sig att det förekommer potentiellt skadliga aktiviteter i informationssystemet. Den automatiska analysen utgår från ett fördefinierat regelverk där det framgår vilka parametrar och tröskelvärden som ska generera ett larm.

4.15.4 Övning och utvärdering

Ett bra sätt att testa och utvärdera både styrdokument, personella resurser och tekniska hjälpmedel som används i en funktion för säkerhetsövervakning är att genomföra övningar. Genom samarbete med penetrationstestare kan funktionen för säkerhetsövervakning öva olika angreppsscenarion i informationssystemet, vilket gör att exempelvis tröskelvärden för generering av larm kan testas och finjusteras. Genom ett oannonserat angrepp med hjälp av penetrationstestare kan även verksamhetsutövarens incidenthantering sättas på prov och utvärderas.

Figur 10 En konceptuell illustration av logg och säkerhetsövervakning.



4.16 Åtgärder för att upprätthålla kontinuitet

§ *4 kap. 32 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

I en säkerhetskänslig verksamhet där ett informationssystem är skyddsvärt utifrån perspektiven riktighet och tillgänglighet är det nödvändigt med åtgärder för att upprätthålla kontinuitet. Detta ska verksamhetsutövaren säkerställa genom att nödvändiga rutiner och funktioner finns på plats.

Åtgärder att upprätthålla kontinuitet ska finnas för it-funktionen som tillhandahåller informationssystemet, men bör även finnas hos den verksamheten som nyttjar informationssystemet för sin säkerhetskänsliga verksamhet.

För it-funktionen är kraven på kontinuitet och återställningsförmåga omfattande. Dessa innefattar bland annat krav på redundans för komponenter eller hela informationssystemet, samt förmåga att återställa informationssystemet på samma eller annan plats. Därtill behöver tillgång till kompetens och andra resurser säkerställas över tid. Allt beroende på när i tid skada för Sveriges säkerhet kan uppstå.

+ *De konkreta bedömningarna som gjorts bör redovisas i den särskilda säkerhetskyddsbedömningen, se avsnitt 5.1 Särskild säkerhetsskyddsbedömning.*

It-funktionen som förvaltar och ansvarar för drift av informationssystemet behöver kontinuitetsrutiner (en kontinuitetsplan). Rutinerna kan omfatta allt från instruktioner som möjliggör att olika it-tekniker kan lösa varandras uppgifter till total återställning av informationssystemet. Både funktioner och rutiner bör provas och övas.

4.17 Kontroll av säkerhetskopior

§ *4 kap. 33 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Säkerhetskopiering utgör en viktig livlina. Det kan få stora konsekvenser om denna är bristfällig, eftersom information som regel är en verksamhetsutövares viktigaste resurs. Brister i säkerhetskopieringen kan vid dataförlust åsamka verksamhetsutövaren stor skada. Även förlust av till synes oviktig information kan ofta skada verksamheten.

Verksamhetsutövaren bör därför ta fram rutiner för hur säkerhetskopiering ska hanteras. Viktiga aspekter att beakta i detta sammanhang är:

- att data säkerhetskopieras enligt ett intervall som verksamhetsutövaren fastställt,
- att säkerhetskopior förvaras på betryggande sätt i verksamhetsutövarens lokaler (bör vara i annan brandcell om det är i samma lokal), helst på flera geografiskt åtskilda platser,
- att verksamhetsutövaren, enligt ett testintervall som verksamhetsutövaren fastställt, dock minst en gång per år, verifierar att säkerhetskopiorna kan återskapas, och
- att säkerhetskopior som innehåller säkerhetsskyddsklassificerade uppgifter hanteras och förvaras enligt den högsta säkerhetsskyddsklassen i systemet.


Den särskilda säkerhetsskyddsbedömningen ska redovisa skyddsvärden, vilka säkerhetshot och sårbarheter som föreligger kring dessa skyddsvärden, samt hur den säkerhetskänsliga verksamheten i stort påverkas av driftsättningen.

5 Förberedande åtgärder inför driftsättning av ett informationssystem

5.1 Särskild säkerhetsskyddsbedömning

§ *3 kap. 1 och 4 §§ säkerhetsskyddsförordningen*

§ *2 kap. 13 § och 4 kap. 3 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Enligt säkerhetsskyddslagstiftningen ska verksamhetsutövaren inför vissa förfaranden göra en särskild säkerhetsskyddsbedömning. Ett av dessa förfaranden är driftsättning av informationssystem som har betydelse för säkerhetskänslig verksamhet.

Det finns inte något krav på upprättande av en särskild säkerhetsskyddsbedömning inför en väsentlig förändring av ett informationssystem. Den metod som bör användas för att kunna bedöma om det är frågan om en väsentlig förändring eller inte, liksom för att fastställa om det krävs några ändringar i säkerhetskraven eller några nya säkerhetsskyddsåtgärder, är densamma som vid upprättandet av en särskild säkerhetsskyddsbedömning.

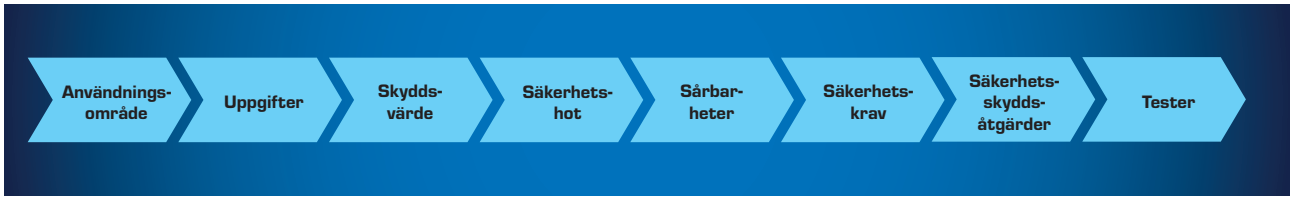
Den särskilda säkerhetsskyddsbedömningen ska genomföras innan ett informationssystem tas i drift. Bedömningen ska redovisa skyddsvärden, det vill säga vilka säkerhetsskyddsklassificerade uppgifter som kan komma att behandlas i systemet eller på vilket annat sätt systemet i övrigt är av betydelse för säkerhetskänslig verksamhet. I det senare fallet ska konsekvensnivån bedömas utifrån den skada för Sveriges säkerhet en antagonistisk handling mot informationssystemet kan medföra (jfr 2 kap. 3–5 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd).

Den särskilda säkerhetsskyddsbedömningen ska också beskriva vilka säkerhetshot och sårbarheter som föreligger kring dessa skyddsvärden, samt hur den säkerhetskänsliga verksamheten i stort påverkas av driftsättningen.

Med utgångspunkt i ovanstående ska verksamhetsutövaren i den särskilda säkerhetsskyddsbedömningen ta ställning till vilka säkerhetskrav som är motiverade att ställa på informationssystemet och beskriva hur säkerhetsskyddet utformas med hjälp av åtgärder i och kring informationssystemet (säkerhetsskyddsåtgärder), i syfte att leva upp till kraven.

Verksamhetsutövaren ska dokumentera både de preskriptiva kraven som följer av säkerhetskyddslagstiftningen och de behov av ytterligare säkerhetskrav (säkerhetsskyddsåtgärder) som verksamhetsutövaren identifierar utifrån skyddsvärden, sårbarheter och säkerhetshot. Om verksamhetsutövaren angivit att informationssystemet är skyddsvärt ur perspektiven riktighet eller tillgänglighet (konsekvensnivå) ska verksamhetsutövaren definiera vilka säkerhetskrav och

Figur 11 Översikt av innehållet i en särskild säkerhetsskyddsbedömning.



tillhörande säkerhetsskyddsåtgärder som krävs för att upprätthålla dessa skyddsvärden. Ett exempel på denna typ av krav som verksamhetsutövaren själv ska identifiera är tillgänglighetskrav, vilka bör specificera efter hur lång tid en störning i en viss funktion ger skada för Sverige. Kraven möts i sin tur av säkerhetsskyddsåtgärder i form av till exempel teknisk redundans och återställningsförmåga. Säkerhetsskyddsåtgärderna ska testas och sedan jämföras med säkerhetskraven för informationssystemet.

Den särskilda säkerhetsskyddsbedömningen utgör ett lämpligt styrdokument för säkerhetsskyddsarbetet i och kring informationssystemet och behöver hållas uppdaterat och användbart under systemets livstid, från driftsättning till avveckling. Den särskilda säkerhetsskyddsbedömningen är ett bra underlag för de som ska sköta systemet och dess säkerhetsskydd.
Den särskilda säkerhetsskyddsbedömningen är:

1. Ett ställningstagande/beslut
2. En dokumentation som
   - beskriver skyddsvärden, säkerhetshot, sårbarheter, säkerhetskrav och säkerhetsskyddsåtgärder,
   - används som styrdokument och hålls uppdaterad under systemets livstid, och
   - i förekommande fall används som underlag vid samråd med Säkerhetspolisen.

Det finns inga formkrav på den särskilda säkerhetsskyddsbedömningen utöver att den ska dokumenteras och fastställas av säkerhetsskyddschefen. Dokumentet bör vara anpassat till verksamhetsutövarens organisation på ett sätt som gör dokumentet användbart för personal som ska hantera systemet.

Den särskilda säkerhetskyddsbedömningen behöver vara tydlig i frågorna om:

1. att alla säkerhetskrav är omhändertagna eller, om kravet inte är applicerbart, att det motiveras varför,
2. vilka säkerhetsskyddsåtgärder omhändertar säkerhetskravet, samt
3. att säkerhetsskyddsåtgärderna bedöms vara tillräckliga och relevanta för respektive krav.

Detta för att möjliggöra såväl framtida bedömningar av huruvida en förändring i informationssystemet är en väsentlig förändring eller inte, som eventuellt nödvändigt samråd med Säkerhetspolisen.

Notera:
Verksamhetsutövaren måste själv identifiera säkerhetskraven för tillgänglighet och riktighet för sina konsekvensnivåindelade informationssystem. Ingångsvärdena för detta återfinns i säkerhetsskyddsanalysen.

Se vidare i Vägledning i säkerhetsskydd –Säkerhetsskyddsanalys avsnitt 3.4 där det understryks att frågan efter hur lång tid bristande tillgänglighet riskerar att medföra skada för Sveriges säkerhets är helt central. Den tid som anges i säkerhetsskyddsanalysen är styrande för säkerhetskraven [säkerhetsskyddsåtgärdena].

Se även avsnitten 4.16–17 i denna vägledning.

I de fall krav på säkerhetsskyddsåtgärder i form av rutinbeskrivningar eller annan dokumentation följer av Säkerhetspolisens föreskrifter om säkerhetsskydd kan detta beskrivas direkt i den särskilda säkerhetsskyddsbedömningen eller i till exempel bilagor eller annan dokumentation som den särskilda säkerhetsskyddsbedömningen hänvisar till.

Att tänka på-lista för en särskild säkerhetsskyddsbedömning

Nedan är några av de saker en verksamhetsutövare bör tänka på och hantera

Användningsområde

- ☐ För vilket syfte?
- ☐ För vilken verksamhet?
- ☐ För vilka användare eller användargrupper?

Uppgifter

- ☐ Befintliga
- ☐ Vilka in- och utflöden?
- ☐ Vad nyskapas eller förädlas?

Skyddsvärden
(med stöd ur säkerhetsskyddsanalysen)

Varför är informationssystemet skyddsvärt?
Motivera varför eller varför inte för varje säkerhetsskyddsaspekt nedan

- ☐ Vilken är högsta nivån på säkerhetsskyddsklassificerade uppgifter?
- ☐ Vilken är konsekvensnivån vid bristande tillgänglighet?
- ☐ Vilken är konsekvensnivån vid bristande riktighet?

Hot
(med stöd ur säkerhetsskyddsanalysen)

- ☐ Från säkerhetsskyddsanalysen
- ☐ Nya identifierande hot efter analys ur informationssystemets perspektiv

Sårbarheter

- ☐ Ur informationssystemets roll i den säkerhetskänsliga verksamheten
- ☐ Informationssystemets exponering
- ☐ Aktuella sårbarheter utifrån teknikval och arkitektur
- ☐ Utveckling, förvaltning och drift. Har jag rådighet över informationssystemet?

Författningsreglerade krav
Alla författningsrelaterade krav ska omhändertas!

- ☐ Om verksamhetsutövaren anser att något inte är applicerbart ska detta motiveras.
- ☐ De säkerhetsskyddsåtgärder som omhändertar säkerhetskravet ska bedömas vara tillräckliga och relevanta

Egna säkerhetskrav

- ☐ Komplettera med säkerhetskyddskrav som är anpassade för er verksamhets behov inom konfidentialitet, riktighet och tillgänglighet
- ☐ Om konsekvensnivå D eller högre för riktighet eller tillgänglighet ska relevanta säkerhetskrav, som preciserar de rutiner och funktioner som krävs för att upprätthålla kontinuiteten i den säkerhetskänsliga verksamheten, tas fram (PMFS 4 kap. 32 §)
- ☐ De säkerhetsskyddsåtgärder som omhändertar säkerhetskravet ska bedömas vara tillräckliga och relevanta

Säkerhetsskyddsåtgärder

- ☐ En eller flera till varje säkerhetskrav
- ☐ De åtgärder som beskrivs ska ha argument och ställningstagande av verksamhetsutövaren att de är tillräckliga och relevanta, det vill säga att kravet är omhändertaget.

Tester

- ☐ Strukturerade, relevanta tekniska och administrativa tester som omhändertar säkerhetskraven

5.2 Godkännande från säkerhetsskyddssynpunkt inför driftsättning

§ *3 kap. 3 § säkerhetsskyddsförordningen*

§ *1 kap. 4 § Säkerhetspolisens föreskrifter om säkerhetsskydd*

Innan informationssystemet tas i drift ska verksamhetsutövaren skriftligen godkänna systemet från säkerhetsskyddssynpunkt. I praktiken ska detta göras innan systemet börjar användas i den säkerhetskänsliga verksamheten, till exempel genom att börja hantera säkerhetsskyddsklassificerade uppgifter i systemet eller att den säkerhetskänsliga verksamheten börjar använda systemet. Detta är inte med nödvändighet detsamma som när systemet för första gången startas. Ur ett it-driftperspektiv har systemet sannolikt redan varit igång under en tid innan driftsättning sker.

Även under anskaffning, utveckling och testning av informationssystemet behöver säkerhetsaspekterna beaktas. Detta för att säkerställa att informationssystemet inte blir korrupt innan driftsättning.

Om driftsättningen kräver samråd med Säkerhetspolisen ska samrådet göras innan verksamhetsutövaren godkänner informationssystemet från säkerhetsskyddssynpunkt. Om driftsättningen varit föremål för samråd med Säkerhetspolisen bör Säkerhetspolisens yttrande ses som en del av underlaget till beslutet om godkännande.

Notera:
Innan ett godkännande av ett system från säkerhetsskyddssynpunkt ska det finns en särskild säkerhetsskyddsbedömning framtagen där säkerhetsskyddskrav och säkerhetsskyddsåtgärder fastställts. Vidare krävs att tester påvisar att fastställda säkerhetsskyddsåtgärder omhändertar säkerhetskraven. Dessutom ska det framgå att verksamhetsutövaren har bedömt vilka resurser och kompetenser som krävs för att bibehålla fastställt säkerhetsskydd under informationssystemets förväntade livstid.

5.3 Samråd med Säkerhetspolisen inför driftsättning av informationssystem

§ *3 kap. 2 § säkerhetsskyddsförordningen*

Inför driftsättning av ett informationssystem som förväntas behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre ska skriftligt samråd ske med Säkerhetspolisen. Om verksamhetsutövaren tillhör Försvarsmaktens eller Försvarets materielverks tillsynsområde ska denne i stället samråda med Försvarsmakten. Samrådsskyldigheten gäller även för informationssystem där obehörig åtkomst till systemet kan medföra en skada för Sveriges säkerhet som inte är obetydlig (konsekvensnivå A, B eller C). Med obehörig åtkomst avses påverkan på riktighet och tillgänglighet.

5.3.1 Samråd inför driftsättning av ett informationssystem

Vid ett samråd behöver Säkerhetspolisen i den särskilda säkerhetsskyddsbedömningen kunna utläsa vilka krav på säkerhetsskyddsåtgärder i och kring informationssystemet som verksamhetsutövaren identifierat och på vilka sätt dessa krav uppfylls. Säkerhetspolisen måste också kunna utläsa på vilket sätt de författningskrav som gäller för informationssystemet enligt säkerhetsskyddslagstiftningen uppfylls.

Ett samråd avslutas alltid med ett slutligt yttrande från Säkerhetspolisen till verksamhetsutövaren. En kopia på yttrandet skickas till verksamhetsutövarens tillsynsmyndighet. I yttrandet lämnas synpunkter kring de säkerhetsskyddsåtgärder verksamhetsutövaren har vidtagit, eller har för avsikt att vidta, och hur dessa förhåller sig till bestämmelserna om säkerhetsskydd i de olika författningarna.

För att kunna lämna ett kvalitativt yttrande behöver Säkerhetspolisen i den särskilda säkerhetsskyddsbedömningen kunna utläsa följande:

- Att alla tillämpliga säkerhetskrav som följer av lag, förordning och föreskrift omhändertagits
- Att alla andra säkerhetskrav som verksamhetsutövaren tagit ställning till motiveras från säkerhetsskyddssynpunkt
- Och hur verksamhetsutövaren omhändertagit säkerhetskraven med säkerhetsskyddsåtgärder

5.3.2 Samråd vid väsentlig förändring av ett informationssystem

Även inför en väsentlig förändring av ett informationssystem bör verksamhetsutövaren genomföra en särskild säkerhetsskyddsbedömning. Det finns inget legalt krav på upprättande av en särskild säkerhetsskyddsbedömning vid en sådan förändring. En sådan bedömning motsvarar fullt ut den fördjupade analys som behöver göras. Genom den särskilda säkerhetsskyddsbedömningen eller den fördjupande analysen identifierar verksamhetsutövaren vilka säkerhetsskyddsåtgärder som ska vidtas i och med att förändringen genomförs.

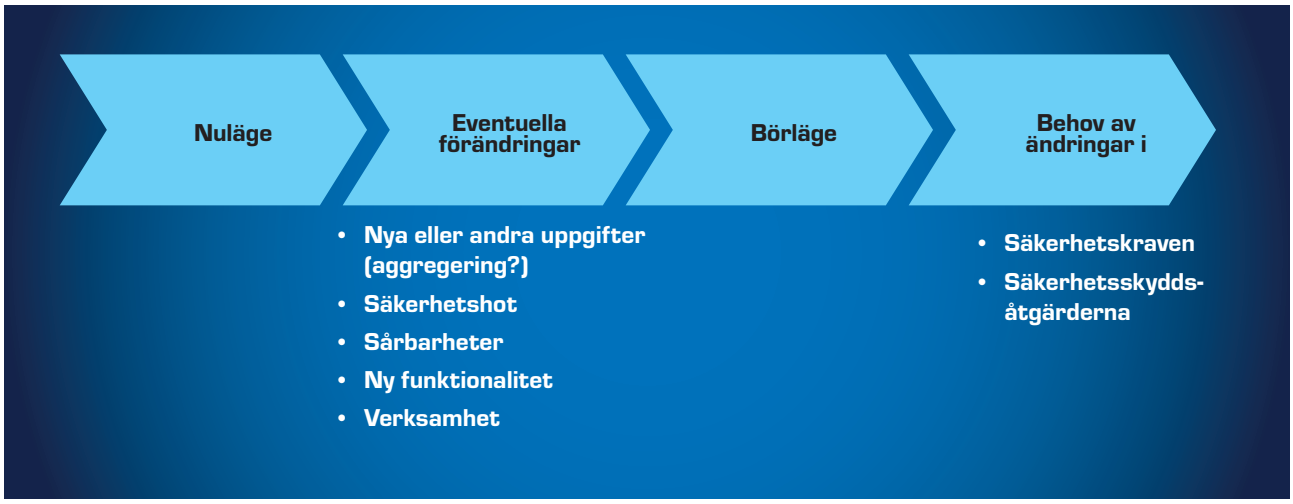
På motsvarande sätt som vid ett samråd inför driftsättning lämnar Säkerhetspolisen alltid ett skriftligt yttrande till verksamhetsutövaren med kopia till verksamhetsutövarens tillsynsmyndighet. I ett sådant yttrande lämnas synpunkter kring de säkerhetsskyddsåtgärder verksamhetsutövaren har vidtagit, eller har för avsikt att vidta, och hur dessa förhåller sig till säkerhetsskyddslagstiftningen.

Lämplig metod för att värdera huruvida det är frågan om en väsentlig förändring eller inte är att göra en uppdaterad särskild säkerhetsskyddsbedömning för informationssystemet för att kunna bedöma om befintliga säkerhetskrav eller säkerhetsskyddsåtgärder hanterar den förändring som planeras i informationssystemet. Om det behövs ändrade eller kompletterande säkerhetskrav eller ändrade säkerhetsskyddåtgärder är det frågan om en väsentlig förändring.

Vad som utgör en väsentlig förändring i ett informationssystem kan vara svårt att avgöra. En väsentlig förändring skulle exempelvis kunna vara när:

- Ett befintligt informationssystem ska hantera uppgifter med en högre säkerhetsskyddsklassificering än tidigare. Till exempel när nya uppgifter tillförs eller när aggregering uppstår (se avsnitt 2.4 Samling av uppgifter).
- Ett befintligt informationssystem ska integreras eller kommunicera med andra informationssystem eller av något annat skäl få ökad exponering.
- Ett befintligt informationssystem ska användas i en annan säkerhetskänslig verksamhet (om inte en sådan hantering omfattas av det ursprungliga samrådet).
- Förändringen medför att hotbilden förändras.

Figur 12 Bedömning om väsentlig förändring.



6 Vad gäller för informationssystem som driftsatts före den 1 april 2019?

Som redan beskrivits i avsnitt 3.1 ovan (Krav på godkännande av informationssystem) gäller bestämmelsen i 3 kap. 3 § säkerhetsskyddsförordningen, om krav på godkännande från säkerhetsskyddssynpunkt inför driftsättning, endast informationssystem som driftsatts efter den 1 april 2019. Bestämmelsen i 3 kap. 1 § Säkerhetspolisens föreskrifter om säkerhetsskydd gäller däremot alla informationssystem som hanterar säkerhetsskyddsklassificerade uppgifter, oberoende av när informationssystemet driftsattes.

Ett godkännande av informationssystemet innebär att systemet minst ska uppfylla alla säkerhetskrav som gäller för den säkerhetsskyddsklass på uppgifterna som hanteras i systemet. Metoden för att identifiera säkerhetskraven och därmed kunna vidta rätt säkerhetsskyddsåtgärder bör vara desamma som angetts i kapitel 5.

Det finns alltså inget legalt krav på en särskild säkerhetsskyddsbedömning, men upprättandet av en sådan är en lämplig metod för att säkerställa ett fullgott resultat.

Noteras vidare bör att bestämmelsen i 3 kap. 2 § säkerhetsskyddsförordningen, om krav på samråd inför väsentlig förändring, gäller alla säkerhetskänsliga informationssystem, oberoende av när de driftsatts. För att kunna bedöma om en planerad åtgärd utgör en väsentlig förändring eller inte behövs analyser för såväl nuläge som tänkt börläge. De analyser som behöver finnas på plats inför en bedömning motsvarar särskilda säkerhetsskyddsbedömningar. Även detta talar alltså för att särskilda säkerhetsskyddsbedömningar behöver upprättas för informationssystem som driftsatts före 2019. Vid ett eventuellt samråd med Säkerhetspolisen är det den informationen som tas fram i en särskild säkerhetsskyddsbedömning som yttrandet baseras på.

Slutligen bör noteras att 3 kap. 4 § säkerhetsskyddsförordningen anger att verksamhetsutövaren ska vidta lämpliga skyddsåtgärder för att kunna upptäcka, försvåra och hantera skadlig inverkan på informationssystemet samt obehörig avlyssning av, åtkomst till och nyttjande av informationssystemet. Verksamhetsutövaren ska också se till att spårbarhet finns för händelser som är av betydelse för säkerheten i systemet samt beakta förekomsten av röjande signaler och vidta lämpliga skyddsåtgärder. Metoden för att identifiera säkerhetskraven och därmed kunna vidta rätt säkerhetsskyddsåtgärder bör vara densamma som används för särskilda säkerhetsskyddsbedömningar.

Text: Säkerhetspolisen. Form: Intellecta. Tryck: Stibo Complete.

Säkerhetspolisen har tagit fram ett antal vägledningar som kan fungera som ett stöd för verksamhetsutövare i tillämpningen av säkerhetsskyddsregelverket.

1. Introduktion till säkerhetsskydd
2. Säkerhetsskyddsanalys
3. Personalsäkerhet
4. Fysisk säkerhet
5. Informationssäkerhet
6. Skyldigheter vid exponering av säkerhetskänslig verksamhet
7. Besök och delegationer
8. Avlyssnade utrymmen

Säkerhetspolisen

Box 12312, 102 28 Stockholm
010-568 70 00 | sakerhetspolisen@sakerhetspolisen.se
www.sakerhetspolisen.se