Vägledning i säkerhetsskydd

Säkerhetsskyddsanalys

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 Januari 2023

Denna vägledning riktar sig till verksamhetsutövare (enskilda verksamhetsutövare, statliga myndigheter, regioner och kommuner) som ska upprätta eller uppdatera en säkerhetsskyddsanalys.

Denna vägledning beskriver såväl metoden som de olika delarna i framtagandet av en säkerhetsskyddsanalys samt ger vägledning i tillämpningen av relevanta bestämmelser i säkerhetsskyddslagen (2018:585), säkerhetsskyddsförordningen (2021:995) och Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd.

För riksdagen och dess myndigheter finns bestämmelser om säkerhetsskyddsanalys i 3 § 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 Vägledning i säkerhetsskydd – Introduktion i säkerhetsskydd.

I vägledningen finns ett antal rutor, vilka innehåller sådant som är viktigt att tänka på i arbetet med säkerhetsskyddsanalysen.

Innehåll


Vad ska skyddas?
Mot vad ska det skyddas?
Hur ska det skyddas?

1 Vad är en säkerhetsskyddanalys?

§ *1 kap. 1–2 §§ och 2 kap. 1 § säkerhetsskyddslagen (2018:585)*

§ *2 kap. 1 § säkerhetsskyddsförordningen (2021:955)*

§ *2 kap. 1–9 §§ Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Säkerhetsskyddsanalysen är den grundläggande delen i ett strukturerat och systematiskt säkerhetsskyddsarbete och utgör en förutsättning för att kunna vidta nödvändiga säkerhetsskyddsåtgärder. Säkerhetsskyddsanalysen ska ge svar på följande frågor:

- Vad ska skyddas?
- Mot vad ska det skyddas?
- Hur ska det skyddas?

I säkerhetsskyddsanalysen ligger fokus på att identifiera och bedöma skyddsvärden utifrån ett konsekvensperspektiv, det vill säga utifrån vilken skada en händelse kan medföra för Sveriges säkerhet. Detta skiljer sig exempelvis från många andra typer av analyser som även tar hänsyn till hur sannolikt det är att en händelse inträffar och får negativa konsekvenser.

1.1 Vem ska göra en säkerhetsskyddsanalys?

§ *2 kap. 1 § säkerhetsskyddslagen (2018:585)*

Den som till någon del bedriver säkerhetskänslig verksamhet är skyldig att utreda behovet av säkerhetsskydd. Detta görs genom en säkerhetsskyddsanalys. Med utgångspunkt i säkerhetsskyddsanalysen ska verksamhetsutövaren planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter.

För vissa verksamheter är det inte tydligt om de bedriver säkerhetskänslig verksamhet eller inte. I sådana fall bör metoden för säkerhetsskyddsanalys användas i syfte att bedöma om så är fallet. Om verksamheten kommer fram till att ingen säkerhetskänslig verksamhet bedrivs bör slutsatserna dokumenteras trots att kravet på att göra en säkerhetsskyddsanalys inte föreligger.

En leverantör som endast deltar i någon annans säkerhetskänsliga verksamhet med stöd av ett säkerhetsskyddsavtal bör som utgångspunkt inte anses bedriva säkerhetskänslig verksamhet och behöver därför inte heller göra en säkerhetsskyddsanalys. Att en leverantör deltar i någon annans säkerhetskänsliga verksamhet utesluter dock inte att leverantören samtidigt bedriver egen säkerhetskänslig verksamhet. En leverantör som har flera uppdrag som omfattas av krav på säkerhetsskyddsavtal kan i vissa fall, genom sina samlade uppdrag, anses bedriva säkerhetskänslig verksamhet. Säkerhetsskyddslagstiftningen kan alltså i sådana fall bli direkt tillämplig på leverantören av tjänsterna. Detta medför att leverantören ska genomföra en säkerhetsskyddsanalys för att bedöma behovet av ytterligare säkerhetsskydd i den egna verksamheten än vad som redan följer av åtagandena i de säkerhetsskyddsavtal som ingåtts.

1.2 Vägen fram till en säkerhetsskyddsanalys

Planera genomförandet

Innan arbetet med säkerhetsskyddsanalysen påbörjas behöver verksamhetsutövaren tillgodose att det finns förutsättningar för att säkerhetsskyddet ska kunna upprätthållas under arbetet.

Om arbetet leder fram till att säkerhetsskyddsklassificerade uppgifter upprättas och behöver hanteras i verksamheten behöver nödvändiga säkerhetsskyddsåtgärder vidtas för att det ska vara möjligt att genomföra arbetet. Detta ställer exempelvis krav på lämpliga rum och förvaringsutrymmen, rutiner för hur dokumentationen ska gå till, behov av annan teknisk utrustning och eventuella behov av säkerhetsskyddsavtal.

Olika funktioner och kompetenser kommer att behöva delta i olika delar av säkerhetsskyddsanalysen. Exempelvis bör representanter med god kännedom om verksamhetens olika delar delta vid identifieringen av skyddsvärden och representanter från säkerhetsorganisationen vid bedömningen av vilka säkerhetsskyddsåtgärder som ska vidtas. En bedömning behöver även göras om de som kommer att delta i arbetet med de olika delarna av säkerhetsskyddsanalysen innehar befattningar som behöver vara placerade i säkerhetsklass och om de anställda är i behov av utbildning i säkerhetsskydd.

Genomförandet av en säkerhetsskyddsanalys behöver ges tid och resurser. Det är därför viktigt att säkerhetsskyddsanalysen och dess arbete i ett tidigt skede förankras hos verksamhetens högsta chef eller motsvarande organ som ska fastställa säkerhetsskyddsanalysen.

Det praktiska genomförandet av en säkerhetsskyddsanalys är inte så sekventiellt som metoden visar.

Se metoden för säkerhetsskyddsanalys, sid 7.

Eftersom de olika delarna är beroende av varandra kan de i vissa fall göras parallellt. För att arbetet ska resultera i en säkerhetsskyddsanalys där delarna är harmoniserade och har en tydlig koppling till varandra, behöver säkerhetsskyddsanalysen löpande uppdateras om förutsättningarna i en av delarna av säkerhetsskyddsanalysen förändras.

För att säkerställa spårbarhet i arbetet med säkerhetsskyddsanalysen är det viktigt att utförligt dokumentera säkerhetsskyddsanalysen och dess tillhörande arbete. Ett exempel på tillhörande arbete är underliggande motiveringar och ställningstaganden i arbetet som leder fram till slutsatserna i säkerhetsskyddsanalysen. Detta underlättar för kommande uppdateringar av säkerhetsskyddsanalysen och kan ge en förståelse för implementering av säkerhetsskyddsanalysen i det kontinuerliga säkerhetsskyddsarbetet. Motiveringar och ställningstaganden är också förutsättningar för en tillsynsmyndighets möjlighet att bedöma en säkerhetsskyddsanalys inom ramen för sin tillsynsverksamhet.

För att minska risken för missförstånd och göra säkerhetsskyddsanalysen lättare att ta till sig bör verksamhetsutövaren använda vedertagna begrepp. Begrepp som har en legaldefinition bör i säkerhetsskyddsanalysen ges samma innebörd som de har i säkerhetsskyddslagstiftningen.

För att kunna bedöma vilka säkerhetsskyddsåtgärder som är nödvändiga att vidta är det viktigt att tydligt motivera och beskriva:

- skyddsvärden (avsnitt 3)
- säkerhetshot (avsnitt 4)
- sårbarheter (avsnitt 5).

De säkerhetskyddsåtgärder (avsnitt 6) som beskrivs i säkerhetsskyddsanalysen ska sammanställas i en separat säkerhetsskyddsplan (avsnitt 8).

Säkerhetsskyddsanalysen kan delvis eller i sin helhet innehålla säkerhetsskyddsklassificerade uppgifter. Detta påverkar såväl det praktiska arbetet som hantering av dokumentation samt vilka som kan engageras i arbetet. Exempelvis kan sårbarhetsbedömningen innehålla uppgifter som är indelade i en högre säkerhetsskyddsklass jämfört med de andra delarna av säkerhetsskyddsanalysen, vilket påverkar vem som är behörig att ta del av den.

Beroenden och användning av andra analyser

En verksamhetsutövare kan vara beroende av en annan verksamhet för att kunna bedriva sin verksamhet. Det kan därför vara nödvändigt att samverka med externa aktörer i arbetet med säkerhetsskyddsanalysen. Verksamhetsutövaren behöver beakta att det, i den utsträckning det förekommer säkerhetsskyddsklassificerade uppgifter i denna samverkan, föreligger krav på säkerhetsskyddsavtal i vissa fall.

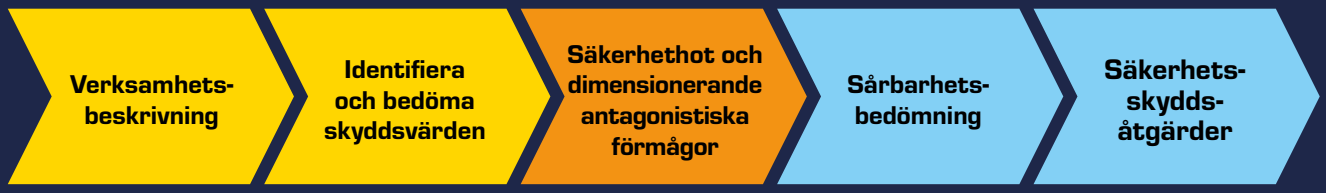
I arbetet med säkerhetsskyddsanalysen kan verksamhetsutövaren som underlag använda andra befintliga analyser som är relevanta för verksamheten. Exempelvis har risk- och sårbarhetsanalyser och andra riskanalyser beröringspunkter med säkerhetsskyddsanalysen. Även i dessa analyser är det centralt att analysera vad som ska skyddas, mot vad det ska skyddas och hur det ska skyddas. Trots beröringspunkterna är det viktigt att i arbetet vara medveten om och beakta de skillnader som finns mellan analyserna. Exempelvis tar risk- och sårbarhetsanalyser hänsyn till miljön och ekonomiska värden, vilket inte ska beaktas i

säkerhetsskyddsanalysen. Ytterligare en viktig distinktion är att säkerhetsskyddsanalysen inte tar hänsyn till den bedömda sannolikheten för att olika händelser ska inträffa, och inte heller till kostnaderna för de åtgärder som ska vidtas, vilket riskanalyser vanligtvis behöver förhålla sig till.

Notera:
Efter varje del i metoden, från och med *avsnitt 2* nedan och framåt, finns en checklista som kan användas som stöd i framtagandet av säkerhetsskyddsanalysen. Checklistorna är inte uttömmande; även andra aktiviteter kan vara nödvändiga att genomföra.

Säkerhetsskyddsanalysen ska ge svar på följande frågor

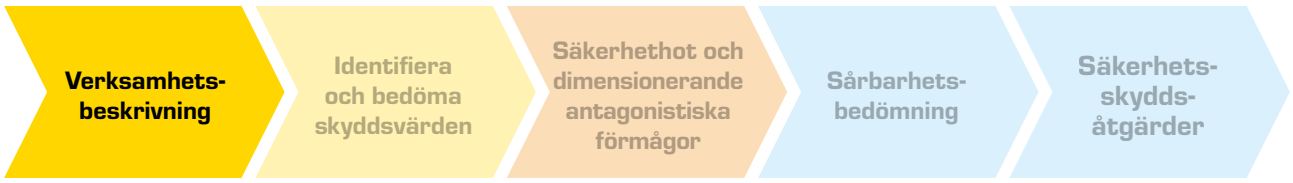
Säkerhetspolisens metod för att ta fram en säkerhetsskyddsanalys är indelad i fem delar



Säkerhetsskyddsplanen ska redogöra för hur behovet av säkerhetsskyddsåtgärder som identifierats i säkerhets-skyddsanalysen omhändertas.


I verksamhetsbeskrivningen
ska verksamhetsutövaren
övergripande beskriva
sin verksamhet och specificera
vilka delar av verksamheten
som är säkerhetskänslig.

2 Verksamhetsbeskrivning



§ *2 kap. 2 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Syftet med verksamhetsbeskrivningen är att övergripande beskriva sin verksamhet och specificera vilka delar av verksamheten som är säkerhetskänslig.

Exempel på vad som kan vara av betydelse för Sveriges säkerhet är tjänster, leveranser, funktioner eller förmågor. En verksamhetsbeskrivning kan öka förståelsen för helheten hos läsaren.

Att en verksamhet ofta förändras med tiden medför ett behov av sådan konkretion att det tydligt framgår hur verksamheten såg ut när säkerhetsskyddsanalysen upprättades eller senast uppdaterades.

I bedömningen av vilka delar av verksamheten som är av betydelse för Sveriges säkerhet behöver de bakomliggande resonemangen som ligger till grund för den slutliga bedömningen redovisas.

Det bör också framgå om det finns delar av verksamheten som bedömts men inte ansetts utgöra säkerhetskänslig verksamhet. En sådan bedömning bör motiveras för att det ska finnas spårbarhet till de bakomliggande resonemangen. Detsamma gäller eventuell verksamhet som tidigare bedömts vara säkerhetskänslig men som inte längre bedöms vara det.

Utgångspunkten i verksamhetsbeskrivningen är den egna verksamheten som bedrivs (tjänster, leveranser, funktioner och förmågor) men det finns även exempel på när den egna verksamheten inte står i fokus. Till exempel kan det vara så att ens egen verksamhet inte bedöms som säkerhetskänslig men att det någonstans i verksamheten hanteras uppgifter som säkerhetsskyddsklassificerats av en annan verksamhetsutövare som bedriver säkerhetskänslig verksamhet. Om denna hantering sker utan krav på säkerhetsskyddsavtal, och om säkerhetsskyddet inte heller regleras på något annat tillräckligt sätt, kan denna hantering i sig anses utgöra säkerhetskänslig verksamhet, vilken får till följd att säkerhetsskyddslagen blir fullt tillämplig på den delen av ens verksamhet.

Specificeringen av hur de identifierade delarna av verksamheten är av betydelse för Sveriges säkerhet görs enligt följande kategorier:

- Sveriges yttre säkerhet
- Sveriges inre säkerhet
- nationellt samhällsviktig verksamhet
- verksamhet av betydelse för Sveriges ekonomi
- verksamhet som kan generera skada på annan säkerhetskänslig verksamhet.

De fem kategorierna beskrivs mer i detalj på nästa sida. Observera att en verksamhet kan omfattas av flera kategorier.

Specificeringen av hur de identifierade delarna av verksamheten är av betydelse för Sveriges säkerhet görs enligt kategorierna:

Sveriges yttre säkerhet
Sveriges förmåga att upprätthålla nationellt försvar (territoriell suveränitet) samt upprätthållande av Sveriges integritet, oberoende och handlingsfrihet (politisk självständighet).

En viktig beståndsdel är den nationella försvarsförmågan av Sveriges territorium, där Försvarsmakten har huvudansvaret. I den uppgiften ligger att kunna försvara Sverige, upptäcka och avvisa kränkningar av svenskt territorium samt värna om Sveriges suveräna rättigheter och nationella intressen inom Försvarsmaktens verksamhetsområde. Utöver verksamhet som bedrivs av Försvarsmakten finns andra verksamheter som är viktiga för det militära försvarets förmåga att utföra sitt uppdrag, såsom verksamheter i det civila försvaret och försvarsindustrier.

Sveriges inre säkerhet
Sveriges förmåga att upprätthålla och säkerställa grundläggande strukturer, inklusive det demokratiska statsskicket, rättsväsendet och den brottsbekämpande förmågan på nationell nivå. Detta handlar till stor del om att skydda anläggningar, funktioner och informationssystem som är kritiska för dessa grundläggande strukturer.

Nationellt samhällsviktig verksamhet
Tjänster, leveranser, funktioner och förmågor som är nödvändiga för samhällets funktionalitet på nationell nivå.

Verksamheter som definieras som nationellt samhällsviktiga ur ett säkerhetsskyddsperspektiv återfinns bland annat inom områdena energiförsörjning, elektroniska kommunikationer, finansiella tjänster (centrala betalningssystem), livsmedelsförsörjning, vattenförsörjning och transporter. Avgörande för om sådan verksamhet kan anses vara av betydelse för Sveriges säkerhet är om en antagonistisk handling (exempelvis spionerі, sabotage eller terroristbrott) skulle kunna medföra direkta eller uppenbart indirekta skadekonsekvenser på nationell nivå.

Exempel på sådana verksamheter kan vara:

- Anläggningar, system och funktioner som genom sitt läge eller sin funktion i transmissionsnätet har en viktig roll för upprätthållandet av det nationella elsystemet. Dessa återfinns till exempel hos elproducenter och eldistributörer.
- Anläggningar, system och funktioner som genom sitt läge eller funktion i infrastrukturen för elektronisk kommunikation har en viktig roll för upprätthållandet av kommunikationen på nationell nivå. Dessa återfinns till exempel hos teleoperatörer och leverantörer av datakommunikation.

Notera:
Kategorin nationellt samhällsviktig verksamhet ur ett säkerhetsskyddsperspektiv är inte att likställa med samhällsviktig verksamhet. Alla samhällsviktiga verksamheter är alltså inte av betydelse för Sveriges säkerhet. För att en samhällsviktig verksamhet ska vara av betydelse för Sveriges säkerhet behöver en antagonistisk handling kunna medföra skador på nationell nivå.

Verksamhet av betydelse för Sveriges ekonomi
Tjänster, leveranser, funktioner eller förmågor som är nödvändiga för den nationella betalningsförmågan. Vidare avses förmågan att hantera, administrera, granska, styra och stödja den nationella finansiella stabiliteten.

Vägledande för om en sådan verksamhet är av betydelse för Sveriges säkerhet är om konsekvenserna av en antagonistisk handling mot verksamheten har en direkt eller uppenbart indirekt påverkan på Sveriges betalningsförmåga.

Exempel på sådan verksamhet kan vara de centrala system som genom sina funktioner i infrastrukturen är kopplade till det centrala betalningssystemet och har en viktig roll för upprätthållandet av betalningsflödena på nationell nivå.

Verksamhet som kan generera skada på annan säkerhetskänslig verksamhet
En skadegenererande verksamhet är en verksamhet som vid en antagonistisk handling kan generera skada på andra säkerhetskänsliga verksamheter genom påverkan på liv, hälsa eller infrastruktur. Påverkan på liv och hälsa kan uttryckas i att många människor förväntas att dö eller skadas, och påverkan på infrastruktur avser fysisk förstöring av annan säkerhetskänslig verksamhet. Sådana anläggningar eller objekt är ofta redan identifierade och klassificerade utifrån annan lagstiftning – till exempel farlig verksamhet enligt 2 kap. 4 § lagen (2003:778) om skydd mot olyckor – med den skillnaden att säkerhetskyddslagstiftningen endast omfattar anläggningar som direkt eller uppenbart indirekt kan generera skadekonsekvenser på nationell nivå.

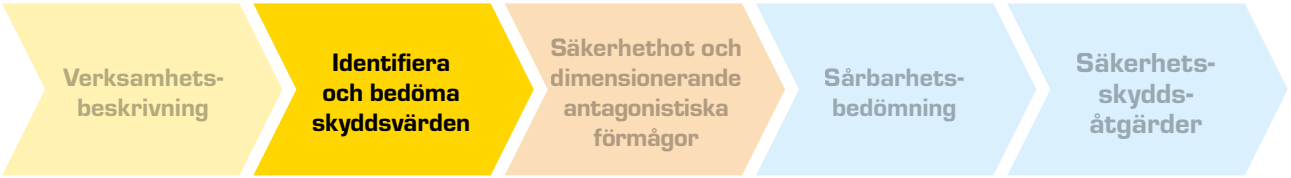
Exempel på skadegenererande verksamheter kan vara kärntekniska verksamheter, större dammar och kemiska industrier som vid en antagonistisk handling skulle påverka andra säkerhetskänsliga verksamheter.

Verksamhetsbeskrivning

- ☐ Hela den verksamhet som omfattas av säkerhetsskyddsanalysen har beskrivits övergripande.
- ☐ Det framgår av verksamhetsbeskrivningen utifrån vilken eller vilka kategorier delarna av verksamheten är av betydelse för Sveriges säkerhet.
- ☐ De bakomliggande resonemangen som ligger till grund för bedömningarna framgår.

Verksamhetsutövaren ska identifiera och bedöma specifika skyddsvärden samt bedöma från vilket eller vilka perspektiv dessa är skyddsvärda.

3 Identifiera och bedöma skyddsvärden



§ *2 kap. 3 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

En säkerhetskänslig verksamhet innehåller ett eller flera skyddsvärden. Syftet med denna del av säkerhetsskyddsanalysen är att identifiera och bedöma specifika skyddsvärden samt att bedöma från vilket eller vilka perspektiv dessa är skyddsvärda. En utgångspunkt för att identifiera skyddsvärdena är att utgå från verksamhetsbeskrivningen och de delar av verksamheten som är av betydelse för Sveriges säkerhet. Eventuella interna eller externa beroenden bör även beskrivas för respektive skyddsvärde.

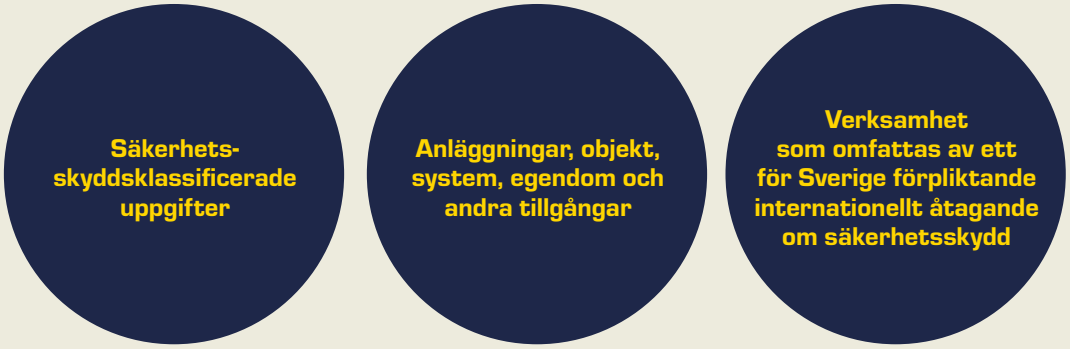
Följande tre typer av skyddsvärden ska identifieras och bedömas (dessa förklaras närmare i detta avsnitt):

- säkerhetsskyddsklassificerade uppgifter
- anläggningar, objekt, system, egendom och andra tillgångar
- verksamhet som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd.

Uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd utgör säkerhetsskyddsklassificerade uppgifter och ryms därför per definition även inom den första typen av skyddsvärde.

Om verksamhetsutövaren i sin identifiering av skyddsvärden har kommit fram till att ingen säkerhetskänslig verksamhet bedrivs, bör bedömningarna dokumenteras och arbetet med säkerhetsskyddsanalysen avslutas. Eftersom det inte finns några skyddsvärden behöver inga bedömningar av säkerhetshot, sårbarheter och säkerhetsskyddsåtgärder genomföras.

Tre typer av skyddsvärden ska identifieras och bedömas



3.1 Säkerhetsskyddsklassificerade uppgifter

§ *1 kap. 2 § och 2 kap. 5 § säkerhetsskyddslagen (2018:585)*

§ *2 kap. 3 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Med säkerhetsskyddsklassificerade uppgifter avses 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 lagen hade varit tillämplig. Om en viss sekretessbestämmelse i OSL är relevant för säkerhetsskyddsklassificeringen beror på vilket intresse bestämmelsen avser att skydda och om detta skyddsintresse har tillräcklig koppling till Sveriges säkerhet. Några vanligt förekommande bestämmelser om sekretess i OSL som kan vara av relevans för säkerhetsskyddsklassificering är:

§ *15 kap. 1 – 1b §§ 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 för bestämmelser om sekretess i OSL som kan vara av relevans vid säkerhetsskyddsklassificering. Det är dock endast sekretessbestämmelser till skydd för allmänna, inte enskilda intressen som kan vara av relevans för säkerhetsskyddsklassificering.

I säkerhetsskyddsanalysen ska de säkerhetsskyddsklassificerade uppgifter som finns i verksamheten identifieras. Säkerhetsskyddsklassificerade uppgifter ska löpande delas in i någon av de fyra säkerhetsskyddsklasserna, utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet:

1. kvalificerat hemlig (synnerligen allvarlig skada)
2. hemlig (allvarlig skada)
3. konfidentiell (inte obetydlig skada)
4. begränsat hemlig (endast ringa skada).

Att redovisa varje enskild uppgift inom ramen för en säkerhetsskyddsanalys kan beroende på verksamhetens storlek, vara ett alltför omfattande arbete. Förekomsten av säkerhetsskyddsklassificerade uppgifter kan därtill förändras snabbt i många verksamheter, vilket medför att en sådan sammanställning snart skulle bli inaktuell. Det kan därför vara lämpligt att i säkerhetsskyddsanalysen redovisa uppgifter på en mer övergripande nivå, till exempel utifrån typer av uppgifter.

För säkerhetsskyddsklassificerade uppgifter (som är indelade i säkerhetsskyddsklass utifrån den skada ett röjande kan medföra för Sveriges säkerhet) behöver det i säkerhetsskyddsanalysen framgå högsta säkerhetsskyddsklass som förekommer för respektive typ av uppgift.

Nedan följer ett exempel på hur en verksamhetsutövare kan redovisa detta i säkerhetsskyddsanalysen.

En verksamhetsutövare har genom systematiska kontroller av säkerhetsskyddet samt interna rapporteringar av säkerhetshotande händelser identifierat sårbarheter för skyddsvärden och den säkerhetskänsliga verksamheten i stort. Dessa kontroller, rapporter och sammanställningar är av varierande omfattning och visar på sårbarheter av olika allvarlighetsgrad. De säkerhetsskyddsklassificerade uppgifterna som tagits fram i samband med detta är indelade i säkerhetsskyddsklasserna hemlig, konfidentiell eller begränsat hemlig. I säkerhetsskyddsanalysen kan verksamhetsutövaren exempelvis redovisa sårbarhetsdokumentation som en typ av säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass hemlig eller lägre. Detta medför att verksamhetsutövaren inte behöver redovisa varje enskild uppgift i säkerhetsskyddsanalysen.

Notera:
Indelningen av uppgifter i säkerhetsskyddsklass är inte primärt ett moment i säkerhetsskyddsanalysen, utan ska göras fortlöpande när uppgifterna upprättas eller behandlas i det dagliga arbetet. Om verksamhetsutövaren, under genomförandet av säkerhetsskyddsanalysen, upptäcker att säkerhetsskyddsklassificerade uppgifter inte har delats in i säkerhetsskyddsklass, ska dock en indelning av dessa göras trots att varje enskild uppgift inte behöver redovisas i säkerhetsskyddsanalysen.

Den uppgift i informationssystemet som har högst säkerhetsskyddsklass är dimensionerande för hur informationssystemet ska skyddas. Aggregering innebär att det genom att kombinera uppgifter i en uppgiftssamling går att härleda ny information, i betydelsen en eller flera uppgifter som inte framgår av de enskilda uppgifterna i uppgiftssamlingen var och en för sig. En uppgift som är resultatet av en aggregering ska säkerhetsskyddsklassificeras och kan därvid bedömas ha en annan säkerhetsskyddsklass än uppgifterna i den uppgiftssamling ur vilken den nya uppgiften har härletts.

+ *För ytterligare stöd att bedöma uppgiftssamlingar, se Vägledning i säkerhetsskydd – Informationssäkerhet.*

Notera:
Om ett informationssystem innehåller en eller flera säkerhetsskyddsklassificerade uppgifter ska det betraktas som ett informationssystem som har betydelse för säkerhetskänslig verksamhet.

3.2 Verksamhet som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd

§ *2 kap. 5 § säkerhetsskyddslagen (2018:585)*

§ *3 kap. 9 § säkerhetsskyddsförordningen (2021:955)*

§ *2 kap. 3 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Sverige har ingått ett antal internationella överenskommelser om säkerhetsskydd, såväl bilaterala som multilaterala, med andra stater och mellanfolkliga organisationer som exempelvis EU och Nato. Sveriges säkerhetsskyddsöverenskommelser publiceras normalt på regeringens webbplats i serien Sveriges internationella överenskommelser (SÖ). Överenskommelsernas bestämmelser syftar huvudsakligen till att reglera hur uppgifter som kräver säkerhetsskydd ska hanteras av mottagande part.

Uppgifter som redan delats in i säkerhetsskyddsklass av en annan stat eller en mellanfolklig organisation ska inte delas in i säkerhetsskyddsklass på nytt hos den verksamhetsutövaren som har tagit emot uppgifterna, utan ska behandlas i enlighet med det internationella åtagandet. I internationella åtaganden om säkerhetsskydd framgår det vanligtvis vilka säkerhetsskyddsklasser som används i respektive land eller mellanfolklig organisation som är part i åtagandet. Det är endast de benämningarna som framgår av gällande överenskommelse som får användas av parterna. Dessa benämningar varierar mellan olika länder beroende på den nationella lagstiftningen. Det finns ingen enhetlig internationell nomenklatur för de olika säkerhetsskyddsnivåerna och antalet nivåer kan variera från land till land. Skyddsvärden i verksamheter som inte är uppgifter, och omfattas av ett internationellt åtagande om säkerhetsskydd, behöver på samma sätt som uppgifter förhålla sig till det internationella åtagandet.

Som exempel kan nämnas EU:s olika säkerhetsskyddsklasser (motsvarande svenska inom parentes):

TRÈS SECRET UE	EU TOP SECRET	(kvalificerat hemlig)
SECRET UE	EU SECRET	(hemlig)
CONFIDENTIEL UE	EU CONFIDENTIAL	(konfidentiell)
RESTREINT UE	EU RESTRICTED	(begränsat hemlig)

Om uppgifterna inte har indelats i säkerhetsskyddsklass av den andra parten ska de delas in i säkerhetsskyddsklass utifrån den skada som ett röjande kan medföra för Sveriges förhållande till annan stat eller mellanfolklig organisation eller, om detta motiverar en högre säkerhetsskyddsklass, den skada ett röjande kan medföra för Sveriges säkerhet.

Notera:
Om en eller flera verksamheter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd har identifierats, anses verksamhetsutövaren bedriva säkerhetskänslig verksamhet och omfattas då av säkerhetsskyddslagen.

3.3 Anläggningar, objekt, system, egendom och andra tillgångar

§ *2 kap. 3 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Skyddsvärden som utgörs av anläggningar, objekt, system, egendom och andra tillgångar ska delas in i konsekvensnivåer. För att avgöra konsekvensnivå behöver verksamhetsutövaren ingående beskriva de bakomliggande resonemangen som ligger till grund för den slutliga bedömningen av respektive skyddsvärde. Det innebär att respektive bedömning, exempelvis att ett skyddsvärde är skyddsvärt ur perspektivet tillgänglighet och att ett otillgängliggörande skulle leda till allvarlig skada för Sveriges säkerhet, behöver motiveras med angivande av underliggande fakta eller väl underbyggda antaganden snarare än att presenteras som ett konstaterande. Verksamhetsutövaren behöver också på ett tydligt sätt beskriva hur respektive skyddsvärde är kopplat till Sveriges säkerhet, vilket medför behov av konkretisering av konsekvenser på nationell nivå, inte enbart lokala och regionala konsekvenser.

När det gäller anläggningar, objekt, system, egendom och andra tillgångar kan det vara svårt att avgöra i vilken omfattning ett skyddsvärde ska brytas ned i olika delar. Att underlåta att bryta ned övergripande skyddsvärden kan försvåra det vidare arbetet med att identifiera sårbarheter och bedöma vilka säkerhetsskyddsåtgärder som är nödvändiga att vidta. Samtidigt är det lämpligt att avgränsa identifieringen så att skyddsvärdena inte bryts ned till en detaljeringsgrad som inte är av relevans för vilka säkerhetsskyddsåtgärder som behöver vidtas. Som redan påtalats ska verksamhetsutövaren identifiera anläggningar, objekt, system, egendom och andra tillgångar som är av betydelse för Sveriges säkerhet. Det kan därför vara lämpligt att bryta ned ett skyddsvärde till motsvarande nivå. I vissa fall behöver skyddsvärdet brytas ned ytterligare för att en verksamhetsutövare ska kunna bedöma vilka säkerhetsskyddsåtgärder som är nödvändiga att vidta. I dessa fall är en vägledande princip att bryta ned det som är skyddsvärt till en nivå där nödvändiga säkerhetsskyddsåtgärder kan identifieras.

Exempel:
En verksamhetsutövare bedriver säkerhetskänslig verksamhet i form av tillhandahållande av positioneringsdata åt myndigheter med betydelse för Sveriges inre säkerhet. Myndigheterna ges tillgång till positioneringsdata genom en applikation som i sin tur hämtar uppgifterna från en databas i ett informationssystem.

Om myndigheterna skulle förlora sin åtkomst till positioneringsdata under mer än en viss tid skulle det riskera att medföra en inte obetydlig skada för Sveriges säkerhet. Skadan kan sägas vara en uppenbart indirekt konsekvens av ett avbrott i verksamhetsutövarens verksamhet.

För att informationssystemet ska fungera behövs en lokal med fungerande kraftförsörjning, kommunikation, kylsystem etc. Kylsystemet i sin tur består av exempelvis pumpar och värmeväxlare vilka i sin tur kan brytas ner ytterligare hela vägen ner till komponentnivå med till exempel termostater och flödesmätare.

I det här fallet är bedömningen att det finns ett skyddsvärde: informationssystemet. Detta innebär att kraftförsörjningen och kylsystemet (samt dess termostater och flödesmätare) inte redovisas som skyddsvärden i säkerhetsskyddsanalysen eftersom de inte medför ett ytterligare behov av säkerhetsskyddsåtgärder.

Notera:
Anläggningar, objekt, system, egendom och andra tillgångar ska delas in i konsekvensnivå och inte säkerhetsskyddsklass.

3.4 Perspektiven konfidentialitet, riktighet och tillgänglighet

§ *2 kap. 4 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Verksamhetsutövaren ska bedöma från vilket eller vilka perspektiv (konfidentialitet, riktighet och tillgänglighet) som de identifierade skyddsvärdena är skyddsvärda. Bedömningen görs lämpligen i samband med identifieringen av skyddsvärden.

Säkerhetsskyddsklassificerade uppgifter (inklusive sådana uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd) är alltid skyddsvärda utifrån perspektivet konfidentialitet, men kan även vara skyddsvärda utifrån perspektiven riktighet eller tillgänglighet.

+ *För ytterligare stöd i hur de olika perspektiven kan bedömas när det gäller uppgifter, se Vägledning i säkerhetsskydd – Informationssäkerhet.*

Konfidentialitet

Om det uppstår skada för Sveriges säkerhet till följd av att uppgifter obehörigen röjs är de skyddsvärda utifrån perspektivet konfidentialitet.

Säkerhetsskyddsklassificerade uppgifter ska delas in i säkerhetsskyddsklass utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet. Detta är en bedömning utifrån uppgifternas konfidentialitet.

Även när det gäller säkerhetsskyddsklassificerade uppgifter som omfattas av ett för Sverige förpliktande internationellt åtaganden om säkerhetsskydd avser åtagandet främst skydd utifrån konfidentialitet.

Riktighet

Om det uppstår skada för Sveriges säkerhet till följd av att uppgifter obehörigen ändras, är de skyddsvärden som behandlar eller förvarar uppgifterna skyddsvärda utifrån perspektivet riktighet.

Exempel: En verksamhetsutövare med ansvar för ledning av nationella insatser är beroende av ett informationssystem som med GPS automatiskt positionerar resurser. Ifall uppgifter om var resurser befinner sig obemärkt manipuleras av en antagonist kommer insatserna inte kunna ledas, med skada för Sveriges säkerhet som följd.

Tillgänglighet

Om det uppstår skada för Sveriges säkerhet till följd av att skyddsvärden obehörigen görs otillgängliga eller förstörs är de skyddsvärda utifrån perspektivet tillgänglighet.

I bedömningen ska det beaktas vilken skada som kan uppstå för Sveriges säkerhet om förväntad tillgänglighet inte uppfylls på grund av en antagonistisk handling. Frågan efter hur lång tid bristande tillgänglighet riskerar medföra skada för Sveriges säkerhet är därvid central.

Exempel: En säkerhetskänslig verksamhet har ett skyddsvärde i form av en driftcentral som är i drift dygnet runt. Vid ett strömavbrott bedöms en skada för Sveriges säkerhet uppstå om bortfallet varar längre än två timmar. I detta fall är skyddsvärdet skyddsvärt utifrån perspektivet tillgänglighet.

3.5 Konsekvensnivåer

§ *2 kap. 5 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Anläggningar, objekt, system, egendom och andra tillgångar som är av betydelse för Sveriges säkerhet ska delas in i konsekvensnivå utifrån en bedömning av den skada för Sveriges säkerhet en antagonistisk handling mot skyddsvärdet kan medföra. Vid bedömningen behöver beaktas från vilket eller vilka perspektiv – konfidentialitet, riktighet eller tillgänglighet – respektive skyddsvärde är skyddsvärt. Indelningen sker enligt följande:

- synnerlig allvarlig skada för Sveriges säkerhet (nivå A)
- allvarlig skada för Sveriges säkerhet (nivå B)
- inte obetydlig skada för Sveriges säkerhet (nivå C)
- endast ringa skada för Sveriges säkerhet (nivå D).

Notera:
Såväl digitala som fysiska samlingar av uppgifter (exempelvis en pärm med rutiner för återställning av informationssystem som har betydelse för Sveriges säkerhet) kan vara skyddsvärda utifrån perspektiven riktighet eller tillgänglighet. Även uppgiftstillgångar kan således utgöra exempel på andra tillgångar som ska delas in i konsekvensnivå.

Konsekvensnivåerna

Nivå A	**Synnerligen allvarlig skada för Sveriges säkerhet**	Kritiska tjänster, leveranser, funktioner eller förmågor slås ut eller påverkas mycket allvarligt som i sin tur kan medföra att Sverige skulle komma att förlora sin suveränitet, handlingsfrihet eller oberoende, eller synnerligen allvarlig skada för Sveriges säkerhet till följd av skada på andra säkerhetskänsliga verksamheter, och mycket svårt att återgå till normalläge.
Nivå B	**Allvarlig skada för Sveriges säkerhet**	Kritiska tjänster, leveranser, funktioner eller förmågor påverkas allvarligt som i sin tur kan medföra allvarliga begränsningar i Sveriges suveränitet, handlingsfrihet eller oberoende, eller allvarlig skada för Sveriges säkerhet till följd av skada på andra säkerhetskänsliga verksamheter, och svårt att återgå till ett normalläge.
Nivå C	**Inte obetydlig skada för Sveriges säkerhet**	Kritiska tjänster, leveranser, funktioner eller förmågor påverkas påtagligt som i sin tur kan medföra att Sveriges suveränitet, handlingsfrihet eller oberoende skulle komma att påverkas men i begränsad omfattning, eller inte obetydlig skada för Sveriges säkerhet till följd av skada på andra säkerhetskänsliga verksamheter, och möjligt att återgå till normalläge inom rimlig tid.
Nivå D	**Endast ringa skada för Sveriges säkerhet**	Kritiska tjänster, leveranser, funktioner eller förmågor påverkas ringa som i sin tur kan medföra påverkan på Sveriges suveränitet, handlingsfrihet eller oberoende men i i liten omfattning, eller ringa skada för Sveriges säkerhet till följd av skada på andra säkerhetskänsliga verksamheter, och möjligt att relativt snabbt återgå till ett normalläge.

Identifiera och bedöma skyddsvärden

Skyddsvärde
– Säkerhetsskyddsklassificerade uppgifter

- ☐ Samtliga identifierade typer av säkerhetsskyddsklassificerade uppgifter har redovisats och den högsta säkerhetsskyddsklassen för respektive typ av uppgifter framgår.
- ☐ Säkerhetsskyddsklassificerade uppgifter som tidigare inte har säkerhetsskyddsklassificerats har delats in i säkerhetsskyddsklasser.

Skyddsvärde
– Verksamhet som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd

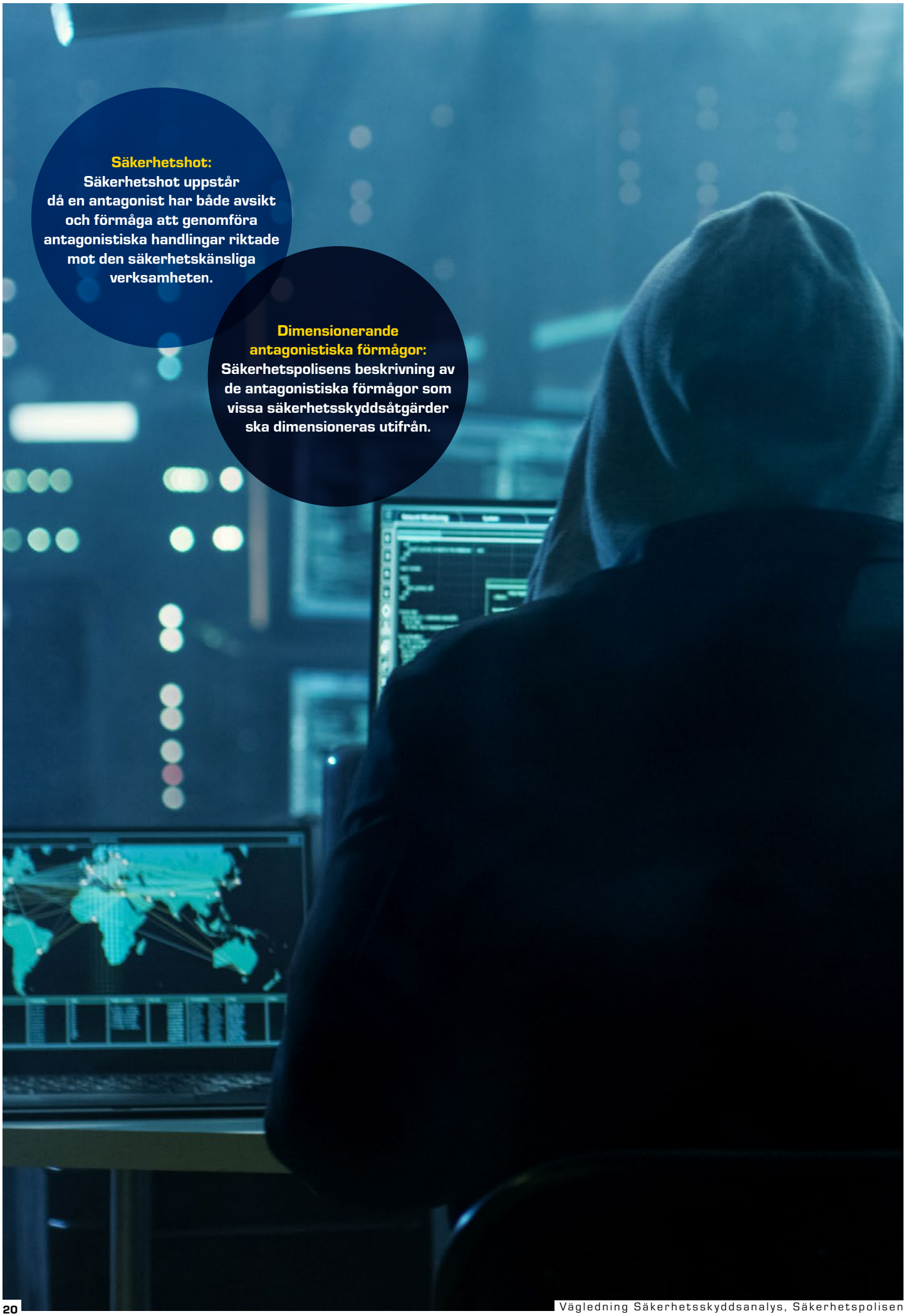
- ☐ Uppgifter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd har identifierats.
- ☐ Verksamhet som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd på annan grund än att det behandlas säkerhetsskyddsklassificerade uppgifter har identifierats.
- ☐ Uppgifter som omfattas av ett internationellt säkerhetsskyddsåtagande och som inte har klassificerats av annan stat har delats in i säkerhetsskyddsklasser.
- ☐ För varje verksamhet eller uppgift som omfattas av ett internationellt säkerhetsskyddsåtagande framgår det vilket internationellt säkerhetsskyddsåtagande som är tillämpligt.

Skyddsvärde
– Anläggningar, objekt, system, egendom och andra tillgångar

- ☐ Anläggningar, objekt, system, egendom och andra tillgångar som är av betydelse för Sveriges säkerhet har identifierats.
- ☐ Varje identifierad anläggning, objekt, system, egendom och annan tillgång av betydelse för Sveriges säkerhet har delats in i konsekvensnivå.
- ☐ Varje identifierad anläggning, objekt, system, egendom och annan tillgång av betydelse för Sveriges säkerhet som är skyddsvärd utifrån perspektivet tillgänglighet har kompletterats med tidsaspekt som tydliggör när skada för Sveriges säkerhet kan uppstå.

Skyddsvärde
– Samtliga

- ☐ Varje skyddsvärde har tilldelats ett namn, identifikationsuppgift eller på annat sätt gjorts lätt att följa genom säkerhetsskyddsanalysen.
- ☐ Varje skyddsvärde har beskrivits så pass detaljerat att vad som är skyddsvärt tydligt framgår.
- ☐ Konsekvensen av att respektive skyddsvärde röjs, inte är tillgängligt eller otillbörligen ändras eller förstörs har bedömts och beskrivits.
- ☐ Varje identifierat skyddsvärde har delats in i ett eller flera perspektiv:
  - ☐ konfidentialitet
  - ☐ riktighet
  - ☐ tillgänglighet.
- ☐ Eventuella interna eller externa beroenden har tydliggjorts för respektive skyddsvärde.


Säkerhetshot:
Säkerhetshot uppstår då en antagonist har både avsikt och förmåga att genomföra antagonistiska handlingar riktade mot den säkerhetskänsliga verksamheten.
Dimensionerande antagonistiska förmågor:
Säkerhetspolisens beskrivning av de antagonistiska förmågor som vissa säkerhetsskyddsåtgärder ska dimensioneras utifrån.

4 Säkerhetshot och dimensionerande antagonistiska förmågor

§ *2 kap. 1 § säkerhetsskyddsförordningen (2021:955)*

§ *2 kap. 6–7 §§ Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Det går inte att avgöra om vidtagna eller planerade säkerhetsskyddsåtgärder tillfredsställer behovet av säkerhetsskydd utan att först ta ställning till vad säkerhetsskyddet ska klara av att skydda mot. För att besvara denna fråga behöver verksamhetsutövaren identifiera säkerhetshot kopplade till de identifierade skyddsvärdena och den säkerhetskänsliga verksamheten i stort.

För att stödja verksamhetsutövare i arbetet med att identifiera sårbarheter och bedöma vilka säkerhetsskyddsåtgärder som är nödvändiga ska Säkerhetspolisen, om Säkerhetspolisen inte bedömer att det i det enskilda fallet är olämpligt, tillhandahålla en beskrivning av dimensionerande antagonistiska förmågor till verksamhetsutövare som bedriver säkerhetskänslig verksamhet. En verksamhetsutövare är skyldig att göra sin säkerhetsskyddsanalys även om någon beskrivning av dimensionerande antagonistiska förmågor inte tillhandahållits av Säkerhetspolisen.

Verksamhetsutövaren behöver förhålla sig till både egna identifierade säkerhetshot och tillhandahållen beskrivning av dimensionerande antagonistiska förmågor i säkerhetsskyddsanalysen. Oavsett vilka säkerhetshot som verksamhetsutövaren identifierar behöver verksamhetsutövaren minst utgå från den beskrivning av dimensionerande antagonistiska förmågor som tillhandahållits av Säkerhetspolisen.

I det fall identifierade säkerhetshot överstiger vad som följer av tillhandahållen beskrivning av dimensionerande antagonistiska förmågor ska verksamhetsutövaren utgå från de egna identifierade säkerhetshoten vid bedömningen av vilka säkerhetsskyddsåtgärder som är nödvändiga.

4.1 Säkerhetshot

§ *2 kap. 6 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Säkerhetshot uppstår då en antagonist har både avsikt och förmåga att genomföra antagonistiska handlingar riktade mot den säkerhetskänsliga verksamheten. Verksamhetsutövaren ska identifiera säkerhetshot kopplade till de identifierade skyddsvärdena och för den säkerhetskänsliga verksamheten i stort. För att identifiera säkerhetshot kan verksamhetsutövaren exempelvis använda sig av:

- egna incidenter
- information från öppna källor
- omvärldsbevakning eller från samverkan med liknande verksamheter.

Exempel på säkerhetshot är cyberangrepp, spionage, stöld och sabotage. Säkerhetshot som inte är av relevans för de identifierade skyddsvärdena eller den säkerhetskänsliga verksamheten i stort ska inte redovisas i säkerhetsskyddsanalysen.

4.2 Beskrivning av dimensionerande antagonistiska förmågor

§ *2 kap. 7 och 9 §§ Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Med beskrivning av dimensionerande antagonistiska förmågor avses en beskrivning från Säkerhetspolisen av de antagonistiska förmågor som vissa säkerhetsskyddsåtgärder ska dimensioneras utifrån, oavsett om verksamhetsutövaren själv identifierat motsvarande säkerhetshot mot den säkerhetskänsliga verksamheten eller inte.

I framtagandet av beskrivningen av dimensionerande antagonistiska förmågor har Säkerhetspolisen beaktat förmågor kopplade till spionerі, sabotage, terroristbrott och andra brott som kan hota säkerhetskänsliga verksamheter.

Underlaget tar höjd för så kallade gråzonshandlingar som en statlig aktör kan företa men samtidigt förneka inblandning i, exempelvis genom att maskera handlingen som annan brottslig verksamhet. En gråzonshandling är en handling som sker i en gråzon mellan fred och väpnad konflikt och syftar till att vinna en politisk målsättning samtidigt som en väpnad konflikt undviks.

Verksamhetsutövaren ska, utifrån erhållen beskrivning av dimensionerande antagonistiska förmågor, dimensionera säkerhetsskyddsåtgärderna för att upptäcka, försvåra och hantera obehörigt tillträde eller skadlig inverkan. Verksamhetsutövaren ska dessutom, utifrån erhållen beskrivning av dimensionerande antagonistiska förmågor, dimensionera och godkänna förvaringsutrymmen samt dimensionera säkerhetsskyddsåtgärderna för skydd mot röjande signaler, skydd mot obehörig avlyssning och skydd mot obehörig insyn.

De antagonistiska förmågor som framgår i en beskrivning av dimensionerande antagonistiska förmågor har sin utgångspunkt i Säkerhetspolisens referensunderlag om vilka förmågor potentiella antagonister bedöms inneha. Referensunderlaget bygger på Säkerhetspolisens omvärldsbevakning, underrättelser, forskningsprojekt, analyser samt information inhämtad från öppna källor om misstänkta, planerade och genomförda antagonistiska handlingar.

Säkerhetspolisen tillhandahåller en beskrivning av dimensionerande antagonistiska förmågor efter att tillsynsmyndigheten uppmärksammat Säkerhetspolisen på vilka verksamhetsutövare inom tillsynsmyndighetens tillsynsområde som har behov av en sådan.

\+ *För mer information om detta ska verksamhetsutövare kontakta sin tillsynsmyndighet.*

Säkerhetshot och dimensionerande antagonistiska förmågor

- ☐ Utifrån den inhämtade informationen har säkerhetshoten som är relevanta för den egna verksamheten identifierats, beskrivits och kopplats till de identifierade skyddsvärdena eller den säkerhetskänsliga verksamheten i stort.
- ☐ De antagonistiska förmågorna som framgår av erhållen beskrivning av dimensionerande antagonistiska förmågor har redogjorts och kopplats till de identifierade skyddsvärdena och den säkerhetskänsliga verksamheten i stort.

Information om säkerhetshot har hämtats från flera olika källor. Exempelvis:

- ☐ Den egna verksamhetens incidenter
- ☐ Årsböcker från Säkerhetspolisen, Militära underrättelse- och säkerhetstjänsten och Försvarets radioanstalt
- ☐ Ämnesspecifika rapporter från Totalförsvarets forskningsinstitut och Myndigheten för samhällsskydd och beredskap
- ☐ Samverkan med andra verksamheter i samma bransch, respektive tillsynsmyndighet inom säkerhetsskyddet och polismyndigheten.

Sårbarhet inom informationssäkerhet

Ett exempel är om programvara i ett informationssystem som har betydelse för Sveriges säkerhet inte hålls uppdaterade vilket innebär att det finns säkerhetsbrister i nformationssystemet.

Sårbarhet inom fysisk säkerhet

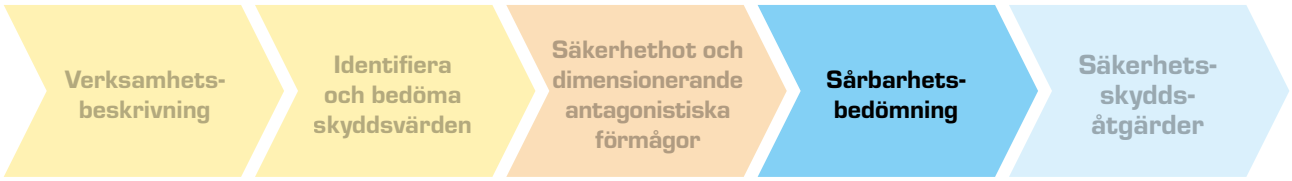
Ett exempel är om det enligt beskrivningen av dimensionerande antagonistiska förmågor finns en antagonistisk förmåga att detonera sprängämne på 125 kg TNT-ekvivalent* intill en anläggning där säkerhetskänslig verksamhet bedrivs. Anläggningens befintliga fysiska säkerhetsskyddsåtgärder motstår enbart en explosion på 100 kg TNT-ekvivalent. Resultatet är att vid en antagonistisk handling mot anläggningen riskerar de befintliga säkerhetsskyddsåtgärderna att inte kunna upprätthålla den fysiska säkerheten, vilket medför en påverkan på den säkerhetskänsliga verksamheten som i sin tur kan medföra skada för Sveriges säkerhet.

**mått för att kvantifiera energimängden som frigörs vid explosioner.*

Sårbarhet inom personalsäkerhet

Ett exempel är om anställda i den säkerhetskänsliga verksamheten inte fått utbildning i säkerhetsskydd eller om grundutredningen inte omfattar betyg eller referenser.

5 Sårbarhetsbedömning



§ *2 kap. 8 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

I denna del ska verksamhetsutövaren utifrån identifierade säkerhetshot och beskrivningen av dimensionerande antagonistiska förmågor, om Säkerhetspolisen tillhandahållit en sådan, identifiera sårbarheter för respektive skyddsvärde och den säkerhetskänsliga verksamheten i stort.

Sårbarhet är ett begrepp som har olika innebörd beroende på inom vilket ämnesområde eller kontext som begreppet används. I arbetet med säkerhetsskyddsanalys kan en sårbarhet avse avsaknad av fullgoda säkerhetsskyddsåtgärder i förhållande till författningskrav, dimensionerande antagonistiska förmågor eller andra identifierade säkerhetshot. Avsaknad av fullgoda säkerhetsskyddsåtgärder innebär att åtgärderna inte har vidtagits eller inte bedöms vara tillräckligt verkansfulla. För att identifiera sårbarheter behöver verksamhetsutövaren därmed beskriva och utvärdera sitt befintliga säkerhetsskydd samt analysera om skyddet är fullgott i förhållande till författningskrav, dimensionerande antagonistiska förmågor och andra identifierade säkerhetshot.

För att kunna identifiera sårbarheter är det nödvändigt att ha god kunskap om skyddsvärdena i verksamheten och dess egenskaper. En sårbarhet i den säkerhetskänsliga verksamheten i stort är en sårbarhet som är av relevans för samtliga eller flera av skyddsvärdena i verksamheten. Det kan exempelvis vara att anställda i den säkerhetskänsliga verksamheten inte fått utbildning i säkerhetsskydd vilket är av relevans för samtliga skyddsvärden i verksamheten och som därmed inte nödvändigtvis behöver hänföras till respektive skyddsvärde.

+ *För exempel på sårbarheter se s. 24.*

Identifieringen kan resultera i att ett stort antal sårbarheter identifieras i verksamheten. I arbetet med säkerhetsskyddsanalysen ska enbart de sårbarheterna som är av relevans för de identifierade skyddsvärdena eller den säkerhetskänsliga verksamheten i stort redovisas.

För att identifiera sårbarheter kan verksamhetsutövaren exempelvis tänka sig in i rollen som antagonist. Vilka sårbarheter skulle kunna nyttjas för att komma åt verksamhetens skyddsvärden med de till buds stående medel som finns i erhållen beskrivning av dimensionerande antagonistiska förmågor eller som förekommer i den egna bedömningen av föreliggande säkerhetshot?

I sårbarhetsbedömningen kan även penetrationstester av informationssystem och analys av inträffade incidenter ingå. Testerna samt andra underlag kan sedan sammanställas och bedömas i syfte att föreslå lämpliga säkerhetsskyddsåtgärder.

Vilka personer som ska delta i sårbarhetsbedömningen bör anpassas utifrån vilken typ av befintliga säkerhetsskyddsåtgärder som undersöks. Exempelvis kan personer med kompetens inom internrevision delta för att granska processer och rutiner där skyddsvärden finns, medan extern expertis kan behöva anlitas för praktiska tester av befintligt säkerhetsskydd. Att anlita extern expertis kan i vissa fall medföra ett behov av säkerhetsskyddsavtal.

+ *För mer information om säkerhetsskyddsavtal, se Vägledning i säkerhetsskydd – Skyldigheter vid exponering av säkerhetskänslig verksamhet.*

Sårbarhetsbedömning

- ☐ Med utgångspunkt i författningskrav, dimensionerande antagonistiska förmågor och andra identifierade säkerhetshot samt skyddsvärdenas egenskaper har sårbarheter i det befintliga säkerhetsskyddet identifierats och beskrivits.
- ☐ Sårbarheterna har kopplats till de identifierade skyddsvärdena eller den säkerhetskänsliga verksamheten i stort.
- ☐ Sårbarheter för respektive skyddsvärde och den säkerhetskänsliga verksamheten i stort har identifierats exempelvis genom att:
  - ☐ praktiskt testa befintligt säkerhetsskydd
  - ☐ granska befintlig säkerhetsskyddsanalys
  - ☐ granska tidigare revisioner
  - ☐ granska befintlig risk- och sårbarhetsanalys
  - ☐ granska verksamhetens egna incidenter
  - ☐ granska andra sårbarhetsbedömningar/tester
  - ☐ granska om processer och rutiner gällande säkerhetsskydd efterlevs och om där finns brister som kan medföra sårbarheter
  - ☐ verksamhetsutövaren föreställer sig vara en antagonist och nyttjar de till buds stående medel som finns i erhållen beskrivning av dimensionerande antagonistiska förmågor eller som de aktörer som förekommer i säkerhetshoten kan förväntas besitta för att komma åt verksamhetens skyddsvärden.


Bedömningen av vilka
säkerhetsskyddsåtgärder
som är nödvändiga
att vidta ska utgå från:
skyddsvärden,
säkerhetshot,
sårbarheter samt
dimensionerande
antagonistiska förmågor

6 Säkerhetsskyddsåtgärder

§ *2 kap. 2–4 §§ säkerhetsskyddslagen (2018:585)*

§ *2 kap. 1 § säkerhetsskyddsförordningen (2021:955)*

§ *2 kap. 9 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

I denna del ska verksamhetsutövaren bedöma vilka säkerhetsskyddsåtgärder som är nödvändiga att vidta, utifrån vad som framkommit vid identifiering och bedömning av skyddsvärden, säkerhetshot och sårbarheter. Verksamhetsutövare som erhållit en beskrivning av dimensionerande antagonistiska förmågor ska även dimensionera vissa av säkerhetsskyddsåtgärderna utifrån denna.

Om verksamhetsutövaren inte har vidtagit en säkerhetsskyddsåtgärd som enligt författningskrav ska finnas, ska åtgärden beskrivas i säkerhetsskyddsanalysen så att den kommer med i säkerhetsskyddsplanen.

För att säkerhetsskyddsåtgärderna ska ge avsedd effekt och resultera i ett heltäckande säkerhetsskydd är det viktigt att beakta att säkerhetsskyddsåtgärderna som vidtas samverkar och bildar en helhet. I exemplet nedan illustreras vikten av detta.

Exempel:
En verksamhetsutövare har vidtagit nödvändiga säkerhetsskyddsåtgärder för den fysiska säkerheten. En antagonist kan inte tillskansa sig åtkomst till den säkerhetskänsliga verksamheten genom att ta sig förbi de fysiska säkerhetsskyddsåtgärderna.

Däremot har verksamhetsutövaren inte vidtagit tillräckliga åtgärder för att säkerställa att personalen är lojal och pålitlig från säkerhetssynpunkt. Istället för att försöka ta sig förbi det fysiska säkerhetsskyddet kan antagonisten genom värvning av verksamhetsutövarens personal tillskansa sig åtkomst till den säkerhetskänsliga verksamheten och därmed orsaka skada för Sveriges säkerhet.

Bedömningen av vilka säkerhetsskyddsåtgärder som är nödvändiga att vidta ska utgå från och vara spårbara till de skyddsvärden, säkerhetshot och sårbarheter som identifierats samt de antagonistiska förmågor som framgår i erhållen beskrivning av dimensionerande antagonistiska förmågor.

+ *Säkerhetspolisens vägledningar i informationssäkerhet, personalsäkerhet och fysisk säkerhet ger ett stöd i bedömningen av säkerhetsskyddsåtgärder.*

+ *Säkerhetsskyddsåtgärderna sammanställs i en säkerhetsskyddsplan där det även ska framgå när åtgärderna ska vidtas och vilken funktion som ansvarar för dem, se avsnitt 7 Säkerhetsskyddsplan.*

Säkerhetsskyddsåtgärder

Säkerhetsskyddsåtgärderna inom informationssäkerhet:

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

Säkerhetsskyddsåtgärderna inom fysisk säkerhet:

- ☐ förebygger att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där de kan få tillgång till anläggningar, objekt, system, egendom eller andra tillgångar som är av betydelse för Sveriges säkerhet
- ☐ förebygger skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt som avses i punkten ovan.

Säkerhetsskyddsåtgärderna inom personalsäkerhet:

- ☐ förebygger att personer som inte är pålitliga från säkerhetssynpunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av någon annan anledning är säkerhetskänslig
- ☐ säkerställer att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd.

Säkerhetsskyddsåtgärder - Samtliga

- ☐ Relationerna mellan skyddsvärden, säkerhetshot, förmågor i erhållen beskrivning av dimensionerande antagonistiska förmågor, sårbarheter och säkerhetsskyddsåtgärder är tydligt beskrivna och lätta att tillgodogöra sig, till exempel genom att dessa framgår av en tabell.
- ☐ Som stöd i framtagandet av vilka specifika säkerhetsskyddsåtgärder som är nödvändiga att vidta har Säkerhetspolisens vägledningar i informationssäkerhet, fysisk säkerhet och personalsäkerhet använts.
- ☐ Omständigheter som kan påverka om, när och hur en säkerhetsskyddsåtgärd genomförs, till exempel ombyggnation eller flytt av verksamheten har beaktats.

Vill du läsa mer om säkerhetsskyddsåtgärderna inom informationssäkerhet, fysisk säkerhet och personalsäkerhet?

På Säkerhetspolisens webbplats hittar du Vägledningar för Informationssäkerhet, Fysisk säkerhet och Personalsäkerhet.


Säkerhetsskyddsanalysen ska fastställas av verksamhets-utövarens högsta chef eller motsvarande organ.

7 Fastställande av säkerhetsskyddsanalysen

§ *2 kap. 1 § säkerhetsskyddslagen (2018:585)*
§ *2 kap. 1 § säkerhetsskyddsförordningen (2021:955)*
§ *2 kap. 10 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Säkerhetsskyddsanalysen ska fastställas av verksamhetsutövarens högsta chef eller motsvarande organ. Det kan vara generaldirektör vid en myndighet, verkställande direktör för en enskild verksamhetsutövare eller kommunchef för en kommun.

Säkerhetsskyddsanalysen ska uppdateras vid behov och åtminstone vartannat år. Exempel på behov som föranleder att säkerhetsskyddsanalysen ska uppdateras är om verksamhetsutövaren identifierar nya skyddsvärden i verksamheten eller erhåller en beskrivning av dimensionerande antagonistiska förmågor.

Den fastställda säkerhetsskyddsanalysen ska ligga till grund för en säkerhetsskyddsplan.

Det kan finnas behov av att förmedla hela eller delar av säkerhetsskyddsanalysen till den egna verksamheten, men även externt. Exempelvis behöver viss personal veta vad som är skyddsvärt för att kunna hantera skyddsvärdena på ett korrekt sätt. Det kan även vara till fördel att viss personal känner till de identifierade säkerhetshoten och dimensionerande antagonistiska förmågorna som finns mot den aktuella verksamheten för att öka förståelsen för vissa säkerhetsskyddsåtgärder. Samtidigt är det viktigt att tänka på att säkerhetsskyddsanalysen kan vara helt eller delvis säkerhetsskyddsklassificerad. Endast personal som är behörig får ta del av de delar som innehåller säkerhetsskyddsklassificerade uppgifter.

För att skapa förståelse och medvetenhet inom verksamheten kan ett alternativ vara att skapa en generell sammanfattning av säkerhetsskyddsanalysen. Denna görs då mer övergripande och utan detaljer så att den kan delas in i en lägre säkerhetsskyddsklass eller utformas så att den inte innehåller några säkerhetsskyddsklassificerade uppgifter.

Fastställande av säkerhetsskyddsanalysen

- ☐ Säkerhetsskyddsklassificerade uppgifter som uppkommit i samband med arbetet med säkerhetsskyddsanalysen har delats in i säkerhetsskyddsklasser.
- ☐ Uppdateringsfrekvensen har fastställts till minst en gång vartannat år.
- ☐ Verksamhetsutövarens högsta chef eller motsvarande har fastställt säkerhetsskyddsanalysen.
- ☐ Fastställandet av säkerhetsskyddsanalysen har föranlett att en säkerhetsskyddsplan ska upprättats.


Säkerhetsskyddsplanen ska vara ett dokument som verksamhetsutövaren arbetar med kontinuerligt och ska uppdateras vid behov.

8 Säkerhetsskyddsplan

§ *2 kap. 12 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

De säkerhetskyddsåtgärder som beskrivs i säkerhetsskyddsanalysen ska sammanställas i en säkerhetsskyddsplan. Planen ska redogöra för hur behovet av säkerhetsskyddsåtgärder som har identifierats i säkerhetsskyddsanalysen omhändertas. Av planen ska det också framgå när åtgärderna ska vidtas och vilken funktion som ansvarar för respektive åtgärd. Säkerhetsskyddsplanen ska fastställas av säkerhetsskyddschefen.

Säkerhetsskyddsplanen ska vara ett dokument som verksamhetsutövaren arbetar med kontinuerligt och ska uppdateras vid behov. Om det i säkerhetskyddsanalysen identifieras ytterligare behov av säkerhetsskyddsåtgärder behöver planen uppdateras i enlighet med det. I arbetet med säkerhetsskyddsplanen är det lämpligt att ha upprättade rutiner för att följa upp att de nödvändiga säkerhetsskyddsåtgärderna vidtas och fyller avsedd funktion.

I vissa fall kan det finnas behov av att prioritera bland de säkerhetsskyddsåtgärder som behöver vidtas. För att det ska finnas en spårbarhet behöver verksamhetsutövaren motivera sådana prioriteringar med bakomliggande resonemang.

Då säkerhetsskyddsåtgärder kan vara kostsamma och omfatta flera delar av en organisation, kan säkerhetsskyddsplanen behöva förankras hos verksamhetsutövarens högsta chef eller motsvarande innan den slutligen fastställs av säkerhetsskyddschefen.

Det kan finnas ett behov av att förmedla hela eller delar av säkerhetsskyddsplanen i verksamheten för att kunna vidta de säkerhetsskyddsåtgärder som är nödvändiga. Likt säkerhetsskyddsanalysen är det viktigt att tänka på att säkerhetsskyddsplanen kan vara helt eller delvis säkerhetsskyddsklassificerad. Endast personal som är behörig får ta del av de delar av planen som innehåller säkerhetsskyddsklassificerade uppgifter.

Säkerhetsskyddsplan

- ☐ De säkerhetsskyddsåtgärder som beskrivs i säkerhetsskyddsanalysen har sammanställts i en säkerhetsskyddsplan. I planen:
  - ☐ framgår relationen mellan skyddsvärden, säkerhetshot, förmågor i erhållen beskrivning av dimensionerande antagonistiska förmågor, sårbarheter och säkerhetsskyddsåtgärder
  - ☐ har ansvarig funktion utsetts för respektive säkerhetsskyddsåtgärd
  - ☐ framgår när respektive säkerhetsskyddsåtgärd ska påbörjas och vara genomförd.
- ☐ Innan säkerhetsskyddsplanen har fastställts har den förankrats hos verksamhetsutövarens högsta chef eller motsvarande.
- ☐ Säkerhetsskyddschefen eller den han eller hon bestämmer har fastställt säkerhetsskyddsplanen.

Anteckningar:

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 utländska delegationer
8. Avlyssningsskyddade utrymmen

Säkerhetspolisen

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