Stödmaterial om säkerhetsskydd

Säkerhetsskyddsanalys – ett fiktivt exempel

Säkerhetspolisen

Säkerhetspolisen

PM

Datum: 2025-01-14

Säkerhetsskyddsanalys - Ett fiktivt exempel

Säkerhetspolisen har sett ett behov av en tydligare vägledning kring hur en säkerhetsskyddsanalys kan genomföras. För att vägleda verksamhetsutövare ytterligare har ett fiktivt exempel tagits fram.

Exemplet riktar sig till verksamhetsutövare som ska tillämpa Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1) och som ska upprätta eller uppdatera en säkerhetsskyddsanalys. Syftet är att visa ett exempel på hur dokumentation av en säkerhetsskyddsanalys kan göras i enlighet med Säkerhetspolisens metod för säkerhetsskyddsanalys. Exemplet är fiktivt och förenklat i syfte att tydliggöra hur analysens delar kan knytas samman och vilka typer av resonemang som skulle kunna föras i de olika delarna.

För att kunna tillgodogöra sig innehållet i detta exempel rekommenderas att läsaren har tagit del av Säkerhetspolisens *Vägledning i säkerhetsskyddsanalys.* Läsaren rekommenderas även ha tagit del av Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1), Säkerhetspolisens vägledning *Introduktion till säkerhetsskydd* och promemorian *Vad är säkerhetskänslig verksamhet?* som återfinns på Säkerhetspolisens webbplats.

Säkerhetspolisen

PM

Datum: 2025-01-14

Innehållsförteckning

Säkerhetsskyddsanalys - Ett fiktivt exempel 1

1. Verksamhetsbeskrivning 1

2. Identifiera och bedöma skyddsvärden 2

2.1. Säkerhetsskyddsklassificerade uppgifter 2

2.2. Anläggningar, objekt, system, egendom och andra tillgångar som är av betydelse för Sveriges säkerhet 3

2.3. Internationella åtagande om säkerhetsskydd 3

3. Säkerhetshot och dimensionerande antagonistiska förmågor 4

3.1. Säkerhetshot 4

3.2. Dimensionerande antagonistiska förmågor 4

4. Sårbarhetsbedömning 6

Sammanfattning av sårbarhetsbedömningen 6

4.1. Sårbarhet 1 (SB 1) – Bristfällig utbildning inom säkerhetsskydd 6

4.2. Sårbarhet 2 (SB 2) – Avsaknad av uppdaterad programvara 6

4.3. Sårbarhet 3 (SB 3) – Avsaknad av skriftliga tillstånd för besökare 7

4.4. Sårbarhet 4 (SB 4) – Avsaknad av tillräcklig fysisk säkerhet för att motstå sprängladdningar 7

4.5. Sårbarhet 5 (SB 5) – Avsaknad av tillräcklig fysisk säkerhet för att motstå forcering med fordon 7

5. Säkerhetsskyddsåtgärder 8

5.1. Säkerhetsskyddsåtgärd 1 (SÅ 1) – Utbilda personal inom säkerhetsskydd 8

5.2. Säkerhetsskyddsåtgärd 2 (SÅ 2) – Uppdatera och ta fram en uppdateringsplan för programvaran i informationssystem 8

5.3. Säkerhetsskyddsåtgärd 3 (SÅ 3) – Inför skriftliga tillstånd för besökare 8

5.4. Säkerhetsskyddsåtgärd 4–6 (SÅ 4-SÅ 6) – Förstärkt skydd mot sprängladdningar och forcering med fordon 8

6. Fastställande av säkerhetsskyddsanalysen 10

Bilaga A - Säkerhetsskyddsplan 11

1. Verksamhetsbeskrivning

Verksamhet X *(härefter myndigheten)* är en statlig myndighet med uppdrag att leverera digitala uppgifter som andra verksamhetsutövare inom det civila försvaret är i behov av för att genomföra samordnade övningar och insatser inom ramen för totalförsvaret. De digitala uppgifterna består framförallt av insatsplaner, sammanställd information om aktuella säkerhetshot och information om hur resurser ska samordnas mellan verksamhetsutövarna för att kunna genomföra övningarna och insatserna. Om uppgifterna inte levereras kommer flertalet av de viktigaste samhällsfunktionerna inte kunna upprätthållas i händelse av höjd beredskap. Detta kan medföra att skada för Sveriges säkerhet uppstår vid en antagonistisk handling mot myndigheten.

Myndigheten är lokaliserad i Stockholm och består av cirka 50 anställda. Organisationen består av uppgiftsförmedlingsavdelningen, säkerhetsavdelningen, IT-avdelningen, ekonomiavdelningen, rättsavdelningen och kommunikationsavdelningen. Säkerhetspolisen är myndighetens tillsynsmyndighet enligt 8 kap. 1 § säkerhetsskyddsförordningen (SSF).

Uppgiftsförmedlingsavdelningen bedriver myndighetens kärnverksamhet. Avdelningen ansvarar för att ta fram, analysera och förmedla de digitala uppgifterna. Detta innebär att avdelningen kontinuerligt upprättar och hanterar säkerhetsskyddsklassificerade uppgifter.

Säkerhetsavdelningen ansvarar för att bedriva myndighetens verksamhets- och säkerhetsskyddsarbete. Det innebär exempelvis att systematiskt vidta och upprätthålla de säkerhetsskyddsåtgärder som är nödvändiga inom informationssäkerhet, fysisk säkerhet och personalsäkerhet. I avdelningens ansvar ingår även hanteringen av myndighetens säkerhetsskyddsavtal. Avdelningen upprättar och hanterar säkerhetsskyddsklassificerade uppgifter.

Rättsavdelningen ansvarar bland annat för rättslig rådgivning för myndighetens säkerhetsskyddsarbete. Avdelningen upprättar och hanterar säkerhetsskyddsklassificerade uppgifter.

IT-avdelningen tillhandahåller ett informationssystem som är nödvändigt för att kunna leverera de digitala uppgifterna. Avdelningen hanterar också en fysisk uppgiftssamling i pappersform som möjliggör att informationssystemet kan återställas om systemet görs otillgängligt eller oriktigt.

Säkerhetskänslig verksamhet bedrivs således på uppgiftsförmedlingsavdelningen, säkerhetsavdelningen, rättsavdelningen och IT-avdelningen utifrån kategorin nationellt samhällsviktig verksamhet.

I detta fall görs bedömningen att ekonomiavdelningen och kommunikationsavdelningen inte tar del av några säkerhetsskyddsklassificerade uppgifter eller andra skyddsvärden och bedöms därmed inte bedriva säkerhetskänslig verksamhet.[1]

[1] I det systematiska arbetet med säkerhetsskyddsanalys behöver verksamhetsutövare ta höjd för att förutsättningarna kan ändras. Om ekonomiavdelningen eller kommunikationsavdelningen i framtiden hanterar säkerhetsskyddsklassificerade uppgifter eller andra skyddsvärden bedriver de säkerhetskänslig verksamhet. Observera alltså att delar av en verksamhet som hanterar mer administrativa uppgifter, t.ex. ekonomi, HR, kommunikation och fastighetsförvaltning, mycket väl kan anses bedriva säkerhetskänslig verksamhet beroende på om säkerhetsskyddsklassificerade uppgifter och andra skyddsvärden som hanteras där.

2. Identifiera och bedöma skyddsvärden

I detta avsnitt identifieras och bedöms skyddsvärden i den säkerhetskänsliga verksamheten.

2.1. Säkerhetsskyddsklassificerade uppgifter

Nedan redovisas vilka typer av säkerhetsskyddsklassificerade uppgifter som finns hos myndigheten, högsta säkerhetsskyddsklass inom respektive typ, utifrån vilket eller vilka perspektiv som uppgifterna är skyddsvärda, hur de hanteras och en kortfattad konsekvensbedömning.

2.1.1. Skyddsvärde 1 (SV 1) - Uppgifter som rör myndighetens insatsplanering

Säkerhetsskyddsklass: Högsta säkerhetsskyddsklass är *hemlig.*

Perspektiv: *Konfidentialitet.*

Hanteras: I *Informationssystem Y (SV 4)*, *fysiska handlingar i arkivet* och *fysiska handlingar i medarbetares säkerhetsskåp* hos IT-avdelningen, säkerhetsavdelningen, uppgiftsförmedlingsavdelningen och rättsavdelningen.

Kortfattad konsekvensbedömning: Om de säkerhetsskyddsklassificerade uppgifterna röjs, skulle det möjliggöra för en antagonist att sabotera tillgångar som möjliggör samordnade insatser i händelse av höjd beredskap. Exempelvis uppgifter om var kritiska tillgångar som ledningscentraler och nödvändig materiel är beläget.

2.1.2. Skyddsvärde 2 (SV 2) - Uppgifter som rör andra verksamheters skyddsvärden

Säkerhetsskyddsklass: Högsta säkerhetsskyddsklass är *konfidentiell.*

Perspektiv: *Konfidentialitet.*

Hanteras: I *Informationssystem Y (SV 4).*

Kortfattad konsekvensbedömning: Om de säkerhetsskyddsklassificerade uppgifterna om andra verksamheters skyddsvärden röjs, skulle det underlätta för en antagonist att orsaka skada för Sveriges säkerhet. Uppgifterna rör framförallt andra säkerhetskänsliga verksamheters skyddsvärden som härrör från de samordnade insatserna. Exempelvis skyddsvärda kartor och uppgifter om verksamhetsutövarnas beredskapsplanering.

2.1.3. Skyddsvärde 3 (SV 3) – Uppgifter som rör sårbarheter som identifierats hos myndigheten genom praktiska tester

Säkerhetsskyddsklass: Högsta säkerhetsskyddsklass är *hemlig.*

Perspektiv: *Konfidentialitet.*

Hanteras: I *Informationssystem Y (SV 4)*, *fysiska handlingar i arkivet* och *fysiska handlingar i medarbetares säkerhetsskåp* hos IT- avdelningen, säkerhetsavdelningen, uppgiftsförmedlingsavdelningen och rättsavdelningen.

Kortfattad konsekvensbedömning: Om de säkerhetsskyddsklassificerade uppgifterna om sårbarheter hos myndigheten röjs, skulle en antagonist kunna göra *informationssystem Y (SV 4)* otillgängligt eller oriktigt. Detta innebär att Sverige inte kan upprätthålla sin förmåga till välfungerande insatser vid höjd beredskap. Exempelvis uppgifter som rör sårbarheter hos informationssystemet som identifierats vid penetrationstester eller sårbarheter i det fysiska skalskyddet som identifierats vid praktiska tester.

2.2. Anläggningar, objekt, system, egendom och andra tillgångar som är av betydelse för Sveriges säkerhet

Nedan redovisas konsekvensnivån för skyddsvärdena, utifrån vilket eller vilka perspektiv de är skyddsvärda och en kortfattad konsekvensbedömning.

2.2.1. Skyddsvärde 4 (SV 4) – Informationssystem Y

Konsekvensnivå: *B.*

Säkerhetsskyddsklass: Högsta säkerhetsskyddsklass som hanteras i informationssystemet är *hemlig.*

Perspektiv: *Konfidentialitet, tillgänglighet och riktighet.*

Hanteras: Utpekade lokaler hos *IT-avdelningen.*

Kortfattad konsekvensbedömning: En antagonistisk handling som medför att informationssystemet görs otillgängligt eller oriktigt kan innebära att Sverige inte kan upprätthålla sin förmåga till välfungerande insatser vid höjd beredskap. I förlängningen innebär detta att Sveriges handlingsfrihet blir kraftigt begränsad. Skadan för Sveriges säkerhet kommer att uppstå om informationssystemet är otillgängligt eller oriktigt i cirka 7 dagar.

Se konsekvensbedömning under skyddsvärde 1–3 *(SV 1-SV 3)* för konsekvenserna vid ett röjande av uppgifterna som hanteras i informationssystemet.

Notera: *Informationssystem Y (SV 4*) behöver vara tillgängligt och riktigt för att leveransen ska vara möjlig att genomföra. I informationssystemet kommer dessutom *de säkerhetsskyddsklassificerade uppgifterna (SV 1-SV 3)* som finns hos myndigheten hanteras, vilket innebär att informationssystemet även är skyddsvärt utifrån dess konfidentialitet.

2.2.2. Skyddsvärde 5 (SV 5) – Uppgiftssamling som möjliggör att informationssystem Y kan återställas

Konsekvensnivå: *B*

Perspektiv: *Tillgänglighet och riktighet.*

Hanteras: *Fysiska handlingar i ett säkerhetsskåp som utpekade medarbetare har behörighet till.*

Kortfattad konsekvensbedömning: Om uppgiftssamlingen görs otillgänglig eller oriktig kommer det innebära att det kan uppstå skada för Sveriges säkerhet eftersom det inte finns någon möjlighet att återställa *informationssystem Y (SV 4)*. Skadan för Sveriges säkerhet kommer att uppstå om informationssystemet och uppgiftssamlingen är otillgänglig eller oriktig i cirka 7 dagar.

2.3. Internationella åtagande om säkerhetsskydd

Det finns ingen verksamhet i myndigheten som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd.

3. Säkerhetshot och dimensionerande antagonistiska förmågor

I detta avsnitt redovisas de säkerhetshot och dimensionerande antagonistiska förmågor som är av relevans för de identifierade skyddsvärdena.

Identifieringen av säkerhetshot har haft sin utgångspunkt i omvärldsbevakning, myndighetens egna incidenter och samverkan med andra verksamhetsutövare. Omvärldsbevakningen har bestått av att gå igenom aktuell information som tillhandahållits av Säkerhetspolisen och Försvarsmakten, användning av internettjänster med framtagna sökord och analyser av angreppstrender tillsammans med verksamheter som tar emot de digitala uppgifterna. Myndigheten har underrättats om flertalet kontaktförsök mot egen personal och cyberangrepp som misstänks ha utförts av främmande makt. Antalet kontaktförsök och cyberangrepp har ökat det senaste året. Även flera andra säkerhetskänsliga verksamheter, som har en tongivande roll i arbetet med planering och insatser inom totalförsvaret, har lyft fram att de har utsatts för incidenter som misstänks ha utförts av främmande makt. Det visar att främmande makt har gjort en förskjutning det senaste året och bedöms ha en avsikt att genomföra angrepp mot myndigheten. Eftersom myndigheten bedriver nationellt samhällsviktig verksamhet är grov organiserad brottslighet och enskilda hotaktörer också potentiella antagonister som myndigheten identifierat vid omvärldsbevakningen. Då främmande makt bedöms ha högst förmåga kommer dessa förmågor vara dimensionerande.

3.1. Säkerhetshot

Nedan redovisas de förmågor som är av relevans för de identifierade säkerhetshoten.

3.1.1. Säkerhetshot 1 – Infiltration, kartläggning och värvning

Säkerhetshotet består av att genom infiltration, kartläggning och värvning av verksamhetsutövarens personal få obehörig tillgång till den säkerhetskänsliga verksamheten. Detta kan innebära att de *säkerhetsskyddsklassificerade uppgifterna (SV 1-3*) kan röjas och att *informationssystem Y (SV 4)* och *uppgiftssamlingen (SV 5)* kan saboteras eller manipuleras.

3.1.2. Säkerhetshot 2 – Cyberangrepp

Säkerhetshotet består av att en antagonist genom:

- *Överbelastningsattack* gör *informationssystem Y (SV 4)* otillgängligt eller oriktigt.
- *Otillbörlig fjärråtkomst* gör *informationssystem Y (SV 4)* otillgängligt eller oriktigt. Alternativt att en antagonist får obehörig tillgång till de *säkerhetsskyddsklassificerad uppgifterna (SV 1–3*) som hanteras i informationssystemet.
- *Skadlig kod* gör *informationssystem Y (SV 4)* otillgängligt eller oriktigt. Alternativt att en antagonist får obehörig tillgång till de *säkerhetsskyddsklassificerad uppgifterna (SV 1-3*) som hanteras i informationssystemet.

3.2. Dimensionerande antagonistiska förmågor

Nedan redovisas de dimensionerande antagonistiska förmågor som är av relevans för skyddsvärdena i den säkerhetskänsliga verksamheten.[2]

3.2.1. Dimensionerande antagonistisk förmåga 1 (DAF 1) – Sprängladdningar

Den dimensionerande antagonistiska förmågan består av en sprängladdning på ca [x] kg TNT ekvivalent som kan användas för att sabotera *informationssystem Y (SV 4) och uppgiftssamlingen (SV 5)* så att skyddsvärdena blir otillgängliga.

[2] I en säkerhetsskyddsanalys behöver verksamhetsutövare ta höjd för de andra dimensionerande antagonistiska förmågor som tillhandahållits av Säkerhetspolisen. De dimensionerande antagonistiska förmågorna är framförallt av relevans för fysisk säkerhet. I det förenklade exemplet beaktas enbart två godtyckliga dimensionerande antagonistiska förmågor.

3.2.2. Dimensionerande antagonistisk förmåga 2 (DAF 2) – Forcering med fordon

Den dimensionerande förmågan består av en lastbil med en vikt om ca [y] kg som kan användas för att sabotera *informationssystem Y (SV 4)* och *uppgiftssamlingen (SV 5)* så att skyddsvärdena blir otillgängliga. Förmågan kan även nyttjas för att ta sig in i anläggningen och därmed få tillgång till de *säkerhetsskyddsklassificerade uppgifterna (SV 1-3)* som hanteras i informationssystemet.

4. Sårbarhetsbedömning

I detta avsnitt redovisas sårbarheter för respektive skyddsvärde och för den säkerhetskänsliga verksamheten i stort.

Sammanfattning av sårbarhetsbedömningen

Sårbarhet 1-3 är de sårbarheter som kvarstår hos myndigheten efter analysen av om det befintliga säkerhetsskyddet är tillräckligt i förhållande till författningskraven.

Sårbarhet 4-5 är de sårbarheter som kvarstår hos myndigheten efter analysen av om det befintliga säkerhetsskyddet är tillräckligt i förhållande till de dimensionerande antagonistiska förmågorna.

Myndigheten har inte identifierat några säkerhetshot som överstiger de dimensionerande antagonistiska förmågorna.

4.1. Sårbarhet 1 (SB 1) – Bristfällig utbildning inom säkerhetsskydd

I enlighet med 6 kap. 1 § PMFS 2022:1 ska en verksamhetsutövare säkerställa att den som ska delta i säkerhetskänslig verksamhet får relevant utbildning i säkerhetsskydd innan personen får åtkomst till den säkerhetskänsliga verksamheten. Sådan utbildning ska därefter ges regelbundet i den omfattning som behövs.

För att utvärdera om utbildningen inom säkerhetsskydd är tillräcklig har intervjuer genomförts med dem som är ansvariga för utbildningsverksamheten. Vidare har test av anställdas kunskapsnivå och en översyn av utbildningsrutiner genomförts. Översynen påvisar att den som ska delta i den säkerhetskänsliga verksamheten får utbildning i säkerhetsskydd innan personen påbörjar deltagandet i verksamheten, men därefter ges ingen regelbunden utbildning i säkerhetsskydd i den omfattning som krävs. Testet av anställda visar också att kunskapsnivån i säkerhetsskydd inte är tillräcklig. Detta innebär en sårbarhet då säkerhetsskyddet inte är fullgott i förhållande till författningskravet.

Sårbarheten är av relevans för *samtliga skyddsvärden (härefter den säkerhetskänsliga verksamheten i stort).* Säkerhetshotet *Infiltration, kartläggning och värvning (SH 1)* är av relevans för sårbarheten.

4.2. Sårbarhet 2 (SB 2) – Avsaknad av uppdaterad programvara

I enlighet med 4 kap. 19 § PMFS 2022:1 ska en verksamhetsutövare se till att programvara i informationssystem som har betydelse för säkerhetskänslig verksamhet hålls uppdaterad så att säkerhetsbrister och sårbarheter motverkas. Om det finns särskilda skäl får verksamhetsutövaren besluta om undantag från kravet.

För att utvärdera om säkerhetsskyddsåtgärden har vidtagits har säkerhetsskyddschefen fört en dialog med medarbetarna som är ansvariga för *informationssystem Y (SV 4).* Av dialogen framgår att inga åtgärder har vidtagits för att uppdatera programvaran. Det har även konstaterats att det inte heller finns några särskilda skäl att inte göra det, vilket innebär att det är en sårbarhet i den säkerhetskänsliga verksamheten då säkerhetsskyddet inte är fullgott i förhållande till författningskravet.

Sårbarheten är av relevans för *informationssystem Y (SV4)* och de *säkerhetsskyddsklassificerade uppgifterna (SV 1-3)* som hanteras i informationssystemet. Säkerhetshotet *cyberangrepp (SH2)* är av relevans för sårbarheten.

4.3. Sårbarhet 3 (SB 3) – Avsaknad av skriftliga tillstånd för besökare

I enlighet med 5 kap. 3 § PMFS 2022:1 ska en verksamhetsutövare utfärda skriftliga tillstånd för besökare till eller inom områden där säkerhetskänslig verksamhet bedrivs. För att utvärdera om säkerhetsskyddsåtgärderna har vidtagits har det förts samtal med fastighetsansvariga och medarbetarna som är ansvariga för *informationssystem Y (SV 4*) och det har visat sig att inga tillstånd utfärdas, vilket innebär att det är en sårbarhet i den säkerhetskänsliga verksamheten då säkerhetsskyddet inte är fullgott i förhållande till författningskravet.

Sårbarheten är av relevans för *den säkerhetskänsliga verksamheten i stort*. Säkerhetshotet *Infiltration, kartläggning och värvning (SH1)* är av relevans för sårbarheten.

4.4. Sårbarhet 4 (SB 4) – Avsaknad av tillräcklig fysisk säkerhet för att motstå sprängladdningar

I enlighet med den dimensionerande antagonistiska förmågan för *Sprängladdningar (DAF 1)* antas förmågan bestå av [x] kg TNT ekvivalent. För att utvärdera om de befintliga säkerhetsskyddsåtgärderna är tillräckliga har besiktningar och datorsimuleringar gjorts för byggnadens fysiska säkerhet. Resultatet visar att anläggningen bara kan motstå drygt halva den mängden TNT ekvivalent för de delar av byggnaden som är aktuella för de relevanta skyddsvärdena, vilket innebär att det är en sårbarhet i den säkerhetskänsliga verksamheten.

Sårbarheten är av relevans för *informationssystem Y (SV 4)* och *uppgiftssamlingen (SV 5)*. Den dimensionerande antagonistiska förmågan *Sprängladdningar (DAF 1)* är av relevans för sårbarheten.

4.5. Sårbarhet 5 (SB 5) – Avsaknad av tillräcklig fysisk säkerhet för att motstå forcering med fordon

I enlighet med den dimensionerande antagonistiska förmågan *Forcering med fordon (DAF 2)* antas förmågan bestå av en lastbil med en vikt på cirka [y] kg som kan användas för att sabotera *informationssystem Y (SV 4) och uppgiftssamlingen (SV 5)* så att skyddsvärdena blir otillgängliga. Förmågan kan även nyttjas för att ta sig in i anläggningen och därmed få tillgång till de *säkerhetsskyddsklassificerade uppgifterna (SV 1-3)* som hanteras i informationssystemet. Genom beräkning av hållfastheten för byggnadens väggar och genom lärdomar från praktiska försök har det påvisats att de befintliga väggarna inte kan motstå den antagna förmågan för de delar av byggnaden som är aktuella för de relevanta skyddsvärdena. Detta innebär att det är en sårbarhet i den säkerhetskänsliga verksamheten.

Sårbarheten är av relevans för den säkerhetskänsliga verksamheten i stort. Den dimensionerande antagonistiska förmågan *Forcering med fordon (DAF 2)* är av relevans för sårbarheten.

5. Säkerhetsskyddsåtgärder

Nedan redovisas vilka säkerhetsskyddsåtgärder som är nödvändiga att vidta utifrån vad som har framkommit vid identifiering och bedömning av skyddsvärden, säkerhetshot och sårbarheter.

5.1. Säkerhetsskyddsåtgärd 1 (SÅ 1) – Utbilda personal inom säkerhetsskydd

Av sårbarhetsbedömningen framgår att det inte ges någon kontinuerlig utbildning i säkerhetsskydd. Följande säkerhetsskyddsåtgärder kommer att vidtas för denna sårbarhet:

- Ta fram en utbildningsplan.
- Utvidga utbildningsverksamheten genom att ta fram nytt utbildningsmaterial, rekrytera fler som arbetar med utbildning och säkerställa interna processer för att behov av utbildning ska fångas upp.

Säkerhetsskyddsåtgärden är relevant för *den säkerhetskänsliga verksamheten i stort*, säkerhetshotet *Infiltration, kartläggning och värvning (SH 1)* samt sårbarheten *Bristfällig utbildning inom säkerhetsskydd (SB 1).*

5.2. Säkerhetsskyddsåtgärd 2 (SÅ 2) – Uppdatera och ta fram en uppdateringsplan för programvaran i informationssystem

Av sårbarhetsbedömningen framgår att programvaran i *informationssystem Y (SV 4)* inte är uppdaterad. Följande säkerhetsskyddsåtgärder kommer att vidtas för denna sårbarhet:

- Uppdatera programvaran.
- Ta fram en uppdateringsplan för kommande uppdateringar av programvaran.

Säkerhetsskyddsåtgärden är relevant för *informationssystemet Y (SV 4)* och de *säkerhetsskyddsklassificerade uppgifterna (SV 1-SV 3)* som hanteras i informationssystemet, *Avsaknad av programvara (SB 2)* och *Cyberangrepp (SH 2).*

5.3. Säkerhetsskyddsåtgärd 3 (SÅ 3) – Inför skriftliga tillstånd för besökare

Av sårbarhetsbedömningen framgår att det saknas rutiner för utfärdande av skriftliga besökstillstånd i den säkerhetskänsliga verksamheten. Den administrativa funktionen kommer att införa skriftliga tillstånd som utfärdas i receptionen innan tillträde ges till den säkerhetskänsliga verksamheten.

Säkerhetsskyddsåtgärden är relevant för *den säkerhetskänsliga verksamheten i stort*, *Avsaknad av skriftliga tillstånd för besökare (SB 3)* samt *Infiltration, kartläggning och värvning (SH 1).*

5.4. Säkerhetsskyddsåtgärd 4–6 (SÅ 4-SÅ 6) – Förstärkt skydd mot sprängladdningar och forcering med fordon

Av sårbarhetsbedömningen framgår att det finns en avsaknad av tillräcklig byggnadsteknisk fysisk säkerhet för att motstå sprängladdningar och forcering med fordon. För att omhänderta detta så kommer följande säkerhetsskyddsåtgärder att upprättas:

- Byggnadstekniska förstärkningar av byggnaden. (SÅ 4)
- Upprättande av pollare utanför byggnaden. (SÅ 5)
- Flytta den säkerhetskänsliga verksamheten längre in i byggnaden, bort från fasaden. (SÅ 6)

Säkerhetsskyddsåtgärderna (SÅ 4 och SÅ 6) är relevanta för *den säkerhetskänsliga verksamheten i stort, Explosivämnen (DAF 1)*, *Forcering med fordon (DAF 2)* och *Avsaknad av tillräcklig fysisk säkerhet för att motstå sprängladdningar (SB 4)* och *Avsaknad av tillräcklig fysisk säkerhet för att motstå forcering med fordon (SB 5).*

Säkerhetsskyddsåtgärden (SÅ 5) är relevant för *den säkerhetskänsliga verksamheten i stort, Forcering med fordon (DAF 2)* och *Avsaknad av tillräcklig fysisk säkerhet för att motstå forcering med fordon (SB 5).*

6. Fastställande av säkerhetsskyddsanalysen

Säkerhetsskyddsanalysen har fastställts av generaldirektör [Namn Namn] den [år-månad-dag]. Analysen kommer att uppdateras vartannat år eller vid behov.

Underskrift Datum Ort

Bilaga A - Säkerhetsskyddsplan

Säkerhetsskyddsåtgärderna som presenteras i säkerhetsskyddsplanen finns beskrivna i säkerhetsskyddsanalysen. I säkerhetsskyddsplanen beskrivs relationen mellan skyddsvärde, säkerhetshot, dimensionerande antagonistisk förmåga, sårbarhet och säkerhetsskyddsåtgärder. Det framgår även vilken funktion som är ansvarig för att vidta säkerhetsskyddsåtgärderna.

I säkerhetsplanen framgår också en prioritering av säkerhetsskyddsåtgärderna. Prioriteringen utgår från tre nivåer (prio 1–3) där säkerhetsskyddsåtgärderna med högst prioritering benämns prio 1. För att prioritera säkerhetsskyddsåtgärderna har en sammanvägd bedömning gjorts. Exempel på frågor som beaktats är:

- Finns det några av sårbarheterna som är mer allvarliga än de andra och därmed behöver prioriteras?
- Finns det några sårbarheter som omgärdar de högsta skyddsvärdena hos myndigheten och därmed behöver prioriteras?
- Finns det några säkerhetsskyddsåtgärder som är tids- och kostnadseffektiva som kan genomföras direkt?
- Finns det några av säkerhetsskyddsåtgärderna som antas ge särskilt god effekt?
- Kan vi uppnå några synergieffekter genom att vidta någon eller några av säkerhetsskyddsåtgärderna?

Säkerhetsskyddsåtgärderna 1-2 (SÅ 1-2) ges prio 1. Dessa säkerhetsskyddsåtgärder hanterar de sårbarheter (SB 1-2) som bedöms allvarligast. Vidare bedöms säkerhetsskyddsåtgärderna ge bäst effekt och är tids- och kostnadseffektiva då det finns befintlig kompetens inom personalsäkerhet och informationssäkerhet samt upparbetade rutiner som kan användas i implementeringen.

Säkerhetsskyddsåtgärd 3 (SÅ 3) ges prio 2. Säkerhetsskyddsåtgärden hanterar sårbarhet 3 (SÅ3) som bedöms vara mindre allvarlig än sårbarhet 1-2 (SB 1-2) men allvarligare än sårbarhet 4-5 (SB 4-5). Säkerhetsskyddsåtgärden bedöms vara mycket tids- och kostnadseffektiv att genomföra då det redan finns en administrativ funktion för att ta emot besökare.

Säkerhetsskyddsåtgärderna 4-6 (SÅ 4-6) ges prio 3. Säkerhetsskyddsåtgärderna hanterar sårbarhet 4-6 (SB 4-6) som bedöms vara lika allvarliga som sårbarhet 3 (SB 3). Däremot finns inte kompetensen för att genomföra säkerhetsskyddsåtgärderna och arbetena är mer tidskrävande i sig än för de andra säkerhetsskyddsåtgärderna. Därmed bedöms dessa säkerhetsskyddsåtgärder ge sämre effekt.

Notera: Säkerhetsskyddsplanen är ett fristående dokument och ska fastställas av säkerhetsskyddschefen.

Datum: 2025-01-14

Säkerhetsskyddsåtgärd	Prio (1-3)	När ska åtgärden påbörjas?	När ska åtgärden vara genomförd?	Ansvarig	Relaterar till skyddsvärde	Relaterar till säkerhetshot och dimensionerande antagonistisk förmåga	Relaterar till sårbarhet
Utbilda personal inom säkerhetsskydd (SÅ 1)	Prio 1	maj-25	okt-25	Personalsäkerhets-handläggare hos säkerhetsavdelningen	Samtliga	SH 1	SB 1
Genomför insats för att uppdatera programvara i informationssystem (SÅ 2)	Prio 1	maj-25	okt-25	Informationssäkerhets-handläggare hos säkerhetsavdelningen	SV 1-4	SH 2	SB 2
Inför skriftliga tillstånd för besökare (SÅ 3)	Prio 2	jun-25	dec-25	Receptionisterna tillhörande uppgifftsförmedlnings-avdelningen	Samtliga	SH 1	SB 3
Genomför byggnadtekniska förstärkningar av byggnaden (SÅ 4)	Prio 3	okt-25	apr-26	Kommande handläggare i fysisk säkerhet hos säkerhetsavdelningen	Samtliga	DAF 1-2	SB 4-5
Upprätta pollare utanför byggnaden (SÅ 5)	Prio 3	okt-25	apr-26	Kommande handläggare i fysisk säkerhet hos säkerhetsavdelningen	Samtliga	DAF 2	SB 5
Avskilj säkerhetskänsliga delar av verksamheten från fasaden (SÅ 6)	Prio 3	okt-25	apr-26	Kommande handläggare i fysisk säkerhet hos säkerhetsavdelningen	Samtliga	DAF 1-2	SB 4-5

Figur 1: Säkerhetsskyddsplan.