Vägledning i säkerhetsskydd

Fysisk säkerhet

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 December 2023

Denna vägledning beskriver innebörden av fysisk säkerhet samt ger vägledning i tillämpningen av relevanta bestämmelser i säkerhetsskyddslagen (2018:585), säkerhetsskyddsförordningen (2021:995) och Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd.

Målgruppen för denna vägledning är säkerhetsskyddschefer och personer som arbetar med fysisk säkerhet. Vägledningen beskriver såväl grundläggande som mer avancerade aspekter av fysisk säkerhet, varför vissa förkunskaper kan krävas för att fullt ut ta till sig innehållet i vägledningen.

För att kunna tillgodogöra sig innehållet i denna vägledning rekommenderas att läsaren tagit del av Säkerhetspolisens Vägledning i säkerhetsskydd – Introduktion till säkerhetsskydd.

För riksdagen och dess myndigheter finns bestämmelser om fysisk säkerhet i 7 § lagen (2019:109) om säkerhetsskydd i riksdagen och dess myndigheter.

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

Innehåll

1 Vad är fysisk säkerhet?

§ *2 kap. 3 § säkerhetsskyddslagen*

§ *4 kap. 1 § säkerhetsskyddsförordningen*

Fysisk säkerhet ska förebygga att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där säkerhetskänslig verksamhet i övrigt bedrivs. Fysisk säkerhet ska också förebygga skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt. Skadlig inverkan kan exempelvis vara att med explosivämnen eller vapenverkan stoppa verksamheten. Det omfattar även skydd mot att någon, med eller utan tekniska hjälpmedel, obehörigen får insyn i den säkerhetskänsliga verksamheten.

Fysisk säkerhet kan beskrivas som ett system uppbyggt av personal, rutiner, byggnadsteknik och säkerhetsteknik. Tillsammans skapar dessa de upptäckande, försvårande och hanterande säkerhetsskyddsåtgärder som ska förebygga obehörigt tillträde och skadlig inverkan. Genom fysisk säkerhet tillgodoses det identifierade behov av säkerhetsskydd som framkommer i en säkerhetsskyddsanalys. Detta innebär mer konkret att omhänderta de sårbarheter som finns i förhållande till den säkerhetskänsliga verksamhetens skyddsvärden, identifierade säkerhetshot samt Säkerhetspolisens beskrivningar av dimensionerande antagonistiska förmågor.

Se Figur 1 till höger.

Notera:
Fysisk säkerhet är endast en del av det system av åtgärder som krävs för ett fullgott säkerhetsskydd. För att säkerhetsskyddet ska vara tillfredställande måste den fysiska säkerheten integreras med säkerhetsskyddsåtgärderna personalsäkerhet och informationssäkerhet. Fysisk säkerhet är till exempel beroende av tillfredställande informationssäkerhet i informationssystem som används för fysiska säkerhetsskyddsåtgärder, såsom kameraövervakning och elektroniska passersystem.

Figur 1.

Fysisk säkerhet är ett system med flera ingående delar som syftar till att förebygga obehörigt tillträde och skadlig inverkan.

Utgångspunkten för fysisk säkerhet är det behov och de förutsättningar som framkommer i verksamhetens säkerhetsskyddsanalys.

Fysisk säkerhet byggs upp genom en kombination av personal, rutiner, byggnadsteknik och säkerhetsteknik.

Fysisk säkerhet skapar en förmåga att upptäcka, försvåra och hantera säkerhetshotande händelser.

1.1 Hur fungerar fysisk säkerhet?

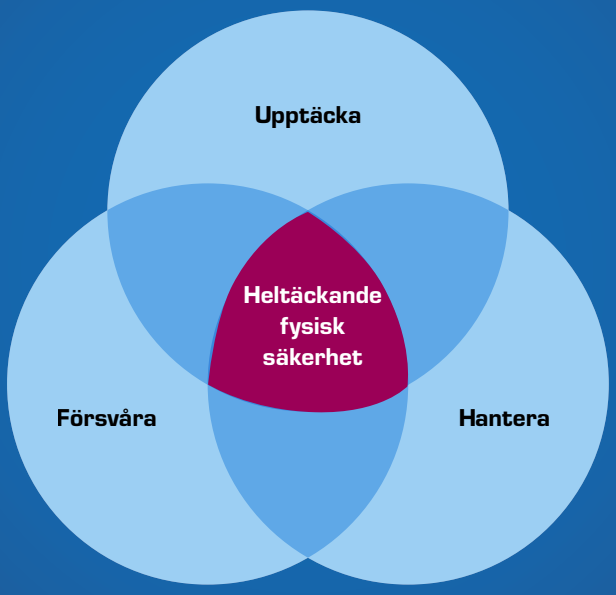
Säkerhetsskyddsåtgärderna inom fysisk säkerhet för att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan är systemsamverkande och har stor påverkan på varandra. Ett obehörigt tillträde måste till exempel upptäckas tidigt i syfte att ge hanterande förmågor tillräckligt med tid att avbryta eller omhänderta en antagonist innan skada för Sveriges säkerhet hinner uppstå. Även hanterande och försvårande säkerhetsskyddsåtgärder påverkar i hög grad varandra. Hur länge ett obehörigt tillträde behöver fördröjas avgörs till exempel av tiden det tar att vidta hanterande säkerhetsskyddsåtgärder.

Figur 2 nedan illustrerar behovet av alla fysiska säkerhetsskyddsåtgärder.

Om det saknas upptäckande säkerhetsskyddsåtgärder kommer exempelvis ett obehörigt tillträde inte att kunna hanteras, eftersom det inte upptäcks. Om det istället saknas försvårande säkerhetsskyddsåtgärder kommer ett obehörigt tillträde att upptäckas, men riskerar att hinna slutföras innan det har hanterats. Saknas hanterande säkerhetsskyddsåtgärder kommer ett obehörigt tillträde att kunna slutföras, oavsett hur lång tid det tar, eftersom det inte kommer att hanteras.

Notera:
Fysisk säkerhet är ett system av säkerhetsskyddsåtgärder som är beroende av varandra, vilket innebär att enskilda säkerhetsskyddsåtgärder i sig inte utgör heltäckande fysisk säkerhet. Exempelvis är ett larm som upptäcker ett obehörigt tillträde relativt verkningslöst om det inte finns några säkerhetsskyddsåtgärder för att hantera larmet. På samma sätt är en säkerhetsdörr som fördröjer ett obehörigt tillträde otillräcklig om det obehöriga tillträdet inte upptäcks.

Figur 2.
Alla förmågor inom fysisk säkerhet påverkar varandra.



Följande exempel beskriver verkan av de olika säkerhetsskyddsåtgärderna och vissa av principerna inom fysisk säkerhet vid en antagonistisk handling:

- Inledningsvis inhämtar antagonisten information om den säkerhetskänsliga verksamheten via bland annat öppna källor och i vissa fall även genom rekognosering på plats. Skydd mot obehörig insyn och avlyssning försvårar detta. Även principer som att skapa variation i den fysiska säkerheten samt minska exponeringen av eventuella svagheter kan vara verkansfulla.
- När antagonisten har påbörjat sin antagonistiska handling är det viktigt att det finns upptäckande säkerhetsskyddsåtgärder. Upptäckande säkerhetsskyddsåtgärder syftar till att tidigt upptäcka en antagonist, gärna redan under rekognoseringsfasen eller i vart fall åtminstone i början av själva genomförandet. Exempel på sådana åtgärder är rörlig personell bevakning, kamerabevakning och områdeslarm.
- När antagonisten är upptäckt och efterhand rör sig in mot sitt mål behövs försvårande säkerhetsskyddsåtgärder, både för att fördröja antagonisten och reducera skadan av den antagonistiska handlingen. Exempel på fördröjande åtgärder är förstärkta omslutningsytor som väggar, dörrar och fönster samt, enligt principen om balanserad fysisk säkerhet, lika starka golv och tak. Även här kan principen om variationer i den fysiska säkerheten försvåra ytterligare för antagonisten genom att hindra denne från att veta vad som väntar härnäst.
- Så fort antagonisten har upptäckts larmas den hanterande förmågan, som har till uppgift att avbryta eller reducera konsekvensen av den antagonistiska handlingen. Det är generellt bättre om relevanta hanterande förmågor finns på plats i verksamheten istället för att behöva tillkallas utifrån. Detta eftersom det är svårare för antagonisten att tvingas konfrontera och ta sig förbi hanterande förmågor än att ha försprång och till exempel kunna barrikadera vägen för efterföljare.

Se avsnitt 4 Principer för fysisk säkerhet.

Tiden för att hantera en antagonistisk handling varierar beroende på antagonistens förmåga i form av verktyg, kunskap och färdigheter samt antagonistens mål och syfte. Vissa typer av antagonistiska handlingar, till exempel att föra ut lagringsmedia med säkerhetsskyddsklassificerade uppgifter, innebär att en antagonist behöver fly från platsen för att lyckas. Andra typer av handlingar, till exempel sabotage av säkerhetskänsliga system, kräver inte flykt för att lyckas, och kan därför ske på kortare tid.

Notera:
I andra sammanhang än säkerhetsskydd räknas ibland ”avskräckande åtgärder”, såsom belysning och skyltning om kamerabevakning, in i fysisk säkerhet. Den avskräckande effekten är dock svår att bedöma, särskilt i fråga om en kvalificerad antagonist med tydligt mål att orsaka skada för Sveriges säkerhet. En eventuell avskräckande effekt av exempelvis brottspreventiv bebyggelse bör därför snarare ses som en positiv sidoeffekt än en säkerhetsskyddsåtgärd.

Se avsnitt 4.6 Bebyggelseinriktad brottsprevention.

2 Preskriptivt och funktionsbaserat synsätt

Ett preskriptivt synsätt på fysisk säkerhet kan beskrivas som att den fysiska säkerheten utformas för att uppfylla en viss norm, standard eller annan detaljerad beskrivning som en regelutgivare anvisar. Utformningen kan då ske utan hänsyn till verksamhetsspecifika omständigheter. För verksamhetsutövare kan ett preskriptivt synsätt ibland innebära mindre analysarbete men utgör samtidigt ett hinder mot att anpassa den fysiska säkerheten till den egna verksamheten.

Med ett preskriptivt synsätt kan det även bli svårt för verksamhetsutövare att avgöra om den fysiska säkerheten verkligen är tillfredställande eller inte. Detta gäller särskilt eftersom fysisk säkerhet ska utformas utifrån såväl relationen mellan upptäckande, försvårande och hanterande säkerhetsskyddsåtgärder som identifierade säkerhetshot och dimensionerande antagonistiska förmågor.

Se avsnitt 3.2.3 Säkerhetshot och dimensionerande antagonistiska förmågor.

Vidare kan ett preskriptivt synsätt leda till en ojämn nivå av säkerhetsskydd inom en verksamhet eller verksamhetsutövare emellan.

Se Figur 3 nedan.

För förklaring av begreppen och beräkningarna i exemplet, se avsnitt 5.3 Upptäcktsfaktor och 8.1 Angreppsanalys.

Kapitel 5 i Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd är i huvudsak utformat utifrån ett funktionsbaserat synsätt. Med ett funktionsbaserat synsätt kan verksamhetsutövare till skillnad från ett preskriptivt synsätt utforma den fysiska säkerheten utifrån det identifierade behovet av säkerhetsskydd som grundar sig i resultatet av verksamhetsutövarens säkerhetsskyddsanalys, identifierade säkerhetshot och i förekommande fall beskrivningar av dimensionerande antagonistiska förmågor. Vissa preskriptiva krav förekommer dock även i fråga om fysisk säkerhet, exempelvis att verksamhetsutövare ska ha en förteckning över kort, nycklar och koder.

Se avsnitt 6.2.7 Kort, nycklar och koder.

Ett funktionsbaserat synsätt är mer flexibelt och ger verksamhetsutövare större möjlighet att utforma den fysiska säkerheten i förhållande till hur åtgärderna samspelar såväl med varandra som med andra säkerhetsskyddsåtgärder. Detta kan exempelvis ske genom att säkerställa att upptäckt sker tidigare längs en antagonists angreppsväg, att fördröjningstiden ökas eller att hanteringstiden förkortas. Ett annat exempel är hur fysisk uppdelning av verksamheten i olika sektioner, så kallad sektionering, och tillämpning av passersystem kan bidra till att tillgodose behovet av autentisering vid åtkomst till informationssystem.

Om en verksamhetsutövare inte har möjlighet att säkerställa tidigare upptäckt, längre fördröjningstid eller kortare hanteringstid, kan det finnas anledning att se över valet av plats där den säkerhetskänsliga verksamheten bedrivs. Om det inte heller finns någon möjlighet att anpassa valet av plats kan det istället vara nödvändigt att se över och förändra de skyddsvärden som den fysiska säkerheten ska skydda.

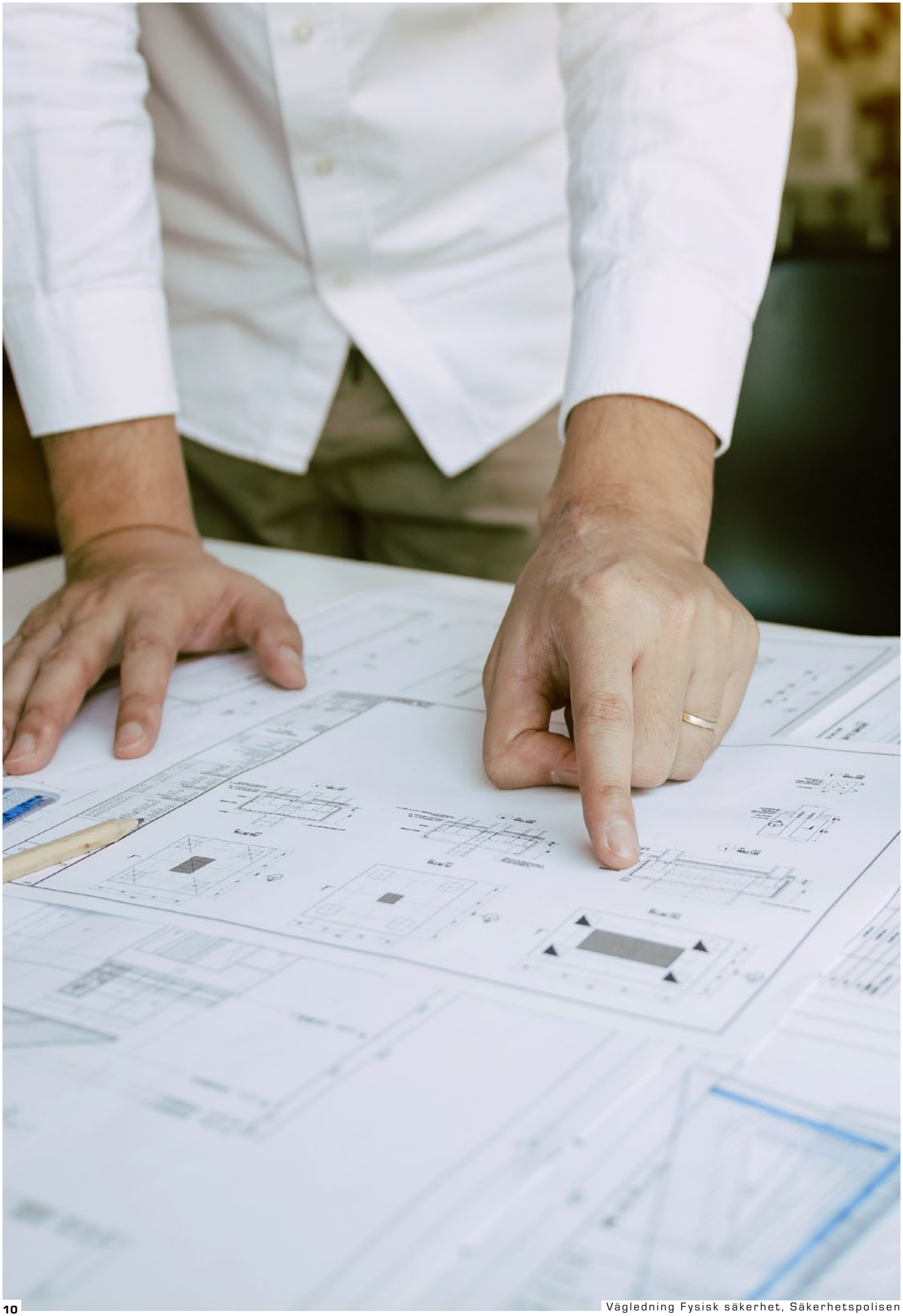
Figur 3.
Exempel på två utformningar av fysisk säkerhet utifrån ett preskriptivt krav på säkerhetsskåp som certifierats enligt Stöldskyddsföreningens norm SSF 3492 och enligt denna erbjuder en fördröjningstid på 10 minuter.

Båda anläggningarna, A respektive B, lever upp till det preskriptiva kravet men har olika förutsättningar i övrigt. Detta medför att medan det i fall A i realiteten inte finns en tillfredställande fysisk säkerhet (på grund av för sen upptäckt i förhållande till hanteringstiden) är den fysiska säkerheten i fall B istället överdimensionerad med både larm, vakt och flera dörrar/väggar före säkerhetsskåpet.

	Anläggning A	Anläggning B
Upptäckt	På förvaringsenheten (vibrationslarm)	Utanför byggnaden (staketlarm)
Hanteringstid	20 min	5 min
Fördröjningstid efter upptäckt	10 min	20 min
Återstående tid	–10 min	15 min

Anläggning A:
En enkel kontorslokal utan särskilda skyddsåtgärder och en gata som är öppen för allmänheten utanför.

Anläggning B:
En mer robust byggnad med avspärrat område och larm utanför.



3 Utformning av fysisk säkerhet

3.1 Processen för utformning och vidmakthållande av fysisk säkerhet

Utformningen av den fysiska säkerheten är en del av säkerhetsskyddsanalysen och syftar till att konkretisera hur den säkerhetskänsliga verksamheten ska skyddas mot obehörigt tillträde och skadlig inverkan.

Se avsnitt 3.2 Säkerhetsskyddsanalys.

Den fysiska säkerheten måste också implementeras, vilket sker genom säkerhetsskyddsplanen, och vidmakthållas i perioderna mellan säkerhetsskyddsanalyserna. Processen för utformning och vidmakthållande kan delas in i fyra steg.

Se översiktlig beskrivning av processen i figur 4.

Figur 4.
Processen för utformning av fysisk säkerhet

Underrubrikerna i varje steg återfinns även som egna avsnitt i vägledningen.

Ingångsvärden

Utformningen av den fysiska säkerheten ska utgå från de inledande delarna av säkerhetsskyddsanalysen. Där ska verksamhetsutövare beskriva:

- den säkerhetskänsliga verksamheten och därmed vilken kontext den fysiska säkerheten ska verka i (verksamhetsbeskrivning),
- vad den fysiska säkerheten konkret ska skydda (skyddsvärden)
- vad den fysiska säkerheten ska skydda mot (identifierade säkerhetshot och dimensionerande antagonistiska förmågor)
- eventuella sårbarheter som behöver hanteras.

Först när detta har klargjorts kan verksamhetsutövaren gå vidare till nästa steg och avgöra hur säkerhetsskyddet ska utformas, i detta fall med fysisk säkerhet.

Utformning

Nästa steg är att utforma den fysiska säkerheten så att det finns säkerhetsskyddsåtgärder för att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan. Utformningen görs utifrån vad som framkommit i säkerhetsskyddsanalysens inledande delar, särskilda krav om exempelvis styrning av tillträde samt genom att tillämpa olika principer för fysisk säkerhet, se senare avsnitt i vägledningen. Syftet är att den fysiska säkerheten ska bli heltäckande men även anpassad till verksamheten.

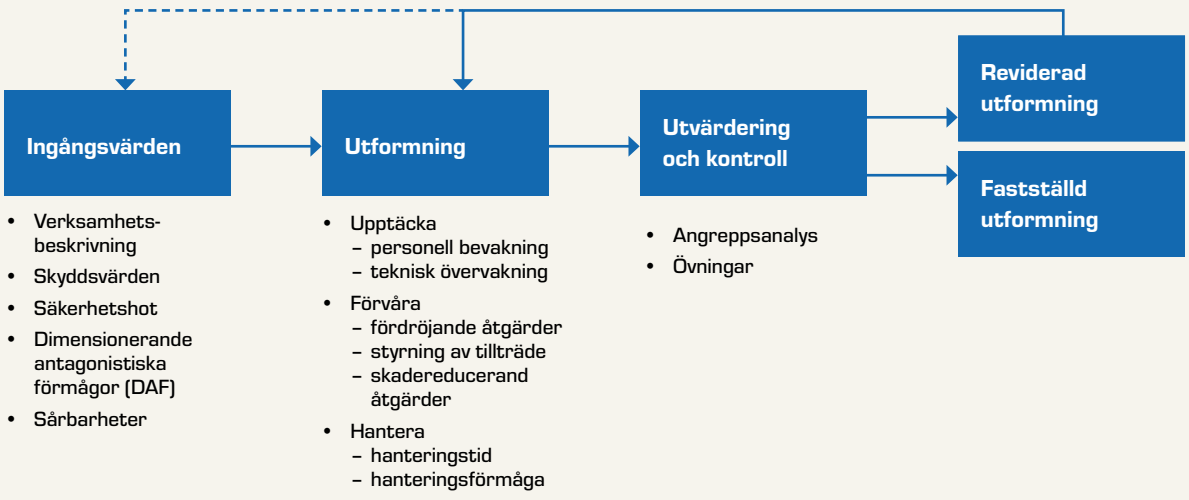
Utvärdering och kontroll

När verksamhetsutövaren har ett förslag på hur den fysiska säkerheten ska utformas behöver detta förslag verifieras som tillräckligt innan slutgiltigt beslut om utformning tas. Utvärdering och kontroll kan bestå av exempelvis olika analyser, övningar och funktionstester som syftar till att säkerställa att den fysiska säkerheten är utformad på ett sådant sätt att den lever upp till ställda krav. Utvärdering och kontroll berör ofta både planerad och befintlig fysisk säkerhet vars funktion behöver vidmakthållas.

Fastställd utformning eller behov av reviderad utformning

Beroende på resultatet av utvärdering och kontroll fattas antingen beslut om fastställd utformning och implementering genom säkerhetsskyddsplanen, eller beslut om att revidera utformningen av den fysiska säkerheten. Konstaterar verksamhetsutövaren att utformningen inte är tillfredställande, det vill säga att det kvarstår sårbarheter, kan dessa hanteras genom att exempelvis öka den upptäckande förmågan, förlänga fördröjningstiden, anpassa skadereducerande säkerhetsskyddsåtgärder eller förkorta hanteringstiden.

Om verksamhetsutövaren inte har tillräckliga möjligheter att göra justeringar i utformningen av den fysiska säkerheten kan det i vissa fall gå att göra förändringar i skyddsvärdena så att konsekvenserna av en fullföljd antagonistisk handling blir lägre. Därmed minskar i förlängningen de identifierade säkerhetshot och dimensionerande antagonistiska förmågor som den fysiska säkerheten behöver klara av att skydda mot. Sådana justeringar i de inledande delarna av säkerhetsskyddsanalysen kan dock innebära att stora delar av den behöver revideras.



3.2 Säkerhetsskyddsanalys

Grunden för adekvat fysisk säkerhet är att säkerhetsskyddsanalysens första delar detaljerat redogör för vad som ska skyddas (skyddsvärden) och vad dessa skyddsvärden ska skyddas mot (identifierade säkerhetshot och dimensionerande antagonistiska förmågor). Utifrån dessa parametrar kan sedan sårbarheter identifieras och därefter bedömas hur verksamheten ska skyddas (med säkerhetsskyddsåtgärder, däribland fysisk säkerhet).

För mer information om metoden för att genomföra en säkerhetsskyddsanalys och de olika begreppens innebörd se Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys.

Nedan förklaras och exemplifieras endast kortfattat för de ingående delarna i förhållande till processen för utformning av säkerhetsskyddsåtgärder med avseende på fysisk säkerhet.

3.2.1 Verksamhetsbeskrivning

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

Verksamhetsbeskrivningen utgör den inledande delen av säkerhetsskyddsanalysen och syftar till att övergripande beskriva den säkerhetskänsliga verksamheten. Där ska redovisas på vilket sätt och vilka delar av verksamheten som är av betydelse för Sveriges säkerhet. Verksamhetsbeskrivningen kan bli en viktig utgångspunkt för många av de val som behöver göras vid utformning av fysisk säkerhet. Exempelvis kommer styrning av tillträde att kunna utformas olika beroende på om verksamhetsutövare har ett uppdrag att tillhandahålla service för allmänheten i sina lokaler eller inte.

3.2.2 Identifiera och bedöma skyddsvärden

§ *2 kap. 3-5 §§ Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Identifieringen av skyddsvärden ska konkret klargöra vad i verksamheten som är skyddsvärt och vilka konsekvenser en antagonistisk handling samt vissa andra händelser kan medföra för Sveriges säkerhet. Identifieringen ska även klargöra utifrån vilka av perspektiven konfidentialitet, riktighet och tillgänglighet som de identifierade skyddsvärdena är skyddsvärda. Resultatet av identifieringen kan komma att spela en stor roll vid utformningen av den fysiska säkerheten. Till exempel behöver den fysiska säkerheten för en verksamhet med många informationssystem och stora krav på tillgänglighet utformas annorlunda än för en verksamhet där det bara förvaras säkerhetsskyddsklassificerade handlingar som endast är skyddsvärda ur perspektivet konfidentialitet.

3.2.3 Säkerhetshot och dimensionerande antagonistiska förmågor

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

Det är svårt att avgöra hur den fysiska säkerheten ska utformas och om den eventuella befintliga fysiska säkerheten uppfyller behovet av säkerhetsskydd utan att först ta ställning till vad den fysiska säkerheten konkret ska klara av att skydda mot. Detta ingår därför också i arbetet med säkerhetsskyddsanalysen.

Till exempel är det stor skillnad på vilka fysiska säkerhetsskyddsåtgärder som behövs för att fördröja ett obehörigt tillträde genom ett fysiskt angrepp med en kofot eller en bensindriven motorkap. Likaså är det väsentlig skillnad på att skydda mot en mindre kontra större sprängladdning eller att skydda mot generell överhörning jämfört med att skydda mot avlyssning med tekniska hjälpmedel.

En utgångspunkt för vad den fysiska säkerheten ska klara av att skydda mot kan vara standarder och normer som beskriver den lägsta nivå av skydd som krävs för att upptäcka, försvåra och hantera obehörigt tillträde eller skadlig inverkan. Dessa standarder och normer är dock vanligen inte framtagna för säkerhetskänslig verksamhet och tar oftast bara höjd för grundläggande antagonistiska förmågor. Säkerhetskänsliga verksamheter ska därför utforma den fysiska säkerheten utifrån egna mer relevanta identifierade säkerhetshot och i förekommande fall de beskrivningar av dimensionerande antagonistiska förmågor (DAF) som Säkerhetspolisen tillhandahåller. Säkerhetspolisen tillhandahåller i regel dessa efter att verksamhetsutövare anmält att de bedriver säkerhetskänslig verksamhet till sin tillsynsmyndighet och denne i sin tur uppmärksammat Säkerhetspolisen på ett föreliggande behov.

De förmågor som framgår av de beskrivningar som Säkerhetspolisen tillhandahåller är sådana som säkerhetsskyddsåtgärderna ska klara av att skydda mot, oavsett om de motsvaras av något av verksamhetsutövaren identifierat säkerhetshot eller inte. Säkerhetsskyddsåtgärder baserade på dimensionerande antagonistiska förmågor medför en långsiktighet som tar höjd för förändringar över tid och behöver därför inte förändras i samma takt som de identifierade säkerhetshoten förändras. Om de identifierade säkerhetshoten kortvarigt förändras på ett sådant sätt att de överstiger vad den fysiska säkerheten är dimensionerad utifrån kan istället mer tillfälliga säkerhetsskyddsåtgärder, så kallat kompensatoriska åtgärder, behöva vidtas.

Vilka antagonistiska förmågor som är tillämpliga vid dimensionering av fysisk säkerhet beror på både från vilket perspektiv ett skyddsvärde är skyddsvärt (konfidentialitet, riktighet och tillgänglighet) och den skada för Sveriges säkerhet som kan uppstå vid en antagonistisk handling (från ringa skada upp till synnerligen allvarlig skada). Detta innebär exempelvis att en verksamhetsutövare som endast har skyddsvärden som är skyddsvärda från perspektivet konfidentialitet inte behöver beakta antagonistiska förmågor som avser sabotage och otillgängliggörande av skyddsvärden vid dimensionering av den fysiska säkerheten. Vidare beror nivån på tillämpliga antagonistiska förmågor på skyddsvärdets betydelse för Sveriges säkerhet. Generellt innebär detta att mer betydelsefulla skyddsvärden åtföljs av en högre förmåga.

Nedan ges exempel på antagonistiska förmågor som kan rymmas inom identifierade säkerhetshot eller dimensionerande antagonistiska förmågor och som

säkerhetskänsliga verksamheter kan behöva beakta vid utformningen av fysisk säkerhet.

Obehörigt tillträde:

- Öppen forcering med manuella verktyg
- Öppen forcering med motordrivna verktyg
- Öppen forcering med fordon
- Öppen forcering med explosivämnen
- Tyst och dold forcering med dyrkar och manipulering av lås

Skadlig inverkan:

- Sabotage med explosivämnen
- Sabotage med farliga ämnen, även kallat CBRN
- Sabotage genom anlagd brand
- Sabotage med skjutvapen
- Avlyssning av samtal med tekniska hjälpmedel
- Insyn med tekniska hjälpmedel

3.2.4 Sårbarhetsbedömning

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

Sårbarhetsbedömningen är den fjärde delen i säkerhetsskyddsanalysen och hör tätt ihop med den resterande processen för utformningen av den fysiska säkerheten. Det är viktigt att sårbarhetsbedömningen grundar sig på vad som framkommit i de tre första stegen för att kunna ligga till grund för efterkommande bedömningar av vilka säkerhetsskyddsåtgärder som är nödvändiga. Vid arbete med säkerhetsskyddsanalys kan en sårbarhet avse avsaknad av fullgoda säkerhetsskyddsåtgärder i förhållande till identifierade säkerhetshot, dimensionerande antagonistiska förmågor eller författningskrav. En sårbarhet kan alltså finnas för att det helt saknas säkerhetsskyddsåtgärder eller att dessa inte bedöms tillräckligt verkansfulla men även om säkerhetsskyddsåtgärderna inte lever upp till preskriptiva krav. Om det exempelvis saknas en förteckning över kort, nycklar och koder så är detta en sårbarhet (på grund av bristande kontroll) även om själva föremålen i praktiken förvaras på ett tillräckligt säkert sätt i förhållande till en viss antagonistisk förmåga.

+ *Se avsnitt avsnitt 6.2.7 Kort, nycklar och koder.*

Verksamhetsutövare har ofta små möjligheter att påverka de ingående parametrarna i form av skyddsvärden, identifierade säkerhetshot och dimensionerande antagonistiska förmågor samt preskriptiva krav. Sårbarheterna kan däremot överbryggas på många olika sätt och påverkas dessutom av de säkerhetsskyddsåtgärder verksamhetsutövaren väljer. Exempelvis kan valet att förlägga en verksamhet under jord för att skydda mot sabotage med skjutvapen skapa nya sårbarheter i förhållande till sabotage med farliga ämnen genom ventilationssystem. Ett annat exempel är hur digitalisering av säkerhetsskyddsklassificerade handlingar för att förändra behovet av skydd mot obehörigt tillträde i sin tur kan föranleda ett behov av skydd mot röjande signaler.

Eftersom det finns många sätt att komma till rätta med sårbarheter, och ibland även möjlighet att påverka de ingående parametrarna, kan sårbarhetsbedömningen med fördel göras iterativt eller ”teoretiskt upprepat”.

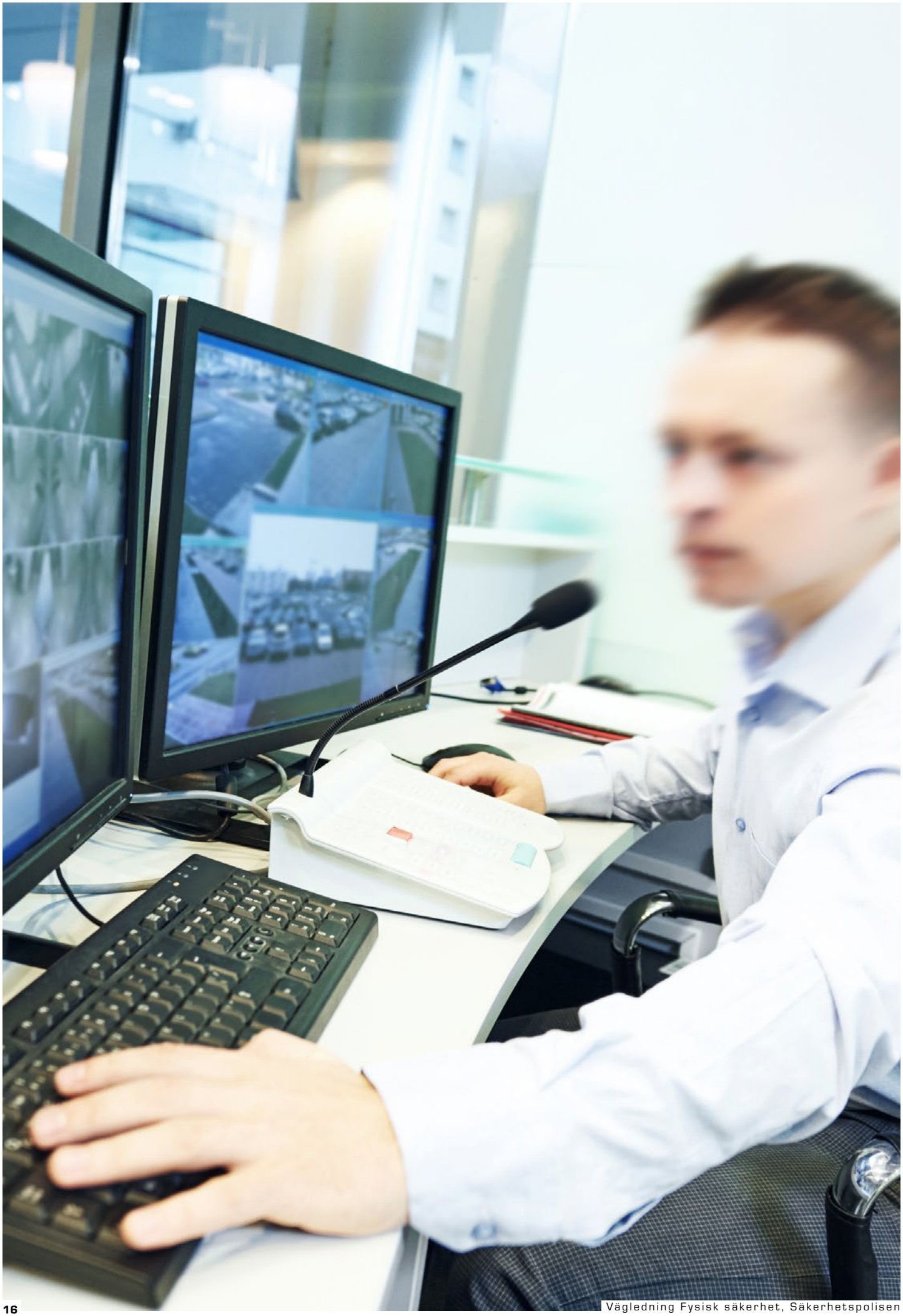
+ *För mer information se figur 4.*

Att tankemässigt göra bedömningen flera gånger, främst utifrån existerande men även planerade säkerhetsskyddsåtgärder, möjliggör en analys av hur olika alternativ påverkar varandra innan den definitiva lösningen väljs och säkerhetsskyddsanalysen fastställs. En iterativ process ger också verksamhetsutövare större möjlighet att utforma säkerhetsskyddet med hänsyn till vad som passar bäst för den aktuella verksamheten, under förutsättning att resultatet blir ett fullgott säkerhetsskydd.

3.2.5 Säkerhetsskyddsplan

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

Den fastställda utformningen kan innebära att det behöver göras förändringar av den/de personal, rutiner, byggnadsteknik och säkerhetsteknik som bygger upp den fysiska säkerheten. Dessa förändringar dokumenteras i säkerhetsskyddsplanen som utgör grunden för implementering av de lösningar som har valts. Säkerhetsskyddsplanen ska redogöra för hur behovet av säkerhetsskyddsåtgärder omhändertas samt när åtgärderna ska vidtas och vilken funktion som ansvarar för dem. Efterhand kommer åtgärder som har sin grund i den fastställda teoretiska utformningen såsom att skapa sektioner med nya väggar och dörrar att slutföras. Samtidigt kommer andra åtgärder att tillkomma, exempelvis sådana som är resultatet av utvärdering och kontroll av befintlig fysisk säkerhet, till exempel uppgradering sam modernisering av larm- och kamerasystem.



4 Principer för fysisk säkerhet

4.1 Lökprincipen

Uttrycket lökprincipen åsyftar det vanligt förekommande sättet att bygga fysisk säkerhet med flera på varandra följande "skal" och där det som ska skyddas är placerat i centrum.
Se Figur 5 nedan.

Lökprincipen användes redan i medeltidens borgar där flera koncentriska murar omgärdade centrum där värdeföremål och nödvändiga matförråd fanns samlade. Idag är skyddsvärden ofta utspridda på olika platser, men lökprincipen är fortfarande användbar och går att applicera genom att skapa öar med skyddsvärden omgivna av lager med säkerhetsskyddsåtgärder.

Lökprincipen kan beskrivas som ett ”utifrån och in”-perspektiv där en antagonist måste ta sig igenom flera lager av säkerhetsskyddsåtgärder och förflytta sig över ytor på vägen in till skyddsvärden som befinner sig i centrum. Varje lager/utrymme enligt lökprincipen kan innehålla en eller flera systemsamverkande säkerhetsskyddsåtgärder för att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan. Fysisk säkerhet som byggts upp enligt lökprincipen kan utvärderas på ett strukturerat sätt med hjälp av så kallad angreppsanalys.

För mer information se avsnitt 8.1 Angreppsanalys.

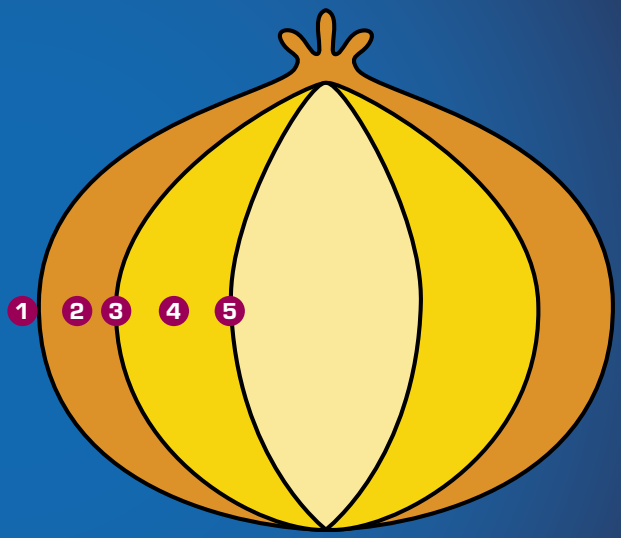
Figur 5.
Exempel på tre på varandra följande lager och därimellan två områden/utrymmen med det skyddsvärda placerat längst in i centrum enligt lökprincipen.

1 2 Staket med larm följt av ett område som det tar tid för antagonisten att förflytta sig över utgör upptäckande och försvårande säkerhetsskyddsåtgärder

3 Yttervägg med säkerhetsdörrar och säkerhetsglas utgör försvårande säkerhetsskyddsåtgärder

4 Rum med larm i form av passiv infraröd sensor samt stationär vakt i byggnaden utgör upptäckande och hanterande säkerhetsskyddsåtgärder

5 Säkerhetsskåp med magnetkontakt och vibrationssensor utgör försvårande och upptäckande säkerhetsskyddsåtgärder



4.2 Balans i den fysiska säkerheten

Balans i den fysiska säkerheten innebär att det inte finns någon del som är svagare än de andra. För försvårande säkerhetsskyddsåtgärder innebär detta till exempel att en dörr till ett utrymme måste ha samma motståndskraft som väggen dörren sitter i. Detsamma gäller eventuella fönster, tak, golv och inkrypningsvägar till utrymmet. På motsvarande sätt måste låsanordningen och säkerheten i ett eventuellt passersystem dimensioneras för att vara i paritet med dörrens motståndskraft. Likaså går det att uppnå balans hos upptäckande säkerhetsskyddsåtgärder, genom att till exempel säkerställa att ett obehörigt tillträde upptäcks oavsett vilken väg in i utrymmet antagonisten väljer att ta.

4.3 Sektionering

En princip för att uppnå systematik i utformningen av den fysiska säkerheten är att, där det är möjligt, dela in byggnader, anläggningar och objekt i olika sektioner. Sektionering syftar till att tydliggöra och avgränsa var olika verksamheter bedrivs hos en verksamhetsutövare. Sektionering är också ett sätt att förtydliga vilka krav på fysiska säkerhetsskyddsåtgärder som finns för olika delar av en byggnad, anläggning eller objekt som innefattar både säkerhetskänslig och annan verksamhet.

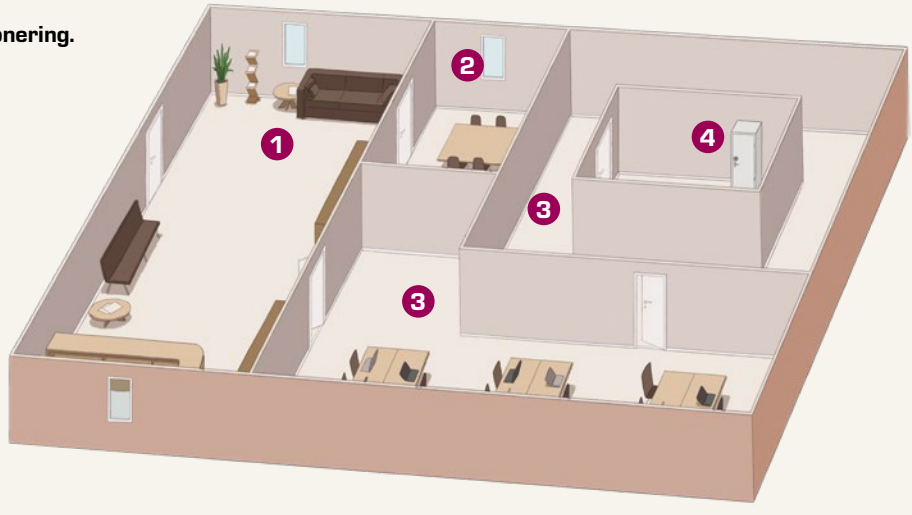
Vilka säkerhetsskyddsåtgärder som gäller för respektive typ av sektion har sin utgångspunkt i verksamhetsutövarens säkerhetsskyddsanalys. Genom denna ställs olika krav på säkerhetsskyddsåtgärder i respektive typ av sektion. Till exempel kan en reception vara öppen för allmänheten, medan utrymmen där säkerhetskänslig verksamhet bedrivs kan behöva ha en högre nivå av fysisk säkerhet och endast få beträdas av egen personal med särskild behörighet. Genom att placera de säkerhetskänsliga delarna längre in i verksamheten skapas samtidigt flera lager enligt lökprincipen.

Se Figur 6 nedan.

Notera:
Sårbarheter kan uppstå på grund av utrymningsbehov. Exempel på sådana sårbarheter är att utrymningsvägar kan öppnas inifrån med hjälp av en insider och att de kan användas som en flyktväg efter genomförd antagonistisk handling. Ju färre som vistas i närheten av den säkerhetskänsliga verksamheten, desto bättre, och detta kan gynnas av sektionering. Om den säkerhetskänsliga verksamheten i Figur 6 placerats där det externa mötesrummet är markerat skulle principerna om sektionering och flera lager frångåtts, med en sämre fysisk säkerhet som följd.

Figur 6. Exempel på sektionering.

1. Reception
2. Externt mötesrum
3. Arbetsutrymmen
4. Säkerhetskänslig verksamhet



4.4 Variation i den fysiska säkerheten

Variation i den fysiska säkerheten handlar om att försvåra för en antagonist att kartlägga och utnyttja svagheter i olika typer av säkerhetsskyddsåtgärder. Genom att undvika standardiserade och förutsägbara lösningar försvåras planering och utförande av obehörigt tillträde och skadlig inverkan. Variationer kan göras i hela systemet av personal, rutiner, byggnadsteknik och säkerhetsteknik som tilsammans bygger upp den fysiska säkerheten. Väl utförda kommer variationerna att ställa motstridiga krav på antagonistens förmåga, exempelvis att denne dels måste bära med sig tung och otymplig utrustning, dels måste röra sig snabbt över områden för att undvika upptäckt.

Några exempel på variationer för personal och rutiner är att variera vem i bevakningspersonalen som gör vad, när och hur. Om ronderingar sker med ett oregelbundet schema blir det svårare för antagonisten att välja en fördelaktig tidpunkt för sin handling. Detsamma gäller för inpasseringskontroller där slumpvisa och mer noggranna genomsökningar kan försvåra för någon att ta in otillåtna föremål. Ett annat exempel är att säkerställa att koder till tekniska övervakningssystem och förvaringsenheter ändras från standardiserade format, exempelvis genom att inte alla har samma antal tecken eller varieras på ett sådant sätt att de skiljer sig från fabriksinställda koder. På motsvarande sätt kan vissa passersystem konfigureras så att det utomhus, där en antagonist enklare kan rekognosera, används en pin-kod medan det inomhus är en annan, kanske även den med att annat antal siffror.

Byggnadstekniska lösningar som ingår i den fysiska säkerheten kan också varieras, så att det behövs olika typer av verktyg för att lyckas med ett obehörigt tillträde. Exempelvis är galler och plåtförstärkningar relativt svårforcerade med motorsåg men desto mer sårbara för termiska skärverktyg. Det motsatta gäller för exempelvis väggkonstruktioner av träreglar och cementfiberskivor. Denna typ av variationer tvingar en antagonist att bära med sig flera olika typer av verktyg och skyddsutrustning samtidigt som möjligheten att antagonistens utrustning går sönder eller slutar fungera ökar.

Variationer handlar inte bara om att försvåra i förhållande till antagonistens materiella förmåga, det kan även handla om immateriell förmåga som kunskap och erfarenhet. Exempelvis kan variationer i passersystem göra att antagonisten både behöver kunna dyrka mekaniska lås och koppla förbi elektroniska lås. Detsamma gäller i larmsystem där olika typer av principer för upptäckande funktion medför att den som försöker ta sig förbi oupptäckt behöver större tekniska kunskaper och träning än om samma typ av larmsensor används överallt.

4.5 Skydd mot sårbarhetsexponering

Skydd mot sårbarhetsexponering innebär reducering av möjligheten för en antagonist att inhämta information om verksamheten genom öppna källor, visuell spaning och/eller teknisk inhämtning. Ett sätt att reducera denna typ av sårbarhetsexponering är att begränsa spridning av ritningsunderlag och andra uppgifter, även om de inte är säkerhetsskyddsklassificerade, som kan utnyttjas av en antagonist vid val av mål och planering av antagonistiska handlingar. Det kan exempelvis vara lämpligt att se över utrymningsritningar som sitter i publika delar av verksamheten och överväga om de kanske visar mer information än nödvändigt, till exempel hur lokalerna är utformade bortom de delar som besökare ska vistas i och vid brand utrymma genom.

4.6 Bebyggelseinriktad brottsprevention

Bebyggelseinriktad brottsprevention handlar om att med åtgärder i bebyggelse och omgivning förebygga brottsligt beteende. Det är i fråga om kvalificerade antagonister svårt att förebygga brottsligt beteende men det går ändå att använda bebyggelseinriktade åtgärder för att skapa en bättre fysisk säkerhet. Till exempel kan förutsättningarna för att upptäcka ett obehörigt tillträde ökas genom anpassningar av vegetationen på en plats från vilken en antagonistisk handling skulle kunna inledas genom att rensa skymmande träd och buskar längs en fasad. Det går också att nyttja olika typer av belysning i samma syfte. Genom att anpassa terrängen runt ett objekt går det att styra person- och trafikrörelsemönster, exempelvis genom tydligt markerade och avgränsade gångbanor samt fordonshinder. Denna typ av åtgärder gör det enklare att upptäcka personer vars beteende eller körväg avviker från det normala och som kan vara tecken på att denne är på väg att initiera en antagonistisk handling.

Bebyggelseinriktad brottsprevention kan också användas för att förtydliga ytor, exempelvis genom att sätta upp ett yttre staket som markerar gränser och som i kombination med skyltar upplyser om att det krävs särskild behörighet för att vistas där. Sådana åtgärder kan försvåra för en antagonist som försöker rekognosera och i vissa fall möjliggöra exempelvis kontroll av personens identitet och vad denne bär med sig.

Se avsnitt 9 Skyddsobjekt och skyddslagen.

Bebyggelseinriktad brottsprevention kan också ha positiva effekter för verksamhetens övriga skyddsbehov, så kallat verksamhetsskydd, eller för att öka den upplevda tryggheten hos personalen. Även om det i fråga om kvalificerade och målinriktade antagonister är svårt att bedöma åtgärders avskräckande effekt kan det vara möjligt att avskräcka mer vardagliga brott såsom stölder ur fordon och skadegörelse på byggnader.

4.7 Kompensatoriska insatser

I det fall en säkerhetsskyddsåtgärd fallerar eller de identifierade säkerhetshoten hastigt ökar uppstår en eller flera sårbarheter som behöver hanteras för att bibehålla en tillfredställande nivå av säkerhetsskydd. Detta kan ske genom olika former av insatser där säkerhetsskyddsåtgärder av mer tillfällig art vidtas för att temporärt ersätta den funktion som försvunnit eller för att förstärka den fysiska säkerheten. Exempel på sådana säkerhetsskyddsåtgärder är att placera ut en vakt om en kamera går sönder eller att förstärka med tillfälliga skydd mot forcering med fordon vid identifiering av nya säkerhetshot som inbegriper detta men som inte tagits höjd för vid dimensioneringen av fysisk säkerhet. Det kan även handla om insatser såsom att tillfälligt stänga ner eller flytta verksamhet till säkrare lokaler. För att kompensatoriska insatser ska fungera i praktiken bör de så långt det är möjligt och rimligt vara analyserade och förberedda, exempelvis genom instruktioner och avtal som gör det möjligt att avropa extra bevakningspersonal.

Exempel på en kompensatorisk insats är att använda personell bevakning om en kamera går sönder.

4.8 Redundans och diversitet i den fysiska säkerheten

Det finns vissa säkerhetsskyddsåtgärder som är av så central betydelse för den fysiska säkerheten att de inte får fallera ens kortvarigt och som i vissa fall inte heller går att ersätta med kompensatoriska åtgärder. I dessa fall krävs redundans i form av på förhand vidtagna åtgärder för att upprätthålla en funktion, exempelvis separat kraftförsörjning till ett passersystem eller en larmcentral. Det är viktigt att analysera vilka beroenden och gemensamma nämnare som finns bland redundansåtgärderna. Ett exempel på detta är ifall el från såväl batteribackup som reservkraftverk leds genom samma kabel eller en gemensam elcentral. I så fall kan ett sabotage mot någon av dessa punkter slå ut kraftförsörjningen.

Redundansen kan med fördel byggas upp av diversifierade åtgärder som har liten risk att drabbas av samma fel, exempelvis ett batteri som redundant kraftförsörjning i stället för elnätet eller larmkommunikation via mobilnät som redundans för fiber. Andra exempel är att använda övervakningskameror från olika tillverkare eller att inte uppdatera alla kameror samtidigt ifall det finns oupptäckta sårbarheter i mjukvarorna. Utöver att öka driftsäkerheten kan diversifierade åtgärder genom den variation de erbjuder även göra det svårare för en antagonist att planera och genomföra ett angrepp.

Exempel på diversitet är att använda övervakningskameror från olika tillverkare eller att inte uppdatera alla kameror samtidigt ifall det finns oupptäckta sårbarheter i mjukvarorna.

4.9 Fysiska säkerhetsskyddsåtgärder mot insiderhot

Fysisk säkerhet kan också bidra till att förebygga insiderhot. Bland annat kan lökprincipen och styrning av tillträde vara en del i de förebyggande åtgärderna mot insiderhot. Till exempel kan ett lager närmast ett skyddsvärde ha upptäckande funktioner och det innersta utrymmet vara uppdelat med låsta förvaringsenheter för varje användare. Andra exempel på åtgärder är extra kontroller vid tillträde till särskilt skyddsvärda utrymmen och system som kräver att två personer närvarar med var sitt passerkort. Utöver detta är det också möjligt att använda larm som upptäcker sabotage och manipulation av delar i den fysiska säkerheten.

5 Upptäckande säkerhetsskyddsåtgärder

Upptäcka | Försvåra | Hantera

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

Verksamhetsutövare ska, utifrån identifierade säkerhetshot och, om Säkerhetspolisen tillhandahållit en sådan, beskrivningen av dimensionerande antagonistiska förmågor, använda personell bevakning, teknisk bevakning eller en kombination av dessa för att upptäcka obehörigt tillträde eller skadlig inverkan.

Upptäckt kan beskrivas som en kedjereaktion av detektion, överföring och verifiering. För att tillförlitlig upptäckt ska ske måste alla dessa delar, det vill säga detektion, överföring och verifiering, fungera. Det är viktigt att upptäcka obehörigt tillträde och försök till skadlig inverkan i tid, gärna så tidigt som möjligt, så att fördröjande säkerhetsskyddsåtgärder kan bidra till att fördröja en antagonist under tiden hanterande säkerhetsskyddsåtgärder vidtas.

Notera:
Delar som är kritiska för tillgängligheten av upptäckande funktioner, exempelvis strömförsörjning till tekniska övervakningssystem, behöver också skyddas.

I sin enklaste form kan upptäckande säkerhetsskyddsåtgärder bestå av stationär personell bevakning som både detekterar och omedelbart verifierar vad som har hänt. Ofta används dock en kombination av personell bevakning och teknisk övervakning för upptäckt. Till exempel kan upptäckt ske med tekniska system som reagerar och larmar vid rörelse, ljud av krossat glas eller liknande. Larmet kan sedan överföras via en kommunikationskanal till en bevakningscentral, där personalen med hjälp av kameror verifierar larmorsaken.

Upptäckt – en kedjereaktion av detektion, överföring och verifiering.

Detektion

Detektion kan till exempel ske med någon form av sensor i ett larmsystem eller av en närvarande person

Överföring

Överföring kan till exempel ske med teleförbindelse eller radioanrop till en larmcentral

Verifiering

Verifiering kan till exempel ske med kameror uppkopplade till en larmcentral eller genom att skicka personal till platsen

5.1 Personell bevakning

Personell bevakning syftar till att upptäcka obehörigt tillträde eller skadlig inverkan och i förlängningen leda till att hanterande säkerhetsskyddsåtgärder vidtas. Vid personell bevakning kan kedjereaktionen för upptäckt ske på kort tid eftersom en och samma person så gott som momentant kan detektera och verifiera exempelvis ett obehörigt tillträde. Personell bevakning kan bestå av personal som utför fast bevakning vid ingångar och entréer, eller som patrullerar med oförutsägbara mönster. Personell bevakning som en upptäckande säkerhetsskyddsåtgärd är mest effektiv i kombination med teknisk övervakning, mycket beroende på mänskliga faktorer såsom trötthet och förmågan att upprätthålla koncentrationen under långa perioder.

Personell bevakning kan även användas för att övervaka en utomstående person som ska få tillträde till säkerhetskänslig verksamhet, exempelvis en extern reparatör eller en intern tekniker som normalt inte arbetar i en säkerhetskänslig del av verksamheten. Här är det viktigt att klargöra ledsagarens roll i de fall det krävs särskild kompetens för att övervaka vad personen gör. Detta i syfte att kontrollera att personen inte bara befinner sig på rätt plats utan även endast utför det arbete som är avsett. Särskilt viktigt blir detta vid arbeten i informationssystem, och personell bevakning behöver alltså inte nödvändigtvis utföras av bevakningspersonal såsom väktare och skyddsvakter.

5.2 Teknisk bevakning

Teknisk bevakning syftar, på samma sätt som personell bevakning, till att upptäcka obehörigt tillträde eller skadlig inverkan för att i förlängningen leda till att hanterande säkerhetsskyddsåtgärder vidtas. I Säkerhetspolisens vägledningar delas teknisk bevakning upp i kategorierna yttre larm, inre larm och objektslarm. Andra indelningar förekommer, exempelvis baserat på olika larms tekniska principer eller egenskaper.

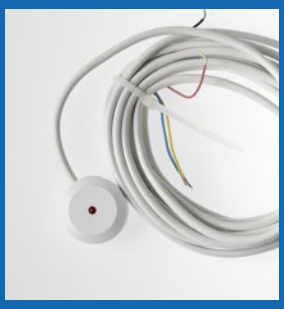
Säkerhetspolisen har valt att följa det ”utifrån och in”-perspektiv som används vid utvärdering av den fysiska säkerheten.

Se avsnitt avsnitt 8.1 Angreppsanalys.

Yttre larm består av bevakning av omgivningar, till exempel ett staket som utgör gräns för en anläggning, så kallat perimeterlarm, eller ytan och luftrummet runtomkring, så kallat områdeslarm. Detta kan

Olika typer av teknisk bevakning:

Yttre larm:
Staketlarm, Marklarm, Mikrovågssensor, Aktiv infraröd sensor



Inre larm:
Glaskrossensor, Magnetkontakt, Passiv infraröd sensor

Objektslarm:
Tryckplatta, Tiltsensor, Vibrationssensor

exempelvis göras med sensorer som, något förenklat, reagerar på vibrationer i staketet eller mikrovågssensorer som reagerar på rörelse inom ett område. Inre larm är sådana som bevakar omslutningsytor samt inre volymer och strukturer, exempelvis en byggnads ytterväggar och glasrutor respektive rum och innerdörrar. Detta kan exempelvis göras med sensorer som reagerar när någon rör sig genom en rumsvolym eller på att en dörr öppnas. Objektslarm är övervakning av en specifik sak, till exempel en förvaringsenhet som försetts med vibrationssensor och tiltsensor som känner av om ett objekt utsätts för yttre påverkan, flyttas eller lutas.

Vid val av larmsensorer är det viktigt att känna till att alla har sina egna styrkor och svagheter kopplade till principerna för respektive typ av upptäckande funktion. Ett staketlarm kan till exempel reagera på att vilda djur vidrör staketet och behöver i så fall anpassas för att reducera antalet oönskade larm. Exempelvis kan två staket användas, där det yttersta inte har någon larmsensor utan fungerar som en barriär. Detsamma gäller andra larmsensorer. Exempelvis kan en passiv infraröd sensor vara känslig för förändringar i värmestrålning från föremål medan en mikrovågssensor kan reagera på vattenytor som sätts i rörelse.

5.2.1 Kamerabevakning

§ *Kamerabevakningslagen (2018:1200)*

Teknisk bevakning med hjälp av kameror, så kallad kamerabevakning, ger ökade möjligheter att bevaka undanskymda eller viktiga platser, grindar samt inpasseringsställen som saknar personell bevakning. I vissa fall kan det krävas tillstånd till kamerabevakning av en plats dit allmänheten har tillträde. Det kan även ställas andra krav i samband med kamerabevakning, exempelvis på korrekt behandling av personuppgifter. Korrekt behandling av personuppgifter krävs även i andra fall, exempelvis i passersystem, men i fråga om kamerabevakning kan det vara komplicerat att anonymisera bilder och videofilmer. Kamerabevakning kan därför kräva noggranna överväganden av såväl tekniska lösningar som rutiner för exempelvis hantering av inspelat materiel.

Kamerabevakning spelar en viktig roll när det gäller att verifiera larm och utreda händelser i efterhand. Kamerabevakning av larmade områden, byggnader, anläggningar, lokaler och objekt är ett utmärkt komplement till övriga upptäckande funktioner och kan motverka onödiga insatser i händelse av oönskade larm, men kan också utgöra stöd i samband med hantering av ett utlöst skarpt larm.

För att uppnå tillfredställande kamerabevakning är det viktigt att varje kameras syfte tydliggörs, så att kameran utrustas för att klara av det som respektive kamera syftar till. Det är till exempel skillnad på en kamera som ska användas för att upptäcka personer på ett inhägnat område, verifiera om en dörr öppnats med nyckel eller brutits upp, eller kontrollera identiteten på en person vid en fjärrmanövrerad dörr. Som nämnts ovan kan kamerabevakningens utformning påverka behovet av tillstånd och behandling av personuppgifter. Det är alltså inte alltid den lösning som ger bäst bildkvalitet och längst lagring som passar bäst för den specifika situationen, utan en bedömning måste göras från fall till fall.

Kamerabevakning i syfte att upptäcka obehörigt tillträde ställer höga krav på kamerabevakningssystemet, ljusmiljön och inte minst kameraoperatören. Forskning på området visar att mänskliga faktorer som bland annat trötthet och bristande koncentrationsförmåga utgör stora begränsningar när det gäller att upptäcka händelser på en skärm. Intelligent videoanalys (IVA) kan därför vara ett komplement som utökar den upptäckande förmågan hos en kameraoperatör. IVA kan beskrivas som en mjukvara som utgör ett stöd åt kameraoperatörer genom att uppmärksamma förutbestämda incidenter, till exempel ett obehörigt tillträde genom ett staket. Utvecklingen inom kamerabevakning går mycket snabbt och särskilt inom IVA där produkter som i varierande grad använder sig av maskininlärning eller så kallade artificiell intelligens tillkommer fortlöpande.

Notera:
Värmekameror, som fångar bilder på infraröd strålning, kan vara ett bra komplement till övriga upptäckande säkerhetsskyddsåtgärder. Värmekameror kan många gånger undantas från tillståndsplikten, men bedömning görs av Integritetsskyddsmyndigheten i varje enskilt fall.

5.3 Upptäcktsfaktor

Det finns ingen upptäckande säkerhetsskyddsåtgärd som är helt tillförlitlig i alla lägen och i alla miljöer. Såväl åtgärder inom personell bevakning och teknisk bevakning har sina respektive styrkor som svagheter. Trötthet och felriktad uppmärksamhet är exempel på sådant som kan påverka en stationär vakts upptäckandeförmåga och leda till lägre grad av tillförlitlighet. Likaså kommer en larmsensor inte kunna kalibreras till att alltid upptäcka en person – oavsett om denne springer, går eller kryper förbi – utan att medföra många obefogade larm från exempelvis djur och väderstörningar. För att undvika alltför många obefogade larm måste istället en lägre känslighet väljas.

Då tillförlitligheten varierar mellan upptäckande säkerhetsskyddsåtgärder finns ett behov av att kunna jämföra dem med varandra och i olika kombinationer. Upptäcktsfaktor (F_U) är en variabel mellan 0 och 1 som visar på tillförlitligheten och där en högre upptäcktsfaktor innebär högre tillförlitlighet att upptäcka ett obehörigt tillträde. Upptäcktsfaktorn för respektive upptäckande säkerhetsskyddsåtgärd bestäms genom försök och beräknas genom att dividera antalet lyckade upptäckter med antalet försök.

Beräkning av upptäcktsfaktor

Upptäcktsfaktorn beräknas genom att dividera antalet lyckade upptäckter med antalet försök enligt formeln nedan.

Exempelvis skulle 8 upptäckter på 10 försök ge en upptäcktsfaktor på 0.8.

$$F_U = \frac{\text{Antal upptäckter}}{\text{Antal försök}}$$

För att resultatet ska bli rättvisande är det viktigt att försöken genomförs på ett realistiskt sätt, exempelvis genom att en testperson försöker smyga förbi rörelsesensorer eller håller sig i skuggorna för att undvika upptäckt av ett system för kamerabevakning med intelligent videoanalys. Helst ska varje upptäckande säkerhetsskyddsåtgärd testas var för sig men i en större verksamhet kan detta bli för tidskrävande och behöva ersättas med stickprov på ett representativt urval. Verksamhetsutövaren bör då beakta om det finns skillnader i rumsvolymer, ålder på teknik, nersmutsningsgrad och omgivningsmiljön med olika typer av störkällor eller liknande som kan påverka resultatet. Exempel på detta är om vibrationssensorer används på olika platser i en byggnad där vissa utrymmen angränsar till en starkt trafikerad väg. Vibrationssensorerna behöver då ställas in med olika känslighet för att inte orsaka obefogade larm vilket påverkar tillförlitligheten och därmed också urvalet av vilka sensorer som bör testas.

Även om upptäcktsfaktorn för en enskild upptäckande säkerhetsskyddsåtgärd kan vara låg, kan kombinationen av flera upptäckande säkerhetsskyddsåtgärder innebära att den totala upptäcktsfaktorn blir högre.

Den totala upptäcktsfaktorn

Den total upptäcktsfaktorn beräknas med formeln nedan som kan utökas med godtyckligt antal (n) upptäckande säkerhetsskyddsåtgärder.

$$F_U \text{ total} = 1 - \{(1 - F_{U1}) \times (1 - F_{U2}) \times \ldots \times (1 - F_{Un})\}$$

Exempel

En passiv infraröd larmsensor (PIR) med $F_U = 0.7$ och en magnetkontakt (MK) med $F_U = 0.85$. Totala upptäcktsfaktorn blir vid denna kombination 0.95.

1 –	(1 – F_U PIR)	×	(1 – F_U MK)	= Total F_U
1 –	(1 – 0.7)	×	(1 – 0.85)	= Total F_U
1 –	(0.3)	×	(0.15)	= 0.955
				F_U 0.95

För att formeln för kombinationer ska vara giltig måste den logiska beslutsregeln i ett larmsystem vara att det räcker med reaktion från någon av larmsensorerna. Om kombinationen i stället görs så att det krävs rektion från flera larmsensorer kommer den totala upptäcktsfaktorn att sjunka. Detta blir tydligt i exemplet ovan med kombinationen av en PIR och en magnetkontakt. Multiplikationsprincipen ger att den totala upptäcktsfaktorn i detta scenario blir 0,7 x 0,95 = 0,665, det vill säga lägre. Dessutom kommer, ifall exempelvis PIR:en är skymd eller magnetkontakten trasig, en antagonist att kunna passera utan upptäckt eftersom det krävs att båda larmsensorerna reagerar. Fördelen med en logisk

beslutsregel som baseras på reaktion från flera larmsensorer kan vara att minska mängden obefogade larm, exempelvis att reaktion från en vibrationssensor på en förvaringsenhet måste föregås av reaktion från en PIR som övervakar rumsvolymen för att undvika obefogade larm orsakade av vibrationer från närliggande trafik. Detta måste dock vägas mot möjligheten att en antagonist kan ta sig fram till förvaringsenheten utan att passera genom rummet, exempelvis genom golvet.

Upptäcktsfaktorn är användbar på många sätt, både i processen för utformning av fysisk säkerhet och för kontroll av redan existerande lösningar. Upptäcktsfaktorn kan användas för att jämföra tillförlitligheten hos larmsensorer av olika fabrikat eller som använder olika detektionsprinciper för att hitta den mest kostnadseffektiva lösningen. Den kan även användas vid kravställning eller kontroll och uppföljning av att den upptäckande förmågan inte försämras över tid. Att i förväg testa och dokumentera upptäcktsfaktorn ger ett bra utgångsläge för val av kompensatoriska åtgärder, exempelvis om utrustning går sönder. Beräkning av den totala upptäcktsfaktorn för en kombination av upptäckande säkerhetsskyddsåtgärder kan även användas för att få en balanserad förmåga till upptäckt längs olika angreppsvägar in mot ett skyddsvärde.

Notera
Även om upptäcktsfaktorn i teorin inte kan vara 1 kan det i praktiken vara lämpligt att avrunda till det beroende på antal lyckade försök och behovet av noggrannhet i beräkningarna. Det är sällan praktiskt meningsfullt att räkna med mer än två decimaler.

6 Försvårande säkerhetsskyddsåtgärder

Verksamhetsutövare ska, utifrån identifierade säkerhetshot och, om Säkerhetspolisen tillhandahållit en sådan, beskrivningen av dimensionerande antagonistiska förmågor vidta försvårande åtgärder i syfte att fördröja obehörigt tillträde så länge som krävs för att hanterande åtgärder ska hinna vidtas och i andra fall reducera skadlig inverkan.

6.1 Fördröjande säkerhetsskyddsåtgärder

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

Fördröjande säkerhetsskyddsåtgärder syftar till att fördröja ett obehörigt tillträde tillräckligt länge för att hanterande säkerhetsskyddsåtgärder ska hinna avbryta eller reducera konsekvenserna av angreppet.

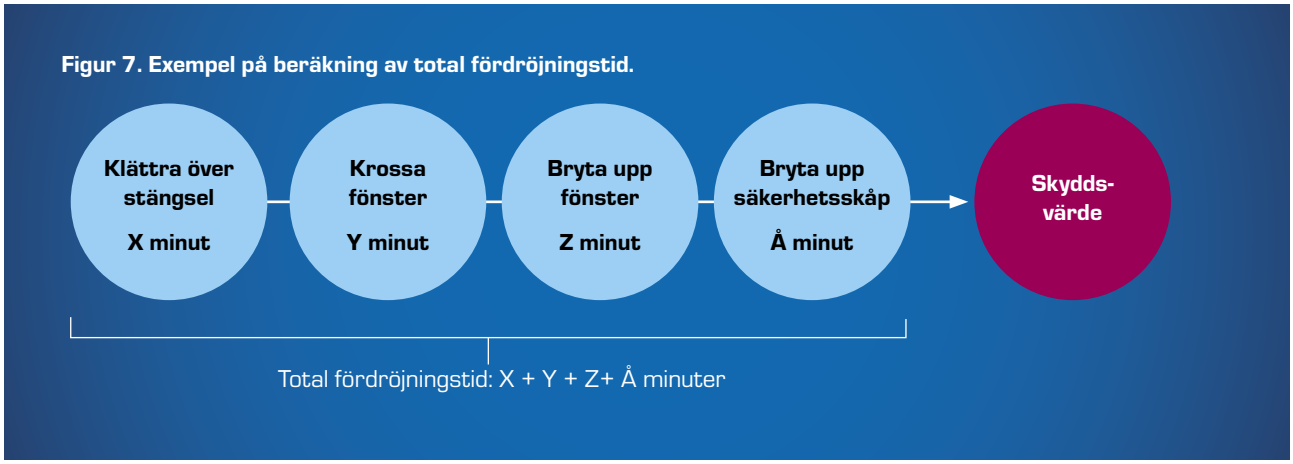
6.1.1 Mekaniskt inbrottsskydd

Fördröjande säkerhetsskyddsåtgärder inom fysisk säkerhet omfattar ofta, men är inte begränsat till, mekaniskt inbrottsskydd. Mekaniskt inbrottsskydd syftar till att fördröja obehörigt tillträde och består till exempel av:

- stängsel och andra typer av inhägnader,
- rotations- och gånggrindar samt passeringsslussar,
- inkrypningsskydd och galler,
- tak, golv, väggar, fönster, luckor, dörrar och portar,
- låsenheter och
- förvaringsenheter

När det gäller mekaniskt inbrottsskydd måste hela omslutningsytan beaktas för att säkerställa balans i den fysiska säkerheten. Det räcker alltså inte med att ett utrymme har en kraftig säkerhetsdörr för att det mekaniska inbrottsskyddet ska vara tillfredställande, utan även tak, väggar, fönster, luckor och andra delar i omslutningsytan måste utformas på sådant sätt att de bidrar till en fördröjning som motsvarar dörrens.

Utöver mekaniskt inbrottsskydd kan fördröjande säkerhetsskyddsåtgärder även bestå av avstånd och naturliga hinder som till exempel vatten eller svårgenomtränglig vegetation. Även aktiva säkerhetsskyddsåtgärder som att mörklägga ett utrymme eller använda dimgeneratorer och störande blixtljus kan ha viss fördröjande effekt.



6.1.2 Fördröjningstid

Fördröjningstid (T_F) är ett mått på hur verkansfull en försvårande säkerhetsskyddsåtgärd är och mäts i den tid det tar för en antagonist att forcera eller på annat sätt övervinna denna.

Fördröjningstid (T_F)
T_F beräknas genom formeln nedan,
där T2 är tiden då angreppet har slutförts
och T1 är tiden då angreppet initieras.
T_F = T2 – T1

Varje typ av fördröjande säkerhetsskyddsåtgärd har en egen T_F. Den totala T_F för den fysiska säkerheten kan beräknas som summan av fördröjningstiden för varje del i det mekaniska inbrottsskyddet längs en angreppsväg, räknat utifrån var det obehöriga tillträdet påbörjas (Figur 7).

En fördröjande säkerhetsskyddsåtgärd som inte kombineras med föregående säkerhetsskyddsåtgärder för upptäckt ger i teorin ett begränsat, om ens något, bidrag till den fysiska säkerheten. Ett exempel på detta är ett fönster med en sensor som reagerar på krossat glas och där det finns ett galler som utgör mekaniskt inbrottsskydd (Figur 8).

I det fall gallret är monterat på utsidan av fönstret kan en antagonist angripa detta ostört utan att upptäckas, vilket gör att gallrets T_F inte kan tillgodoräknas vid kontroll och utvärdering av den fysiska säkerheten. Om gallret däremot är monterat på insidan kommer larmet att aktiveras innan forcering av gallret kan påbörjas, eftersom antagonisten behöver krossa glaset först. Det innebär att gallret bidrar till den totala T_F för den fysiska säkerheten.

Den totala T_F beräknas från den punkt i den fysiska säkerheten där ett obehörigt tillträde upptäcks. Ett obehörigt tillträde som påbörjas och upptäcks djupt inne i en byggnad, till exempel egen personal som utan behörighet tar sig in i en datahall i en central del av byggnaden, kommer vanligen innebära att T_F blir betydligt kortare än om det obehöriga tillträdet påbörjas och upptäcks utanför byggnaden. En förutsättning i båda fallen är alltså att det finns upptäckande förmågor vid datahallen respektive utanför byggnaden, utan upptäckande förmåga blir T_F = noll oavsett var antagonisten startar ifrån.

Andra faktorer som påverkar T_F är en antagonists verktyg, kunskaper och färdigheter. En säkerhetsdörr som fördröjer ett angrepp med en kofot i fem minuter kan ha en betydligt kortare T_F mot ett angrepp av en kvalificerad antagonist som till exempel använder en bensindriven motorkap.

Figur 8.
Två situationer med ett fönster som är larmat så att upptäckt sker när glaset krossas. Om gallret är monterat på utsidan bidrar detta mycket lite till den fysiska säkerheten eftersom antagonisten kan arbeta ostört och ta lång tid på sig. Om gallret däremot är monterat på insidan så bidrar det mer till den fördröjande förmågan eftersom antagonisten måste slutföra uppgiften innan hanterande åtgärder hinner vidtas.

6.1.3 Förvaringsutrymmen

§ *5 kap. 10 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

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

§ *4 kap. 11 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

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

Verksamhetsutövare ska fatta beslut om vilka förvaringsutrymmen som är godkända för förvaring av vissa föremål när dessa inte är under kontroll. De föremål som avses är sådana kort, nycklar och anteckningar om kod som var för sig ger åtkomst till platser där säkerhetskänslig verksamhet bedrivs.

+ *Se avsnitt 6.2.7 Kort, nycklar och koder.*

Godkända förvaringsutrymmen krävs även för säkerhetsskyddsklassificerade handlingar (om dessa inte skyddas av godkända kryptografiska funktioner) samt anteckningar med uppgift om lösenord som ger tillgång till informationssystem som är av betydelse för säkerhetskänslig verksamhet.

+ *Se Vägledning i säkerhetsskydd – Informationssäkerhet.*

Med att ett föremål är under kontroll menas att det omedelbart kan upptäckas om en obehörig försöker komma åt det, exempelvis ett passerkort som användaren ständigt bär med sig och ofta använder eller en säkerhetsskyddsklassificerad handling som förvaras i en väska som är under uppsikt.

Begreppet förvaringsutrymme är inte tydligt definierat utan det är upp till verksamhetsutövare att avgöra var de fysiska gränserna går. Det kan exempelvis vara någon form av mindre enskild förvaringsenhet, såsom säkerhetsskåp, eller ett helt rum, till exempel en arkivlokal. Precis som för fysisk säkerhet i övrigt behöver därför verksamhetsutövare analysera och besluta hur förvaring ska ske i förhållande till identifierade säkerhetshot och, om Säkerhetspolisen tillhandahållit en sådan, beskrivningen av dimensionerande antagonistiska förmågor.

Det funktionsbaserade synsättet medför att endast förvaringsutrymmen som är försedda med eller omges av tillräckliga åtgärder för att upptäcka, försvåra och hantera obehörigt tillträde får godkännas. Det innebär samtidigt att verksamhetsutövare har en stor frihet att välja de förvaringsutrymmen och rutiner för användning av dessa som passar bäst i det aktuella fallet. Förvaringsutrymmen kan alltså komma att skilja sig åt, både inom och mellan verksamheter, beroende på vilka förutsättningar som råder och skyddsvärdets art.

Exempel:
En verksamhetsutövare beslutar efter analys att säkerhetsskyddsklassificerade handlingar som hanteras i särskilt anpassade och behörighetsstyrda projektrum kan förvaras i mappsystem medan det i cellkontor med gipsväggar krävs individuella förvaringsenheter i form av säkerhetsskåp. De huvudnycklar som ger tillträde till samtliga rum kräver en ännu högre nivå av fysisk säkerhet. Det beslutas därför att de ska förvaras i ett elektroniskt nyckelskåp i den ständigt bemannade bevakningscentralen och med särskilda rutiner för användning.

Observera att det i fråga om förvaringsutrymmen för säkerhetsskyddsklassificerade handlingar i säkerhetsskyddsklassen kvalificerat hemligt gäller att beslutet om godkännande ska fattas av verksamhetsutövarens högsta chef eller motsvarande organ eller den som beslutsrätten delegerats till. Detta är i linje med andra bestämmelser som gäller för dessa handlingar, exempelvis beslut om huruvida de får kopieras eller medföras från verksamhetsutövarens lokaler.

Förvaringsutrymmen i form av enskilda förvaringsenheter såsom säkerhetsskåp som är certifierade och provade enligt Stöldskyddsföreningens norm SSF 3492 är vanligt förekommande och kan vara en lämplig utgångspunkt då dessa ger ett skydd mot mycket grundläggande antagonistiska förmågor. De kan därmed ofta anses tillräckliga för att säkerställa att personer som gemensamt är behöriga till en lokal inte obehörigen och utan upptäckt kan komma åt varandras individuella handlingar samtidigt som de ger ett visst skydd mot antagonister som kommer utifrån. Men, i likhet med val av dörrar, väggar och andra omslutningsytor måste beslutet grunda sig i en analys baserad på identifierade säkerhetshot och eventuell beskrivning av dimensionerande antagonistiska förmågor. Utan denna analys kan skyddet komma att bli underdimensionerat. Exempelvis kan ett säkerhetsskåp fördröja en antagonist med låg förmåga under lång tid medan samma säkerhetsskåp endast klarar av att motstå ett angrepp av en antagonist med hög förmåga under någon enstaka minut. Ett säkerhetsskåp är som standard inte heller försett med teknisk bevakning utan måste kompletteras med eller omgärdas av exempelvis vibrationssensorer respektive passiva infraröda sensorer för att skapa en upptäckande förmåga.

Exempel:
En verksamhetsutövare beslutar efter analys att flyttbara säkerhetsskåp certifierade enligt Stöldskyddsföreningens norm SSF 3492 ger ett tillräckligt skydd för en viss typ av förvaring i verksamhetens kontorsbyggnad. Men, till övriga byggnader på området finns körbara vägar och bevakningspersonalens hanteringstid är längre. Därför beslutas att dessa lokaler ska vara larmade och att säkerhetsskåpen ska vara fast förankrade i golv och vägg i syfte att förebygga att en antagonist kan ta dem med sig för att sedan öppna på annan plats.

I de fall då innehållet i ett förvaringsutrymme är skyddsvärt ur ett tillgänglighetsperspektiv bör även brandskyddet för det aktuella förvaringsutrymmet analyseras samtidigt som skydd mot obehörigt tillträde. Brandskydd är ofta frivilligt att pröva när enskilda förvaringsenheter i form av säkerhetsskåp och liknande certifieras enligt vanligt förekommande standarder, även om det finns undantag. I de fall brandskydd provas är det dock ofta med avseende på olyckor och bränder där den eventuella avsikten inte är att skada förvaringsenhetens innehåll. Det kan alltså i praktiken vara nödvändigt med en kombinationslösning där obehörigt tillträde förebyggs genom förvaringsenheter som placeras i ett rum som i sin tur förses med brandskydd för att förebygga skadlig inverkan genom anlagd brand.

När det gäller skydd mot brand måste även lokalernas brandbelastning, räddningstjänstens insatstid och skyddsvärdets fysiska egenskaper beaktas, exempelvis om det är fråga om en pappershandling med säkerhetsskyddsklassificerade uppgifter eller datamedia. Vidare är det inte bara tid och temperatur som avgör skyddet mot brand, utan även om en förvaringsenhet exempelvis ska klara av att falla igenom ett bjälklag eller tåla ras ovanifrån.

6.2 Styrning av tillträde och hantering av olämpliga föremål

Styrning av tillträde kan kortfattat beskrivas som en samling beslut och åtgärder för att reglera vem som vistas inom en säkerhetskänslig verksamhet, under vilka förutsättningar samt att säkerställa detta. Syftet är att endast behöriga ska få tillträde till områden, byggnader, anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs. Det kan även röra platser eller utrymmen inom dessa ifall den säkerhetskänsliga verksamheten till exempel endast bedrivs i vissa delar av en byggnad. Styrning av tillträde syftar även till att förebygga att de behöriga som ges tillträde inte medför föremål som är olämpliga från säkerhetssynpunkt.

Behovet av styrning av tillträde kan vara mer eller mindre omfattande. Ibland räcker det med särskilda rutiner för utomstående och i andra fall kan det behövas omfattande styrning även av den egna personalen. Exempelvis kan det behövas regler för vad som inte får medföras till vissa utrymmen, såsom mobiltelefoner, smarta klockor, verktyg eller farliga ämnen. Vidare kan det krävas särskild utbildning för att få tillträde. Härutöver kan behovet och lösningarna för att styra tillträdet variera, exempelvis genom användning av fysiska nycklar, manuella kontroller eller elektroniska passersystem med biometri.

Följande avsnitt i vägledningen har ett exempel bestående av åtta delar som bör läsas i tur och ordning.

6.2.1 Behörighetstilldelning

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

Grunden för styrning av tillträde är de beslut som avgör vem som får vistas ”var, när och hur”. Dessa beslut kallas även behörighetstilldelning och syftar till att i förlängningen på individnivå reglera vem som får tillträde till en viss plats (var), vid vilken tidpunkt/tillfälle (när) och under vilka eventuella andra särskilda förutsättningar (hur). Avgörande för en adekvat behörighetstilldelning är en fullödig säkerhetsskyddsanalys med tydligt identifierade skyddsvärden, en sammanhållen fysisk säkerhet med exempelvis sektionering samt personalsäkerhetsåtgärder såsom förteckning över befattningar med krav på säkerhetsprövning och identifierade utbildningsbehov.

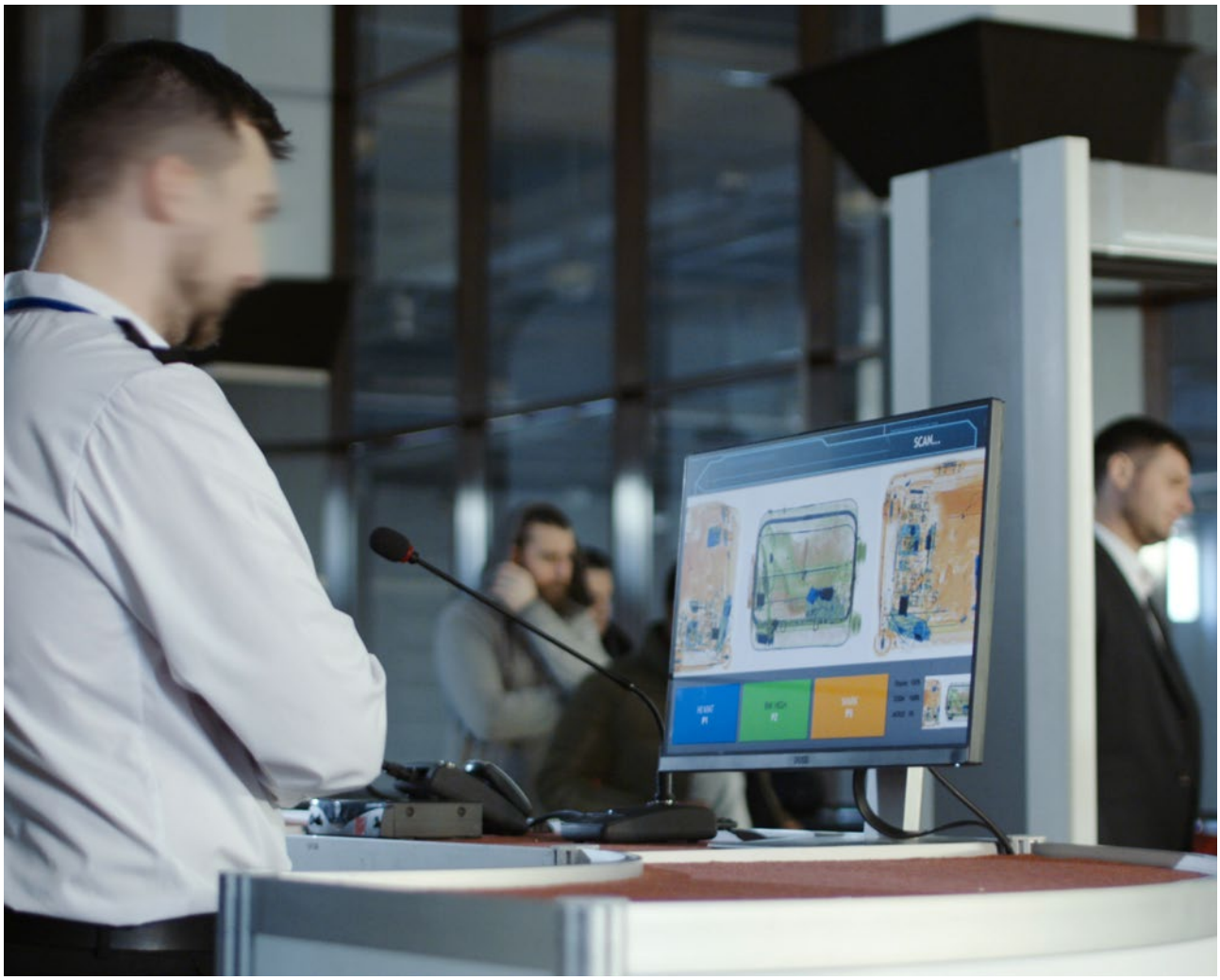
+ *Se Vägledning i säkerhetsskydd – Personalsäkerhet.*

Säkerhetsskyddsanalysen ska innehålla de skyddsvärden som behöver skyddas med fysiska säkerhetsskyddsåtgärder, exempelvis säkerhetsskyddsklassificerade handlingar eller informationssystem som behöver vara tillgängliga. Det kan även vara fråga om exempelvis säkerhetsskyddsklassificerade uppgifter som förmedlas genom samtal eller bildvisning.

Se avsnitt 6.3.6 Skydd mot obehörig avlyssning av samtal.

Ju tydligare skyddsvärdena är identifierade, desto lättare blir det att avgöra på vilka platser de finns och hur behörighetstilldelningen ska kunna göras på bästa sätt. De platser (var) som behörighetstilldelningen gäller kan alltså vara både hela eller delar av områden, byggnader eller andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs. I praktiken tilldelas ofta flera nivåer av behörighet, exempelvis till gemensamma ytor, verksamhetsspecifika utrymmen och enskilda arbetsrum.

Den fysiska säkerheten och övriga säkerhetsskyddsåtgärder kan både vara givna förutsättningar och variabler i fråga om behörighetstilldelning. Förutsättningar som exempelvis en byggnads konstruktion kan hämma möjligheterna till sektionering medan vilka metoder som används för autentisering i informationssystem kan vara enklare att ändra, vilket i sin tur kan påverka behovet av att styra tillträdet. Tilldelningen av högre eller lägre behörigheter kan även påverka personalsäkerheten och vilket behov av utbildning om särskilda rutiner med mera som krävs samt behovet av säkerhetsprövning. Vid behörighetstilldelning måste därför beaktas det grundläggande kravet på att en anställning eller deltagande endast får placeras i säkerhetsklass om behovet av säkerhetsskydd inte kan tillgodoses på ett annat sätt, såsom genom sektionering. Det blir i fråga om behörighetstilldelning tydligt hur de tre säkerhetsskyddsåtgärderna informationssäkerhet, fysisk säkerhet och personalsäkerhet påverkar varandra.



Det är därför av flera skäl lämpligt att beakta behörighetstilldelning i ett tidigt skede vid utformning av den fysiska säkerheten medan det finns möjlighet att hypotetiskt testa och välja mellan olika lösningar.

Målet för behörighetstilldelning bör vara att så få personer som möjligt ges tillträde till de säkerhetskänsliga delarna av verksamheten och att de inte heller ges större tillträde än nödvändigt. Det kan därför vara lämpligt att exempelvis inte bara reglera vilka platser (var) de behöriga får tillträde till utan också vid vilka tidpunkter eller tillfällen (när). Stor försiktighet bör iakttas med omfattande behörigheter, till exempel sådana som gäller "överallt och närsomhelst", som ibland tilldelas utryckningsväktare och fastighetsjour. Dessa bör endast användas mycket restriktivt och under särskilda förutsättningar, exempelvis i kombination med åtgärder som förebygger användning av tvång eller att till exempel nycklar, kort etc. stjäls eller kopieras som antagonistiskt tillvägagångssätt. Det kan även behövas att de befattningar som verkligen behöver tilldelas behörigheten inplaceras i en högre säkerhetsklass.

Exempel, del 1:
En verksamhetsutövare beslutar att det för behörighet till en ledningscentral (var) krävs att personen antingen är anställd och ska tjänstgöra där eller är entreprenör och ska utföra ett särskilt påkallat arbete (när). Biometriska uppgifter om de personer som är aktuella läggs in i ett elektroniskt passersystem.

Utöver att bestämma vem som får vistas var och när inom en säkerhetskänslig verksamhet kan det efter analys behövas beslut om vilka andra förutsättningar (hur) som ska vara uppfyllda för att tillträdet ska vara behörigt. Det kan exempelvis röra särskilda regler för tillträde såsom krav på särskild utbildning, beslut av högre chef eller att minst två personer närvarar. Dessa beslut om hur tillträde ska ske kommer i slutändan att påverka utformningen av de åtgärder som ska säkerställa att endast behöriga får tillträde och i vissa fall även beröra de beslut och åtgärder som krävs för hantering av föremål som är olämpliga från säkerhetsskyddssynpunkt. Om exempelvis två personer måste närvara för att öppna ett förvaringsutrymme med stora mängder säkerhetsskyddsklassificerade uppgifter kan de ömsesidigt kontrollera varandras identitet och behörighet. Om det istället beslutas att det räcker med en person kan det kanske krävas att passersystemet förses med funktioner för kontroll av biometri för att uppnå samma nivå av fysisk säkerhet. Det är därför, precis som i fråga om behörighetstilldelning i övrigt, lämpligt att beakta detta i ett tidigt skede vid utformning av fysisk säkerhet.

Se avsnitt 6.2.5 Hantering av föremål som är olämpliga från säkerhetsskyddssynpunkt.

Exempel, del 2:
Verksamhetsutövaren beslutar även att alla som vistas i ledningscentralen ska ha genomgått en särskild utbildning som ska förnyas årligen. Information om vilka som genomgått utbildningen läggs även in i passersystemet tillsammans med ett sista datum för repetitionsutbildning. För entreprenörerna krävs dessutom att arbetet ska vara beslutat av fastighetschefen, som då även utfärdar ett skriftligt tillstånd som ska medföras.

6.2.2 Behörighetskontroll

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

Åtgärder för kontroll av personers identitet och behörighet, även kallat behörighetskontroll, syftar till att säkerhetsställa att personer som ska beviljas tillträde är samma som tilldelats behörighet och att denna behörighet i sin tur gäller för den aktuella platsen samt att eventuella övriga förutsättningar är uppfyllda. Det kan också avse att fastställa att de som beviljats tillträde även lämnar platsen eller att inget otillåtet förs ut från den säkerhetskänsliga verksamheten.

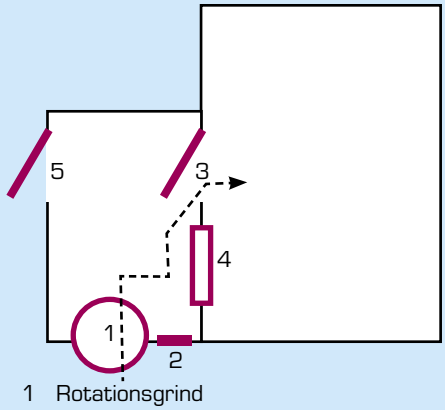
Behörighetskontroll kan med andra ord beskrivas som den praktiska implementeringen av de beslut som behandlas i avsnitten ovan. Platsen i fråga kan avse hela eller delar av områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs. I praktiken genomförs ofta flera behörighetskontroller av varierande grad i en verksamhet, exempelvis först vid entré, sedan vid inpasseering till våningsplan och slutligen till enskilt arbetsrum. Dokumentation från behörighetskontroller kan vara till stor hjälp vid utredning av exempelvis vem som haft tillträde till ett utrymme som lämnats olåst eller för att i efterhand utreda ett händelseförlopp.

Grunden för behörighetskontroll brukar beskrivas som att identitet och behörighet kan styrkas på ett eller flera av tre sätt: något en person har, vet eller är. Något personen "har" kan exempelvis vara en nyckel eller passerkort och något personen "vet" ett lösenord eller pin-kod till ett passerkort. Något personen "är" relaterar till personen som sådan och avser ofta någon form av biometrisk uppgift som kan kontrolleras, exempelvis fingeravtryck, irismönster eller ansiktsform.

Behörighetskontroll kan göras på många olika sätt och verksamhetsutövare är fria att själva analysera och besluta om den lösning som passar bäst i förhållande till de identifierade säkerhetshot, dimensionerande antagonistiska förmågor och förutsättningar i övrigt som gäller för den aktuella verksamheten. Exempelvis kan det i en mindre lokal med få personer som arbetar tillsammans räcka med att en person har nyckel och släpper in övriga medan det i en större och mer komplex verksamhet kan krävas ett elektroniskt passersystem. Det kan vidare vara fråga om att med bevakningspersonal manuellt kontrollera legitimationer eller tillstånd att utföra arbeten som gäller för den aktuella platsen. Behörighetskontroll kan även i vissa fall påverka de beslut och åtgärder som krävs för hantering av föremål som är olämpliga från säkerhetsskyddssynpunkt.

+ *Se avsnitt 6.2.5 Hantering av föremål som är olämpliga från säkerhetsskyddssynpunkt.*

Exempel, del 3:
Inpassering till ledningscentralen sker genom en slussfunktion. Först genom en rotationsgrind som säkerställer enpersonpassage in i slussen. Därefter kontrollerar någon i ledningscentralen genom glasrutan att personen antingen ska tjänstgöra eller har ett tillstånd från fastighetschefen och öppnar inifrån.



1 Rotationsgrind
2 Passersystem
3 Säkerhetsdörr
4 Glasruta
5 Reservdörr

6.2.3 Passersystem

Med passersystem avses ofta ett elektroniskt system som används för styrning av tillträde och då främst behörighetskontroll. Passersystem används för att styra, identifiera och registrera personers åtkomst till utrymmen och platser där säkerhetsskyddsklassificerade uppgifter finns eller där säkerhetskänslig verksamhet i övrigt bedrivs. Syftet med passersystem är att förebygga obehörigt tillträde, men de kan också användas för att fortlöpande granska vem som haft tillträde till utrymmen samt i efterhand utreda händelseförlopp.

Utformningen av passersystem behöver ställas i relation till övriga säkerhetsskyddsåtgärder. Det är exempelvis ingen större mening med ett avancerat passersystem om den fysiska säkerhetsskyddsåtgärden i övrigt består av en obevakad spärr som går att hoppa över. Avgörande för utformningen av passersystem är behovet av att identifiera och tillåta behöriga att passera, men även andra funktioner kan vara viktiga, exempelvis om systemet ska registrera antal passager och om behörigheter snabbt ska kunna ändras. Passersystem är därför i många fall integrerade med andra system i en byggnad, exempelvis larmsystem, kameraövervakning, annan säkerhetsövervakning eller behörighetsstyrning av informationssystem.

Den idag vanligaste formen av passersystem är elektroniska lås anslutna till en behörighetsdatabas, där den som ska passera använder kort eller nyckelbricka i kombination med en personlig kod. Denna form av system ger en registrerad passage och behörigheterna är enkla att uppdatera, men systemet ger å andra sidan en inte särskilt tillförlitlig identifiering av vem som passerar eftersom både kort och kod går att kopiera eller tvinga till sig. I det fall verksamheten kräver en högre skyddsnivå kan passersystem exempelvis förses med biometriska läsare eller logik som kräver att två personer tillsammans måste öppna passagen till utrymmet eller kompletteras med exempelvis identifiering genom kameror kopplade till en bevakningscentral.

Notera:
Ett passersystem kan med fördel kombineras med upptäckande säkerhetsskyddsåtgärder, exempelvis automatisk eftersökning av explosivämnen och radioaktivitet vid in- och utpassering som hindrar passage och sänder en larmsignal ifall detektorerna reagerar.

Exempel, del 4:
Rotationsgrinden till slussen in till ledningscentralen aktiveras av det elektroniska passersystemet som genom biometri identifierar personen och verifierar att det inte gått för lång tid sedan denne gick den särskilda utbildning som krävs för att vara behörig.

6.2.4 Andra sätt att systematiskt styra tillträde

Utöver passersystem finns andra sätt att systematiskt styra tillträde, exempelvis mekaniska lås i kombination med loggbok för nyckelkvittering eller manuell kontroll och registring med hjälp av bevakningspersonal. Det finns även mer utvecklade varianter där en fysisk nyckel och elektronisk nyckelbricka kombinerats till vad som ibland kallas digitalt låssystem. Den tekniska utvecklingen har gjort att det idag finns en uppsjö av variationer och benämningar, men grundsyftet är fortfarande detsamma: att styra, identifiera och registrera personers åtkomst till säkerhetskänslig verksamhet. Oavsett vilken typ av passersystem eller lösning som används bör både inpassering och utpassering registreras på ett sådant sätt att det möjliggör uppföljning och kontroll av tillträdet i efterhand.

Även om passersystem är det vanligaste sättet att styra tillträde finns ofta ett parallellt system med vanliga fysiska nyckar och låscylindrar som alternativ ifall det elektroniska passersystemet slutar fungera. Det är då viktigt att även detta system utformas att vara lika säkert som det ordinarie passersystemet och ställs i relation till övriga säkerhetsskyddsåtgärder. Det

kan exempelvis krävas att nycklar till det alternativa systemet hanteras enligt särskilda rutiner för att inte en antagonist genom ett enkelt inbrott ska kunna komma åt huvudnycklar.

Se avsnitt 6.1.3 Förvaringsutrymmen.

Exempel, del 5:
Inne i ledningscentralen finns en nyckel till ett mekaniskt lås på en reservdörr vid sidan om rotationsgrinden in till slussen. Detta för att kunna släppa in personer om passersystemet slutar fungera eller för att ta in gods som inte får plats i rotationsgrinden. Användning av nyckeln dokumenteras i en loggbok.

6.2.5 Hantering av föremål som är olämpliga från säkerhetsskyddssynpunkt

5 kap. 7 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd

Vilka föremål som är olämpliga från säkerhetsskyddssynpunkt varierar beroende på vilka skyddsvärden som finns i verksamheten. Det kan exempelvis gälla verktyg, vapen och andra föremål som kan användas för att orsaka skada på den säkerhetskänsliga verksamheten eller kameror och flyttbara lagringsmedium som kan användas för att kopiera säkerhetsskyddsklassificerade uppgifter. Vilka föremål som är olämpliga är därför i stort upp till verksamhetsutövare att analysera och besluta om utifrån de förutsättningar som råder i den aktuella verksamheten. Både identifierade säkerhetshot, eventuell beskrivning av dimensionerande antagonistiska förmågor och redan vidtagna samt i förlängningen planerade säkerhetsskyddsåtgärder kan alltså påverka vilka föremål som ska anses olämpliga.

Det finns dock ett uttryckligt förbud mot elektronisk utrustning som kan möjliggöra obehörig avlyssning vid samtal som behandlar säkerhetsskyddsklassificerade uppgifter varför vanliga mobiltelefoner, smartklockor, trådlösa hörlurar, kamerautrustning och bärbara datorer i regel bör anses olämpliga oavsett var samtalet sker. Personlig utrustning såsom elektroniska hörapparater kan också möjliggöra obehörig avlyssning och kräver särskilda överväganden och hantering.

För mer information om elektronisk utrustning se Vägledning i säkerhetsskydd – Avlyssningsskyddade utrymmen.

Förbudet mot att medföra elektronisk utrustning är nära förknippat med de krav som ställs på utrymmen som används för regelbundna samtal där säkerhetsskyddsklassificerade uppgifter avhandlas.

Se avsnitt 6.3.6 Skydd mot obehörig avlyssning av samtal.

Om ett samtal sker i ett utrymme kan exempelvis rumsinstallationer såsom konferensteknik och teleslingor vara problematiska, även om det i strikt mening inte är fråga om elektronisk utrustning som medförts till samtalet. Vid behov av sådan teknik kan det dock, enligt kraven för själva utrymmet, krävas specialanpassning som omöjliggör avlyssning. Kravbilderna för samtal och utrymmen bör därför analyseras tillsammans och sättas i relation till de dimensionerande antagonistiska förmågor som gäller för verksamheten.

Verksamhetsutövare ska ha rutiner för att säkerställa att olämpliga föremål inte förs till eller inom områden, byggnader och anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs. Även dessa rutiner är det upp till verksamhetsutövare att besluta om, och utformningen kan skilja sig åt beroende på exempelvis andra säkerhetsskyddsåtgärder, behov och legala förutsättningar. Hos en verksamhetsutövare kan det exempelvis behövas kontroll av väskor och försändelser vid inpassering och godsmottagning medan det hos en annan kan räcka med rutiner för vissa särskilda delar av anläggningen.

Åtgärderna och rutinerna för kontroll av föremål behöver inte vara påtvingade och integritetskänsliga, såsom kroppsvisitationer eller genomsökning av väskor. Det kan även vara fråga om exempelvis tydlig skyltning om mobiltelefonförbud. Om exempelvis två personer ska diskutera säkerhetsskyddsklassificerade uppgifter så är en grundförutsättning att båda är behöriga till uppgifterna, och därmed minskar behovet av påtvingad kontroll. Det kan då kanske istället räcka med att personerna innan samtalet påminner varandra om att lägga undan eventuell elektronisk utrustning de burit med sig. Motsvarande rutiner för kontroller av olämpliga föremål finns även i andra säkerhetssammanhang, exempelvis inom forskning, industrier och verksamheter med känslig utrustning eller som hanterar brandfarliga och explosiva varor. Det kan då finnas synergieffekter av att samordna rutiner, utbildning, skyltning av utrymmen etc.

Exempel, del 6:
Verksamhetsutövaren beslutar att det i ledningscentralen inte får förekomma någon utomstående elektronisk utrustning eller föremål som kan användas för att orsaka skadlig inverkan. Eventuella verktyg och kemikalier som entreprenörer behöver ska bedömas, godkännas och registreras vid utfärdandet av tillstånd för det aktuella arbetet. Innan de som befinner sig i ledningscentralen släpper in personen som väntar i slussen ställs kontrollfrågor om de bär med sig någon elektronisk utrustning samt kontrolleras att de inte för med sig några föremål som inte finns med i tillståndet.

6.2.6 Besökstillstånd

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

När personer som i vanliga fall inte har tillträde till områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs ska besöka sådana platser ska skriftligt besökstillstånd utfärdas.

För besökare behövs rutiner på samma sätt som för styrning av tillträde i övrigt. Dessa rutiner kan exempelvis gälla identifiering och praktisk hantering av själva besöket, såsom krav på legitimering med godkänd id-handling och inskrivning i en förteckning med ankomsttid, uppgift om vilken verksamhet denna representerar samt vem som tar emot och vilket ansvar denne besöksmottagare har.

Besökare som har medgivits tillträde bör också förses med besökskort som ska bäras väl synligt och som återkrävs efter besöket. Besökskorten bör på ett tydligt sätt skilja sig från den egna personalens tjänstekort, som också bör bäras väl synliga när den egna personalen befinner sig inom verksamhetsutövarens områden, byggnader, anläggningar eller objekt.

Utformningen av tjänstekort och besökskort kan skilja sig åt både inom verksamheten och mellan verksamhetsutövare. Varje verksamhetsutövare får själv analysera för- och nackdelar med att exempelvis skriva ut namn och personuppgifter, användning av fotografi eller att exempelvis förse korten med funktionalitet för passersystem. Om besökaren är återkommande och hela tiden ledsagas är det kanske inte nödvändigt att skriva ut dennes namn (som kan vara olämpligt att skriva ut av andra skäl). Istället kan det räcka med en ”blank” besöksbricka vars enda syfte är att uppmärksamma andra anställda på att personen i fråga är besökare.

Observera att en besökare kan vara, men inte nödvändigtvis är, att anse som deltagare i den säkerhetskänsliga verksamheten. Att någon är att anse som besökare beror på om personen i vanliga fall har tillträde till platsen och om denne därmed omfattas av de ordinarie åtgärderna för styrning av tillträde. En besökare kan exempelvis vara en anställd som besöker ett annat kontor men vars nyckelbricka inte aktiverats för den aktuella platsen och istället släpps in av en kollega. Personen har alltså både tilldelats behörighet och fått denna kontrollerad men registreras inte som normalt i passersystemet varför istället ett besökstillstånd utfärdas för att möjliggöra uppföljning och kontroll. En besökare kan exempelvis även vara någon från en annan verksamhetsutövare som det finns ett säkerhetsskyddsavtal med eller någon som deltar i en utbildning där det förekommer säkerhetsskyddsklassificerade uppgifter. Denna typ av besökare är deltagare i den säkerhetskänsliga verksamheten och ska vara säkerhetsprövade.

Alla besökare är dock inte att anse som deltagare i den säkerhetskänsliga verksamheten och får inte heller

Figur 9. Exempel på kategorispecifika besökskort som skiljer sig mot en verksamhetsutövares egna tjänstekort.

alltid tillträde till en plats där säkerhetskänslig verksamhet bedrivs. Många verksamhetsutövare har en skyldighet att erbjuda service till allmänheten och dessa besökare har i vissa fall rätt att vara anonyma. Om en verksamhetsutövare exempelvis anordnat så besökarna hålls avskilda från den säkerhetskänsliga verksamheten med en reception eller servicedisk, behövs inget besökstillstånd. Bestämmelsen om besökstillstånd gäller för besökare ”till eller inom” anläggningar etc. Detta möjliggör för verksamhetsutövare att analysera och definiera vilka platser som avses på eller i områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs. I vissa fall kan det vara så att besökstillstånd krävs redan vid fastighetsgränsen, i andra fall endast vid besök till vissa utrymmen.

Beroende på vilka säkerhetsskyddsåtgärder som vidtagits och andra omständigheter som råder kan det i praktiken ofta finnas besökare som utgör ett mellanting mellan deltagare som ska vara säkerhetsprövad och sådana som kan beviljas anonymt tillträde. Om exempelvis en entreprenör ska få tillträde till en plats där det bedrivs säkerhetskänslig verksamhet men hela tiden ledsagas så att denne inte kan ta del av säkerhetsskyddsklassificerade uppgifter och inte heller kan orsaka skada på verksamheten så är denne inte deltagare. Men, eftersom personen inte heller omfattas av de ordinarie åtgärderna för styrning av tillträde till platsen kan det krävas ett besökstillstånd för att möjliggöra uppföljning och kontroll. Styrning av tillträde för besökare kan vara mångsidigt och behöver analyseras inom ramarna för både fysisk säkerhet och personalsäkerhet eftersom åtgärder inom det ena området kan påverka det andra. Ju tydligare analyserna är gjorda, desto enklare blir det att skapa rutiner och implementera åtgärderna.

Exempel, del 7:
En skada på en modul i ledningscentralen behöver åtgärdas akut. Felet är av sådan art att ordinarie anställda inte kan åtgärda det och personen som besitter kompetensen saknar den särskilda utbildningen som krävs för behörighetstilldelning. Istället stängs ledningscentralen ner tillfälligt och utrustning samt kartor som inte ska exponeras för obehöriga täcks över. Personen som ska utföra reparationen tilldelas ett besökstillstånd, släpps in genom reservdörren vid sidan om rotationsgrinden (utan biometrisk identifiering och registrering i passersystemet) och ledsagas under hela arbetet så att denne inte kan ta del av säkerhetsskyddsklassificerade uppgifter eller orsaka annan skada. Besöks- och arbetstillstånd dokumenteras enligt rutinerna och tillträdet registreras i loggboken för tillträde med nyckel.

6.2.7 Kort, nycklar och koder

§ *5 kap. 5 och 6 §§ Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

§ *2 kap. 15 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Verksamhetsutövare ska säkerställa att kort, nycklar och anteckningar om kod som var för sig ger åtkomst till områden, byggnader och andra anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs är under kontroll eller förvaras i ett godkänt förvaringsutrymme.

+ *Se avsnitt 6.1.3 Förvaringsutrymmen.*

Syftet är att säkerställa att exempelvis reservnycklar och liknande varken kan försvinna utan att det upptäcks eller förvaras på ett sådant sätt att de omgärdas av lägre nivå av fysisk säkerhet än de ordinarie nycklar, kort, nyckelbrickor etc. som används i ett passersystem. Det kan även vara fråga om kort som inte kräver pin-kod eller omvänt koder till kodlås på till exempel dörrar och enskilda förvaringsenheter som inte kräver användning av ett kort. Även sådana måste förvaras på betryggande sätt.

Till kort, nycklar och anteckningar om kod som var för sig ger åtkomst bör även, om inga andra säkerhetsskyddsåtgärder vidtagits, räknas exempelvis kort till nyanställda och som ännu inte tagits i bruk och som därför förvaras tillsammans med pin-kod eller har förinställda koder som är enkla att gissa eller följer ett givet mönster. Detsamma gäller för så kallade vakt- eller fastighetskort som används för rondering, larmutryckning, fastighetsjour etc. och som ofta har pin-kod antecknad på en fastsatt bricka eller använder en gemensam kod för flera kort.

Notera:
Undvik enkla sifferkombinationer, telefonnummer, personnummer, årtal över historiska händelser eller liknande vid val av kod, då dessa kan vara lätta att gissa sig till.

Om det befaras att kort, nycklar, koder eller liknande har stulits, förlorats eller kopierats ska detta hanteras som en säkerhetshotande händelse. Detta gäller oavsett om den aktuella komponenten bara förvaras eller är i bruk. Det gäller även oavsett om komponenten i sig är tillräcklig för att ge åtkomst, till exempel en nyckel, eller om det krävs en kombination av exempelvis kort och pin-kod.

Hur skyndsamt hanteringen behöver ske och vilka åtgärder som kan krävas för att händelsen inte ska medföra skada för Sveriges säkerhet är upp till verksamhetsutövaren själv att analysera och besluta om i sina rutiner.

Verksamhetsutövare ska ha en förteckning över kort, nycklar, koder och liknande som ger åtkomst till platser där säkerhetskänslig verksamhet bedrivs. Av förteckningen ska det framgå till vem och när de lämnades samt var eventuell reservkod eller reservnyckel förvaras. Det ska vidare framgå om och i så fall när återlämnande skett. Syftet med förteckningen är att även den praktiska implementeringen av behörighetstilldelning ska ske på ett systematiskt sätt och möjliggöra uppföljning och kontroll.

Exempel, del 8:
Verksamhetsutövaren överväger olika alternativ för hantering av den nyckel som kan användas för att öppna reservdörren vid sidan om rotationsgrinden in till slussen. Bedömningen görs att genom att förvara nyckeln inne i ledningscentralen så omgärdas den av en högre nivå av fysisk säkerhet än utrymmet som den ger åtkomst till (slussen). Uthämtning av nyckeln dokumenteras i loggboken.

Se exempel del 5.

6.3 Skadereducerande säkerhetsskyddsåtgärder

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

Skadereducerande säkerhetsskyddsåtgärder syftar till att minska skadeverkningarna av antagonistiska handlingar som sker hastigt, på distans eller som av annan anledning inte går att upptäcka och fördröja tills de hanterande säkerhetsskyddsåtgärderna kan hindra förloppet. Sådana åtgärder kan till exempel vara att förhindra forcering med fordon, reducera skadan av ett angrepp med kemiska eller biologiska ämnen, skydd mot avsiktliga elektromagnetiska hot eller skapa skyddsavstånd samt att använda byggnadstekniska förstärkningar för att minimera verkan av splitter eller stötvågseffekter och förhindra fortskridande ras.

Skadereducerande säkerhetsskyddsåtgärder ska även förebygga att någon med eller utan tekniska hjälpmedel obehörigen får insyn i den säkerhetskänsliga verksamheten. Dessa typer av säkerhetsskyddsåtgärder består av bland annat nyttjandet av avlyssningsskyddade utrymmen, skydd mot obehörig insyn och avbildning samt skydd mot inhämtning av röjande signaler.

Skadereducerande säkerhetsskyddsåtgärder är precis som fysisk säkerhet i övrigt starkt kopplat till säkerhetsskyddsanalysen med identifierade säkerhetshot och, om Säkerhetspolisen tillhandahållit en sådan, beskrivningen av dimensionerande antagonistiska förmågor. Olika typer av fordonshinder, till exempel pollare, är konstruerade för att kunna motstå olika typer av påkörningar utifrån fordonens vikt, höjd, hastighet och anslagsvinkel. Även byggnadstekniska förstärkningar såsom skydd mot explosioner måste anpassas utifrån vilken totalvikt av explosivämnen de ska klara av att skydda mot.

6.3.1 Skydd mot forcering med fordon

Skydd mot forcering med fordon handlar om att reducera hastigheter och hindra obehöriga fordon från att ta sig in på platser där säkerhetskänslig verksamhet bedrivs. På så sätt skapas ett avstånd mellan säkerhetshotet och aktuella skyddsvärden, och därmed kan skador undvikas eller begränsas. Genom att sänka hastigheten kan man minska ett fordons rörelseenergi och därmed den skada fordonet kan orsaka.

För att skydda mot forcering med fordon kan säkerhetskyddssåtgärder i form av stoppande hinder användas, exempelvis murar, pollare eller naturliga hinder. Det finns även hastighetsreducerande säkerhetsskyddsåtgärder såsom chikaner och spikmattor. De flesta verksamheter behöver åtminstone tillfälligtvis tillåta någon form av fordonstrafik för att transportera gods eller personal. I dessa fall kan behovet lösas genom exempelvis omlastning till intern logistik med kontroll av fordon och förare. Oavsett hur skyddet utformas är det viktigt att även beakta framkomligheten för räddningstjänst och ambulans vid nödlägen såsom brand och olycksfall.

6.3.2 Skydd mot farliga ämnen (CBRN)

Skydd mot farliga ämnen och hantering av situationer med sådana brukar i säkerhetsskyddsammanhang delas in kategorierna kemiska, biologiska och radioaktiva. Ibland används uttrycket ”radiologiska” för att även inkludera situationer med till exempel apparater som genererar joniserande strålning på annat vis än med radioaktiva ämnen. I såväl svenska som internationella sammanhang kallas ofta farliga ämnen för ”CBRN” där bokstäverna står för motsvarande kategorier på engelska, det vill säga chemical, biological och radioactive/radiological. Bokstaven N åsyftar primärt situationer med och skydd mot nukleära vapen (nuclear) som ofta, men inte alltid eller enbart, resulterar i spridning av radioaktiva ämnen som kan påverka verksamheten. Nukleära vapen kan exempelvis även medföra elektromagnetiska pulser vilka kan orsaka skador på informationssystem. Skydd mot verkningar av radiologiska eller nukleära vapen ingår inte i denna vägledning. Ibland används förkortningen CBRN med tilläggsbokstaven E på slutet som då åsyftar explosivämnen (explosive). Skydd mot explosioner är dock i många avseenden annorlunda än skydd mot farliga ämnen och avhandlas därför separat.

+ *Se avsnitt 6.3.3 Skydd mot explosioner.*

Om den fysiska säkerheten ska klara av att skydda mot angrepp med farliga ämnen kräver detta noggrann analys och val bland de olika typer av säkerhetsskyddsåtgärder som kan vidtas. Till exempel kan kontroll av inkommande post och gods behövas för att upptäcka försändelser med farliga ämnen.

+ *Se avsnitt 6.2.5 Hantering av föremål som är olämpliga från säkerhetsskyddssynpunkt.*

Ytterligare exempel på säkerhetsskyddsåtgärder mot farliga ämnen är att sektionera lufttillförsel, anordna automatisk nedstängning av ventilation vid detektion och att nyttja filter vid luftintag för att förhindra spridning av giftiga gaser, biologiska smittämnen eller liknande.

6.3.3 Skydd mot explosioner

Ett stort antal parametrar inverkar på hur skydd mot explosioner ska utformas, särskilt om det behövs skydd mot en explosion inne i exempelvis en byggnad. Samtliga aspekter gällande stötvåg, värme och splitter

behöver tas i beaktande vid utformandet av skadereducerande säkerhetsskyddsåtgärder mot explosioner. I vissa fall kan byggnadstekniska förstärkningar vara en framkomlig väg men skydd mot explosioner handlar många gånger om att skapa avstånd till laddningen. Avståndet som krävs från laddningen beror på typen av explosivämne och laddningens storlek som ofta anges som TNT-ekvivalent vilket är ett jämförelsemått för den energimängd som frigörs i explosioner. Energin räknas om till motsvarande vikt TNT för att möjliggöra jämförelser av stötvågor mellan laddningar av olika explosivämnen.

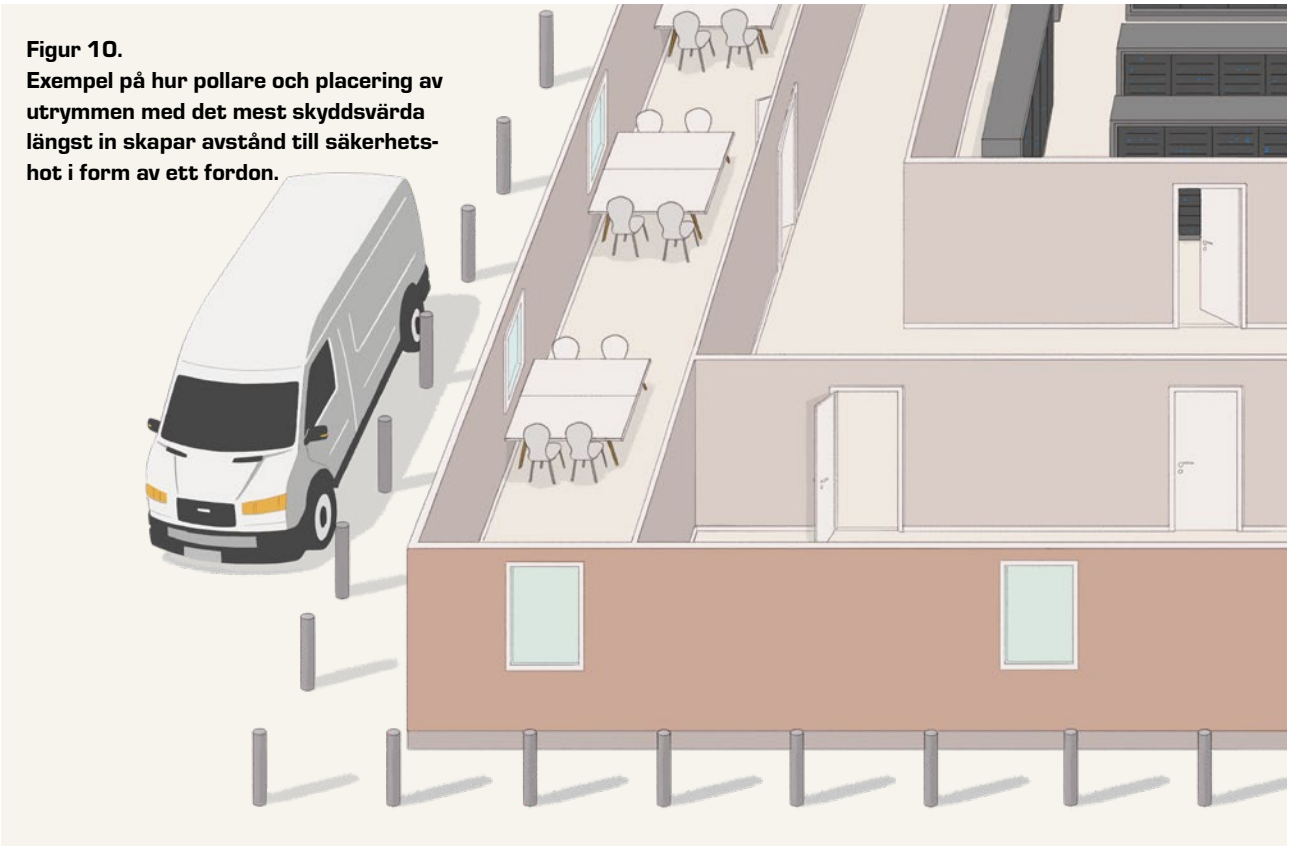
Figur 10 illustrerar två olika exempel på hur det går att skapa avstånd till en laddning, dels genom att placera skyddsvärden så centralt som möjligt i en byggnad, dels genom nyttjandet av pollare för att skapa ytterligare avstånd mellan en fordonsburen laddning och yttervägg.

6.3.4 Skydd mot avsiktliga elektromagnetiska hot

Avsiktliga elektromagnetiska hot kan beskrivas som generering av skadlig elektromagnetisk energi i syfte att införa brus eller signaler som har tillräckligt hög nivå för att störa eller skada elektriska och elektroniska system. Skydd mot avsiktliga elektromagnetiska hot kan bland annat bestå av att skydda elektriska ledare med transientskydd och filter, genom att skapa avstånd från säkerhetshotet eller att avskärma skyddsvärda system från elektromagnetiska signaler.

6.3.5 Skydd mot obemannade luftfartyg (drönare)

Skydd mot obemannade luftfartyg, ofta kallade ”drönare”, kan utformas på motsvarande sätt som den fysiska säkerheten i övrigt med upptäckande, försvårande och hanterande förmågor. Detta då drönare främst används som plattformar för andra säkerhetshot, exempelvis att leverera explosiv last eller få insyn genom bildupptagning. Ifall en verksamhet behöver skyddas mot drönare som bär på explosiv last kan samma metoder användas som vid skydd mot fordonsburna laddningar, bland annat att skapa barriärer eller skyddsavstånd. Behöver verksamheten istället skyddas mot drönare med bildupptagningsförmåga kan istället metoder för skydd mot obehörig insyn tillämpas såsom olika former av insynsskydd. Den stora skillnaden gentemot markbundna säkerhetshot är att ett mer tredimensionellt tankesätt måste tillämpas vid utformningen av den fysiska säkerheten eftersom drönare verkar i luftrummet.



Figur 10.
Exempel på hur pollare och placering av utrymmen med det mest skyddsvärda längst in skapar avstånd till säkerhetshot i form av ett fordon.

Drönare är ett komplext och relativt nytt säkerhetshot. Det är därmed också föränderligt och det finns såväl tekniska som juridiska begränsningar i möjligheten att vidta hanterande säkerhetsskyddsåtgärder, som att använda störsändare eller på andra sätt stoppa fortsatt flygning. Även om de senaste åren inneburit en snabb utveckling av skydd mot drönare är byggnadstekniska förstärkningar fortfarande några av de mest effektiva skydden idag. Detta kan komma att ändras allteftersom lagar anpassas och metoder för att upptäcka och hantera drönare utvecklas.

Drönare kallas ibland även för UAV (förkortning av den engelska benämningen unmanned aerial vehicle) och de kompletta drönarsystemen med all kringutrustning för UAS (förkortning av den engelska benämningen unmanned aerial systems). Säkerhetspolisen har dock för enkelhets skull valt att i denna vägledning använda den mer vardagliga benämningen drönare. Men även den mer korrekta benämningen obemannade luftfartyg förkommer frekvent i andra sammanhang och så även de engelska beteckningarna varför dessa inkluderas i vägledningen för att ge ökad sökbarhet.

6.3.6 Skydd mot obehörig avlyssning av samtal

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

Obehörig avlyssning inkluderar både att obehörigen i realtid lyssna på eller vidarebefordra ett samtal och att spela in det. Obehörig avlyssning kan ske med eller utan tekniska hjälpmedel för återgivning av ljud. Ett sätt att skapa ett skydd mot obehörig avlyssning är att använda särskilda avlyssningsskyddade utrymmen (även kallade ASK-utrymmen).

+ *För mer information om avlyssningsskyddade utrymmen, se Vägledning i säkerhetsskydd – Avlyssningsskyddade utrymmen.*

Verksamhetsutövare ska fatta beslut om vilka utrymmen som är godkända för regelbundna samtal som behandlar säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre. Observera att detta avser själva utrymmet medan det i fråga om hantering av föremål som är olämpliga från säkerhetsskyddssynpunkt finns ett generellt förbud mot att medföra elektronisk utrustning som kan möjliggöra obehörig avlyssning oavsett säkerhetsskyddsklass och plats där samtalet förs.

+ *Se avsnitt 6.2.5 Hantering av föremål som är olämpliga från säkerhetsskyddssynpunkt.*

Syftet med bestämmelsen är att skydda mot obehörig avlyssning och därigenom förebygga att de säkerhetsskyddsklassificerade uppgifterna röjs, oavsett om röjandet sker till en antagonist med avsikt att ta del av uppgifterna, exempelvis vid spioneri, eller i andra fall såsom till en annan anställd som inte är behörig till uppgifterna och som arbetar i ett intilliggande utrymme. Den obehöriga avlyssningen kan ske både med och utan tekniska hjälpmedel och ett beslut om att godkänna ett utrymme får därför endast ske om utrymmet är försett med eller omges av åtgärder för att försvåra obehörig avlyssning utifrån identifierade säkerhetshot och, om Säkerhetspolisen tillhandahållit en sådan, beskrivningen av dimensionerande antagonistiska förmågor.

Att endast utrymmen som används för regelbundna samtal behöver godkännas hör ihop med den förutsägbarhet detta innebär i förhållande till vissa antagonistiska förmågor, exempelvis att montera dolda mikrofoner, och den mängd säkerhetsskyddsklassificerade uppgifter en antagonist med hjälp av sådana förmågor skulle kunna ta del av över tid. Att det saknas krav på godkännande av andra platser och utrymmen som endast används tillfälligtvis eller för säkerhetsskyddsklassen begränsat hemlig innebär dock inte att det saknas krav på skydd mot avlyssning i dessa fall. Det är exempelvis inte tillåtet att samtala om säkerhetsskyddsklassificerade uppgifter på en fullsatt buss bara för att det sker tillfälligtvis eller för att det som avhandlas är i säkerhetsskyddsklass begränsat hemlig, på samma sätt som det inte är tillåtet att behandla säkerhetsskyddsklassificerade uppgifter i offentliga miljöer.

Undantaget för tillfälliga utrymmen syftar till att möjliggöra enstaka möten, exempelvis om det av tekniska eller andra skäl inte går att använda ett utrymme. Undantaget för uppgifter i säkerhetsskyddsklass begränsat hemlig korrelerar med att det generellt ställs lägre krav på dokumenterbar systematik i fråga om dessa, exempelvis saknas krav på kvittering och dokumentation av förstöring.

Av beslutet om att godkänna ett utrymme ska, i likhet med vad som gäller för skydd mot obehörig insyn, framgå den högsta säkerhetsskyddsklass för de uppgifter som får avhandlas i utrymmet.

Samtal där säkerhetsskyddsklassificerade uppgifter inte sker i klartext utan istället redan är skyddade med godkända kryptografiska funktioner är undantagna från kraven på skydd mot avlyssning. Om exempelvis en uppgift krypterats på annan plats och därefter förmedlas per telefon behöver samtalet inte skyddas mot obehörig avlyssning på samma sätt som att den krypterade uppgiften hade kunnat skickas med vanligt brev eller e-post. Observera skillnaden gentemot samtal som sker i klartext och krypteras först vid överföringen, till exempel med kryptotelefon. Dessa samtal måste sker i utrymmen som godkänts och skyddats mot obehörig avlyssning enligt detta avsnitt.

Vidare måste beaktas att om uppgiften är utskriven eller på annat sätt medförs i klartext, eller om någon form av kodnyckel, tabell eller liknande används för att skapa koden allteftersom, kan detta i sin tur medföra att samtalet måste ske på en plats som är skyddad från obehörig insyn enligt följande avsnitt.

I praktiken kan skydd mot obehörig avlyssning sammanfalla med skydd mot obehörig insyn, exempelvis i fråga om sektionering, behörighetstilldelning, städrutiner och uppmärkning av utrymmen. Det kan därför vara lämpligt att samordna analyser, säkerhetsskyddsåtgärder och beslut om att godkänna utrymmen för samtal om och behandling av säkerhetsskyddsklassificerade uppgifter.

6.3.7 Skydd mot obehörig insyn

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

Verksamhetsutövare ska fatta beslut om vilka utrymmen som är godkända för regelbunden behandling av säkerhetsskyddsklassificerade uppgifter. Med behandling avses i detta fall i princip allting som går att göra med uppgifterna och oberoende av teknik, exempelvis ordbehandling i ett informationssystem, delgivning genom bildvisning eller hantering av utskrivna säkerhetsskyddsklassificerade handlingar, tryckta kartor etc.

Syftet med bestämmelsen är att skydda mot obehörig insyn och därigenom förebygga att de säkerhetsskyddsklassificerade uppgifterna röjs, oavsett om röjandet sker till en antagonist med avsikt att ta del av uppgifterna, exempelvis vid spioneri, eller i andra fall såsom till en lokalvårdare som rengör whiteboards i ett mötesrum. Den obehöriga insynen kan ske både med och utan tekniska hjälpmedel och ett beslut om att godkänna ett utrymme får därför endast fattas om utrymmet är försett med eller omges av åtgärder för att försvåra obehörig insyn utifrån identifierade säkerhetshot och, om Säkerhetspolisen tillhandahållit en sådan, beskrivningen av dimensionerande antagonistiska förmågor.

Säkerhetsskyddsklassificerade uppgifter som skyddas med godkända kryptografiska funktioner är undantagna på samma sätt som de är undantagna från kravet på godkända förvaringsutrymmen. Detta gäller så länge uppgifterna inte dekrypteras i utrymmet, till exempel genom visning, utskrift eller liknande. Observera dock att exempelvis signalskyddsnycklar som används för att skapa den kryptografiskt skyddade uppgiften behöver skyddas mot obehörig insyn och förvaras i godkända förvaringsutrymmen.

+ *Se avsnitt 6.1.3 Förvaringsutrymmen.*

Att endast utrymmen som används för regelbunden behandling behöver godkännas hör ihop med den förutsägbarhet detta innebär i förhållande till vissa antagonistiska förmågor, exempelvis inmonterade dolda kameror, och den mängd säkerhetsskyddsklassificerade uppgifter en antagonist med hjälp av sådana förmågor skulle kunna ta del av över tid. Att det saknas krav på godkännande av andra platser och utrymmen som endast används tillfälligtvis innebär inte att det saknas krav på skydd mot obehörig insyn i dessa fall. Det är exempelvis inte tillåtet att behandla säkerhetsskyddsklassificerade uppgifter i offentliga miljöer bara för att det sker tillfälligtvis, på samma sätt som det inte är tillåtet att samtala om säkerhetsskyddsklassificerade uppgifter på exempelvis en fullsatt buss. Syftet med undantaget för tillfälliga utrymmen syftar till att möjliggöra enstaka möten, exempelvis om det av tekniska eller andra skäl inte går att använda ett utrymme.

Det finns flera olika sätt att skydda mot att någon obehörig med eller utan tekniska hjälpmedel kan ta del av säkerhetsskyddsklassificerade uppgifter genom exempelvis kameror, kikare eller drönare. Bland annat kan gardiner, film på fönster eller fönsterlösa rum, polariserande filter på skärmar och rutiner för hantering av säkerhetsskyddsklassificerade uppgifter bidra till ett skydd mot insyn. För att skydda mot insyn i interna delar av verksamheten kan även sektionering tillämpas. Verksamhetsutövare är fria att själva analysera och besluta om den lösning som passar bäst i förhållande till de identifierade säkerhetshot, dimensionerande antagonistiska förmågor och förutsättningar i övrigt som gäller för den aktuella verksamheten.

Av beslutet ska, i likhet med vad som gäller för skydd mot obehörig avlyssning, framgå den högsta säkerhetsskyddsklass för de uppgifter som får behandlas i utrymmet. Även i praktiken kan skydd mot obehörig insyn sammanfalla med skydd mot obehörig avlyssning, exempelvis i fråga om sektionering, behörighetstilldelning, städrutiner och uppmärkning av utrymmen. Det kan därför vara lämpligt att samordna analyser, säkerhetsskyddsåtgärder och beslut om att godkänna utrymmen för behandling och samtal om säkerhetsskyddsklassificerade uppgifter.

+ *Se avsnitt 6.3.6 Skydd mot obehörig avlyssning av samtal.*


SKYDDS
VAKT

7 Hanterande säkerhetsskyddsåtgärder

Upptäcka | Försvåra | **Hantera**

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

Verksamhetsutövare ska utifrån identifierade säkerhetshot och, om Säkerhetspolisen tillhandahållit en sådan, beskrivningen av dimensionerande antagonistiska förmågor se till att hanterande säkerhetsskyddsåtgärder kan vidtas i syfte att avbryta obehörigt tillträde eller skadlig inverkan. Åtgärderna ska utgå ifrån säkerhetsskyddsanalysen, med andra ord utifrån vad som ska skyddas och vad den fysiska säkerheten ska klara av att skydda mot.

Den hanteringstid som behövs för att hindra ett obehörigt tillträde eller skadlig inverkan har stor inverkan på behovet av upptäckande och försvårande säkerhetsskyddsåtgärder. Det omvända förhållandet gäller också, men om en verksamhetsutövare är beroende av externa hanterande förmågor, exempelvis polis, kan det finnas mindre möjlighet att påverka hanteringstiden. Vidare måste hanteringsförmågan ställas i relation till de säkerhetshot den fysiska säkerheten ska klara av att skydda mot.

7.1 Hanteringstid

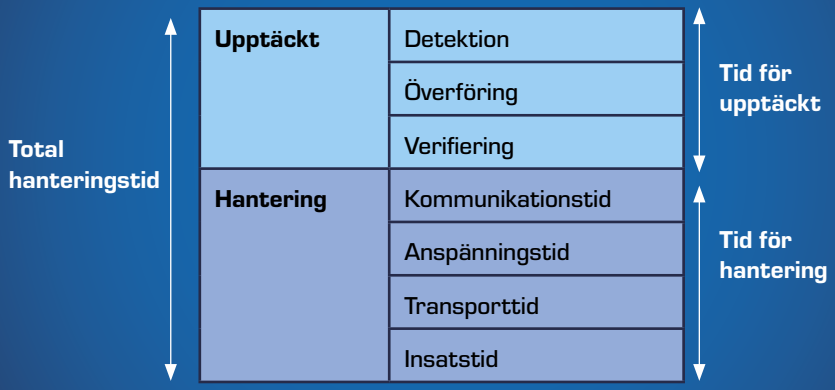
Hanteringstid är den tid som behövs för att initiera och verkställa hanterande säkerhetsskyddsåtgärder i den omfattning som krävs i förhållande till den aktuella händelsen. Total hanteringstid räknas från att en antagonistisk handling upptäcks till dess att den hanterande insatsen ger tillräcklig verkan. Utöver den tid som behövs för den initiala upptäcktskedjan behöver den hanterande förmågan larmas, förbereda insatsen, förflytta sig till platsen och genomföra själva insatsen. Detta kan översättas till kommunikationstid, anspänningstid, transporttid respektive insatstid.

Se Figur 11.

Se avsnitt 5 Upptäckande säkerhetsskyddsåtgärder.

Förmågan att hantera ett angrepp är ofta beroende av externa aktörer, till exempel polis. Hur snabbt hanterande förmågor behöver vara på plats beror i stor utsträckning på hur länge en antagonistisk handling kan fördröjas. Hanteringstiden är således vägledande för utformningen av upptäckande och försvårande åtgärder. Om den upptäckande förmågan utgörs av personell bevakning som även utgör den hanterande förmågan kan den totala hanteringstiden bli mycket kort. Detta eftersom en och samma person så gott som momentant kan detektera och verifiera exempelvis ett obehörigt tillträde samt redan är på plats för att hantera det.

Figur 11. Den totala hanteringstiden består av tiden det tar från första upptäckt till dess att den hanterande insatsen ger tillräcklig verkan.



7.2 Hanteringsförmåga

Den hanterande förmågans kunskaper, utbildning, kommunikationsmöjligheter, utrustning, färdigheter och mandat behöver vara i paritet med en potentiell antagonists och med situationen den förväntas kunna hantera. Det kan exempelvis räcka med grundläggande utbildning och utrustning för att hantera vissa typer av obehörigt tillträde och försök till att störa verksamheten, medan det vid andra tillfällen kan finnas behov av mer kvalificerad förmåga i form av särskilda funktioner inom polisen.

7.3 Olika typer av hantering

Syftet med hanterande säkerhetsskyddsåtgärder är att stoppa en antagonistisk handling eller effekterna av den innan den medför skada för Sveriges säkerhet. Detta kan göras genom att enskilt eller i kombination avbryta handlingen, neutralisera antagonisten och/eller reducera konsekvenserna av handlingen.

Det primära är att på ett eller annat sätt avbryta den antagonistiska handlingen, exempelvis genom att stoppa en antagonist på dennes väg in mot det skyddsvärda eller genom att omhänderta avlyssningsutrustning som placerats i ett utrymme. Om möjligt är det även önskvärt att neutralisera antagonisten så att denne inte kan komma tillbaka och göra ett nytt försök vid ett senare tillfälle. Exempel på neutralisering i dessa fall är att antagonisten grips av polis respektive att identifiera vem som placerat avlyssningsutrustningen och vidta åtgärder mot personen.

I det fall en antagonistisk handling inte går att stoppa fullt ut kan konsekvensreducerande hantering behövas, exempelvis genom att med egen brandstyrka eller extern räddningstjänst släcka en anlagd brand efter att antagonisten neutraliserats. Det kan även vara fråga om hantering som underlättar återgång till ett normalläge, exempelvis genom att stänga av ventilationssystemen för att förhindra större kontaminering vid ett angrepp med farliga ämnen.

8 Utvärdering och kontroll

§ *2 kap. 14 § Säkerhetspolisens föreskrifter (PMFS 2022:1) om säkerhetsskydd*

Utvärdering och kontroll syftar till att bedöma ifall den fysiska säkerheten lever upp till det identifierade säkerhetsskyddsbehovet och ger avsedd effekt. Utvärdering kan exempelvis göras av planerad utformning vid ombyggnationer och regelbundna kontroller av olika slag kan göras för att säkerställa att den befintliga fysiska säkerheten inte försämras över tid. Verksamhetsutövare ska dokumentera de åtgärder som behövs för att omhänderta avvikelser i en plan och använda resultatet av kontroller för att analysera behovet av förändringar i den fysiska säkerheten.

Kontroll av den fysiska säkerheten kan omfatta allt från mindre funktionstester av enskilda larmsensorer (komponentkontroll) till att stora delar av en verksamhetsutövares organisation involveras i övningar i syfte att kontrollera hur den fysiska säkerheten fungerar i sin helhet (helkontroll). Tabell 1 innehåller några exempel på typer av kontroll som kan genomföras i såväl mindre som mer omfattande skala.

En plan för service och underhåll av den fysiska säkerheten bör finnas dokumenterad. En sådan plan bör omfatta såväl mekaniska säkerhetsskyddsåtgärder, till exempel säkerhetsdörrar och säkerhetsglas, som tekniska system. Planen kan också innefatta specifikt underhåll av särskilda utrymmen, exempelvis utrymmen som skyddats mot obehörig insyn och avlyssning.

Det bör även finnas en plan för revision av system och funktioner, i syfte att identifiera eventuella brister i den fysiska säkerheten. Eventuella uppdateringar av system bör också finnas dokumenterade i en plan, i syfte att bland annat kunna tillse att rätt kompetens finns på plats vid uppdatering. För att undvika systemfel är det lämpligt att backup och test av system genomförs innan ett system ska installeras eller uppgraderas. Uppdateringar och uppgradering av system bör ske när systemen är lågt belastade.

Byggnadstekniska åtgärder som vidtas eller tekniska system som införskaffas bör dokumenteras för att säkerställa spårbarhet i den fysiska säkerhetens utveckling.

Notera:
Fysisk säkerhet understöds många gånger av informationssystem för exempelvis styrning av tillträde (passersystem) eller upptäckande förmåga (larm och kamerabevakning). Om dessa informationssystem är av betydelse för den säkerhetskänsliga verksamheten omfattas de av särskilda krav.

+ *Se Vägledning i säkerhetsskydd – Informationssäkerhet.*

Tabell 1. Exempel på kontroll i olika omfattning.

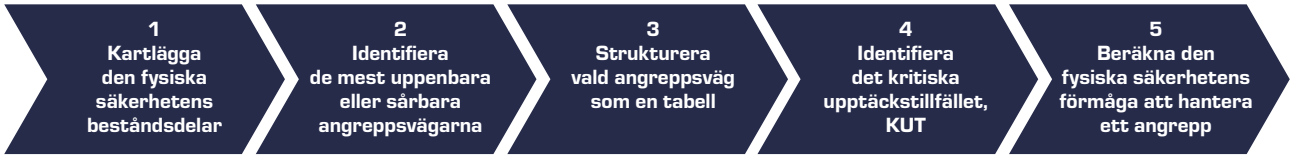
Typ av kontroll	Upptäcka	Försvåra	Hantera
Komponentkontroll	Upptäcker en viss typ av larmsensor rörelse som de ska?	Hur länge fördröjer en typ av dörrar ett obehörigt tillträde?	Finns det rutiner för att hantera obehörigt tillträde och skadlig inverkan?
Funktionskontroll	Fungerar detektion, överföring och verifiering längs en angreppsväg?	Hur länge fördröjs en antagonist av de olika lagren enligt lökprincipen på väg fram mot olika skyddsvärden?	Hur lång tid tar det för hanterande förmågor att komma fram till olika platser?
Systemkontroll	Fungerar alla upptäckande säkerhetsskyddsåtgärder som de ska i hela verksamheten?	Finns tillräckliga försvårande säkerhetsskyddsåtgärder för att fördröja obehörigt tillträde och reducera skadlig inverkan av antagonistiska handlingar som sker utifrån?	Efter upptäckt, följer hanterande förmågor rutiner och planer som har tagits fram tillsammans med verksamhetsutövaren?
Helkontroll	Omfattande kontroll av hur upptäckande, försvårande och hanterande säkerhetsskyddsåtgärder fungerar som ett system.		

8.1 Angreppsanalys

Angreppsanalys kan beskrivas som en analys för att utvärdera huruvida den fysiska säkerheten i sin helhet kan upptäcka, försvåra och hantera antagonistiska handlingar i förhållande till identifierade säkerhetshot och i förekommande fall de beskrivningarna av dimensionerande antagonistiska förmågor som Säkerhetspolisen tillhandahållit. Resultatet av angreppsanalysen kan antingen verifiera att den fysiska säkerheten är tillfredställande eller identifiera sårbarheter som innebär att ytterligare säkerhets-skyddsåtgärder behöver vidtas, det vill säga att utformningen av den fysiska säkerheten behöver revideras. Det finns såväl kvalitativa som kvantitativa metoder för att genomföra angreppsanalyser samt flertalet mer eller mindre avancerade datorprogram för beräkningar och simuleringar.

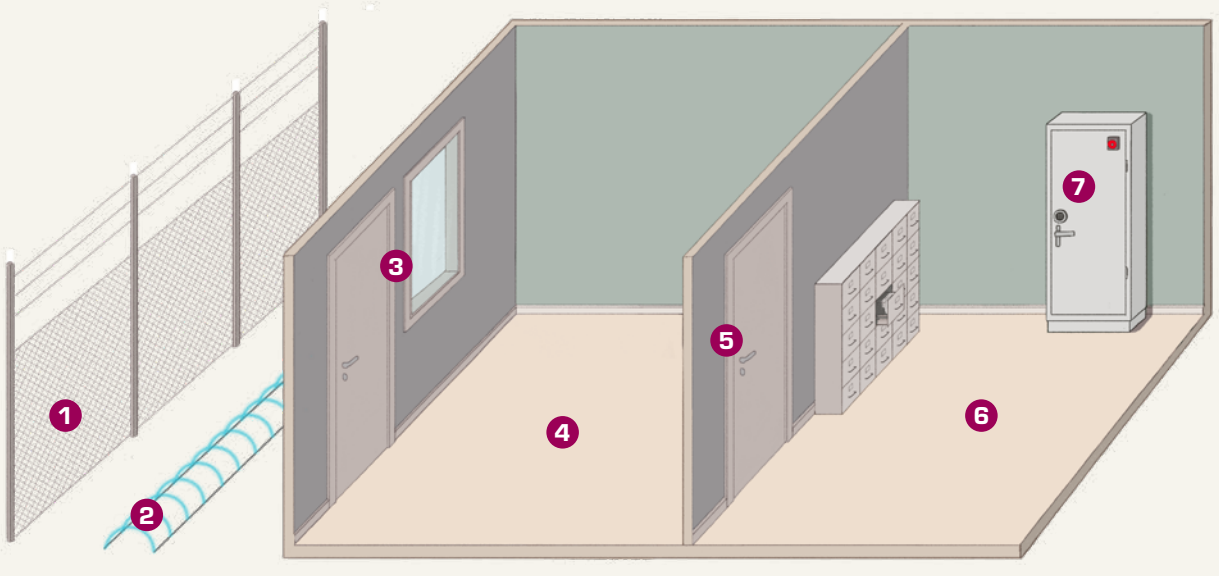
En vanligt förekommande och enkel metod för angreppsanalys är att stegvis kartlägga de uppgifter i form av förflyttningar över områden eller genom utrymmen samt forcering av säkerhetsskyddsåtgärder en antagonist vid ett fysiskt angrepp behöver utföra på väg fram till ett skyddsvärde. Denna typ av analys av så kallade angreppsvägar består av fem steg och utgår från anläggningen som visas i figur 13 nedan.

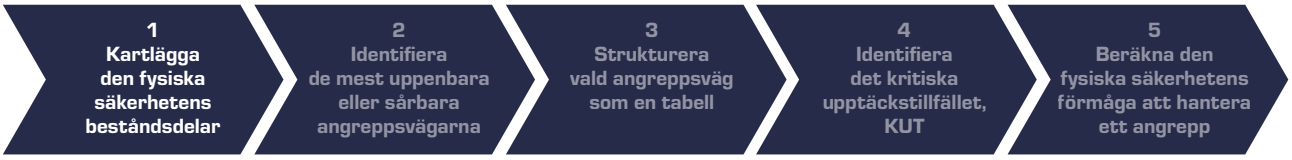
Figur 12. Analys av angreppsväg



Figur 13.
En anläggning omgiven av ett staket som avgränsar ett ytterområde följt av en byggnad med ett yttre och inre utrymme där skyddsvärden hålls inlåsta i en förvaringsenhet. Staketet saknar larm medan ytterområdet har ett nedgrävt och relativt otillförlitligt larm. Byggnadsdelar, utrymmen och förvaringsenheten är larmade.

1. Staket
2. Avspärrat område med larm med larmsensorer nedgrävda i marken
3. Vägg med fönster och ytterdörr
4. Kontor
5. Vägg med säkerhetsdörr
6. Arkivlokal
7. Förvaringsenhet med vibrationslarm





8.1.1 Analys av angreppsväg - Steg 1

Första steget av de fem är att kartlägga den fysiska säkerhetens beståndsdelar. Detta görs genom att dela upp exempelvis en anläggning eller byggnad i fysiska lager och mellanliggande utrymmen med redan förekommande eller planerade säkerhetsskyddsåtgärder i respektive lager eller utrymme. Därefter berikas respektive lager, utrymme och säkerhetsskyddsåtgärd med fördröjningstid (T_F) och upptäcktsfaktor (F_U).

Se Figur 14.

Figur 14.
Exempel på kartläggning av lager av fysisk säkerhet
Observera att då det saknas upptäckande förmåga innan eller på staketet så kan inte heller en eventuell fördröjningstid som staketet erbjuder tillgodoräknas i angreppsanalysen. Detta eftersom antagonisten i princip kan ta hur lång tid som helst på sig för att ta sig över eller igenom staketet utan att upptäckas. Eftersom det är oklart hur lång tid antagonisten behöver för att initiera sitt angrepp och förflytta sig över området samt när detektion hos nedgrävda larmet i så fall sker, kan en eventuell fördröjningstid som området erbjuder inte tillgodoräknas.

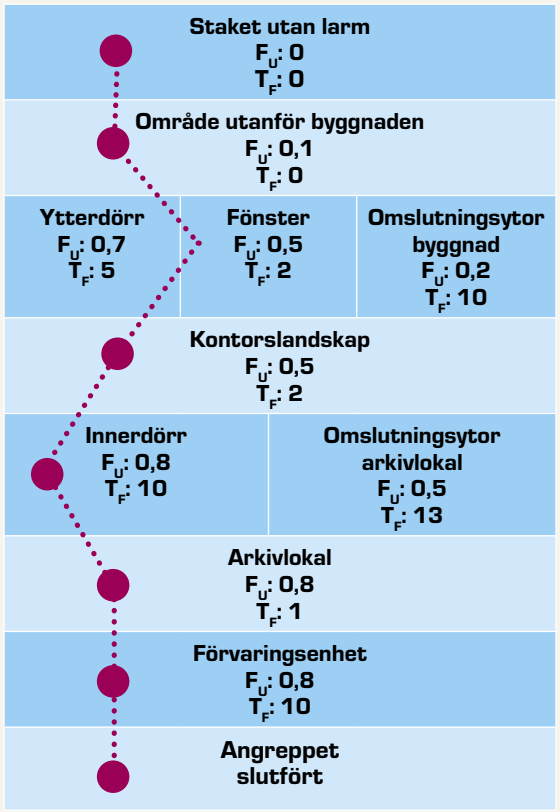
Staket utan larm F_U: 0 T_F: 0		
Område utanför byggnaden F_U: 0,1 T_F: 0		
Ytterdörr F_U: 0,7 T_F: 5	**Fönster** F_U: 0,5 T_F: 2	**Omslutningsytor byggnad** F_U: 0,2 T_F: 10
Kontorslandskap F_U: 0,5 T_F: 2		
Innerdörr F_U: 0,8 T_F: 10	**Omslutningsytor arkivlokal** F_U: 0,5 T_F: 13	
Arkivlokal F_U: 0,8 T_F: 1		
Förvaringsenhet F_U: 0,8 T_F: 10		
Angreppet slutfört		

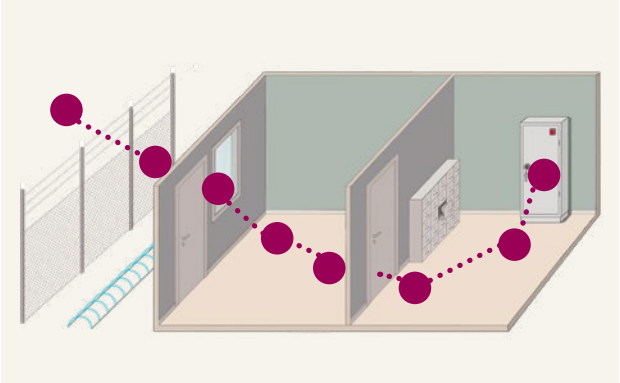
8.1.2 Analys av angreppsväg - Steg 2

Nästa steg handlar om att identifiera de angreppsvägar som är mest uppenbara eller sårbara, det vill säga de angreppsvägar som en antagonist beroende på förmåga och tillvägagångsätt kan väntas använda. I Figur 15 illustreras en av angreppsvägarna där en antagonist först rör sig in mot anläggningen, genom ett fönster, vidare genom ett kontorslandskap för att därefter forcera en säkerhetsdörr in till ett arkiv där skyddsvärdet i form säkerhetsskyddsklassificerade handlingar finns i en förvaringsenhet som antagonisten slutligen bryter upp.

Var observant på om en antagonist kan passera flera lager samtidigt och även undgå upptäckt, till exempel genom tak eller golv. I sådant fall måste analysen utökas med dessa lager och eventuella angreppsvägar som innebär att en antagonist kan förflytta sig från ett lager till ett annat, utan att fördröjas eller riskera att bli upptäckt i ett mellanliggande lager. Ett sådant ”hopp” mellan det andra och fjärde lagret av fysisk säkerhet skulle i Figur 15 kunna vara om antagonisten valde en angreppsväg från våningen ovanför, det vill säga ner genom golvet (kontorets omslutningsyta) direkt till arkivlokalens tak (arkivlokalens omslutningsyta) och därmed inte behövde passera genom det tredje lagret (kontorslandskapet).

Figur 15. Exempel på analys av angreppsväg.





8.1.3 Analys av angreppsväg - Steg 3

I det tredje steget kan vald angreppsväg struktureras som en tabell (Tabell 2) där uppgifterna antagonisten behöver utföra numreras i tur och ordning. Till varje uppgift skrivs fördröjningstid och upptäcktsfaktor från respektive lager eller utrymme som antagonisten övervinner genom uppgiften in i tabellen. När alla uppgifter och fördröjningstider listats kan antagonistens kvarvarande tidsbehov för att fullfölja angreppet från olika platser längs angreppsvägen räknas ut genom att nerifrån och upp addera fördröjningstiderna. Kolumnen ”Kvarvarande tidsbehov” visar alltså den tid antagonisten har kvar till att nå sitt mål precis när respektive uppgift påbörjas. Kolumnen ”KUT” förklaras i steg 4.

Se tabell 2.

Tabell 2.
Angreppsväg med upptäcktsfaktor F_U, fördröjningstid T_F, antagonistens kvarvarande tidsbehov och kritiskt upptäcktstillfälle KUT som förklaras i steg 4. Eftersom staketet saknar larm samt att det är oklart hur lång tid antagonisten behöver för att initiera angreppet och när denna kan komma att upptäckas sätts fördröjningstiderna på de första två uppgifterna till 0 minuter.

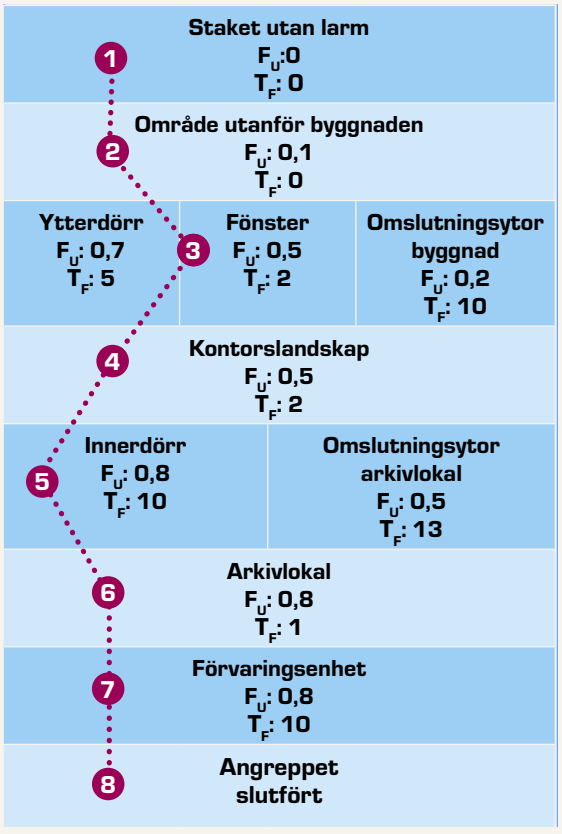
Angreppsväg, Hanteringstid: 15 minuter

Nr	Uppgift	F_U	T_F (min)	Kvarvarande tidsbehov (min)	KUT
1	Hoppa över staketet	0.0	00:00	25:00	
2	Initiera angrepp	0.1	00:00	25:00	
3	Forcera fönster	0.5	02:00	25:00	
4	Röra sig genom kontorslandskap	0.5	02:00	23:00	
5	Forcera innerdörr	0.8	10:00	21:00	X
6	Röra sig genom arkivlokalen	0.8	01:00	11:00	
7	Forcera förvaringsenhet	0.8	10:00	10:00	
8	Angreppet slutfört	–	–	00:00	

Vid en kontrollräkning ska summan av alla fördröjningstider bli samma som antagonistens kvarvarande maximala tidsbehov när denne inleder angreppet. Redan här går det att övergripande bedöma huruvida den fysiska säkerheten är tillfredställande genom att jämföra antagonistens maximala kvarvarande tidsbehov med hanteringstiden. Ifall antagonisten behöver kortare tid än hanteringstiden kommer denne att lyckas, även om angreppet upptäcks omedelbart när det påbörjas.

Notera:
Det är den totala hanteringstiden som måste användas vid jämförelsen. Total hanteringstid inkluderar även den tid som åtgår till detektionskedjan och som i vissa fall kan vara längre än den tid det tar för hanterande förmågor att hinna fram.

Figur 16. Exempel på analys av angreppsväg.



8.1.4 Analys av angreppsväg - Steg 4

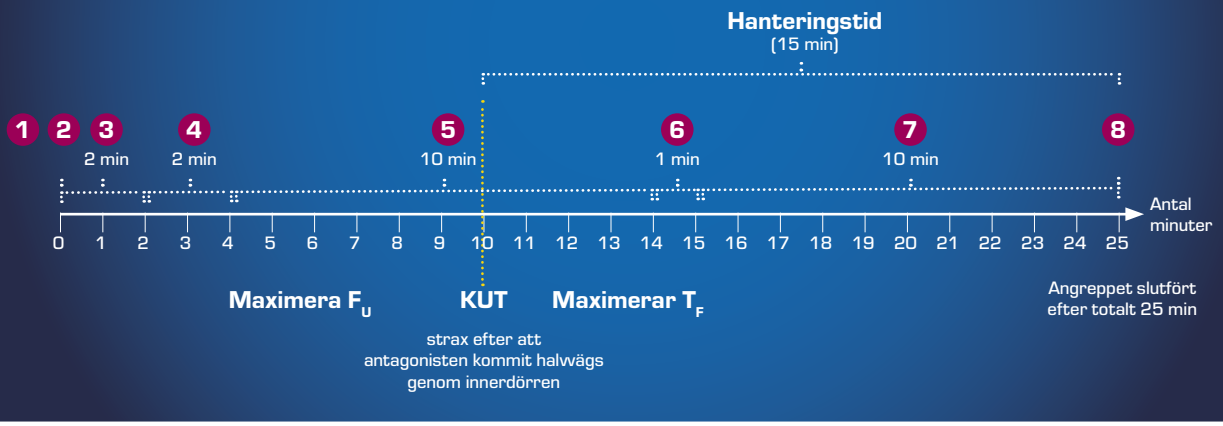
Steg 4 handlar om att identifiera det kritiska upptäcktstillfället, KUT, som är det tillfälle där upptäckt senast måste ske för att hanterande säkerhetsskyddsåtgärder ska hinna hantera angreppet. Med andra ord kommer en antagonist som upptäcks efter KUT att hinna fullborda sitt angrepp innan hanterande förmågor hinner fram.

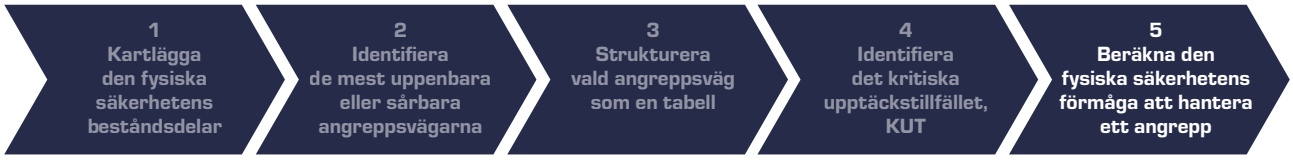
När alla uppgifter är listade och antagonistens kvarvarande tidsbehov räknats ut genom att addera fördröjningstidernafrån skyddsvärdet och utåt kan KUT fastställas genom att ställa hanteringstiden i relation till kvarvarande tidsbehov. I exemplet i Tabell 2 är hanteringstiden 15 minuter och upptäckt måste alltså ske som senast när antagonisten hunnit ungefär halvvägs genom innerdörren till arkivet vilket visualiseras i figur 17. I praktiken blir KUT när antagonisten rör sig fram mot eller, som senast, börjar forcera dörren och har 21 minuter kvarvarande tidsbehov. Exempel på upptäckande säkerhetsskyddsåtgärder kan i detta fall vara passiva infraröda detetorer i kontorslandskapet eller vibrationdetektorer på dörren och väggarna till arkivet. Det blir här mer tydligt varför det är viktigt att använda den totala hanteringstiden som inkluderar hela detektionskedjan. Om tiden för överföring och verifiering är lång kan annars möjligheten att hanterande förmågor kommer fram i tid överskattas.

Generellt sett gäller det att prioritera att upptäcka ett obehörigt tillträde eller skadlig inverkan innan KUT, för att därefter maximera fördröjande säkerhetsskyddsåtgärder. Detta eftersom upptäckt som sker efter KUT ändå innebär att ett angrepp kommer att upptäckas för sent samtidigt som det kan vara svårt eller onödigt kostsamt att anordna starkare skydd ju längre ut från skyddsvärdet man kommer.

Figur 17. Exemplet med angreppsvägen från tabell 2 visualiserad som en tidslinje och de sex av antagonistens uppgifter där det möjlighet att upptäcka denne (nr. 2-7). Tidpunkten då upptäckt senast måste ske, KUT, markerad 10 minuter in i förloppet.

F_U = Upptäcktsfaktor
T_F = Fördröjningstid
KUT = Kritiskt upptäcktstillfälle





8.1.5 Analys av angreppsväg - Steg 5

Det sista steget i angreppsanalysen handlar om att utifrån analyserade angreppsvägar och KUT beräkna den fysiska säkerhetens förmåga att hantera ett angrepp. Förmågan att hantera ett angrepp kan beskrivas som tillförlitligheten att ett angrepp upptäcks tillräckligt tidigt så att hanterande säkerhetsskyddsåtgärder hinner vidtas innan angreppet är slutfört.

Exempel

Då KUT för angreppsvägen (se Tabell 2) är vid uppgift nummer 4 beräknas förmågan att hantera angreppet utifrån den upptäcktsfaktor som existerar fram till dess. Upptäckt kan ske på området utanför byggnaden, vid forcering av fönster samt vid förflyttning genom kontorslandskapet. Detta ger en upptäcktsfaktor på 0.77, vilket har beräknas utifrån formeln nedan:

1 – (1-0.1) × (1-0.5) × (1-0.5) = 0.775.

Ifall innerdörren är försedd med en vibrationsdetektor som reagerar när forceringen av dörren påbörjas kan även den upptäckande förmågan räknas in.

Se avsnitt 5.3 Upptäcktsfaktor.

Genom att använda denna analysform och jämföra den fysiska säkerhetens förmåga att hantera olika angrepp längs potentiella angreppsvägar kan en verksamhetsutövare på ett systematiskt sätt identifiera sårbarheter och obalans i den fysiska säkerheten, reducera dessa samt verifiera huruvida den fysiska säkerheten uppfyller de krav som ställts.

Notera:

Angreppsvägen som analyserats i exemplet utgår från att antagonisten väljer att ta sig in genom innerdörren. Det finns dock även andra vägar in till förvaringsenheten och som har andra värden för T_F och F_U.

8.2 Övningar

Genom att öva kan verksamhetsutövare identifiera sårbarheter såsom sen upptäckt, för kort fördröjningstid eller bristande hanterande förmåga. Övningar kan genomföras som skrivbordsövningar, datorsimuleringar eller tillämpade övningar med praktiska moment. I sin allra enklaste form kan en skrivbordsövning bestå i en kvalitativ angreppsanalys av ett fiktivt scenario. Resultatet av genomförda övningar bör dokumenteras och användas som underlag för förbättringar av den fysiska säkerheten.


STOPP
SKYDDSOBJEKT
FÖRBUD
– mot tillträde utan tillstånd
Enligt skyddslagen (2010:305)
LÄNSSTYRELSEN

9 Skyddsobjekt och skyddslagen

§ *Skyddslagen (2010:305)*

§ *Kamerabevakningslagen (2018:1200)*

Fysisk säkerhet i säkerhetsskyddslagstiftningen har ett nära samband med reglerna i skyddslagen. Beslut om skyddsobjekt enligt skyddslagen ger utökade möjligheter till anpassning av den fysiska säkerheten. Vid bevakning av ett skyddsobjekt har bevakningspersonalen, som benämns skyddsvakter, utökade befogenheter vad gäller exempelvis kontroll av personer och fordon samt att ingripa mot obemannade luftfartyg, så kallade drönare.

Ett beslut om tillträdesförbud till ett skyddsobjekt kan också kompletteras med ett förbud mot att göra avbildningar, beskrivningar och mätningar av eller inom skyddsobjektet. Skyddsobjekt är även under vissa förutsättningar undantagna från kraven på tillstånd och upplysning om kamerabevakning.


FÖRSÖK 5

10 Standarder och normer

Det finns ett antal organisationer som utfärdar standarder och normer för sådant som är relaterat till den fysiska säkerheten. När dessa systematiseras kan de utgöra grunden i normer som utges av exempelvis Stöldskyddsföreningen.

Standarder och normer kan vara vägledande i arbetet med den fysiska säkerheten och utgöra en bra grund som verksamhetsutövare kan anpassa sitt skydd efter. Det är dock viktigt att känna till att en säkerhetsprodukt eller annat som certifierats eller godkänts utifrån en standard eller norm endast uppfyller de krav som den specifika standarden eller normen ställer.

Säkerhetsprodukter som certifierats och godkänts enligt en standard eller norm kan endast förväntas stå emot en antagonist med samma utrustning och tillvägagångssätt som föreskrivs i kraven för provning. Exempelvis kan en säkerhetsdörr provas enligt standarder för inbrott och erbjuda god fördröjningstid mot en antagonist med kofot, men om dörren placeras i marknivå kan ett realistiskt angreppssätt innebära forcering med fordon. Metoderna för certifiering av produkter beaktar vanligen verktyg och tillvägagångssätt, men inte antagonistens mål, kunskaper och färdigheter i övrigt. Det finns till exempel normer som är utformade mot bakgrund av försäkringsbolagens krav på skydd av kommersiella verksamheter, vilket kan vara otillräckligt för säkerhetskänsliga verksamheter. Exempelvis kan en dörr vara provad med avseende på att stå emot ett obehörigt tillträde, men det kanske inte ger tillräckligt skydd ifall verksamheten behöver skyddas mot sabotage genom anlagd brand vilket kräver en mindre öppning och tar kortare tid att få upp.

Då fördröjningstiden avgörs av en antagonists förmåga i form av verktyg, kunskaper och färdigheter, innebär det att samma fysiska säkerhetsskyddsåtgärd kan förväntas ge olika fördröjningstid mot olika typer av antagonister utifrån deras verktyg, kunskaper och färdigheter. Följaktligen är det viktigt att analysera behovet av säkerhetsskyddsåtgärder baserat på vad den fysiska säkerheten ska klara av att skydda mot, det vill säga identifierade säkerhetshot och, om Säkerhetspolisen tillhandahållit en sådan, beskrivningen av dimensionerande antagonistiska förmågor. Med resultatet av denna analys som grund kan verksamhetsutövare motivera säkerhetsskyddsåtgärder som omhändertar säkerhetshoten på ett realistiskt sätt och inte bara hänvisa till standarder och normer.

11 Checklista

Denna checklista kan användas som ett stöd för att på en övergripande nivå identifiera behov av säkerhetsskyddsåtgärder inom fysisk säkerhet och kontrollera att väsentliga aspekter beaktats. Denna checklista är inte heltäckande och en verksamhetsutövare behöver alltid utgå från sin egen säkerhetsskyddsanalys.

Identifiera behov av säkerhetsskyddsåtgärder inom fysisk säkerhet och kontrollera att väsentliga aspekter beaktats.

Utformning av den fysiska säkerheten

- ☐ Den fysiska säkerheten har utformats med säkerhetsskyddsåtgärder för att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan.
- ☐ Utformningen anpassas utifrån skyddsvärden, identifierade säkerhetshot, dimensionerande antagonistiska förmågor och sårbarheter identifierade i säkerhetsskyddsanalysen.
- ☐ Kontroll och utvärdering har skett för att säkerställa att den fysiska säkerheten når upp till de krav som ställs.

Principer för den fysiska säkerheten

- ☐ Lökprincipen med flera lager av skydd har använts vid utformning av den fysiska säkerheten.
- ☐ Det finns balans i den fysiska säkerheten så att kedjan av fysisk säkerhet inte innehåller någon svag länk eller alternativa enklare angreppsvägar som kan utnyttjas av en antagonist.
- ☐ Verksamheten har delats upp i olika fysiska sektioner enligt principen för sektionering.
- ☐ Det finns variation i den fysiska säkerheten som försvårar för en antagonist att med samma metod forcera flera lager vilket kan undergräva nyttan av lökprincipen.
- ☐ Information om säkerhetskänsliga delar av verksamheten och sårbarheter som kan hämtas via öppna källor eller fysisk/teknisk inhämtning har minimerats.
- ☐ Bebyggelseinriktad brottsprevention har använts vid utformning av byggnader och omgivningar.
- ☐ Kompensatoriska åtgärder har förberetts.
- ☐ Diversitet i den fysiska säkerheten har beaktats.
- ☐ Kritiska delar av den fysiska säkerheten har redundans.
- ☐ Den fysiska säkerheten har, vid behov, anpassats för att skydda mot insiders.

Upptäckande säkerhetsskyddsåtgärder

- ☐ Det finns personell bevakning och/eller teknisk bevakning för att tidigt upptäcka obehörigt tillträde och skadlig inverkan.
- ☐ Olika detektionsprinciper och deras lämplighet i det aktuella fallet har beaktas vid val av system för teknisk bevakning.
- ☐ Den totala upptäcktsfaktorn är tillräcklig och det finns en balanserad förmåga till upptäckt längs olika angreppsvägar.

Försvårande säkerhetsskyddsåtgärder

- ☐ Säkerhetsskyddsåtgärder för att fördröja obehörigt tillträde ger tillräcklig tid för att hanterande säkerhetsskyddsåtgärder ska ge avsedd effekt.
- ☐ Det finns säkerhetsskyddsåtgärder för att reducera skadan av angrepp som inte går att upptäcka i tid eller fördröja länge nog.
- ☐ Det finns rutiner och åtgärder för styrning av tillträde och eventuella besökstillstånd för både besökare och egen personal.
- ☐ Det finns rutiner och eventuella passersystem för kontroll av identitet och behörighet.
- ☐ Föremål som är olämpliga från säkerhetsskyddsynpunkt har identifierats och det finns rutiner för att hantera dessa.
- ☐ Det finns rutiner och åtgärder för att säkerställa att elektronisk utrustning som kan möjliggöra obehörig avlyssning inte medförs vid samtal om säkerhetsskyddsklassificerade uppgifter.
- ☐ Det finns beslut om vilka utrymmen som är godkända som förvaringsutrymmen.
- ☐ Kort, nycklar och anteckningar om kod är under kontroll eller förvaras i godkända förvaringsutrymmen.
- ☐ Det finns rutiner för och förteckningar över hantering av kort, nycklar och koder.
- ☐ Det finns beslut om vilka utrymmen som är godkända för regelbundna samtal om säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklass konfidentiell eller högre.
- ☐ Utrymmen som används för samtal om säkerhetsskyddsklassificerade uppgifter är skyddade mot obehörig avlyssning.
- ☐ Det finns beslut om vilka utrymmen som är godkända för behandling av säkerhetsskyddsklassificerade uppgifter.
- ☐ Utrymmen som används för behandling av säkerhetsskyddsklassificerade uppgifter är skyddade mot obehörig insyn.

Hanterande säkerhetsskyddsåtgärder

- ☐ Tiden det tar att vidta hanterande säkerhetsskyddsåtgärder är kortare än den tid som försvårande säkerhetsskyddsåtgärder fördröjer en antagonist.
- ☐ Hanterande säkerhetsskyddsåtgärder har tillfredställande förmåga att hantera de säkerhetshot som den fysiska säkerheten ska skydda mot.
- ☐ Det finns rutiner och förberedda åtgärder för att reducera konsekvenserna av antagonistiska handlingar.

Kontroll av den fysiska säkerheten

- ☐ Den fysiska säkerheten kontrolleras och utvärderas regelbundet genom olika kontroller och övningar.
- ☐ Det finns en dokumenterad plan för åtgärder som behöver vidas för att omhänderta avvikelser.

Service, underhåll och vidmakthållande

- ☐ Det finns en plan för service och underhåll av fysiska säkerhetsskyddsåtgärder.
- ☐ Revision av rutiner och efterlevnad sker fortlöpande.

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