Vägledning i säkerhetsskydd

Fysisk säkerhet

September 2020

Produktion: Säkerhetspolisen, September 2020
Grafisk formgivning: Säkerhetspolisen
Typografi: Eurostile och Swift

Innehåll

1 Introduktion

Denna vägledning riktar sig till personer som arbetar med fysisk säkerhet inom ramen för säkerhetsskydd. Syftet med vägledningen är att tydliggöra bestämmelserna i kapitel 5 i Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd, samt att öka kunskapen kring fysisk säkerhet vid säkerhetskänsliga verksamheter och i förlängningen bidra till ett säkrare Sverige.

Vägledningen är utformad för att beskriva såväl grundläggande som detaljerade delar av fysisk säkerhet. Vissa förkunskaper kan krävas för att fullt ut ta till sig innehållet i vägledningen.

I vägledningen finns ett antal rutor med information som bör noteras vid arbete med den fysiska säkerheten.

2 Vad är fysisk säkerhet?

2 kap. 3 § säkerhetsskyddslagen (2018:585)

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. I detta ligger även att skydda mot att någon med eller utan tekniska hjälpmedel obehörigen får insyn i den säkerhetskänsliga verksamheten.

Fysisk säkerhet kan beskrivas som ett system av personal, rutiner, byggnadsteknik och säkerhetsteknik som utgår ifrån ett identifierat behov av säkerhetsskydd. Tillsammans utgör de upptäckande, försvårande och hanterande säkerhetsskyddsåtgärder som ska förebygga obehörigt tillträde och skadlig inverkan (Figur 1).

Då behovet av säkerhetsskydd varierar mellan olika verksamhetsutövare finns det ingen standardlösning som går att applicera på all säkerhetskänslig verksamhet. Istället måste den fysiska säkerheten anpassas utifrån den situation som gäller för respektive verksamhetsutövare.

Förutom det identifierade behovet av säkerhetsskydd som ska framgå i verksamhetsutövarens säkerhetsskyddsanalys måste även bland annat geografiskt läge, byggnadstekniska förutsättningar och verksamhetens art beaktas vid utformning av den fysiska säkerheten.

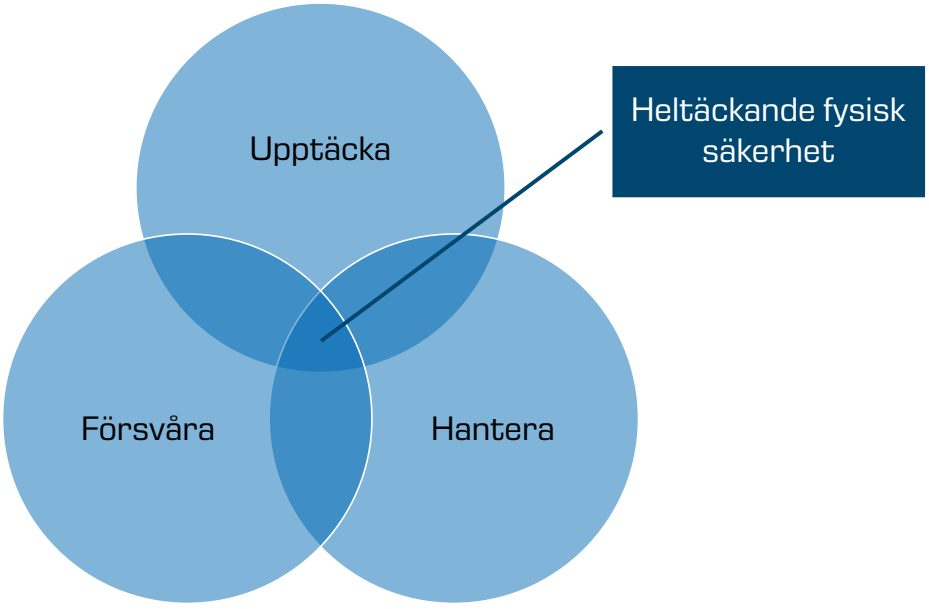
Glöm inte att fysisk säkerhet endast är en del av systemet säkerhetsskydd. För att säkerhetsskyddet ska vara tillfredställande måste den fysiska säkerheten integreras med säkerhetsskyddsåtgärderna personalsäkerhet och informationssäkerhet. Fysisk säkerhet är till exempel beroende av tillfredställande informationssäkerhet när det gäller informationssystem för fysiska säkerhetsskyddsåtgärder som elektroniska passersystem.

Figur 1: Fysisk säkerhet är ett system av säkerhetsskyddsåtgärder som tillsammans upptäcker, försvårar och hanterar obehörigt tillträde och skadlig inverkan.

3 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 allvarliga konsekvenser 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 illustrerar behovet av alla fysiska säkerhetsskyddsåtgärder. Om det saknas upptäckande säkerhetsskyddsåtgärder kommer ett obehörigt tillträde inte att kunna hanteras, eftersom det inte upptäcks. Om det istället saknas försvårande säkerhetsskyddsåtgärder kommer ett obehörigt tillträde att upptäckas, men hinna slutföras innan det har hanterats. Saknas hanterande säkerhetsskyddsåtgärder kommer ett obehörigt tillträde att kunna slutföras, eftersom det inte kommer att hanteras.



Figur 2: Alla förmågor inom fysisk säkerhet påverkar varandra.

Notera: Fysisk säkerhet är ett system av säkerhetsskyddsåtgärder som är beroende av varandra, vilket innebär att enskilda säkerhetsskyddsåtgärder i sig inte utgör 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 dörr som fördröjer ett obehörigt tillträde relativt verkningslös om det obehöriga tillträdet inte upptäcks.

Följande beskriver hur de olika säkerhetsskyddsåtgärderna inom fysisk säkerhet fungerar ur antagonistens och verksamhetsutövarens perspektiv:

- Inledningsvis inhämtar antagonisten information om den säkerhetskänsliga verksamheten via bland annat öppna källor och i vissa fall sker detta även genom rekognosering på plats. Principer för att skapa variation i skyddet och minska exponeringen av eventuella sårbarheter är lämpliga att tillämpa här. Här har även upptäckande säkerhetsskyddsåtgärder en viktig roll att i ett så tidigt skede som möjligt upptäcka dessa typer av förberedelser.
- När antagonisten har påbörjat sin handling är det viktigt att det finns upptäckande och försvårande säkerhetsskyddsåtgärder. Upptäckande säkerhetsskyddsåtgärder syftar till att tidigt upptäcka en antagonist som rekognoserar eller, om det inte lyckas, så tidigt som möjligt under själva genomförandet. Ett exempel på en sådan åtgärd är rörlig personell bevakning. Försvårande säkerhetsskyddsåtgärder syftar till att både fördröja och reducera skadan av den antagonistiska handlingen.
- Efter att antagonisten har upptäckts och upptäckten verifierats larmas den hanterande förmågan, som har till uppgift att avbryta eller reducera konsekvensen av den antagonistiska handlingen.

Tiden för att hantera en antagonistisk handling varierar beroende på antagonistens verktyg, kunskap och färdigheter samt mål och syfte med angreppet. Vissa typer av angrepp, till exempel att föra ut fysiska säkerhetsskyddsklassificerade handlingar, innebär att en antagonist behöver fly från platsen för att lyckas. Andra typer av angrepp, till exempel sabotage av säkerhetskänsliga system, kräver inte flykt för att lyckas, vilket kan innebära att ett angrepp kan ske på kortare tid än ett angrepp där antagonisten inte uppnår sitt mål förrän flykt har skett.

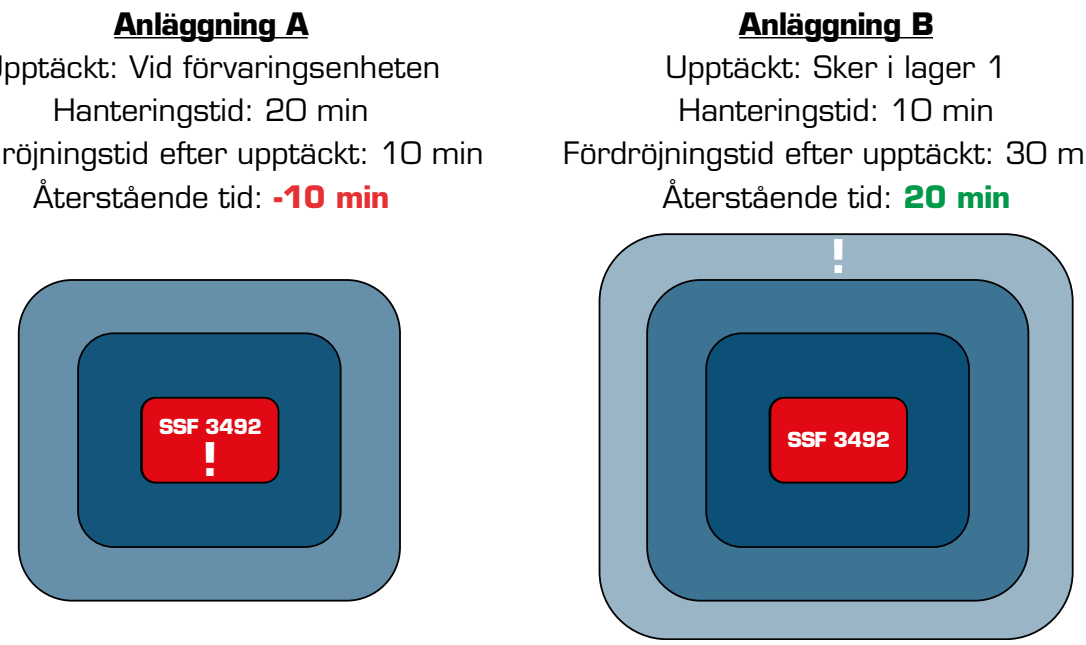
Notera: Eventuell avskräckande effekt som uppstår till följd av fysiska säkerhetsskyddsåtgärder bör ses som en positiv sidoeffekt snarare än ett uttalat mål då den avskräckande effekten är svår att bedöma.

4 Preskriptiva och funktionsbaserade 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 verksamhetens identifierade behov av säkerhetsskydd, säkerhetshot eller andra omständigheter som kan vara relevanta. 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 verksamhetsutövaren att avgöra om den fysiska säkerheten verkligen är tillfredställande eller inte. Detta gäller särskilt eftersom fysisk säkerhet utformas utifrån såväl säkerhetshotet som relationen mellan upptäckande, försvårande och hanterande säkerhetsskyddsåtgärder.

Som Figur 3 illustrerar kan ett preskriptivt synsätt med krav på säkerhetsskåp som certifierats enligt normen SSF 3492, med en fördröjningstid på 10 minuter enligt normen, leda till en obalans i nivån av säkerhetsskydd på anläggning A och B. Båda anläggningarna lever upp till det preskriptiva kravet för förvaringsenheter, men medan anläggning A inte har en tillfredställande fysisk säkerhet (på grund av att upptäckt sker för sent i förhållande till hanteringstiden) har anläggning B istället en överdimensionerad fysisk säkerhet i förhållande till samma säkerhetshot.



Figur 3: Anläggning A och anläggning B uppfyller samma krav på förvaringsenhet enligt ett preskriptivt krav, men har ändå olika förmåga att förebygga obehörigt tillträde (utropstecknet illustrerar var upptäckt sker).

Kapitel 5 i Säkerhetspolisens föreskrifter (PMFS 2019:2) är utformat utifrån ett funktionsbaserat synsätt. Med ett funktionsbaserat synsätt kan verksamhetsutövaren till skillnad från ett preskriptivt synsätt utforma den fysiska säkerheten utifrån verksamhetsutövarens identifierade behov av säkerhetsskydd och resultatet av verksamhetsutövarens säkerhetsskyddsanalys. Utformningen av den fysiska säkerheten kan då exempelvis ske genom att verksamhetsutövaren säkerställer att upptäckt sker tidigare längs antagonistens angreppsväg, att de försvårande säkerhetsskyddsåtgärderna ökas, eller att hanteringstiden förkortas.

Ett funktionsbaserat synsätt är mer flexibelt och ger verksamhetsutövaren en större möjlighet att utforma den fysiska säkerheten så att den samspelar med andra säkerhetsskyddsåtgärder. Om en verksamhetsutövare inte har möjlighet att säkerställa tidigare upptäckt, längre fördröjningstid eller kortare hanteringstid kan det finnas anledning att se över valet av anläggning. Om det inte heller finns någon möjlighet att anpassa valet av anläggning kan det istället vara nödvändigt att se över de skyddsvärden som den fysiska säkerheten ska skydda.

5 Utformning av den fysiska säkerheten

5.1 Processen för utformning av fysisk säkerhet

4 kap. 1 § säkerhetsskyddsförordningen (2018:658)

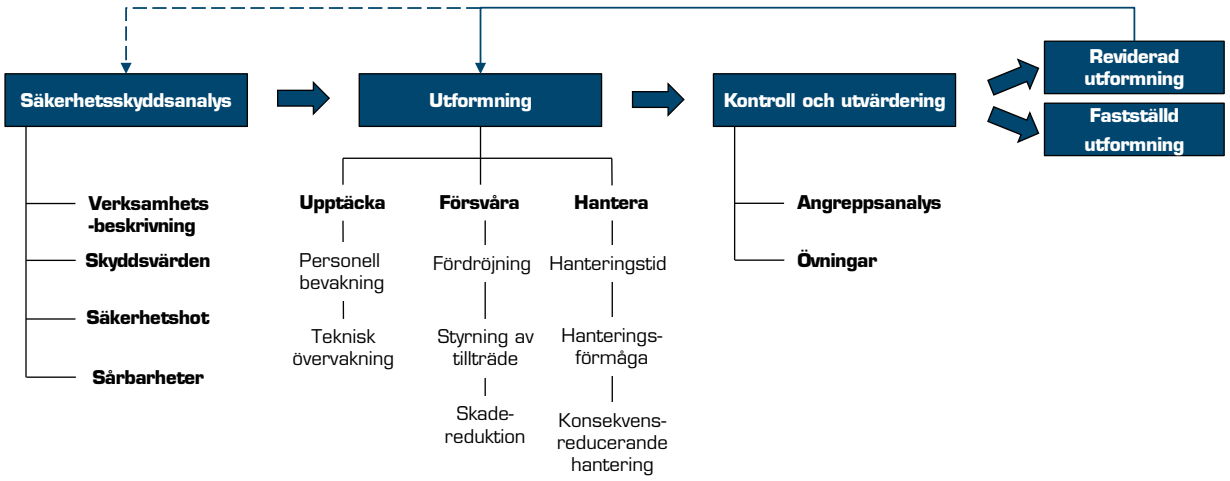
Processen för utformning av fysisk säkerhet är indelad i fyra olika steg (Figur 4). Dessa steg beskrivs nedan:

1. **Säkerhetsskyddsanalys**
   Beslut kring utformning av den fysiska säkerheten ska utgå från säkerhetsskyddsanalysen. Här behöver verksamhetsutövaren identifiera vilken anläggning och verksamhet den fysiska säkerheten ska verka i (verksamhetsbeskrivning), vad den fysiska säkerheten ska skydda (skyddsvärden), vad den fysiska säkerheten ska skydda mot (säkerhetshot) samt eventuella sårbarheter. Först när detta har beaktats och konstaterats kan verksamhetsutövaren gå vidare till nästa steg.

2. **Utformning**
   Nästa steg är att verksamhetsutövaren utformar den fysiska säkerheten så att det finns säkerhetsskyddsåtgärder för att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan. Utformningen anpassas utifrån skyddsvärde, säkerhetshot och sårbarheter.

3. **Kontroll och utvärdering**
   När verksamhetsutövaren har ett förslag på hur den fysiska säkerheten ska utformas behöver kontroll genomföras innan slutgiltigt beslut om utformning tas. Kontroll och utvärdering kan bestå av exempelvis olika analyser och övningar som syftar till att säkerställa att den fysiska säkerheten är utformad på ett sådant sätt att den klarar av de krav som verksamhetsutövaren ställer.

4. **Fastställd utformning eller behov av reviderad utformning**
   Beroende på vad verksamhetsutövaren konstaterar vid kontroll och utvär-



Figur 4: Processen för utformning av fysisk säkerhet.

dering sker antingen beslut om fastställd utformning, eller beslut om att revidera utformningen av den fysiska säkerheten. Konstaterar verksamhetsutövaren att utformningen inte är tillfredställande, det vill säga att det kvarstår sårbarheter som inte kan accepteras, kan det behövas en översyn av säkerhetsskyddsåtgärderna. Detta kan ske genom att till exempel öka den upptäckande förmågan, att förlänga fördröjningstiden, anpassa skadereducerande säkerhetsskyddsåtgärder eller att förkorta hanteringstiden.

Om verksamhetsutövaren inte har möjlighet att göra några justeringar i utformningen av den fysiska säkerheten kan det finnas ett behov av att se över verksamhetsutövarens skyddsvärden och säkerhetshot. Detta kan ske exempelvis genom att påverka skyddsvärdena på ett sådant sätt att konsekvenserna av en antagonistisk handling reduceras, och genom detta ställs inte samma krav på den fysiska säkerheten.

5.2 Skyddsvärden: Vad den fysiska säkerheten ska skydda

Hur den fysiska säkerheten ska utformas beror på vilka konsekvenser ett realiserat antagonistiskt hot kan få på den säkerhetskänsliga verksamheten samt utifrån vilka perspektiv tillgänglighet, konfidentialitet och riktighet som identifierade skyddsvärden behöver skyddas. Till exempel behöver den fysiska säkerheten för en anläggning med stora krav på tillgänglighet utformas annorlunda än för ett objekt där uppgifter som är skyddsvärda ur aspekten konfidentialitet förvaras.

5.3 Säkerhetshot: Vad den fysiska säkerheten ska skydda mot

2 kap. 6-8 §§ Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd

Det är svårt att avgöra om den fysiska säkerheten tillfredsställer behovet av säkerhetsskydd utan att först ta ställning till vad den fysiska säkerheten ska klara av att skydda mot. Detta behöver därför anges i 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 stor skillnad på att skydda mot en sprängladdning på 15 kg eller en på 1500 kg, 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. För särskilt säkerhetskänslig verksamhet ska därför den fysiska säkerheten utformas utifrån en dimensionerande hotbeskrivning (DHB) som Säkerhetspolisen upprättar. Även andra säkerhetskänsliga verksamheter kan med fördel använda sig av en DHB för att tydliggöra skyddsdimensioneringen och underlätta värderingen av att säkerhetsskyddsåtgärder ger avsedd effekt.

En DHB är en beskrivning av de antagonistiska förmågor som säkerhetsskyddsåtgärderna långsiktigt ska klara av att skydda mot, oavsett hur hotbilden ser ut i nuläget. Säkerhetsskyddsåtgärder baserade på en DHB utformas så att de tar höjd för förändringar i hotbilden, och behöver därför inte byggas om i samma takt som hotbilden förändras. I de fall hotbilden förändras på ett sådant sätt att den överstiger skyddsdimensioneringen kan istället kompensatoriska åtgärder vidtas.

Vilka antagonistiska förmågor en DHB ska innehålla förhåller sig till både ur vilket perspektiv ett skyddsvärde har identifierats (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 ur perspektivet konfidentialitet kan exkludera sabotage som resulterar i otillgängliggörande av säkerhetskänsliga verksamhetsdelar i sin skyddsdimensionering. Likaså förhåller sig en antagonists avsikt och förmåga till förväntat resultat, vilket i generella termer innebär att högre förmåga troligen kommer att ansättas mot högre skyddsvärden.

Nedan anges några exempel på antagonistiska förmågor som säkerhetskänsliga verksamheter kan inkludera i sin skyddsdimensionering:

- **Obehörigt tillträde**
  - Forcering med manuella verktyg
  - Forcering med motordrivna verktyg
  - Tyst och dold forcering
  - Forcering med fordon
  - Forcering med explosivämnen
  - Nyttjandet av aktiva eller passiva insiders

- **Skadlig inverkan**
  - Sabotage genom explosivämnen
  - Sabotage genom farliga ämnen
  - Sabotage genom anlagd brand
  - Sabotage genom skjutvapen
  - Avlyssning av samtal genom tekniska hjälpmedel
  - Insyn genom tekniska hjälpmedel
  - Inhämtning av röjande signaler

Notera: Fysisk säkerhet tar lång tid att bygga upp. Säkerhetshotet och skyddsdimensionering är därför en viktig aspekt att ta med tidigt under planeringsstadiet vid exempelvis en ny- eller ombyggnation.

6 Principer för fysisk säkerhet

6.1 Lökprincipen

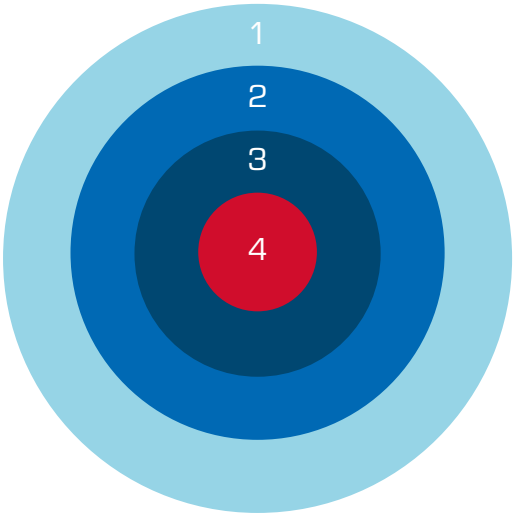
Historiskt användes lökprincipen i medeltidens borgar där flera koncentriska murar omgärdade centrum där värdeföremål och nödvändiga matförråd fanns samlade. Idag är skyddsvärden ofta utspridda på olika platser, men lökprincipen går fortfarande att applicera genom att skapa öar omgivna av lager av säkerhetsskyddsåtgärder. Lökprincipen kan beskrivas som ett ”utifrån och in”-perspektiv där en antagonist måste ta sig igenom flera lager av säkerhetsskyddsåtgärder in till skyddsvärden som befinner sig i centrum.

Varje lager i den så kallade skyddslöken kan innehålla en eller flera systemsamverkande säkerhetsskyddsåtgärder för att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan.

I Figur 5 skulle exempelvis de fyra lagren i skyddslöken kunna bestå av följande säkerhetsskyddsåtgärder i syfte att skydda mot obehörigt tillträde:

- Lager 1: Staket med larm följt av ett område som det tar tid för antagonisten att förflytta sig över utgör upptäckande och försvårande säkerhetsskyddsåtgärder
- Lager 2: Yttervägg med säkerhetsdörrar och säkerhetsglas utgör försvårande säkerhetsskyddsåtgärder, både ur ett fördröjande och skadereducerande perspektiv. Även personell bevakning bidrar till den upptäckande förmågan
- Lager 3: Passiv infraröd sensor och stationär vakt ger upptäckande, försvårande och hanterande säkerhetsskyddsåtgärder
- Lager 4: Säkerhetsskåp med magnetkontakt och vibrationssensor utgör försvårande och upptäckande säkerhetsskyddsåtgärder

Tänk på att nyttjandet av olika typer av säkerhetsskyddsåtgärder i varje lager även kan bidra till att skapa variation i skyddet och, rätt hanterat, även viss redundans.



Figur 5: Exempel på skyddslöken med fyra lager.

6.2 Balans i den fysiska säkerheten

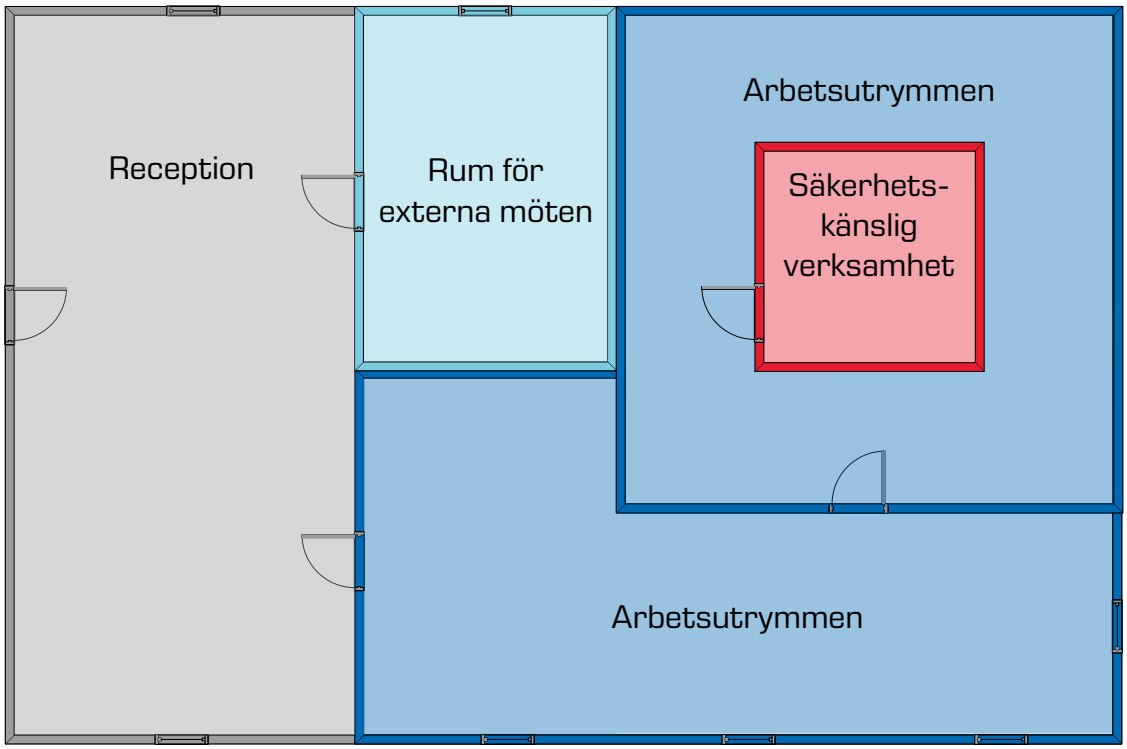
Balans i den fysiska säkerheten innebär att det inte finns någon del av utformningen av den fysiska säkerheten som är svagare än de andra. För försvårande säkerhetsskyddsåtgärder innebär detta till exempel att en dörr till ett utrymme måste ha samma motståndskraft som väggen dörren sitter i. Detsamma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

6.3 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 verksamhetsutövaren. Sektionering är också ett sätt att förtydliga vilka krav på fysiska säkerhetsskyddsåtgärder som finns för olika delar av en anläggning 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 (Figur 6).

Notera: Sårbarheter kan uppstå på grund av utrymningsbehov. Exempel på sådana sårbarheter är att nödutrymningsvägar kan öppnas inifrån med hjälp av en insider och att de kan användas som en flyktväg efter genomförd antagonistisk handling.



Figur 6: Exempel på sektionering.

6.4 Variation i den fysiska säkerheten

Variation i den fysiska säkerheten handlar om att försvåra för en antagonist att kartlägga och utnyttja 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 sammantaget bygger upp den fysiska säkerheten. Väl utförda kommer variationerna att ställa konflikterande krav på antagonistens förmåga, exempelvis att behöva bära med sig tung otymplig utrustning och samtidigt kunna 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. Detsamma gäller för inpasseringskontroller där slumpvisa mer noggranna genomsökningar kan försvåra för någon att ta in otillåtna föremål. Ett annat exempel är att säkerställa att så kallade masterkoder till tekniska övervakningssystem och förvaringsenheter ändras från standardiserade sådana.

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. 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 i anläggningen.

6.5 Skydd mot sårbarhetsexponering

Skydd mot sårbarhetsexponering består av att reducera eventuella sårbarheter kopplade till möjligheten för en antagonist att inhämta information om verksamheten via öppna källor eller genom fysisk och teknisk inhämtning. Ett sätt att reducera denna typ av sårbarhetsexponering är att begränsa spridning av ritningsunderlag och andra uppgifter som kan utnyttjas av en antagonist vid val av mål och planering av angrepp.

6.6 Bebyggelseinriktad brottsprevention

Bebyggelseinriktad brottsprevention handlar om bebyggelseinriktade åtgärder som syftar till att förebygga brottsligt beteende. Till exempel kan förutsättningarna för att upptäcka ett obehörigt tillträde ökas genom att anpassa vegetationen på en plats därifrån ett angrepp skulle kunna initieras genom att rensa skymmande träd och buskar längs fasaden på en anläggning. Det går också att nyttja olika typer av belysning i samma syfte.

Bebyggelseinriktad brottsprevention kan också användas för att förtydliga vissa ytor, genom att till exempel sätta upp ett yttre staket som markerar ett objekts gränser.

Genom att anpassa terrängen runt ett objekt går det också att tvinga fram vissa rörelsemönster.

6.7 Kompensatoriska åtgärder

I det fall en säkerhetsskyddsåtgärd fallerar eller hotbilden hastigt ökar uppstår en eller flera sårbarheter som behöver hanteras för att bibehålla en tillfredställande skyddsnivå. Kompensatoriska åtgärder är sådana som vidtas för att tillfälligt ersätta den funktion som försvunnit eller för att förstärka skyddet. Exempel på kompensatoriska åtgärder är att placera ut en vakt ifall en kamera går sönder eller att flytta säkerhetsskyddsklassificerade handlingar till säkrare lokaler vid kännedom om allvarlig säkerhetshotande verksamhet. För att kompensatoriska åtgärder ska fungera i praktiken bör de så långt det är rimligt och möjligt vara analyserade och förberedda, exempelvis genom instruktioner och avtal som gör det möjligt att avropa extra bevakningspersonal.

6.8 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 åtgärderna, exempelvis så inte batteribackup och reservkraftverk är beroende av samma efterliggande el-central och kablage fram till systemet som ska skyddas. Redundansen kan med fördel byggas upp av diversifierade åtgärder som har liten risk att drabbas av samma fel, exempelvis ett batteri som redundant kraftförsörjning eller larmkommunikation via mobilnät som redundans för fiber. Andra exempel är att använda bevakningskameror från olika tillverkare eller att inte uppdatera alla kameror samtidigt ifall det finns oupptäckta sårbarheter i mjukvarorna. Diversifierade åtgärder kan på så sätt utöver ökad driftsäkerhet även göra det svårare för en antagonist att planera och genomföra ett angrepp.

6.9 Fysiska säkerhetsskyddsåtgärder mot insiderhot

Fysisk säkerhet kan också bidra till att förebygga insiderhot. Bland annat kan lökprincipen och behörighetsstyrning vara en del av att förebygga insiderhot. Inom en bra skyddslök har även lagren närmast skyddsvärden funktioner för att upptäcka en antagonist, och i det innersta utrymmet kan exempelvis varje användare ha egna förvaringsenheter. Andra exempel på åtgärder är kontroller vid tillträde till särskilt säkerhetskänsliga 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 mot delar i den fysiska säkerheten.

7 Upptäckande säkerhets-skyddsåtgärder

5 kap. 2 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd

Verksamhetsutövaren ska, i den omfattning som skyddsdimensioneringen kräver, använda personell bevakning eller teknisk övervakning för att tidigt upptäcka obehörigt tillträde eller skadlig inverkan. De upptäckande säkerhetsskyddsåtgärderna ska anpassas utifrån säkerhetsskyddsanalysen, det vill säga utifrån vad som ska skyddas och vad den fysiska säkerheten ska klara av att skydda mot.

Upptäckt kan beskrivas som en kedjereaktion av detektion, överföring och verifiering. För att upptäckt ska ske måste alla dessa delar, det vill säga detektion, överföring och verifiering ske. Det är viktigt att upptäcka obehörigt tillträde och försök till skadlig inverkan 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. 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.

7.1 Personell bevakning

Personell bevakning syftar till att upptäcka obehörigt tillträde eller skadlig inverkan och i förlängningen leda till att hanterande säkerhetsskyddsåtgärder vidtas. 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 en anläggning. 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.

7.2 Teknisk övervakning

Teknisk övervakning syftar, på samma sätt som personell bevakning, till att upptäcka obehörigt tillträde eller skadlig inverkan och kan i förlängningen leda till att hanterande säkerhetsskyddsåtgärder vidtas. Detta inkluderar att upptäcka en obehörig person som rör sig förbi en linje, rör sig igenom en volym, flyttar på eller rör vid ett objekt. Den

tekniska övervakningen kan utformas med yttre larm, inre larm och objektslarm.

Yttre larm består av bevakning av perimetrar genom till exempel sensorer utmed ett staket eller mikrovågssensorer längs en anläggnings perimeter. Inre larm kan beskrivas som bevakning av förändringar i det bevakade utrymmet, till exempel möjligheten att upptäcka rörelse i ett rum med hjälp av en passiv infraröd sensor. Objektslarm är övervakning av en specifik del inom det bevakade objektet, till exempel ett säkerhetsskåp med vibrationssensor och tiltsensor.

Nedan anges några exempel på vanligt förekommande typer av larm som kan nyttjas vid teknisk övervakning:

- **Yttre larm**
  - Staketlarm
  - Marklarm
  - Mikrovågssensor
  - Aktiv infraröd sensor

- **Inre larm**
  - Glaskrossensor
  - Magnetkontakt
  - Passiv infraröd sensor

- **Objektslarm**
  - Tryckplatta
  - Tiltsensor
  - Vibrationssensor

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 verksamhetsutövaren ska reducera antalet oönskade larm. Detta kan exempelvis ske genom att verksamhetsutövaren använder två staket, där det yttersta inte har någon larmsensor utan fungerar som en barriär. Detsamma gäller andra larmsensorer som exempelvis en passiv infraröd sensor, som kan vara känslig för förändringar i det infraröda spektrumet, eller en mikrovågssensor som kan reagera på stillastående vatten.

7.2.1 Kamerabevakning

Kamerabevakningslagen (2018:1200)

Kamerabevakning ger ökade möjligheter att bevaka undanskymda eller viktiga platser, grindar samt inpasseringsställen som saknar personell bevakning. I vissa fall kan tillstånd till kamerabevakning av en plats dit allmänheten har tillträde krävas.

Kamerabevakning spelar en viktig roll när det gäller att verifiera larm och utreda händelser i efterhand som en del i bevisföring. Kamerabevakning av larmade 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 identifiera en person vid en fjärrmanövrerad dörr.

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 video analys (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.

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

7.3 Upptäcktsfaktor

Det finns ingen upptäckande säkerhetsskyddsåtgärd som är helt tillförlitlig i alla lägen och i alla miljöer. Både åtgärder inom personell bevakning och teknisk övervakning har sina respektive styrkor och svagheter. Exempelvis kan en stationär vakts ouppmärksamhet och trötthet bidra till att tillförlitligheten för att vakten ska upptäcka ett obehörigt tillträde blir lägre. Likaså kommer en larmsensor inte kunna kalibreras till att alltid upptäcka en person som både springer, går eller kryper förbi utan att medföra många obefogade larm vilket i praktiken innebär att en lägre känslighet måste 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, se 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 testpersonen försöker smyga förbi rörelsesensorer eller håller sig i skuggorna för att undvika upptäckt av ett system för kamerabevakning. Helst ska varje upptäckande säkerhetsskyddsåtgärd testas var för sig men i en större anläggning 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 och 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 vad 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 hög. Den totala upptäcktsfaktorn beräknas med formeln nedan som kan utökas med godtyckligt antal (n) upptäckande säkerhetsskyddsåtgärder.

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

Exempelvis kan en passiv infraröd larmsensor (PIR) med $F_U = 0.7$ kompletteras med en magnetkontakt (MK) med $F_U = 0.85$. Den 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 upptäckt från den ena eller den andra larmsensorn. Om kombinationen istället görs så att det krävs upptäckt från både den ena och den andra kommer den totala upptäcktsfaktorn att sjunka. Detta blir tydligt i exemplet ovan med kombinationen av en PIR och en magnetkontakt. Ifall PIR:en är skymd eller magnetkontakten trasig kan en antagonist passera utan upptäckt eftersom båda larmsensorerna inte kommer att reagera.

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 för 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.

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 meningsfullt att räkna med mer än två decimaler.

8 Försvårande säkerhets-skyddsåtgärder

5 kap. 3 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd

Verksamhetsutövaren ska, i den omfattning som skyddsdimensioneringen kräver, vidta försvårande åtgärder i syfte att fördröja obehörigt tillträde eller reducera 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.

8.1 Fördröjande säkerhetsskyddsåtgärder

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

8.1.1 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 och
- låsenheter.

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 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.

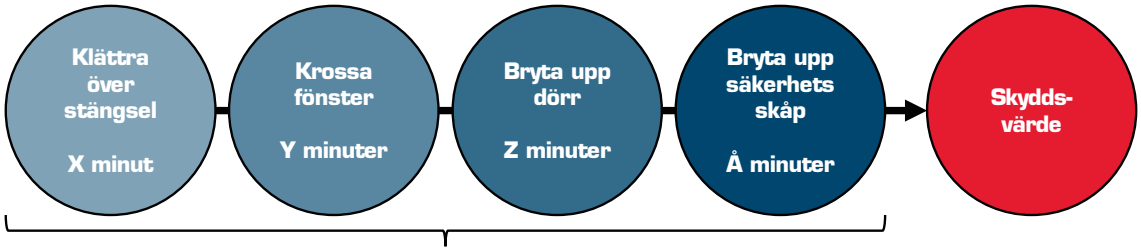
Utöver mekaniskt inbrottsskydd kan fördröjande säkerhetsskyddsåtgärder även bestå av avstånd och naturliga hinder som till exempel vatten eller svårgenomtränglig vegetation. Även aktiva säkerhetsskyddsåtgärder som att mörklägga ett utrymme eller nyttja dimgeneratorer och använda störande blixtljus kan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

8.1.2 Fördröjningstid

Fördröjningstid (T_F) kan beskrivas som den tid den fysiska säkerheten försvårar för en antagonist från att angreppet initieras tills denne når sitt mål. T_F beräknas genom formeln nedan, där T2 är tiden då ett fysiskt angrepp 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, räknat utifrån var det obehöriga tillträdet påbörjas (Figur 7).



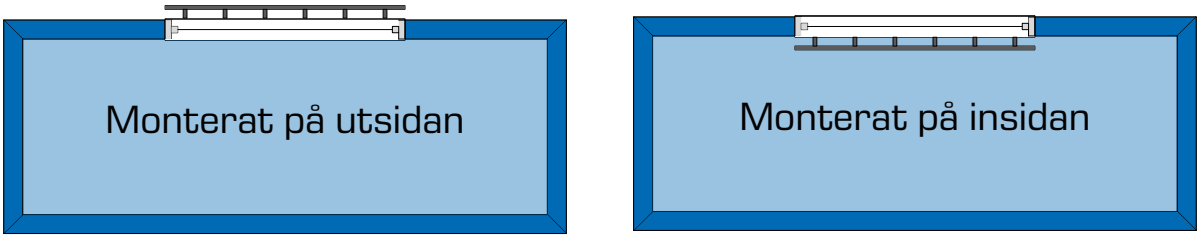
Figur 7: Exempel på beräkning av total fördröjningstid.

En fördröjande säkerhetsskyddsåtgärd som inte kombineras med föregående säkerhetsskyddsåtgärder för upptäckt ger ett begränsat 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. Om gallret däremot är monterat på insidan kommer larmet att aktiveras innan forcering av gallret kan påbörjas, eftersom att 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 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 utanför byggnaden.

T_F beror också på en antagonists verktyg, kunskaper och färdigheter. En dörr 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 använder en bensindriven motorkap.



Figur 8: Galler monterat på insidan bidrar till mer fördröjning än när det är monterat på utsidan i de fall upptäckt först sker när fönsterglaset krossas.

8.1.3 Förvaringsenheter

3 kap. 10 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd

För förvaring av säkerhetsskyddsklassificerade handlingar kan säkerhetsskåp som är certifierade och provade enligt standarden SSF 3492 vara en lämplig utgångspunkt, då dessa ger ett skydd mot grundläggande antagonistiska förmågor. Vilken typ av förvaringsenhet som nyttjas behöver dock ha sin grund i det säkerhetsskyddsbehov som verksamhetsutövaren har identifierat. Val av förvaringsenhet måste alltså utgå från skyddsvärdet, vad förvaringsenheten ska klara av att skydda mot och den fysiska säkerheten i övrigt. 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 högre förmåga under någon enstaka minut.

Notera: En förvaringsenhet i sig utgör inte fysisk säkerhet, utan måste kompletteras med upptäckande och hanterande säkerhetsskyddsåtgärder.

I de fall då innehållet är skyddsvärt ur ett tillgänglighetsperspektiv bör även brandskyddet för den aktuella förvaringsenheten kontrolleras. Brandskydd är ofta frivilligt att pröva när förvaringsenheter certifieras enligt vanligt förekommande standarder, även om det finns undantag.

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

Ansvaret för förvaringsutrymmen där säkerhetsklassificerade handlingar finns bör regleras i verksamhetsutövarens interna bestämmelser.

8.2 Styrning av tillträde

Styrning av tillträde kan beskrivas som styrning av vem som har behörighet att tillträda olika delar av en säkerhetskänslig verksamhet. I vissa fall räcker det att styra tillträdet för utomstående och i andra fall kan det behöva omfatta även vissa delar av den egna personalen. Exempelvis kan det finnas delar av säkerhetskänsliga verksamheter som kräver särskild utbildning för att få tillträdesbehörighet. Ytterligare en del av styrning av tillträdet kan vara att reglera vad som inte får medföras till den säkerhetskänsliga verksamheten, exempelvis mobiltelefoner, smarta klockor, verktyg eller farliga ämnen.

Om flera verksamhetsutövare bedriver verksamhet inom samma anläggning bör samverkan ske kring hur den fysiska säkerheten ska utformas för gemensamma utrymmen.

8.2.1 Behörighetskontroll

5 kap. 5 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd

Den fysiska säkerheten ska utformas med behörighetskontroll i syfte att kontrollera att endast behöriga får tillträde till en plats där säkerhetskänslig verksamhet bedrivs.

Behörighetskontroll kan avse att vid inpassering fastställa en persons identitet och rättighet att få tillträde till verksamhetsutövarens områden, byggnader, anläggningar eller objekt. Det kan också avse att vid utpassering fastställa att de som har besökt verksamhetsutövaren också lämnar platsen, att inget otillåtet förs ut samt vid behov även kontrollera besökares rätt till tillträde och uppehållstid.

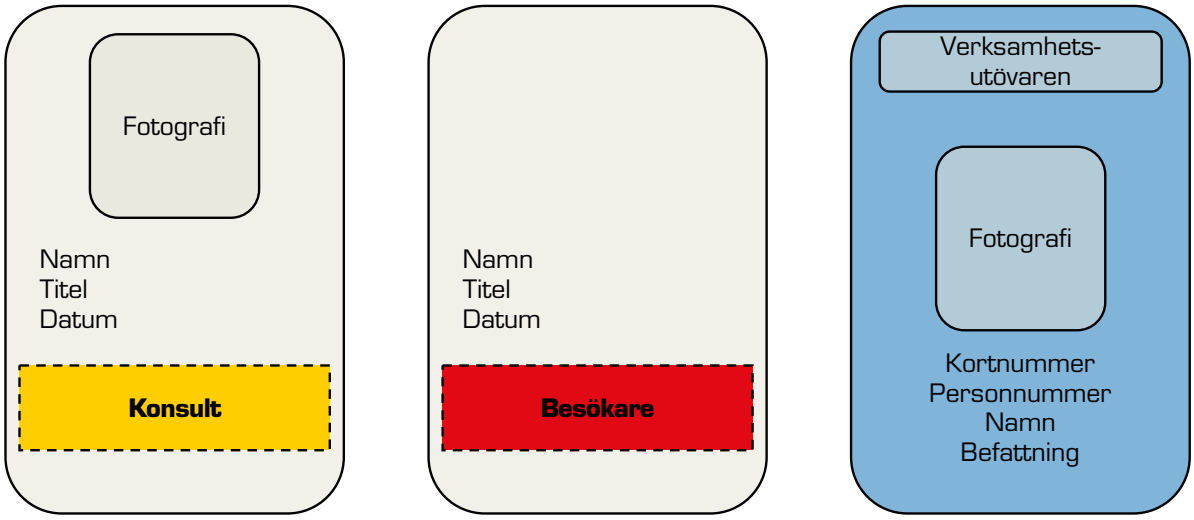
8.2.2 Besökstillstånd

5 kap. 5 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd

När personer som i vanliga fall inte har tillträde till en plats där säkerhetskänslig verksamhet bedrivs ska besöka sådana platser ska skriftligt besökstillstånd utfärdas.

För besökare behövs rutiner gällande identifiering och hantering, som exempelvis krav på legitimering med godkänd legitimation och inskrivning i en förteckning med ankomsttid, uppgift om vilken verksamhet denna representerar samt besöksmottagare.

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 (Figur 9). Verksamhetsutövaren bör även ta fram rutiner som tydliggör hur besökare ska hanteras samt vilket ansvar besöksmottagare har.



Figur 9: Exempel på kategorispecifika besökskort som skiljer sig mot verksamhetsutövarens egna tjänstekort.

8.2.3 Passersystem

5 kap. 6 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd

Verksamhetsutövaren ska ha ett passersystem för identifiering eller behörighetskontroll för åtkomst till utrymmen där det kan ges tillgång till säkerhetskänslig verksamhet. Systemet ska omges av säkerhetsskyddsåtgärder som motsvarar vald skyddsdimensionering.

Passersystem kan beskrivas som en del av åtgärderna för styrning av tillträde. De styr, identifierar och registrerar personers åtkomst till utrymmen och platser där säkerhetsskyddsklassificerade uppgifter finns eller där säkerhetskänslig verksamhet i övrigt bedrivs. Syftet med passersystem är att försvåra 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 består av en obevakad spärr som går att hoppa över. Avgörande för utformningen av passersystem är om det ska kunna identifiera behöriga, men även andra funktioner kan vara viktiga, exempelvis om systemet ska registrera antal passager och om behörigheter snabbt ska kunna ändras.

Oavsett vilken typ av passersystem som används bör både inpassering och utpassering registreras. Där automatiska passersystem finns bör som lägsta nivå kort med personlig kod användas vid både inpassering och utpassering.

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 förses med exempelvis kameraidentifikation, biometriska läsare eller logik som kräver att två personer tillsammans måste öppna passagen till utrymmet.

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

8.2.4 Kort, koder, nycklar och liknande

5 kap. 7 och 8 §§ Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd

Verksamhetsutövaren ska ställa krav på att kort, koder, nycklar eller liknande som ger åtkomst till utrymmen där det kan ges tillgång till säkerhetskänslig verksamhet, förvaras så att någon obehörig inte kan få tillgång till dem. Verksamhetsutövaren bör även ta fram hanteringsregler för nycklar som för tillfället inte förvaras.

Om det befaras att kort, kod, nycklar eller liknande har stulits, förlorats eller kopierats ska detta omedelbart hanteras som en säkerhetshotande händelse.

Verksamhetsutövaren ska ha en förteckning över kort, koder, nycklar eller liknande som hör till utrymmen där det kan ges tillgång till säkerhetskänslig verksamhet. Av förteckningen ska det framgå till vem och när kort, kod, nyckel eller liknande har lämnats och var reservkod eller reservnyckel förvaras. Det ska vidare framgå när återlämnande skett.

Koder bör ändras regelbundet och vid behov, exempelvis om koden misstänks blivit röjd, när ett lås har genomgått underhållsarbete och reparation, eller när en person slutar sin anställning eller inte längre behöver tillgång till det berörda utrymmet.

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

8.3 Skadereducerande säkerhetsskyddsåtgärder

5 kap. 3 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd

Skadereducerande säkerhetsskyddsåtgärder syftar till att minska skadeverkningarna av angrepp 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, skapa skyddsavstånd samt att använda byggnadstekniska förstärkningar för att minimera verkan av splitter eller stötvågseffekter och förhindra fortskridande ras.

Skadereducerande säkerhetsskyddsåtgärder ska även försvåra mot 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 och avsiktliga elektromagnetiska hot.

Varje typ av skadereducerande säkerhetsskyddsåtgärd har egenskaper som måste anpassas utifrån vad den fysiska säkerheten ska klara av att skydda mot. Olika typer av fordonsstoppande skydd, till exempel pollare, är utformade för att kunna motstå olika typer av påkörningar utifrån fordonens vikt, höjd, hastighet och anslagsvinkel. Även byggnadstekniska förstärkningar till skydd mot till exempel explosioner måste anpassas utifrån vilket avstånd och vilken totalvikt av sprängämnen de ska klara av att skydda mot.

8.3.1 Skydd mot obehörig avlyssning av samtal

Obehörig avlyssning kan beskrivas som att i hemlighet obehörigen avlyssna eller spela in samtal. Obehörig avlyssning kan ske med eller utan tekniska hjälpmedel för återgivning av ljud. Det finns flera olika sätt att skydda mot avlyssning av samtal om säkerhetsskyddsklassificerade uppgifter. Dessa säkerhetsskyddsåtgärder har sin utgångspunkt i säkerhetsskyddsanalysen och behöver utformas olika beroende på vilken säkerhetsskyddsklass uppgifterna har samt vad den fysiska säkerheten ska klara av att skydda mot.

Ett sätt att förebygga obehörig avlyssning är att använda särskilda avlyssningsskyddade (ASK) utrymmen. För mer information om hur man kan förebygga obehörig avlyssning av samtal, se Säkerhetspolisens delvägledning i fysisk säkerhet om avlyssningsskyddade utrymmen. Delvägledningen går att hitta på www.sakerhetspolisen.se

8.3.2 Skydd mot röjande signaler

3 kap. 4 § säkerhetsskyddsförordningen (2018:658)

Verksamhetsutövare som ansvarar för ett informationssystem som ska användas i säkerhetskänslig verksamhet ska beakta risken för röjande signaler (RÖS) och vidta lämpliga skyddsåtgärder för systemet om informationssystemet avses behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller om obehörig åtkomst till informationssystemet kan medföra en skada för Sveriges säkerhet som inte är obetydlig.

RÖS är elektromagnetiska eller akustiska signaler som alstras i informationsbehandlande utrustningar och som, om de kan tydas av obehöriga, kan bidra till att information röjs. Skydd mot elektromagnetisk RÖS kan uppnås genom att använda RÖS-inmätt utrustning i kombination med avstånd mellan verksamhetsutövarens yttre och inre delar av skyddslöken.

Utöver avståndet behöver även hänsyn tas till hur mycket de röjande signalerna dämpas av byggnadstekniska egenskaper. Byggnadens material och läge kommer att ha stor påverkan på hur de röjande signalerna kan sprida sig från den signalerande utrustningen. På samma sätt påverkar byggnadens anslutning till elnätet hur ledningsburna signaler sprider sig till omgivningen. I vissa fall behöver tekniska system separeras från varandra för att inte signalerna ska kunna sändas ut externt genom öppna system som exempelvis en radiosändare.

Generellt är det bra att eftersträva att placera denna typ av utrustning så centralt som möjligt, gärna under mark. För en mer noggrann bedömning av dämpande egenskaper kan en så kallad dämpningsmätning utföras.

Skydd mot RÖS kan även uppnås genom att använda ett så kallat RÖS-skyddat utrymme. Ett sådant utrymme omges av ett sammanhängande metallhölje, genomföringar och ledningar, vilket förebygger att röjande signaler sprider sig utanför utrymmet. RÖS-skyddade utrymmen kan också upprättas i mindre skala för särskild utrustning, så kallade RÖS-kabinetter.

Vidare kan vissa verksamhetsutövare ha ett behov av att skydda mot akustiskt röjande signaler, vilket kan uppnås genom liknande säkerhetsskyddsåtgärder som för att skydda mot obehörig avlyssning av samtal.

8.3.3 Skydd mot insyn

Det finns flera olika sätt att skydda mot att någon obehörig med eller utan tekniska hjälpmedel kan se delar av den säkerhetskänsliga verksamheten, eller ta del av säkerhetsskyddsklassificerade uppgifter genom exempelvis kameror eller kikare. Bland annat kan film på fönster 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.

8.3.4 Skydd mot kemiska och biologiska hot

Om den fysiska säkerheten ska klara av att skydda mot angrepp med kemiska och biologiska medel finns flera olika typer av säkerhetsskyddsåtgärder. Till exempel kan kontroll av inkommande post och gods upptäcka försändelser med farliga ämnen. Ytterligare exempel är att sektionera lufttillförsel och att nyttja filter vid luftintag för att förhindra spridning av giftiga gaser.

8.3.5 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 skyddsvärden, och därmed kan skador undvikas eller reduceras. Genom att sänka hastigheten kan man minska ett fordons rörelseenergi och därmed den skada fordonet kan orsaka.

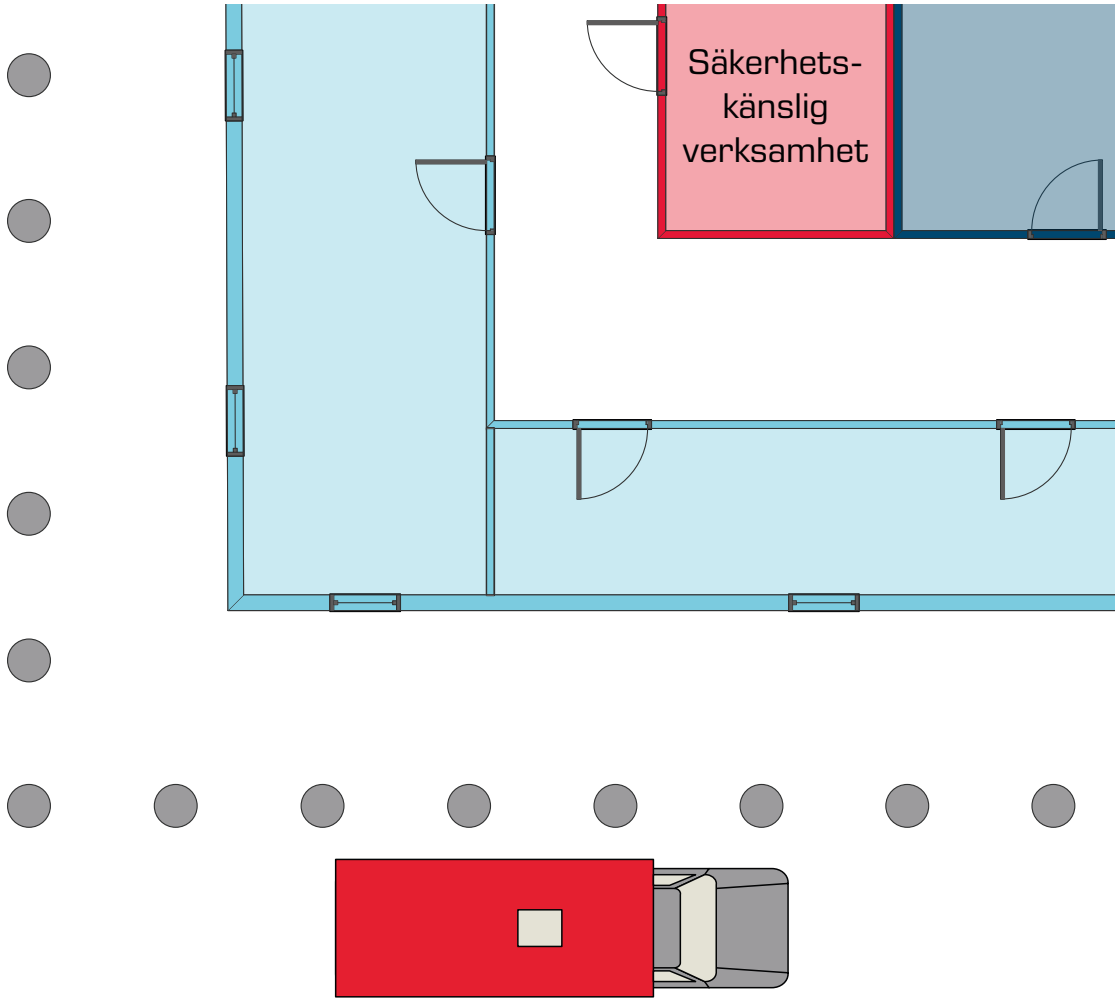
För att skydda mot forcering med fordon kan säkerhetskyddssåtgärder i form av stoppande hinder användas, exempelvis murar, kraftiga pollare eller naturliga hinder, men det finns även hastighetsreducerande säkerhetsskyddsåtgärder såsom chikaner och spikmattor. De flesta verksamheter behöver åtminstone 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.

8.3.6 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 en anläggning. Samtliga aspekter gällande stötvåg, värme och splitter behöver tas i beaktande vid utformandet av skadereducerande säkerhetsskyddsåtgärder mot explosioner.

Att skydda sig mot explosioner handlar dock i grunden om att skapa avstånd till laddningen. Avståndet som krävs från laddningen beror på typen av explosivämne och laddningens storlek.

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 laddning och ytterväggg.



Figur 10: Exempel på pollare och utrymmenas placering som skapar avstånd mellan den säkerhetskänsliga verksamheten och säkerhetshotet.

8.3.7 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.

8.3.8 Skydd mot obemannade luftfartyg (UAS)

Skydd mot UAS kan utformas på motsvarande sätt som den fysiska säkerheten i övrigt, då UAS främst är plattformar för andra säkerhetshot, exempelvis att leverera explosiv last eller få insyn genom bildupptagning. Detta innebär att en UAS behöver upptäckas, försvåras och hanteras, precis som andra typer av säkerhetshot. Innehåller skyddsdimensioneringen att en UAS för med sig explosiv last, kan skyddsåtgärder mot explosioner beaktas, det vill säga att exempelvis skapa skyddsavstånd mellan skyddsvärdet och UAS. Består säkerhetshotet istället av att en UAS får insyn i en säkerhetskänslig verksamhet på distans, kan skyddsåtgärderna mot insyn beaktas, exempelvis genom att använda insynsskyddande film på fönster.

UAS är ett komplext och relativt nytt säkerhetshot. Även om mycket utveckling har skett gällande skydd mot UAS de senaste åren är passiva och byggnadstekniska lösningar fortfarande några av de mest effektiva skydden idag. Detta kan komma att ändras framgent när lagar anpassas och nya metoder för att upptäcka och hantera UAS uppstår.

9 Hanterande säkerhets-skyddsåtgärder

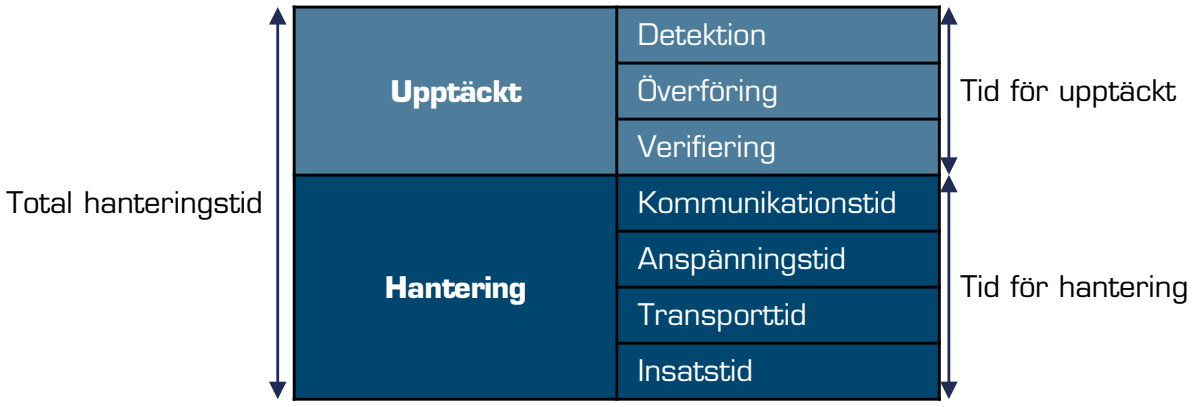
5 kap. 4 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd

Verksamhetsutövaren ska, i den omfattning som skyddsdimensioneringen kräver, 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 förebygga ett obehörigt tillträde eller skadlig inverkan har stor inverkan på behovet av upptäckande och försvårande säkerhetsskyddsåtgärder. Vidare måste hanteringsförmågan ställas i relation till vad den fysiska säkerheten ska klara av att skydda mot.

9.1 Hanteringstid

Hanteringstid är den tid som behövs för att initiera och verkställa hanterande säkerhetsskyddsåtgärder i den omfattning som krävs för att avbryta obehörigt tillträde eller skadlig inverkan. Hanteringstiden räknas från att en antagonist upptäcks till dess att en antagonistisk handling kan avbrytas eller konsekvensreduceras. Hanteringstid består av tiden det tar att upptäcka ett antagonistiskt angrepp och tiden det tar för den hanterande förmågan att larmas, förbereda insatsen, förflytta sig till insatsen och genomföra själva insatsen. Detta kan översättas till kommunikationstid, anspänningstid, transporttid och insatstid (Figur 11).



Figur 11: Den totala hanteringstiden består av tiden det tar från första upptäckt till dess att obehörigt tillträde eller skadlig inverkan kan avbrytas eller konsekvensreduceras.

Förmågan att hantera ett angrepp är ofta beroende av externa aktörer, till exempel vaktbolag eller polisen. Hur snabbt dessa behöver vara på plats beror i stor utsträckning på hur länge ett angrepp kan fördröjas. Hanteringstiden är således vägledande för utformningen av upptäckande och försvårande åtgärder.

9.2 Hanteringsförmåga

Den hanterande förmågans förkunskaper, 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, medan det vid andra tillfällen kan finnas behov av mer kvalificerad förmåga i form av särskilda funktioner inom polisen.

9.3 Konsekvensreducerande hantering

I det fall ett obehörigt tillträde eller skadlig inverkan inte går att förhindra eller hantera fullt ut kan konsekvensreducerande hantering lindra effekterna av ett mer eller mindre lyckat angrepp och underlätta återgång till normalläge. Detta kan exempelvis göras genom att teknik för larm och fastighetsstyrning kopplas samman för att kunna stänga ventilationssystem vid ett angrepp med kemiska ämnen eller genom att förbereda rutiner för att flytta skyddsvärda objekt ifall uppgifter om deras position skulle röjas.

10 Kontroll och utvärdering

2 kap. 26 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd

Utvärdering och kontroll syftar till att bedöma huruvida den fysiska säkerheten lever upp till det identifierade säkerhetsskyddsbehovet och ger avsedd effekt. Utvärdering av planerad utformning kan exempelvis ske inför ombyggnationer och regelbundna kontroller av olika slag kan göras för att säkerställa att den fysiska säkerheten inte försämras över tid. Verksamhetsutövaren ska dokumentera åtgärderna 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 verksamhetsutövarens 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.

Typ av kontroll	Upptäcka	Försvåra	Hantera
Komponentkontroll	Upptäcker en viss typ av larmsensor rörelse som de ska?	Hur länge fördröjer en dörr 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 lagren i skyddslöken 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 anläggningen?	Finns tillräckliga försvårande säkerhetsskyddsåtgärder för att fördröja obehörigt tillträde och reducera skadlig inverkan av ett angrepp 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.			

Tabell 1: Exempel på kontroll i olika omfattning.

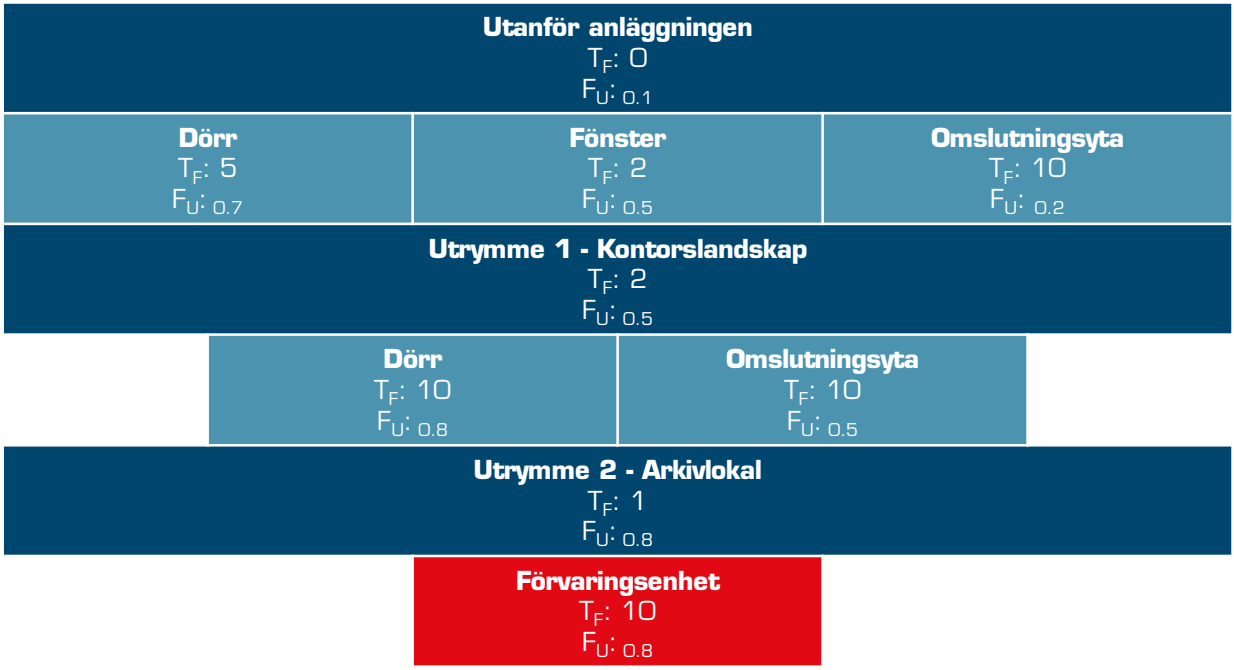
10.1 Angreppsanalys

Angreppsanalys kan beskrivas som en analys av huruvida den fysiska säkerheten upptäcker, försvårar och hanterar de säkerhetshot som verksamhetsutövaren identifierat. Resultatet av angreppsanalysen kan antingen verifiera att den fysiska säkerheten är tillfredställande, eller identifiera sårbarheter som innebär att ytterligare säkerhetsskyddsåtgärder 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 och forcering av lager en antagonist behöver utföra på väg fram till ett skyddsvärde. Denna typ av analys av så kallade angreppsvägar består av fem steg.

10.1.1 Analys av angreppsväg - Steg 1

Första steget är att kartlägga en anläggnings olika lager av fysisk säkerhet. Detta görs genom att dela upp en anläggning i fysiska lager och mellanliggande utrymmen med redan förekommande eller planerade säkerhetsskyddsåtgärder i respektive lager eller utrymme. Efter att en anläggnings fysiska säkerhet har kartlagts berikas respektive lager och säkerhetsskyddsåtgärd med fördröjningstid (T_F) och upptäcktsfaktor (F_U) (Figur 12).

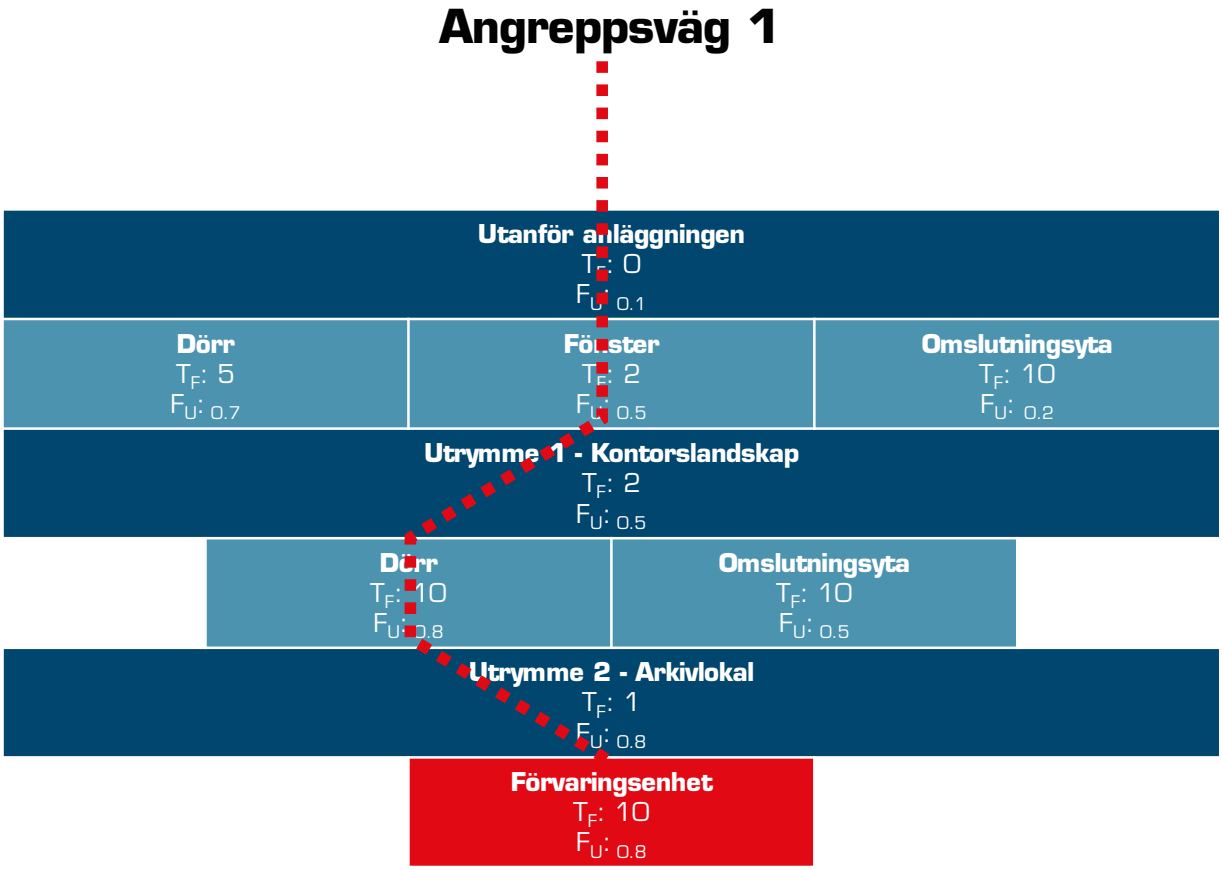


Figur 12: Exempel på kartläggning av en anläggning.

10.1.2 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 13 illustreras detta genom att en antagonist rör sig in till anläggningen genom ett fönster för att därefter ta sig genom en dörr fram till ett arkiv där skyddsvärdet i form av en förvaringsenhet med säkerhetsskyddsklassificerade handlingar finns.

Var observant på om en antagonist kan passera flera lager samtidigt och även undgå upptäckt, till exempel genom tak eller golv. I så fall måste analysen utökas med dessa lager och eventuella angreppsvägar som innebär att en antagonist kan förflytta sig mellan ett lager och ett annat, utan att passera något mellanliggande lager. Det vill säga som att ”hoppa” mellan det första och tredje lagret av fysisk säkerhet i en anläggning, utan att passera det andra lagret.



Figur 13: Exempel på analys av angreppsväg.

10.1.3 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 i skyddslöken 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.

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 på sig kommer denne att lyckas, även om angreppet upptäcks tidigt.

	Angreppsväg 1 Hanteringstid: 15 minuter				
Uppgift		**F_U**	**T_F (min)**	**Kvarvarande tid (min)**	**KUT**
1	Förbereda angrepp	0.1	00:00	25:00	
2	Forcera fönster	0.5	02:00	25:00	
3	Röra sig igenom kontorslandskap	0.5	02:00	23:00	
4	Forcera dörr	0.5	10:00	21:00	X
5	Röra sig igenom arkivet	0.8	01:00	11:00	
6	Forcera förvaringsenhet	0.8	10:00	10:00	
7	Angreppet slutfört	-	-	00:00	

Tabell 2: Angreppsväg 1 med upptäcktsfaktor, fördröjningstid och kritiskt upptäcktstillfälle (KUT)

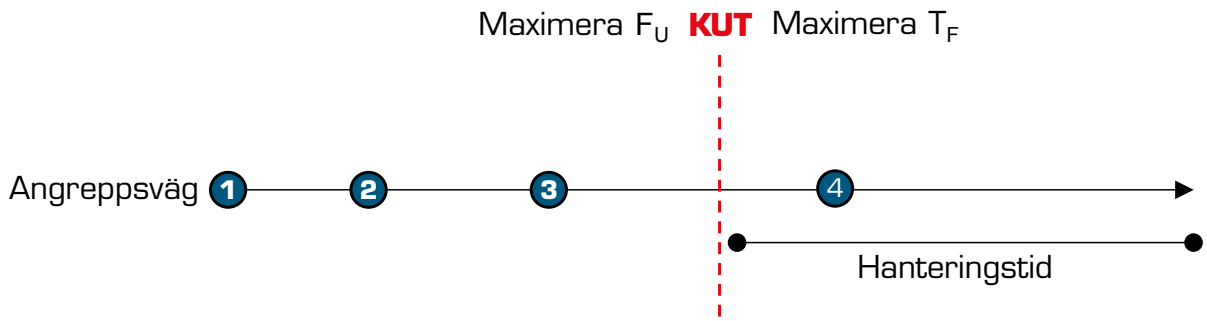
10.1.4 Analys av angreppsväg - Steg 4

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.

Figur 14 illustrerar en angreppsväg med fyra möjligheter till upptäckt. Utifrån hanteringstiden blir brytpunkten för när upptäckt sker för sent någonstans mellan det tredje och fjärde upptäcktstillfället. Eftersom det fjärde tillfället att upptäcka ett obehörigt tillträde sker då hanteringstiden är längre än antagonistens kvarstående tid för att lyckas med sitt angrepp bidrar den inte till den fysiska säkerheten. Då det saknas upptäckande förmåga i brytpunkten blir således det tredje upptäcktstillfället KUT.

När alla uppgifter är listade räknas antagonistens kvarvarande tidsbehov ut genom att addera fördröjningstiderna från skyddsvärdet och utåt. Därefter kan KUT fastställas genom att ställa hanteringstiden i relation till kvarvarande tidsbehov. I exemplet i Tabell 2 är hanteringstiden 15 minuter och upptäckt måste teoretiskt ske innan antagonisten kommit halvvägs genom dörren till arkivet. I praktiken blir KUT när antagonisten rör sig fram mot dörren och börjar forcera den.

Generellt sett gäller att fokusera på att upptäcka ett obehörigt tillträde eller skadlig inverkan innan KUT, för att därefter maximera fördröjande säkerhetsskyddsåtgärder. Detta eftersom att upptäckt som sker efter KUT ändå innebär att ett angrepp kommer att upptäckas för sent.



Figur 14: KUT är tillfället där upptäckt senast måste ske för att hanterande säkerhetsskyddsåtgärder ska hinna hantera angreppet

10.1.5 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.

Då KUT för angreppsväg 1 (Tabell 2) är vid 21:00 (uppgift nummer 4) beräknas förmågan att hantera angreppet utifrån den upptäcktsfaktor som existerar fram till dess. Detta ger en upptäcktsfaktor på 0.89, vilket har beräknas utifrån formeln nedan.

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

10.2 Övningar

Genom att öva kan verksamhetsutövaren identifiera sårbarheter vad gäller exempelvis för 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 kvalitativ angreppsanslys bestå av att analysera ett fiktivt scenario genom exempelvis en skrivbordsövning. Resultatet av dessa övningar bör dokumenteras och användas som underlag för förbättringar av den fysiska säkerheten.

$$1- \quad (1-0.1) \quad \times \quad (1-0.5) \quad \times \quad (1-0.5) \quad \times \quad (1-0.5) \quad = \quad \underline{0.89}$$

11 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 för anpassning av den fysiska säkerheten. Vid bevakning av ett skyddsobjekt har bevakningspersonalen, så kallade skyddsvakter, särskilda befogenheter vad gäller exempelvis kontroll av personer och fordon.

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.

12 Service och underhåll

En plan för service och underhåll av den fysiska säkerheten bör finnas dokumenterad. En sådan plan bör omfatta såväl mekaniska säkerhetsskyddsåtgärder, till exempel dörrar och säkerhetsglas, som tekniska system. Planen kan också innefatta specifikt underhåll av särskilda utrymmen, exempelvis avlyssningsskyddade (ASK) utrymmen.

Det bör även finnas en plan för revision av system och funktioner, i syfte att påträffa 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 bör backup och test av system genomföras 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.

13 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 standarder och normer.

Dessa kan vara vägledande i arbetet med den fysiska säkerheten och utgöra en bra grund som verksamhetsutövaren kan anpassa sitt skydd efter. Det är dock viktigt att känna till att en säkerhetsprodukt 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 norm eller standard kan endast förväntas stå emot en antagonist med samma utrustning och tillvägagångssätt som föreskrivs i kraven för provning. Exempelvis kan en dörr provas 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.

Då fördröjningstiden avgörs av en antagonists 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. Om verksamhetsutövaren enbart utgår ifrån standarder och normer kan säkerhetskänsliga verksamheter komma att kravställa den fysiska säkerheten mot en standard som inte tillfredsställer det identifierade säkerhetsskyddsbehovet. Följaktligen är det viktigt att analysera behovet av säkerhetsskyddsåtgärder baserat på vad den fysiska säkerheten ska klara av att skydda mot. Med detta resultat som grund kan verksamhetsutövaren motivera säkerhetsskyddsåtgärder som omhändertar hoten på ett realistiskt sätt och inte bara hänvisa till standarder och normer.

14 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 verksamhetsutövaren behöver alltid utgå från sin egen säkerhetsskyddsanalys.

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 skyddsvärde, säkerhetshot och sårbarheter identifierade i säkerhetsskyddsanalysen.
- ☐ Kontroll har skett för att säkerställa att den fysiska säkerheten når upp till de krav verksamhetsutövaren ställt.

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 som kan utnyttjas av en antagonist.
- ☐ Kompensatoriska åtgärder har förberetts.
- ☐ 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 i skyddslöken.
- ☐ 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.
- ☐ Diversitet i den fysiska säkerheten har beaktats.
- ☐ Kritiska delar av den fysiska säkerheten har redundans.
- ☐ Den fysiska säkerheten har anpassats för att skydda mot insiders vid behov.

Upptäckande säkerhetsskyddsåtgärder

- ☐ Det finns personell bevakning och/eller teknisk övervakning för att tidigt upptäcka obehörigt tillträde och skadlig inverkan.
- ☐ Principer för upptäckande funktion har beaktats vid val av tekniska övervakningssystem.
- ☐ Upptäckande säkerhetsskyddsåtgärders upptäcktsfaktor är tillräckliga utifrån vald skyddsdimensionering.

Försvårande säkerhetsskyddsåtgärder

- ☐ Säkerhetsskyddsåtgärder för att fördröja obehörigt tillträde ger tillräcklig tid för att hinna vidta hanterande säkerhetsskyddsåtgärder.
- ☐ Det finns säkerhetsskyddsåtgärder för att reducera skadan av angrepp som inte går att fördröja.
- ☐ Det finns rutiner för att hantera och kontrollera behörigheter för både besökare och egen personal.
- ☐ Det finns passersystem för identifiering och/eller behörighetskontroll.
- ☐ Kort, koder, nycklar eller liknande som ger åtkomst till utrymmen där det kan ges tillgång till säkerhetskänslig verksamhet, förvaras så att obehöriga inte kan få tillgång till dem.
- ☐ Det finns rutiner för och förteckningar över hantering av kort, koder, nycklar och liknande.
- ☐ Förvaringsenheter för säkerhetsskyddsklassificerade handlingar har valts utifrån ett identifierat säkerhetsskyddsbehov.

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 för 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.

Service, underhåll och vidmakthållande

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

15 Ändringslogg

15.1 Version 2.0 (september 2020)

Följande rubriker har lagts till:

- 4 Preskriptiva och funktionsbaserade synsätt
- 5.1 Processen för utformning av fysisk säkerhet
- 6.2 Balans i den fysiska säkerheten
- 6.7 Kompensatoriska åtgärder
- 6.8 Redundans och diversitet i den fysiska säkerheten
- 7.3 Upptäcktsfaktor
- 8.3.8 Skydd mot UAS
- 10 Kontroll och utvärdering
- 15 Angreppsanalys

Texten har justerats i följande rubriker:

- 5 Utformning av den fysiska säkerheten
- 6 Principer för fysisk säkerhet
- 7 Upptäckande säkerhetsskyddsåtgärder
- 8 Försvårande säkerhetsskyddsåtgärder
- 11 Skyddsobjekt och skyddslagen
- 13 Standarder och normer

Säkerhetspolisen

Säkerhetspolisen • Box 12312 • 102 28 Stockholm
Tel: 010-568 70 00 • Fax: 010-568 70 10
E-post: sakerhetspolisen@sakerhetspolisen.se
www. sakerhetspolisen.se