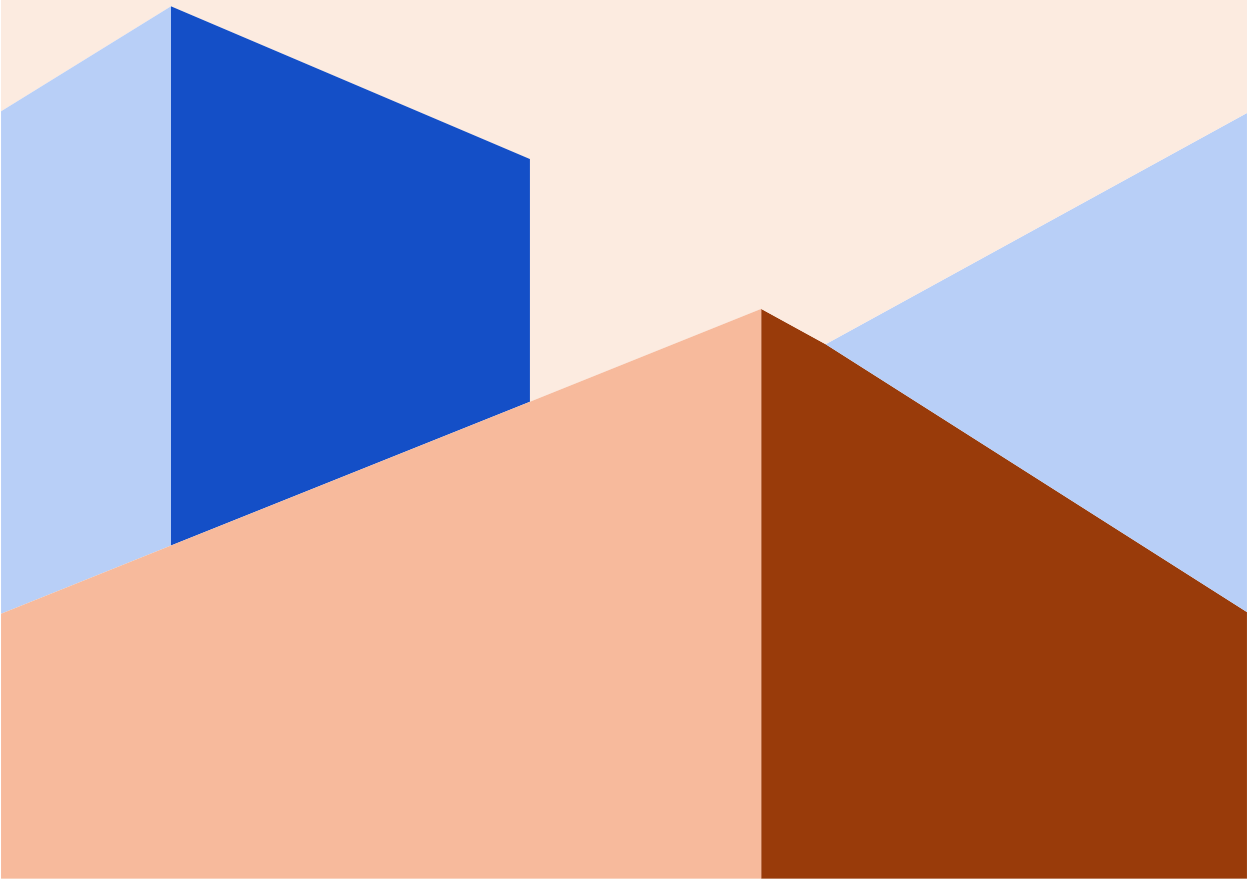


Trygg och säker informations-hantering

OFFENTLIGA FASTIGHETER

Offentliga fastigheter

Samarbetet Offentliga fastigheter består av organisationer som förvaltar många av Sveriges offentliga fastigheter. Tillsammans förvaltar vi skolor, myndighetsbyggnader, militära installationer, sjukhus och fängelser. I vårt nätverk finns en enorm bredd, inte bara av olika slags fastigheter utan också i form av olika slags erfarenheter. För att ta tillvara och utveckla vår breda kompetens har vi gått samman i Offentliga fastigheter.

Vi bedriver gränsöverskridande utvecklingsprojekt som bygger upp och sprider kompetens samt effektiviserar och förbättrar förvaltningen av våra gemensamma fastigheter. Projekten ska vara angelägna och väcka nya tankar. De ska visa på inspirerande exempel och erbjuda praktiska verktyg. Med andra ord projekt som inte bara gynnar oss själva utan också kan hjälpa och vägleda många fler. Bakom Offentliga fastigheter står Kommunfonden (FoU-fonden för kommunernas fastighetsfrågor), Fastighetsrådet (FoU-fonden för regionernas fastighetsfrågor), Fortifikationsverket, Specialfastigheter och Statens fastighetsverk.

Mer information hittar du på **www.offentligafastigheter.se**.

Trygg och säker informations-hantering

Trygg och säker informationshantering

ISBN 978-91-8047-198-5
Upplysningar om innehållet Bo Baudin, bo.baudin@skr.se
Text Lars Lidén Meta Fastighetsadministration AB och
Thomas Nilsson, Certezza AB
Omslagsillustration ETC Kommunikation
Produktion Advant
Webbplats www.offentligafastigheter.se

Förord

Ökad globalisering och digitalisering bidrar till förutsättningar för välstånd och tillväxt, men ökar samtidigt sårbarheter och risker. Den ökade informationsmängden som följer av digitaliseringen och det försämrade säkerhetspolitiska läget medför en ökad kravbild för hur vi hanterar information. Informationsägarskap, konfidentialitet, riktighet och tillgänglighet är centrala begrepp i en klok informationshantering.

Denna skrift tillkom ur ett behov att bemöta frågeställningar som rör informationshantering inom fastighetsområdet. Skriften beskriver hur olika lösningar kan utformas och belyser möjligheter och utmaningar med olika lösningsförslag. Flera av de utmaningar som berörs följer av de lagar och regler som i olika grad träffar verksamheterna.

Projektet har initierats och finansierats av Offentliga fastigheter. Johannes Ryberg, Thomas Nilsson, Greger Westberg och Linus Kilander Xu, Certezza AB samt Lars Lidén och Alexandra Lindgren, Meta Fastighetsadministration AB har varit utredare och skribenter. En styrgrupp bestående av Andreas Persson, Familjebostäder Stockholm; Anders Gidrup, Locum; Henrik Bjerneld, Härnösands kommun; Mats Lidskog, Västfastigheter Västra Götalandsregionen; Kristoffer Hellsten, Regionfastigheter Skåne; Masse Antonsson, Specialfastigheter; John Öberg, Fortifikationsverket och Anna-Karin Wiberg, Statens fastighetsverk har medverkat i arbetet och lämnat värdefulla synpunkter.

Bo Baudin, Sveriges Kommuner och Regioner, har varit projektledare.

Stockholm i september 2023

Gunilla Glasare
Avdelningschef

Peter Haglund
Sektionschef

Avdelningen för Tillväxt och samhällsbyggnad

Sveriges Kommuner och Regioner

Innehåll

Sammanfattning

I och med den nya säkerhetsskyddslagstiftningen tas ett större grepp kring informations- och cybersäkerheten. Detta, tillsammans med att de existerande och kommande EU-direktiven NIS, NIS2 och CER kommer med hårdare krav för en bredare grupp av organisationer, lämnar offentliga fastighetsägare i behov av vägledning och metodik. Tiden då den digitala sfären var relativt oreglerad är förbi.

I många situationer interagerar flera regelverk såsom NIS-direktivet, CER-direktivet och säkerhetsskyddslagen med varandra samt med andra regelverk som exempelvis offentlighets- och sekretesslagen (OSL). En organisation kan träffas av flera av regelverk. Det är inte ovanligt att organisationen kan ha viss verksamhet som träffas av ett regelverk och andra verksamheter som träffas av andra regelverk. Det är därför nödvändigt att känna till var gränserna går mellan olika regleringar samt hur de interagerar med varandra när de samverkar.

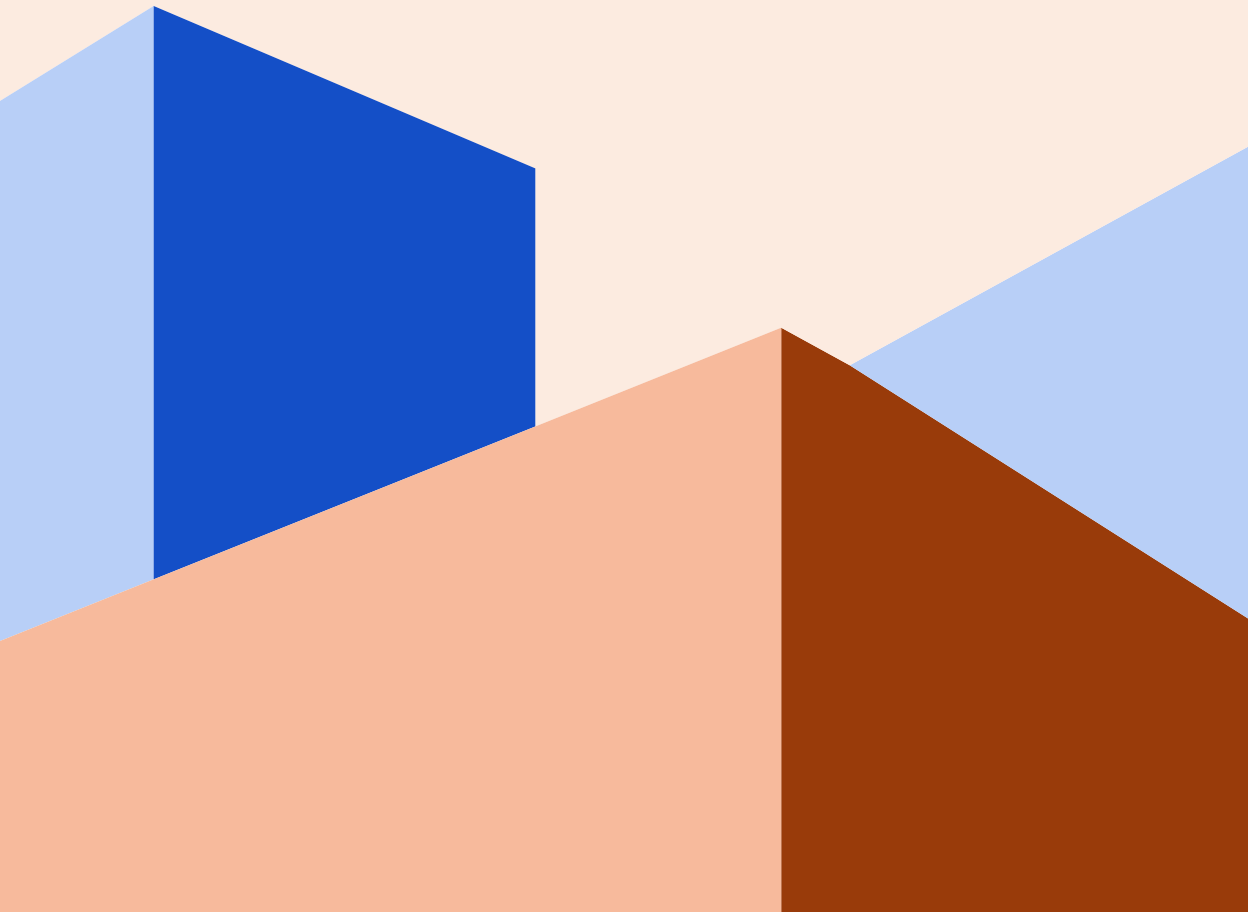
Regelverken från EU är relativt tydliga med vilka verksamheter som berörs. Vad gäller säkerhetsskydd är det den som till någon del bedriver säkerhetskänslig verksamhet som själv ska utreda behovet av säkerhetsskydd genom en säkerhetsskyddsanalys. Den metodiken svarar också på frågan om verksamheten bedriver någon säkerhetskänslig verksamhet. Med utgångspunkt i analysen ska verksamhetsutövaren själv planera och vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning, förekomst av säkerhetsskyddsklassificerade uppgifter och övriga omständigheter.

För att mer detaljerat bedöma hur man ska hantera sina anläggningar/byggnader är det viktigt att identifiera lämpliga analysobjekt och hur detaljerat anläggningen ska studeras. Ett sätt är att utgå från anläggningens uppbyggnad dvs olika byggdelar och tekniska system och med det som grund fundera kring skyddsvärden, hot, sårbarheter och skyddsåtgärder.

Ett systematiskt riskhanteringsarbete är den drivande motorn bakom ett informations- och cybersäkerhetsarbete med förmåga att både säkerställa regelefterlevnad samt för att harmonisera med organisationens strategi och riskarbete i övrigt.

Denna vägledning är tänkt att fungera som en ledstång genom dessa ibland svåra passager där juridik varvas med metodik och handfasta exempel med hög igenkänning i syfte att förenkla säkerhetsarbetet.

1



Inledning

1.1 Bakgrund

Svenska myndigheter och företag har haft ett par år på sig att anpassa sin organisation och sitt arbete till dataskyddsförordningen (GDPR) vilken fick mycket uppmärksamhet. NIS-direktivet, som implementerades i svensk lagstiftning 2018, har däremot hittills inte fått lika mycket uppmärksamhet. Ett förändrat säkerhetspolitiskt världsläge samt nya regleringsinsatser i form av två nya EU-direktiv kan förväntas att leda till ökat fokus på dessa nya regelverk och deras medföljande krav på motståndskraft och informationssäkerhet.

Systematiskt riskhanteringsarbete är grunden till och den drivande motorn bakom ett framgångsrikt informationssäkerhetsarbete. Samtliga ställningstaganden som en organisation, verksamhet, gruppering eller individ tar inom detta område behöver per definition vara motiverat av ett förhållande till risk. Riskhanteringsinsatser består av allt från att ta reda på vilka risker man har och vad de består av till att vidta åtgärder för att hantera risken och sedan följa upp effektiviteten av de vidtagna åtgärderna. Vikten av ett välfungerande riskhanteringsarbete är något som lagstiftarna både i EU och i Sverige har tagit fasta på. Samtliga direktiv, lagar, föreskrifter och vägledningar som har tagits fram nämner ett systematiskt riskhanteringsarbete som en essentiell obligatorisk ingrediens i medlemsländernas, myndigheternas och organisationernas informationssäkerhetsarbete.

Inom ramen för Offentliga fastigheters initiativ *Trygg och säker informationshantering* har ett stort fokus lagts på just riskhantering. Målbilden är att stötta de organisationer som har låg mognadsnivå och som inte sällan har svårt att formulera en risk. Oftast uttrycks mer en oro än en reell risk som går att analysera, värdera och mitigera. Det faktum att mognadsgraden är låg, och att myndigheter och standardiseringsorgan tenderar att dra åt olika håll gör inte saken enklare utan visar ytterligare på behovet av stöd och vägledning i frågan.

1.2 Syfte och målgrupp

I och med den nya säkerhetsskyddslagstiftningen tas ett större grepp kring informationssäkerhet och inte bara ur perspektivet konfidentialitet, utan även riktighet och tillgänglighet. Detta tillsammans med att de existerande och kommande EU-direktiven NIS, NIS2 och CER kommer med hårdare krav för en bredare grupp av organisationer lämnar offentliga fastighetsägare i behov av vägledning och metodik.

Syftet med dokumentet är att informera och orientera offentliga fastighetsägare i förhållningssättet till säkerhetsskyddslagen och de nyligen beslutade EU-direktiven NIS2 och CER samt att tillhandahålla en beskrivning och en vägledning i det systematiska riskhanteringsarbetet.

1.3 Effektmål

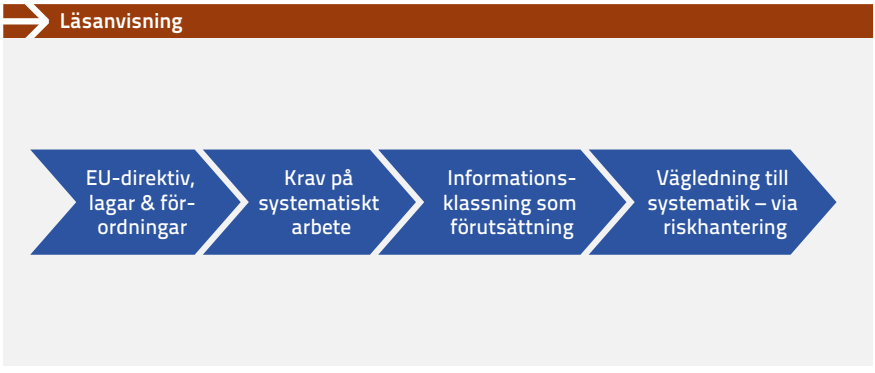
Bidra till ökad kunskap och förmåga att etablera, trygga och säkra informationsmiljöer ur ett offentligt fastighetsförvaltarperspektiv.

1.4 Läsanvisning

Detta dokument är utformad som en introduktion för att beskriva grundläggande delar, centrala begrepp och i förekommande fall vägledning och metodik inom områdena regulatoriska krav, informationskartläggning och -klassificering samt riskhantering. Dokumentet inleds med översiktliga beskrivningar som följs av fördjupning av begrepp. Till stöd för läsaren finns även sammanfattningar av respektive ämnesområde samt kompletterande informationsrutor innehållandes specifik vägledning.

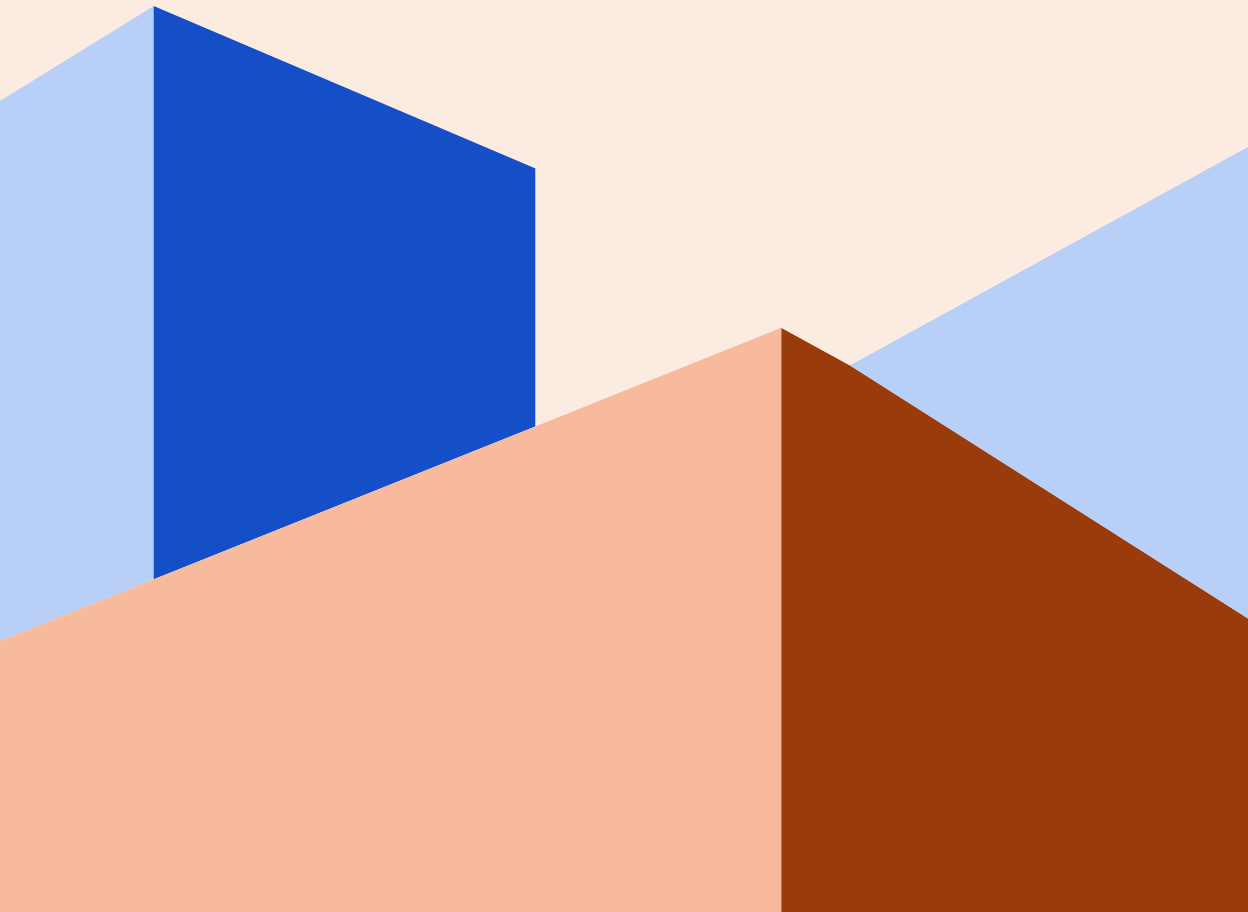
Dokumentet är uppdelat i två huvuddelar där de inledande kapitlen beskriver de regulatoriska konsekvenser som kommer från säkerhetsskyddslagen och de två EU-direktiven CER och NIS 2, och det avslutande kapitlet består av en beskrivning av och en vägledning i det systematiska riskhanteringsarbetet. Ett systematiskt riskhanteringsarbete är den drivande motorn bakom ett informationssäkerhetsarbete med förmåga att både säkerställa efterlevnad av dessa lagkrav samt att harmonisera med organisationens strategi- och riskarbete i övrigt.

Dokumentet kan läsas styckvis för information och vägledning inom utvalt område alternativt i sin helhet. I det senare fallet är dokumentet disponerat utefter ett flöde med utgångspunkt från lagtexterna, via de krav som kan ställas på organisationen till det nödvändiga systematiska informationssäkerhetsarbetet där riskhantering är centralt.



FIGUR 1 ▪ Disposition.

2



Säkerhets-skyddslagen

Säkerhetsskydd är de förebyggande åtgärder som behöver vidtas av organisationer för att skydda sådant som är av betydelse för Sveriges säkerhet. Om vissa myndigheter och företag i Sverige utsätts för antagonistiska (aktörsdrivna) handlingar eller om deras uppgifter röjs, förstörs eller ändras kan detta medföra störningar som kan få allvarliga konsekvenser för Sveriges säkerhet. Det kan till exempel handla om påverkan på verksamheter inom rättsväsendet, telekommunikation, transportsektorn, energi- eller vattenförsörjningen. Därför behöver säkerhetskänsliga verksamheter ett särskilt skydd. Organisationer som bedriver verksamhet eller hanterar information med koppling till Sveriges säkerhet bedriver så kallad säkerhetskänslig verksamhet och omfattas därmed av säkerhetsskyddslagstiftningen. Lagstiftningen ger hanteringsregler för hur säkerhetsskyddet ska utformas i syfte att skydda den säkerhetskänsliga verksamheten och dess information. Uppgifter som omfattas av säkerhetsskydd kallas för säkerhetsskyddsklassificerade uppgifter och måste markeras och hanteras i enlighet med tillsynsmyndighetens krav.

De hot som säkerhetsskydd inriktar sig mot är av antagonistisk karaktär och innefattar bland annat spionerі, sabotage, terrorism och andra brott som till exempel påverkansoperationer. Även verksamheter som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd, till exempel inom ramen för EU, FN eller NATO-samarbeten omfattas av säkerhetsskyddslagstiftningen.

Eftersom det säkerhetspolitiska läget i omvärlden försämrats under ett antal år har hotbilden mot Sverige och svenska intressen ökat. Detta har i sin tur aktualiserat behovet av ett stärkt säkerhetsskydd i de organisationer som bedriver verksamhet eller hanterar information som har betydelse för Sveriges säkerhet.

SAMMANFATTNING

Säkerhetsskydd och säkerhetsskyddsanalyser kan övergripande sammanfattas med följande punkter:

- **Lagen träffar potentiellt alla.** Säkerhetsskyddslagen träffar både myndigheter och privata företag. Sekretess enligt offentlighets och sekretesslagen (OSL) gäller till exempel i dessa fall även för privata företag.
- **Man kan vara träffad av två anledningar.** Träffas av lagen gör verksamhet som antingen:
  - Bedriver säkerhetskänslig verksamhet
  - Hanterar säkerhetsskyddsklassificerade uppgifter
- **Enbart antagonistiska hot** behandlas i säkerhetskyddsarbetet.
- **Säkerhetsskydd ska skapa ett heltäckande skydd** mot alla typer av antagonistiska hot.
- **En säkerhetsskyddsanalys** är alltid nödvändig om man till någon del träffas av lagen.
- **En säkerhetsskyddsanalys behandlar i huvudsak tre frågor**
  1. Vad ska skyddas?
  2. Mot vad ska det skyddas?
  3. Hur ska det skyddas?

2.1 Vad menas med Sveriges säkerhet?

Begreppet Sveriges säkerhet är inte definierat i lag, vilket medför att det kan vara svårt att tolka i detta sammanhang. I dess enklaste form kan det sägas handla om Sveriges oberoende och bestånd. Det inbegriper landets politiska och administrativa självständighet och suveränitet. Detta innefattar rätt till okränkta statsgränser och ett bevarande av det svenska självstyret, det demokratiska statsskicket samt av nationens grundläggande funktionalitet. Uttrycket Sveriges säkerhet tar sikte på sådant som är av grundläggande betydelse för Sverige. I detta ingår bland annat det militära och civila försvaret, den nationella ekonomin, de brottsbekämpande myndigheterna, domstolarna och leveranser av sådana saker som livsmedel, elkraft,

dricksvatten och drivmedel som är nödvändiga för att samhället ska kunna fungera på en nationell nivå. Detta betyder också att det som omfattas av begreppet Sveriges säkerhet är relaterat till samtiden och kan förändras över tid. Begreppet kan därför ha olika innebörd i olika sammanhang.

2.2 Vilken är hotbilden?

Sveriges säkerhet utmanas från flera håll. Den säkerhetspolitiska utvecklingen, som kulminerat med Rysslands invasion av Ukraina, är ett exempel på hur snabbt hotbilden mot Sverige kan förändras. Hela den tidigare gällande europeiska säkerhetsordningen har omkullkastats och det enda som tycks vara konstant är att säkerhetsläget i Sveriges närområde och hoten mot oss som nation och stat är under kontinuerlig förändring. Dessa hot manifesterar sig i ständiga underminerande aktiviteter och angrepp mot enskilda, mot offentlig sektor och mot näringslivet. De riktar sig mot både militära och civila värden och i detta nya säkerhetspolitiska läge som Sverige kastats in i är hotaktörerna villiga att gå allt längre för att nå sina mål.

Ryssland är den statliga aktör med antagonistiska avsikter som medför/kan orsaka störst konsekvenser för Sveriges säkerhet. Svensk teknologi och vetenskap samt kartläggning av kritisk infrastruktur är av säkerhetspolitiskt intresse för Ryssland. Att öka kunskapen om Sveriges totalförsvarsplanering och militära kapacitet är också av intresse.

Kina bedriver till större grad underrättelseinhämtning mot ekonomiska intressen, där tillvägagångssättet bland annat är uppköp av företag med eftertraktad teknologi och cyberangrepp. Intresset är globalt och drivs av en strävan att erhålla ekonomiska fördelar i syfte att bibehålla ekonomisk tillväxt och nationell stabilitet. Verksamheter i Sverige är inte undantagna.

Även Iran är en aktiv aktör. De agerar främst inom industrispionage i syfte att inhämta information om högteknologi som kan främja den iranska utvecklingen av vapensystem. Med avsikt att säkra den iranska regimens fortlevnad är landet också aktivt inom flyktingspionage, särskilt i relation till minoriteter och den iranska diasporan som sökt skydd i Sverige och driver upplysningskampanjer som uppfattas som underminerande och ett hot mot regimen.

2.3 Omfattning av säkerhetsskyddslagen

Det är den som bedriver säkerhetskänslig verksamhet som har det yttersta ansvaret för att skyddet av den säkerhetskänsliga verksamheten lever upp till de lagstadgade kraven.

Säkerhetsskyddslagstiftningen säger att den som bedriver en verksamhet som är av betydelse för Sveriges säkerhet behöver vidta lagstadgade säkerhetsåtgärder för att skydda den säkerhetskänsliga verksamheten och den information och de uppgifter som är kopplade till sådan verksamhet. Lagstiftaren pekar inte ut vilka verksamheter som omfattas av säkerhetsskyddslagen utan har lagt ansvaret på verksamhetsutövarna att själva utreda huruvida ens verksamhet omfattas eller inte.

Detta innebär att man som verksamhetsutövare behöver utreda om ens verksamhet till någon del bedriver säkerhetskänslig verksamhet eller hanterar säkerhetsskyddsklassificerade uppgifter. En följdeffekt av detta är att om det inte redan är klarlagt så behöver en säkerhetsskyddsanalys genomföras för att få svar på om och i vilken omfattning ens verksamhet omfattas av lagen och om det finns behov av säkerhetsskydd.

Då en säkerhetsskyddsanalys medför en mängd specifika krav och förhållningssätt som ställer höga krav på organisationen kan analysen behöva förekommas av ytterligare en initial bedömning för att utreda om en säkerhetsskyddsanalys är nödvändig. En sådan initial bedömning är inte definierad i säkerhetsskyddslagen eller i säkerhetspolisens vägledningar utan får i så fall göras på organisationens eget initiativ i syfte att kunna avgöra om man ”till någon del bedriver säkerhetskänslig verksamhet”[1].

1. 1 § Säkerhetsskyddslagen 2018:585.

VILKEN SPECIFIK PÅVERKAN HAR SÄKERHETS-SKYDDSLAGEN PÅ FASTIGHETSFÖRVALTARE?

Som fastighetsförvaltare är det bra att känna till hur krav på säkerhetsskydd påverkar utformningen av lokaler och hur information som kan kopplas till lokaler, hyresgäster och rörelsemönster behöver hanteras.

Med en förståelse för säkerhetsskydd kan samarbete underlättas med aktörer som bedriver säkerhetskänslig verksamhet, till exempel i de fall en säkerhetsskyddad upphandling behövs och utpekade lokaler på förhand kan göras redo för att möjliggöra anpassning till säkerhetsskydd.

Exempel: Några exempel på byggnader och lokaler som kan bli föremål för säkerhetsskydd är lokaler för förvaring av säkerhetsskyddsklassificerade uppgifter, lokaler där samhällsviktig verksamhet bedrivs samt lokaler som är utpekade ledningsplatser för kris- och krigsledning.

2.4 Beskrivning av säkerhetsskyddsanalys

Enligt säkerhetsskyddslagen ska den som till någon del bedriver säkerhetskänslig verksamhet själv utreda behovet av säkerhetsskydd i en säkerhetsskyddsanalys.

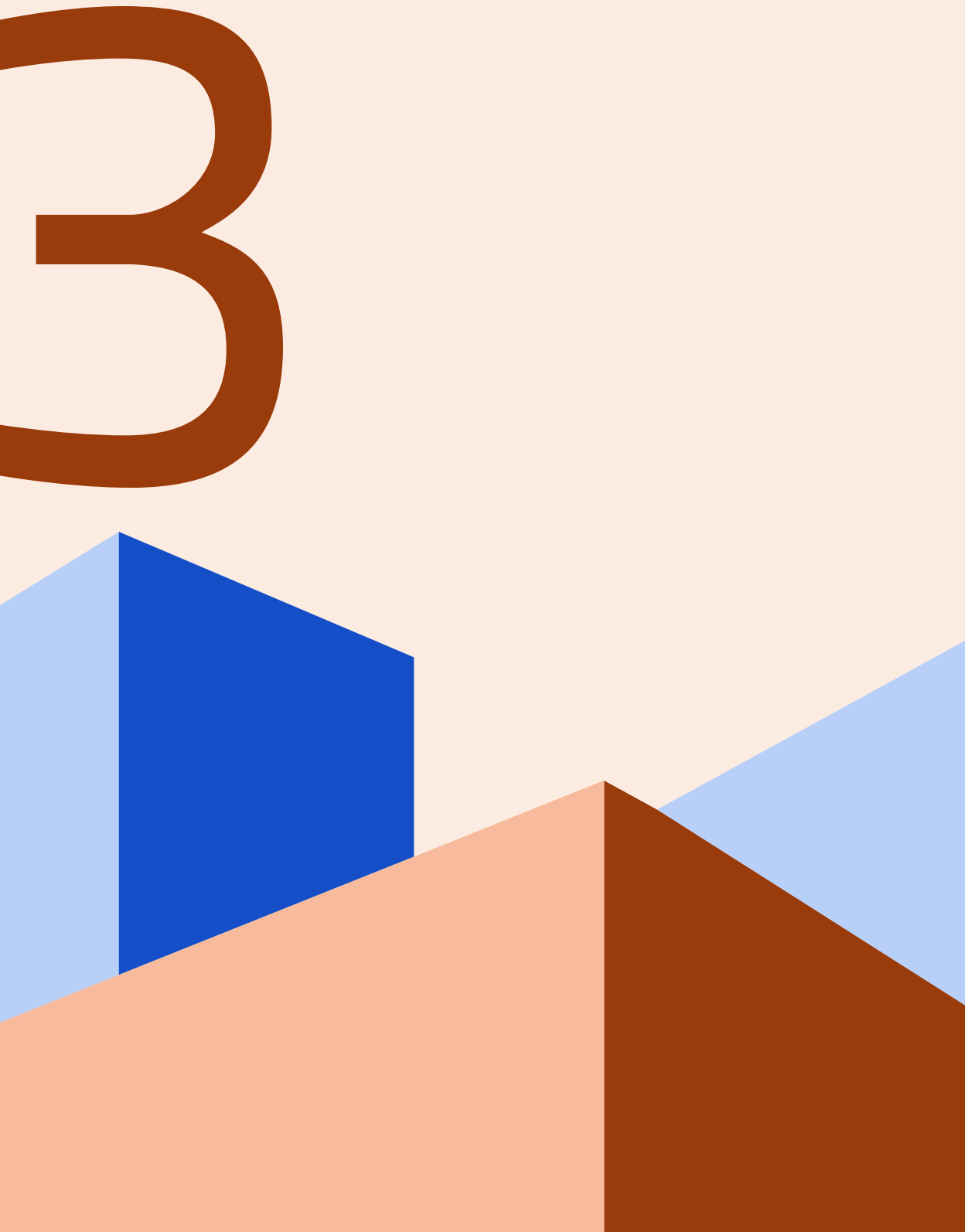
Att påbörja en säkerhetsskyddsanalys utan att veta i vilken utsträckning ens verksamhet omfattas av säkerhetsskyddslagstiftningen kan upplevas som ett omfattande arbete. Oavsett resultat så finns det däremot fördelar med att genomföra en säkerhetsskyddsanalys. Analysen ger inte bara kunskap om verksamheten är säkerhetskänslig eller inte utan ger också god insikt i verksamheten i stort och vad som kan vara värt att skydda, vilket är värdefull kunskap även för egna mål och processer.

Syftet med att genomföra en säkerhetsskyddsanalys är att ta reda på vilka säkerhetsskyddsåtgärder som verksamhetsutövaren faktiskt behöver vidta. Säkerhetsskydd innebär ofta både friktion och kostnad för en verksamhetsutövare. Det är därför vitalt att hitta rätt säkerhetsskyddsnivå och följaktligen att genomföra rätt säkerhetsskyddsåtgärder.

VIKTIGT ATT TÄNKA PÅ FÖR SÄKERHETSSKYDDSANALYSER!

Som hjälp på vägen inför utförandet av en säkerhetsskyddsanalys är följande punkter ett par av de viktigaste sakerna att tänka på:

- **Ibland är man osäker.** För vissa verksamheter är det inte tydligt om de bedriver säkerhetskänslig verksamhet eller inte. I dessa fall bör metoden för säkerhetsskyddsanalys användas i syfte att bedöma om så är fallet.
- **Säkerställ kompetens.** Innan påbörjat arbete med säkerhetsskyddsanalys behöver man tillgodose att det finns förutsättningar för att genomföra analysen tillfulloS
- **Säkerställ förutsättningar.** Innan påbörjat arbete med säkerhetsskyddsanalys behöver man tillgodose att det finns förutsättningar för att säkerhetsskyddet ska kunna upprätthållas under arbetet. Detta ställer exempelvis krav på lämpliga rum och förvaringsutrymmen, rutiner och eventuella säkerhetsskyddsavtal.
- **Förankra.** Intern förankring hos verksamhetens ledning är nödvändig genom hela processen för att säkerställa stöd och resurser.
- **Processtegen i metodiken är en vägledning**. Det praktiska genomförandet av en säkerhetsskyddsanalys är inte så sekventiellt som metoden visar utan arbetet i de olika stegen sker ofta parallellt.
- **En säkerhetsskyddsanalys är ett omfattande åtagande**. Den ställer höga krav på organisationen. Framför allt krävs:
  - God kännedom om verksamheten
  - God förmåga att identifiera skyddsvärden i förhållande till Sveriges säkerhet
  - God förmåga att identifiera antagonistiska hot i relation till identifierade skyddsvärden
  - God förmåga att identifiera sårbarheter för skyddsvärdena



Metodik och vägledning för genomförandet av en säkerhets-skyddsanalys

En säkerhetsskyddsanalys består av tre huvuddelar. Den första delen handlar om att ta reda på om verksamheten bedriver någon form av säkerhetskänslig verksamhet och i så fall vad för något som är skyddsvärt. Den andra delen beskriver hotbilden, det vill säga vad det skyddsvärda behöver skyddas mot. Den tredje och sista delen fångar vilka skyddsåtgärder som behöver vidtas.

I detta stycke beskrivs de olika stegen i hur en säkerhetsskyddsanalys kan genomföras. För vidare vägledning se även säkerhetspolisens vägledningar i säkerhetsskydd. Säkerhetspolisen har tagit fram ett antal vägledningar som är tänkta att fungera som ett stöd för verksamhetsutövare i tillämpningen av säkerhetsskyddsregelverket[2].

- Vägledning - Säkerhetsskyddad upphandling
- Vägledning - Personalsäkerhet
- Vägledning - Fysisk säkerhet
- Vägledning - Avlyssningsskyddade utrymmen
- Vägledning - Informationssäkerhet
- Vägledning - Säkerhetsskyddsanalys
- Vägledning - Introduktion till säkerhetsskydd

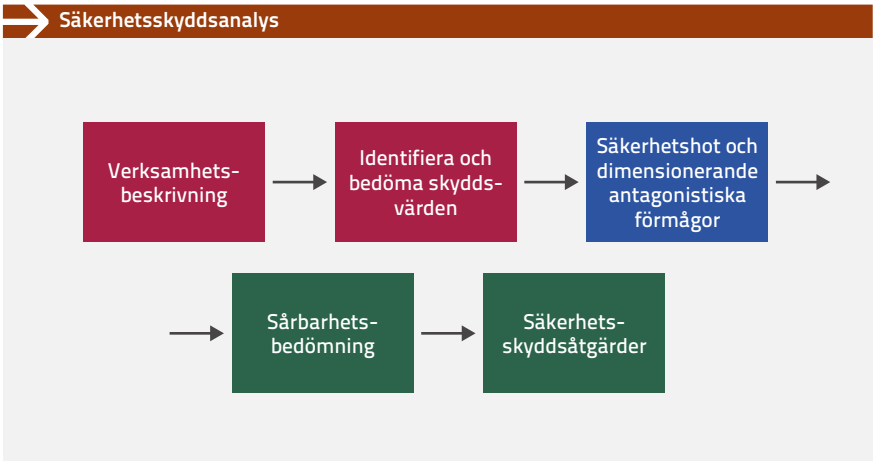
2. https://sakerhetspolisen.se/verksamheten/sakerhetsskydd/vagledningar-sakerhetsskydd.html.

Utöver dessa vägledningar från Säkerhetspolisen finns även informativt material i försvarsmaktens handböcker. Dessa handböcker syftar till att ge metoder och verktyg inom försvarsmaktens verksamhetsutövande inom ett antal områden men kan med fördel användas som referensmaterial även av andra verksamheter. Specifikt kopplat till hur försvarsmakten förhåller sig till ämnet säkerhetsskydd finns följande handböcker[3].

- Handbok - Säkerhetstjänst Informationssäkerhet
- Handbok - Säkerhetstjänst Säkerhetsprövning
- Handbok - Säkerhetstjänst Sekretessbedömning Del A/Del B
- Handbok – Säkerhetstjänst Säkerhetsskyddad upphandling med säkerhetsskyddsavtal
- Handbok - Säkerhetstjänst Fysisk säkerhet

Processbeskrivningen som återfinns nedan tar avstamp i ett behov av att inleda arbetet med att först utreda om ens organisation bedriver säkerhetskänslig verksamhet eller inte. Om resultatet av den första delen blir att säkerhetskänslig verksamhet bedrivs eller att verksamheten hanterar säkerhetsskyddsklassificerade uppgifter fortsätter analysprocessen med efterföljande steg. I annat fall avslutas säkerhetsskyddsanalysen efter den första delen med resultat att säkerhetskänslig verksamhet inte bedrivs och att det inte förekommer några skyddsvärden för Sveriges säkerhet. Detta innebär i detta scenario att en heltäckande säkerhetsskyddsanalys inte behöver genomföras. Om det däremot uppstår vissa tveksamheter huruvida någon del av verksamheten är skyddsvärd eller inte bör denna del involveras i en vidare analys.

3. https://www.forsvarsmakten.se/sv/om-forsvarsmakten/dokument/handbocker.



FIGUR 2 ▪ Källa: Vägledning säkerhetsskyddsanalys – Säkerhetspolisen.

3.1 Del 1 Vad ska skyddas? – Verksamhets-beskrivning och identifierade skyddsvärden

Denna del består av två steg: en verksamhetsbeskrivning samt en identifiering av skyddsvärden. Det första avsnittet beskriver verksamheten samt dess mål och syfte i en verksamhetsbeskrivning. För att identifiera säkerhetskänslig verksamhet är den övergripande frågeställningen att svara på vad konsekvensen hade blivit för Sveriges säkerhet vid störningar som drabbar verksamheten. En ytterligare frågeställning att ställa sig är om en antagonist kan ha intresse av att komma åt verksamheten eller uppgifterna för egen vinning. För att kunna identifiera skyddsvärden i verksamheten är det nödvändigt att bryta ned verksamheten i delverksamheter, processer och tillgångar.

Som nämnt ovan kan påverkan på säkerhetskänslig verksamhet medföra konsekvenser för Sveriges säkerhet. Sveriges säkerhet i sin tur brukar delas upp i fem kategorier, vilket innebär att säkerhetskänslig verksamhet och dess skyddsvärden kan kategoriseras in i någon av dessa. Man bör därmed ta stöd i nedan kategorier när den säkerhetskänsliga verksamheten ska identifieras och beskrivas:

- **Sveriges yttre säkerhet** – Territoriell suveränitet, Sveriges integritet, oberoende och handlingsfrihet.
- **Sveriges inre säkerhet** – Demokratiskt statsskick, rättsväsende och brottsbekämpande förmåga på nationell nivå.
- **Nationellt samhällsviktig verksamhet** – Leveranser, tjänster och funktioner som är nödvändiga för samhällets funktionalitet, t.ex. elförsörjning, vatten- och livsmedelsförsörjning och finansiella tjänster.
- **Sveriges ekonomi** – Sveriges betalningsförmåga, inklusive förmåga att administrera, granska, styra och stödja den nationella finansiella stabiliteten.
- **Skadegenerande verksamhet** – Verksamheten som vid skada kan generera skadekonsekvenser på annan säkerhetskänslig verksamhet. Denna verksamhet är oftast redan identifierad som farlig verksamhet utifrån annan lagstiftning, som lagen (2003:778) om skydd mot olyckor.

Ett ytterligare sätt att bryta ner sin verksamhet och hitta potentiellt säkerhetskänslig verksamhet är att utgå från en identifierad samhällsviktig verksamhet, då en säkerhetskänslig verksamhet nästan utan undantag också är samhällsviktig. Vägledning i identifiering av samhällsviktiga verksamheter finns publicerad av MSB som definierar sådan verksamhet som en ”verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet”[4].

Om verksamheten kan anses utgöra en säkerhetskänslig verksamhet går man vidare i analysen genom att i nästa avsnitt identifiera skyddsvärden. Om det råder osäkerhet kring huruvida en del av verksamheten är säkerhetskänslig eller inte ska denna verksamhet inkluderas i den fortsatta analysen. Ett skyddsvärde är den specifika tillgång eller process som är nödvändig för att säkerställa eller upprätthålla den säkerhetskänsliga verksamheten och som därmed behöver ett särskilt skydd. Ett sätt att identifiera skyddsvärden kan vara genom att identifiera vad verksamheten är beroende av för att kunna fungera, som till exempel anläggningar, system, personal och information. Det är även dessa delar som senare kommer att behöva omfattas av säkerhetsskyddsåtgärder.

4. https://www.msb.se/sv/publikationer/vagledning-for-identifiering-av-samhallsviktig-verksamhet2/.

När skyddsvärden är identifierade är det dags att gå vidare till del två. Precis som ovan, kan det fortfarande vara osäkert om en verksamhet är skyddsvärd eller inte, låt den då följa med till nästa steg i analysen. Om resultatet av verksamhetsbeskrivningen blir att ingen säkerhetskänslig verksamhet bedrivs och inga skyddsvärden har identifierats kan analysen avslutas här.

De skyddsvärden som har identifierats ska i nästa steg bedömas utifrån vilken konsekvens de kan medföra på Sveriges säkerhet. Varje skyddsvärde ska enligt säkerhetspolisen föreskrifter bedömas utifrån följande fyrgradiga skala:

- Synnerligen allvarlig skada för Sveriges säkerhet (nivå A) – Långsiktiga konsekvenser och mycket svårt att återgå till normalläge.
- Allvarlig skada för Sveriges säkerhet (nivå B) – Allvarlig påverkan, svårt att återgå till ett normalläge.
- Inte obetydlig skada för Sveriges säkerhet (nivå C) – Inte obetydlig skada, möjligt att återgå till normalläge inom rimlig tid.
- Endast ringa skada för Sveriges säkerhet (nivå D) – Ringa skada, möjligt att relativt snabbt återgå till ett normalläge.
- Inte mätbart eller inte relevant konsekvens – Bedöms inte som säkerhetskänslig verksamhet.

Förutom att bedöma vilken konsekvens en skada eller störning kan innebära på Sveriges säkerhet ska respektive skyddsvärde också beskrivas utifrån vilket perspektiv det är skyddsvärt. Ett skyddsvärde kan vara skyddsvärt ur ett eller flera av perspektiven; konfidentialitet, riktighet och tillgänglighet. Beskrivningen ska förklara om processen eller tillgången är skyddsvärd utifrån att störst skada uppstår om uppgiften obehörigen röjs (konfidentialitet), om den ändras (riktighet) eller om den görs otillgänglig eller förstörs (tillgänglighet).

När verksamhetens skyddsvärden är identifierade och beskrivna är det dags att beskriva vad som kan hota dessa i del två.

3.2 Del 2 Mot vad ska det skyddas? – Säkerhetshot

I detta avsnitt av säkerhetsskyddsanalysen beskrivs hotbilden. Avsnittet kan inledas med den nationella hotbilden mot Sveriges säkerhet. Här kan man utgå från öppna källor som till exempel Säkerhetspolisens, Försvarsmaktens, MUST:s och FRA:s årsböcker och fundera över hur den nationella hotbilden kan kopplas till den egna verksamheten. Det är bara antagonistiska hot som är av intresse för säkerhetsskyddsanalysen, det vill säga hot från en hotaktör som kan antas ha kvalificerad förmåga och avsikt att orsaka skada.

"Det kanske allvarligaste hotet mot Sverige i fredstid kommer från främmande underrättelseverksamhet."

– MUST:s årsredovisning 2022.

"Det finns ett ökat underrättelsehot där främmande makt riktar sin säkerhetshotande verksamhet mot politiskt beslutsfattande."

– Säkerhetspolisens årsbok 2022–2023.

För att komplettera den nationella hotbilden och förankra hotbilden med verksamhetens egna situation så bör man analysera egna incidentrapporter, tillbudsrapporter eller liknande dokumentation. Syftet med detta avsnitt är få en uppfattning om vad säkerhetsskyddet behöver skydda verksamheten mot och för att i nästa steg kunna ringa in vilka sårbarheter som finns inom den egna verksamheten mot bakgrund av den aktuella hotbilden.

3.3 Del 3 Hur ska det skyddas? – Sårbarhetsbedömning och säkerhetsskyddsåtgärder

För att kunna utveckla rätt säkerhetsskyddsåtgärder och skydda verksamheten med rätt skyddsnivå behöver en sårbarhetsbedömning genomföras. Syftet med den är att identifiera vilka sårbarheter som finns inom och runtomkring ett skyddsvärde och som behöver minimeras för att skydda den säkerhetskänsliga verksamheten. Det handlar om att studera verk-

samhetens förmåga att skydda de identifierade skyddsvärdena mot den dimensionerande hotbilden. Det görs här en bedömning av det nuvarande skyddet och av eventuella identifierade sårbarheter inom verksamheten.

En metod för att identifiera sårbarheterna är att bedöma skyddet runt respektive skyddsvärde utifrån de tre säkerhetsskyddsområdena fysisk säkerhet, personalsäkerhet och informationssäkerhet. Alla sårbarheter som helt eller delvis faller inom dessa områden ska inkluderas, även frågor som rör exempelvis upphandlingar, säkerhet i projekt och relaterad utbildning. Det kan vara viktigt att ha med sig att det i det här avsnittet inte bara är av värde att dokumentera identifierade sårbarheter utan även viktiga kontinuerliga säkerhetsskyddsåtgärder som redan finns på plats. Detta för att säkerställa att dessa åtgärder vidmakthålls och för att minimera risken att det fattas beslut som avvecklar centrala säkerhetsskyddsåtgärder av till exempel besparingsskäl.

Utifrån listade sårbarheter går man sedan vidare i säkerhetsskyddsanalysen genom att börja studera vilka säkerhetsskyddsåtgärder som behöver vidtas för att skydda den säkerhetskänsliga verksamheten och de säkerhetsskyddsklassificerade uppgifterna. Hur säkerhetsskyddet ska utformas framkommer i Säkerhetspolisens föreskrifter[5] om säkerhetsskydd, där det går att läsa vilka hanteringsregler som gäller för de identifierade skyddsvärdena. Tänk på att till skillnad mot traditionella risk- och sårbarhetsanalyser så accepteras ingen riskaptit i frågor som rör Sveriges säkerhet. Det är enbart konsekvensen som ska beaktas i analysen, inte sannolikheten. Detta innebär att alla identifierade sårbarheter behöver minimeras för att säkerställa skyddet av identifierade skyddsvärden.

I bästa fall kommer resultatet av sårbarhetsbedömningen bli att det inte förekommer några sårbarheter. I dessa fall är säkerhetsskyddet fullgott och inga nya säkerhetsskyddsåtgärder behöver vidtas. Detta är dock sällan fallet utan oftast identifieras ett antal sårbarheter som kommer att behöva hanteras. Det kan handla om åtgärder som hamnar inom till exempel att stärka skalskyddet (fysisk säkerhet), rutiner för säkerhetsprövning, behörigheter och utbildning i säkerhetsskydd (personalsäkerhet) eller klassning och skydd av information (informationssäkerhet).

Därutöver kan ytterligare säkerhetsskyddsåtgärder komma att identifieras som exempelvis rör åtgärder kopplat till säkerhetsskyddad upphandling, vilket är aktuellt i de fall en underleverantör kan komma att få del av säkerhetskänslig verksamhet eller säkerhetsskyddsklassificerade uppgifter.

5. PMFS 2022:1.

3.4 Exempel på resonemang kring skyddsvärden och analysobjekt

Ett skyddsvärde är den specifika tillgång eller process som är nödvändig för att säkerställa eller upprätthålla den säkerhetskänsliga verksamheten och som därmed behöver ett särskilt skydd. Ett sätt att identifiera skyddsvärden kan vara genom att identifiera vad verksamheten är beroende av för att kunna fungera, som till exempel anläggningar, system, personal och information. Fokus i den här skriften är byggnader och anläggningar för offentlig sektor, vilket är varför vi utgår från fastighetsägarperspektivet och hur anläggningar kan betraktas.

För att mer detaljerat bedöma hur man ska hantera sina anläggningar/byggnader behöver man fundera kring lämpliga analysobjekt och hur detaljerat man ska studera sin anläggning. Ett sätt är att utgå från anläggningens uppbyggnad dvs olika byggdelar och tekniska system och med det som grund fundera kring skyddsvärden, hot, sårbarheter och säkerhetsskyddsåtgärder.

3.4.1 Exempel på resonemang kring anläggningar och byggnadsverk

Det är i stort sett samma analysobjekt för de flesta anläggningar/byggnader men analysen kommer naturligtvis att se olika ut beroende på vilken typ av verksamhet som bedrivs i lokalerna.

Mark och utemiljö

Mark och utemiljö påverkar till stor del anläggningens funktion och behöver i första hand skyddas mot naturfenomen som översvämningar, erosion och ras. Marksensorer kan ge information om markrörelser och dela information om onormala händelser.

Inom olika offentliga anläggningar används parkeringslösningar för personal och besökare. Ofta hanteras lösningarna av externa leverantörer och utbyte av data sker till exempel för tjänster som visar lediga parkeringsplatser eller för fakturering av elbilsladdning.

Geografiska informationslösningar och karttjänster används bland annat för att ge vägledning till besökare för att hitta rätt. Dessa tjänster kan förekomma både utomhus och inomhus.

Byggnadskonstruktion/skalskydd

Byggnadskonstruktionen omfattar dels stommen som utgör den bärande konstruktionen, dels vägg- och takkonstruktion som skalskydd och klimatskydd mot extern påverkan. Klimatskyddet är skydd mot värme, kyla, vind och vatten. Sensorer kan byggas in och ge information om fukt och annan påverkan.

Modeller och databaser innehåller information om byggnadskonstruktionen. Informationen har tagits fram av leverantörer som projektörer, entreprenörer och producenter och dessa kan också ha fortsatt tillgång till informationen.

Lokaler

För optimering av lokalanvändning krävs data om användning av olika ytor vilket kan fås med hjälp av sensorer. En jämförelse är ett kontor med bokningssystem som talar om när lokalen är ledig och hur den bäst kan anpassas med ljus, ljud och luft eller möblering utifrån ett givet önskemål så att man väljer lokal efter aktivitet.

Besökare kan behöva hjälp för att hitta till rätt lokal eller avdelning, vilket föranleder att olika navigeringstjänster kan förekomma som kräver tillgång till planlösning med information om var olika lokaler finns. Att beakta här är att vissa enskilda funktioner inom en anläggning kan vara skyddsvärda så information om lokalers användning måste värderas.

Installationssystem – generellt

Sensorer och Internet of Things (IoT) ger statusinformation för ingående komponenter i systemen eftersom de flesta komponenter som byggs in på något sätt är uppkopplade och sänder information till överordnade system.

De flesta installationssystem kommunicerar med ett automationssystem för övervakning och styrning. Systemen övervakar drifttider och nyttjandegrader samt upptäcker driftstörningar och kan notifiera behörig personal.

Inom systemen förekommer information som kan betraktas som känslig, exempelvis personuppgifter, larm och felmeddelanden, övervakningsdata och underhållsinformation.

Vattensystem

Vattensystemet säkerställer att byggnaden har tillgång till rent vatten. Systemen är ihopkopplade inom anläggningen men också till samhällets ledningsnät som kan vara av varierande standard. Information om förbrukning delas med ledningsägare.

Avlopps- och avfallssystem

Avloppsystemen inom en anläggning är avgörande för att verksamhet ska kunna bedrivas. Även här finns koppling mot stadens ledningsnät som kan vara av varierande standard. Information om avloppsmängder och partiklar kan delas med ledningsägare.

Avfall delas in i ett antal olika fraktioner och hanteras olika beroende på om det exempelvis är ordinärt avfall, miljöfarliga produkter eller smittfarligt avfall.

Kyla- och värmesystem

System för värme och kyla kan vara lokala inom en anläggning eller byggnad men också förekomma i form av fjärrvärme och fjärrkyla. Behov av att kommunicera värme-/kylbehov samt förbrukning kan finnas och data kan behöva delas med leverantörer samt med omgivande fastighetsägare för att nå olika energieffektiva lösningar genom delning av media.

Luftbehandlingssystem

Luftbehandlingssystemen hanterar ventilation av anläggningen. Sensorer används för att mäta luftkvalitet och är en del av automationssystemen. Ventilationsaggregaten styrs av automationssystemen men kan också skicka data till externa leverantörer.

Elkraftsystem

Elkraftsystemet kan bestå av normalkraft, reservkraft och UPS (obruten kraft). Egen produktion av el genom sol och vind kan förekomma och är uppkopplad mot elleverantören.

I den smarta staden finns en målsättning kring lastbalansering varför delning av data kan ske både med leverantörer och med andra fastighetsägare.

Automationssystem

Automationssystem används för att övervaka och kontrollera tekniska system som ventilations- och klimatanläggningar, belysning, värme och kyla. Automationssystemen är informationssystem som på olika sätt kan vara uppkopplade mot omvärlden.

Automation omfattar också sensorer som sänder data till automationssystem. Behovet av att ta stöd av AI för att analysera stora datamängder och åstadkomma en prediktiv styrning ökar och dessa tjänster kan delas med andra fastighetsägare.

Informations- och kommunikationssystem

Smart positionering av alla personer och objekt via kameror och sensorer talar i realtid om var personer uppehåller sig och var utrustning finns.

Här är det viktigt att lyfta fram frågor som rör säkerhet, integritet och etik, eftersom det ibland kan handla om hantering av känsliga personuppgifter. Hit hör bland annat användning av biometriska data, exempelvis ansiktsigenkänning.

Kommunikationssystem används för att kommunicera mellan personal, besökare och andra användare i byggnaden. Detta kan inkludera trådbundna och trådlösa nätverk, telefoni- och videokonferenssystem, samt kommunikationssystem som används för övervakning.

Gas- och luftsystem

Olika gaser, exempelvis medicinska gaser samt tryckluft och liknande används inom olika anläggningar.

Transportsystem

Transportsystem som hissar, rulltrappor, lyftar och transportband används för att transportera personer och utrustning. Hisskonstruktionen kommunicerar med ett system för övervakning och underhåll av hissen. Systemet övervakar drifttider och nyttjandegrader samt upptäcker driftstörningar och kan notifiera behörig personal.

Säkerhets- och skyddssystem

Säkerhetssystem som övervakningskameror, intrångslarm, och passersystem används för att säkerställa en trygg och säker miljö.

Brandsäkerhetssystem som brandlarm, sprinkleranläggningar och branddörrar används för att upptäcka och förhindra bränder.

Belysnings- och dagsljussystem

Belysningssystemen kan bestå av både normalljus och nödljus och är tillsammans med dagsljus avgörande för att bedriva verksamhet.

Utebelysningen styrs av ljusgivare och tänds vid behov. En strävan är att belysningen inomhus anpassar sig efter dagsljuset så att ljusstyrkan i utrymmen är konstant och släcks när utrymmet inte används.

3.5 Exempel på resonemang kring hot och hothändelser

Här listas några exempel på hot och hothändelser som kan drabba anläggningar:

- Obehörig åtkomst till data, vilket kan exponera känslig information och kränka integritet.
- Manipulation av funktion, vilket kan störa rutiner och påverka verksamheten.
- Sabotage eller skadegörelse, vilket kan störa kritiska processer och tvinga verksamheten att avbryta sin verksamhet.
- Ransomware-attacker, vilket kan leda till driftsstörningar för verksamheten.
- DDoS-attacker som överbelastar kommunikationssystem och orsakar driftsstörningar.
- Insiderhot, där personal eller externa entreprenörer med tillgång till olika system kan använda sin åtkomst för att orsaka skada, stjäla information eller manipulera system.
- Katastrofer och klimatpåverkan – extremväder som skyfall och hårda vindar kan medföra översvämningar, jordskred med mera.
- Brand orsakad av tekniska fel alternativt orsakad av människor, oavsiktligt eller avsiktligt.

3.6 Exempel på resonemang kring sårbarheter

Anslutna enheter är grunden för smarta byggnader, lite skulle kunna åstadkommas utan dem men deras närvaro utgör också en säkerhetsrisk som tekniken måste kunna hantera. En IoT-konfiguration erbjuder flera ingångspunkter för potentiell hacking. Det exponerar både byggnadsinformation och driftstekniska system. Med kritiska fastighetssystem sammankopplade för att möjliggöra fjärrhantering och övervakning, och både IT och OT som kommunicerar med varandra, är risken för korskontaminering verklig.

En metod för att identifiera sårbarheterna är att bedöma skyddet runt respektive skyddsvärde utifrån de tre säkerhetsskyddsområdena fysisk säkerhet, personalsäkerhet och informationssäkerhet.
Exempel på sårbarheter/brister:

- Otillräcklig kontroll och övervakning av åtkomst till styrningssystem, vilket kan leda till obehörig användning och potentiell skada för verksamheten.
- Sårbarheter i trådlös kommunikation, vilket kan leda till att kryptering bryts och känslig information avlyssnas.
- Svagheter i fysisk säkerhet, såsom otillräckligt skyddade styrsystem eller dörrar, vilket kan ge obehöriga personer åtkomst till känsliga områden.
- Brister i återställningsplaner för att hantera säkerhetsincidenter, vilket kan förlänga återhämtningstiden och förvärra konsekvenserna för verksamheten.
- Otillräckliga säkerhetsåtgärder för att skydda data som är lagrad i molnet, vilket kan leda till dataintrång och exponering av känslig information.
- Brister i leverantörs- och underentreprenörsledet, vilket innebär att komponenter eller tjänster kan ha säkerhetsbrister som påverkar hela systemet.

Exempel på konsekvenser:

- Driftstörningar och stillestånd på grund av bristande funktionalitet.
- Juridiska och ekonomiska konsekvenser på grund av överträdelser av lagar och regler kring informationssäkerhet och personsekretess.
- Skadat rykte och förtroende hos kunder, allmänhet och andra intressenter.
- Förlust av data vilket kan försvåra drift, planering och felsökning, och resultera i längre driftstörningar.

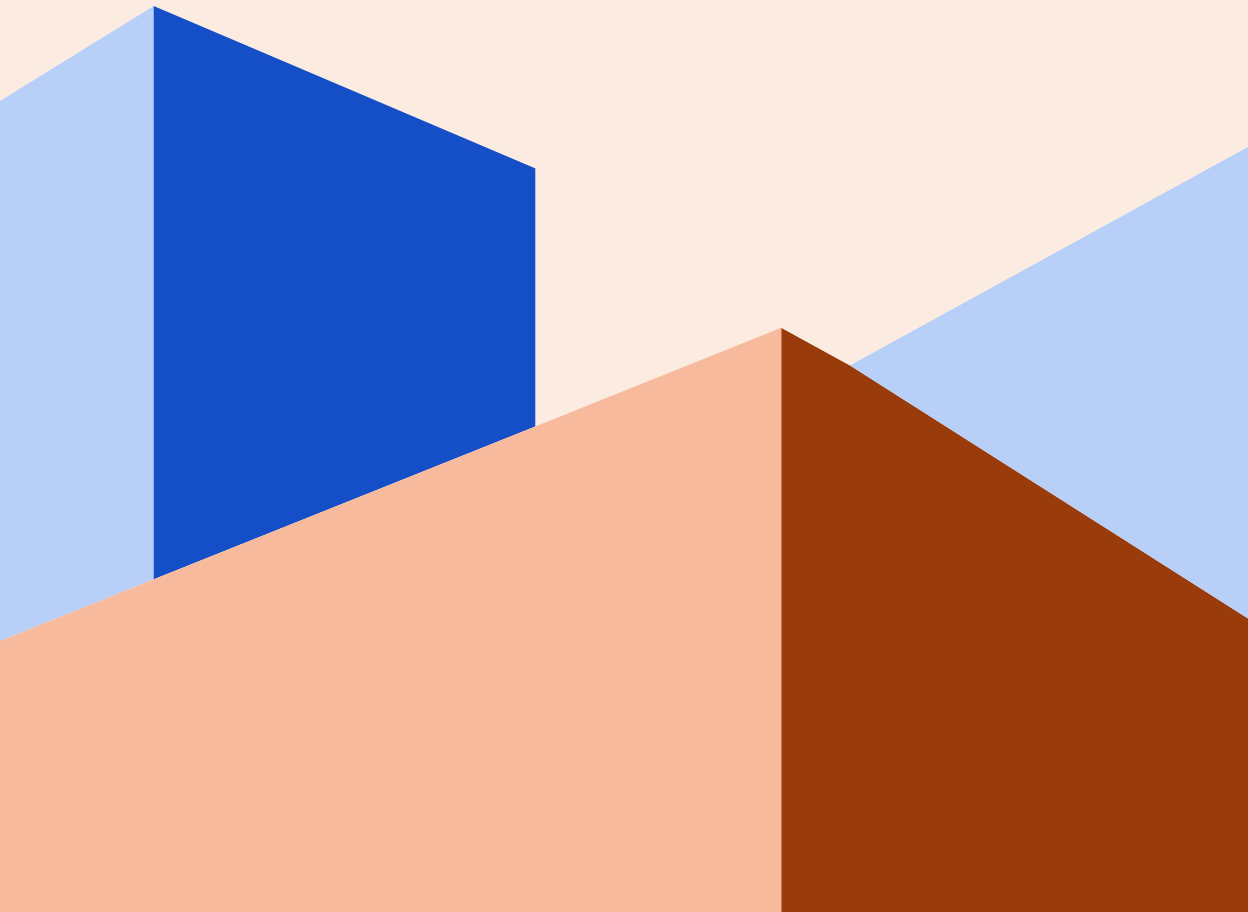
3.7 Exempel på resonemang kring säkerhetsskyddsåtgärder

För att begränsa påverkan av säkerhetshoten måste teknik för smarta byggnader hantera både fysiska risker och cybersäkerhetsrisker. Fysisk byggnadsåtkomst måste övervakas med övervaknings- och kontrollsystem för att upptäcka avvikelser som kan tyda på en cyberattack. Digitala nätverk måste skyddas med brandväggar och datakryptering. Dessutom måste systemintegration säkerställas med enskilda system och terminaler skyddade från åtkomst av obehörig person samt från obehöriga ändringar.

Exempel på säkerhetsskyddsåtgärder att vidta:

- Kontrollera och övervaka åtkomst till styrsystem, för att förhindra obehörig användning och potentiell skada på verksamhet och egen personal.
- Säkra trådlös kommunikation, för att förhindra att kryptering bryts och känslig information avlyssnas.
- Säkra den fysiska säkerheten/skalskyddet, för att skydda åtkomst till lokaler och styrsystem.
- Se över återställningsplaner, för att förkorta återhämtningstiden och minska konsekvenserna för verksamheten vid säkerhetsincidenter.
- Se över säkerhetsåtgärder för att skydda data som är lagrad i molnet, för att förhindra dataintrång och exponering av känslig information och verksamhetsdata.
- Kontrollera leverantörs- och underentreprenörledet, för att säkra att varken komponenter och tjänster som används har säkerhetsbrister som påverkar byggnadens funktion.
- Etablera rutiner för säkerhetsprövning, behörigheter och utbildning i säkerhetsskydd (personalsäkerhet).

4



CER-direktivet

Inom EU har arbetet med att stärka motståndskraften i samhällsviktig verksamhet accelererat de senaste åren. Syftet med arbetet är att stärka förmågan att upprätthålla viktiga samhällsfunktioner.

Verksamheter som tillhandahåller samhällsviktiga tjänster (kritiska entiteter) spelar en oumbärlig roll när det gäller att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet i respektive medlemslands inre marknad. EU-medlemsländerna har därför insett att det är mycket viktigt att det inrättas en unionsram som syftar dels till att stärka kritiska entiteters motståndskraft på den inre marknaden genom att fastställa harmoniserade minimiregler, dels till att bistå entiteterna genom enhetligt och särskilt stöd och tillsynsåtgärder. Detta utfördes genom det beslutade CER-direktivet.

4.1 EU-direktivet

I december 2022 antog EU CER-direktivet[6]. I egenskap av ett EU-direktiv får det inte direkt verkan i medlemsstaterna utan måste även göras till nationell lag. En process som kallas för införlivande. Exakt vad CER-direktivet kommer att innebära för de som omfattas av det kommer alltså inte vara känt förrän svensk lagstiftning finns på plats, vilket ska vara genomfört senast den 17 oktober 2024.

Vissa slutsatser kan dock redan nu dras på en övergripande nivå om vad CER-direktivet kommer att innebära och beskrivs i kommande stycken.

6. Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (CER-direktivet, från engelskans Critical Entities Resilience).

4.2 Omfattning av CER-direktivet

CER-direktivet riktar sig till de verksamheter (så kallade kritiska entiteter) som enligt definitionen tillhandahåller tjänster som enligt CER-direktivet är samhällsviktiga i egenskap av deras betydelse för att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet. CER-direktivet pekar ut elva sektorer inom vilka samhällsviktiga tjänster kan tillhandahållas. Dessa utgör ett minimum av sektorer och innefattar verksamheter inom:

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvård
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Offentlig förvaltning
- Rymden
- Produktion, bearbetning och distribution av livsmedel

Det exakta förfarandet för hur kritiska entiteter ska identifieras kommer att avgöras i den kommande svenska implementationen av CER-direktivet. Vad som framgår av direktivet är dock att identifieringsförfarandet ska utföras av ansvariga myndigheter och ska grunda sig i riskbedömningar inom de olika sektorerna. De ansvariga myndigheterna kommer även att ha ett slutligt ansvar att upprätta en förteckning över de kritiska entiteterna, underrätta dem om att de identifierats som kritiska entiteter samt informera dem om deras skyldigheter[7].

EU-kommissionen ska dessutom i samarbete med medlemsstaterna utarbeta rekommendationer och icke-bindande riktlinjer för att kunna stödja medlemsstaterna i arbetet med att identifiera kritiska entiteter.

7. Artikel 5 och 6, (EU) 2022/2557.

4.3 CER-direktivets innebörd

CER-direktivet skapar skyldigheter för medlemsländerna att upprätta en strategi för kritiska entiteter att, för de samhällsviktiga tjänster de tillhandahåller, säkerställa vad den svenska språkutgåvan av direktivet benämner *motståndskraft*. Motståndskraft definieras här som: ”en kritisk entitets förmåga att förebygga, skydda mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig från en incident”[8]. Denna kombinerade förmåga är ett koncept som ibland även kallas resiliens[9].

Detta medför i sin tur skyldigheter för de kritiska entiteterna att vidta åtgärder för att säkerställa sin motståndskraft. Åtgärderna ska grunda sig i riskbedömningar som ska innehålla en redogörelse för samtliga relevanta risker. För risker orsakade av människan såväl som risker som inte är det. Det inbegriper risker av sektorsövergripande eller gränsöverskridande slag, olyckor, naturkatastrofer, hot mot folkhälsan och hybridhot samt andra antagonistiska hot, inklusive terroristbrott.

Utifrån riskbedömningen ska tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa entitetens motståndskraft vidtas[10]. Åtgärder ska bland annat vidtas för:

- ➔ Att strategiskt planera för och vidta långsiktiga åtgärder för att förhindra incidenter orsakade av katastrofer och klimat.
- ➔ Att säkerställa ett tillfredsställande fysiskt skydd av lokaler och kritisk infrastruktur.

Därtill omfattas kritiska entiteter av en skyldighet att rapportera incidenter som medfört en betydande störning eller kunde ha medfört en betydande störning i tillhandahållandet av samhällsviktiga tjänster[11].

De kan även bli föremål för olika tillsynsåtgärder[12], vilket bland annat kan komma att innebära att tillsynsmyndigheten begär att få tillgång till de lokaler där entiteten bedriver sin verksamhet.

8. Artikel 2.2, (EU) 2022/2557.
9. Resiliens: begreppets olika betydelser och användningsområden, MSB569.
10. Artikel 13, (EU) 2022/2557.
11. Artikel 15, (EU) 2022/2557.
12. Artikel 21, (EU) 2022/2557.

Vid brister i efterlevnad av direktivet kan entiteter även komma att drabbas av sanktioner[13]. Nivån på sanktionsavgifterna lämnas till varje medlemsland att själva besluta men EU-direktivet fastslår att sanktionerna ska vara ”effektiva, proportionella och avskräckande”.

Av NIS 2-direktivet följer att kritiska entiteter även omfattas av NIS 2-direktivet, och således även måste efterfölja kraven i det direktivet[14].

VILKEN SPECIFIK PÅVERKAN HAR CER-DIREKTIVET PÅ FASTIGHETSFÖRVALTARE?

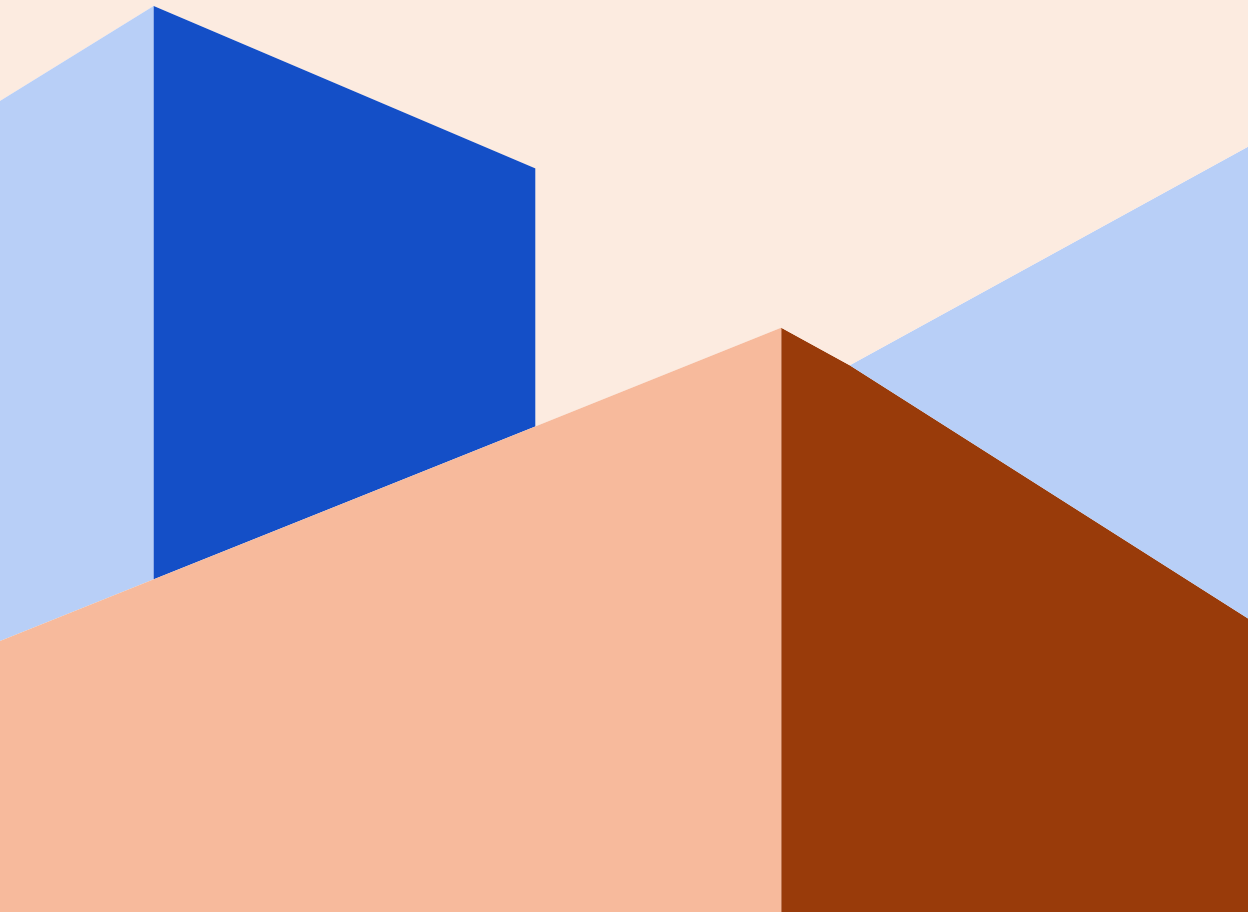
Fastighetsförvaltning är inte en verksamhet som leder till att direkt omfattas av kraven i CER-direktivet. Eventuell omfattning av direktivet kan däremot komma från sekundära håll och beroenden.

Exempel: Hyresgäster som bedriver verksamheter inom sektorerna som listas ovan kan exempelvis komma att ha särskilda behov som att anläggningen eller byggnaden de hyr på olika sätt behöver anpassas för att de ska kunna efterleva kraven i regleringen. Sådana krav på säkerhetsåtgärder bör ställas av hyresgästerna i upphandlingsskedet men kan även tillkomma vid avtalsförnyelse.

På samma sätt kan fastighetsägare komma att påverkas indirekt genom att deras samverkanspartners i närliggande branscher, som exempelvis tillhandahåller eldistribution, dricksvatten och avloppsvattenhantering, träffas av regleringen. Det kan leda till ökade samarbets- och leveranskostnader för fastighetsägarna.

13. Artikel 22, (EU) 2022/2557.
14. Artikel 2.3, (EU) 2022/2555.

5



NIS 2-direktivet

NIS 2-direktivet tillkom, liksom sin föregångare NIS-direktivet, från ett behov av att säkerställa tillförlitligheten och säkerheten hos samhällsviktiga nätverks- och informationssystem samt nätverks- och informationstjänster. Direktivet inriktar sig till leverantörer som tillhandahåller samhällsviktiga tjänster (kritiska entiteter) då de spelar en oumbärlig roll när det kommer till att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet inom unionen.

Tidigare utredningar har konstaterat att medlemsstaterna har mycket olika beredskapsnivåer, vilket i avsaknad av gemensamma krav har lett till skilda tillvägagångssätt i unionen. Resultatet har blivit olika skyddsnivåer för konsumenter och företag, vilket undergräver den allmänna nivån på säkerheten i nätverks- och informationssystem i unionen.

En samhällssituation med allt mer säkerhetsincidenter, som blir allt mer omfattande och får allt större inverkan, medför därutöver ett allvarligt och ett ökat hot mot nätverks- och informationssystemens funktion.

Allt detta tillsammans med ett över tid ökat samarbete och beroende mellan unionsländerna har lett till att EU ansåg det mycket viktigt att det formaliseras en struktur som syftar till att stärka kritiska entiteters motståndskraft inom varje medlemsland genom att definiera harmoniserade minimiregler. Detta utfördes genom NIS-direktivet och det nyligen beslutade NIS 2-direktivet.

5.1 EU-direktivet

I december 2022 antog EU NIS2-direktivet[15]. Direktivet ska enligt beslut vara införlivat i medlemsstaternas nationella lagstiftning senast den 17 oktober 2024 och är en uppdatering av det nu gällande NIS-direktivet[16].

15. Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).
16. Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet).

NIS 2-direktivet är precis som CER-direktivet ett EU-direktiv. Det betyder att det inte får direkt verkan i medlemsstaterna, utan måste göras till nationell lag. Exakt vad NIS 2-direktivet kommer att innebära för de som omfattas av det kommer inte vara känt förrän en svensk lag finns på plats. Detta kommer sannolikt[17] att ske harmoniserat med implementationen av CER-direktivet som beskrivs i mer detalj i kapitel 4.

5.2 Omfattning av NIS 2-direktivet

NIS 2-direktivet omfattar precis som det tidigare NIS-direktivet viss specifik verksamhet inom utvalda sektorer. För NIS 2-direktivet har dessa utökats till att vara följande sexton sektorer:

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvård
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Förvaltning av it-tjänster
- Offentlig förvaltning
- Rymden
- Post- och budtjänster
- Avfallshantering
- Tillverkningsindustri
- Digitala leverantörer
- Forskning

Det är dock inte alla aktörer i de utpekade verksamheterna som omfattas av NIS 2-direktivet. Huvudregeln är att entiteter med fler än 50 anställda eller en omsättning eller balansomslutning på mer än 10 miljoner euro per år omfattas. Det finns dock undantag från huvudregeln och därmed entiteter som omfattas av reglerna oavsett storlek.

17. Kommittédirektiv 2023:30.

Fastighetsförvaltning är därmed inte en verksamhet som direkt leder till att omfattas av kraven i NIS 2-direktivet. Hyresgäster som är aktiva inom de ovan listade sektorerna kan dock komma att ha behov av särskilda anpassningar, att anläggningen eller byggnaden de hyr dimensioneras i enlighet med regleringen.

5.3 NIS 2-direktivets innebörd

En skillnad som framstår mellan NIS- och NIS 2-direktivet är att NIS 2-direktivet i många frågor lämnar ett mindre utrymme för nationellt självbestämmande. Det framgår redan av direktivstexten hur viss del av regleringen måste se ut. Det första NIS-direktivet sätter i stor utsträckning upp mål för vad medlemsstaterna ska åstadkomma på cybersäkerhetsområdet, men för motsvarande regler i NIS 2-direktivet anges även i stor utsträckning hur målen ska uppnås.

Kritiska entiteter som omfattas av NIS 2-direktivet kommer att behöva vidta tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster. Säkerhetsåtgärderna ska ha en allriskansats (eng. *all-hazards approach*), det vill säga ta hänsyn till alla tänkbara risker och scenarion, och ska skydda såväl nätverk och informationssystem som systemens fysiska miljö.

Vidare har entiteter som omfattas av NIS 2-direktivet en skyldighet att rapportera incidenter i nätverk och informationssystem som har en betydande inverkan på tillhandahållandet av deras tjänster[18]. De kan även bli föremål för olika tillsynsåtgärder[19]. Vid tillsyn kan tillsynsmyndigheten komma att begära att få tillgång till de lokaler där entiteten bedriver sin verksamhet.

Vid brister i efterlevnad av direktivet kan entiteter även komma att drabbas av olika sanktioner[20]. Nivån på sanktionsavgifterna har dessutom justerats till att bli än mer kostsam för bristande organisationer och kan komma att uppgå till 10 000 000 EUR eller 2 % av organisationens globala omsättning, beroende på vilken siffra som är högst.

18. Artikel 23, (EU) 2022/2555.
19. Artikel 31–33, (EU) 2022/2555.
20. Artikel 34–36, (EU) 2022/2555.

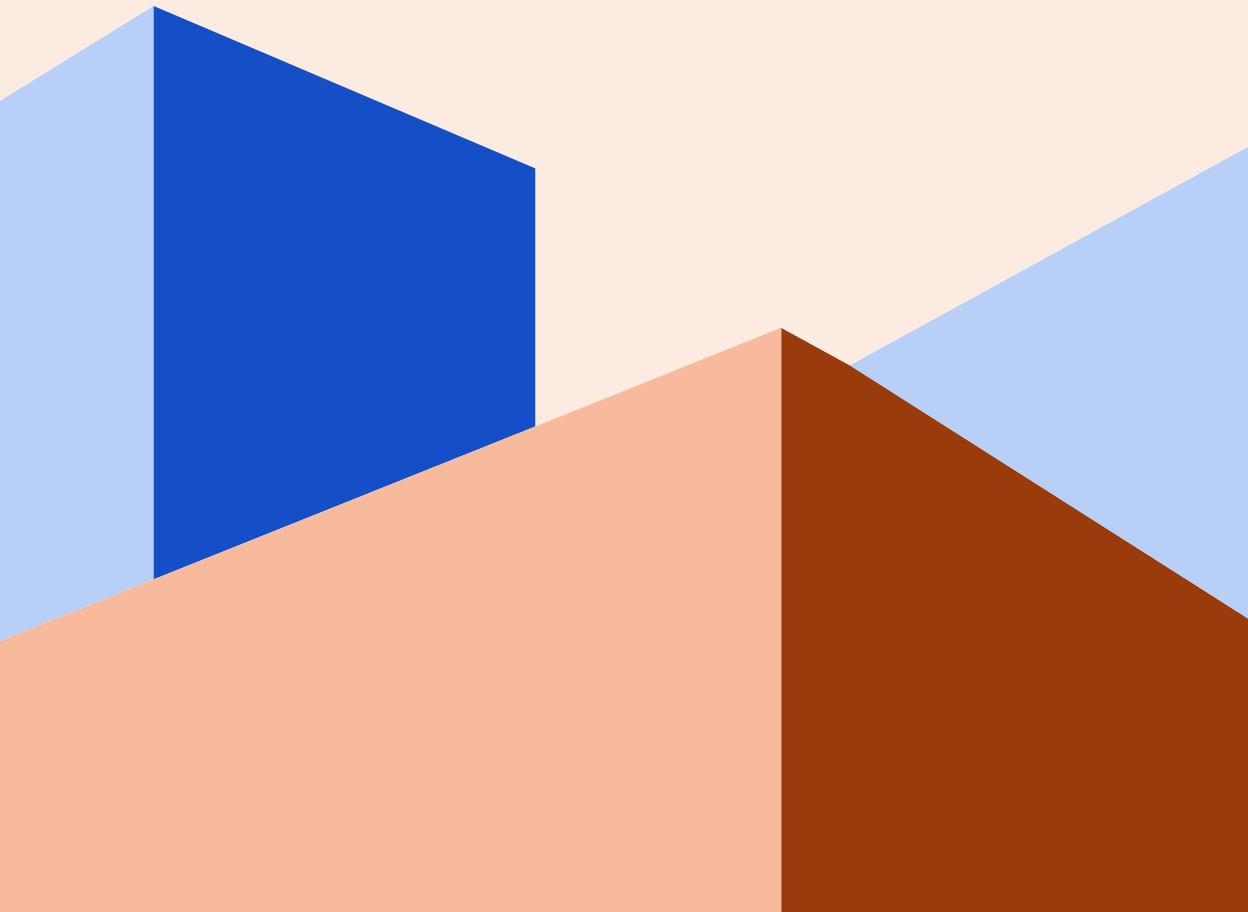
VILKEN SPECIFIK PÅVERKAN HAR NIS 2-DIREKTIVET PÅ FASTIGHETSFÖRVALTARE?

När det kommer till fastighetsbranschen så omfattas man inte, precis som i fallet för CER-direktivet, direkt av kraven för NIS 2. Eventuell omfattning av direktivet kommer i så fall även här från sekundära håll och beroenden.

Exempel: Krav som kommer från fastighetsägarnas hyresgäster på säkerhetsåtgärder för att skydda deras it-miljö. Dessa krav bör ställas av hyresgästerna själva i upphandlingsskedet eller vid avtalsförnyelse. Säkerhetsåtgärderna bör syfta till att reducera verkningar av sådana konsekvenser som hyresgästerna identifierat i de riskanalyser som NIS 2-direktivet kräver.

På samma sätt kan fastighetsägare komma att påverkas indirekt genom att deras samverkanspartners i närliggande branscher, som tillhandahåller exempelvis eldistribution, fjärrvärme eller avlopps- och avfallshantering, träffas av regleringen. Det skulle kunna leda till ökade samarbets- och leveranskostnader för fastighetsägarna.

6



Relationen och interaktionen mellan olika regleringar

I många situationer interagerar NIS-direktiven, CER-direktivet och säkerhetsskyddslagen med varandra samt med andra regelverk som exempelvis offentlighets och sekretesslagen (OSL). En organisation kan enligt regelverkens definitioner träffas av samtliga ovanstående regelverk samtidigt eller bara vissa av dem. Organisationen kan ha viss verksamhet som träffas av ett regelverk och andra verksamheter som träffas av andra regelverk eller inte av något av dem. Det är därför nödvändigt att känna till var gränserna går mellan dessa regleringar samt hur de interagerar med varandra när de samverkar.

→ SAMMANFATTNING

Sammanfattningsvis gäller följande samband och distinktioner mellan lagstiftningarna:

- → Säkerhetsskyddslagen är överordnad NIS-lagen.
- → Säkerhetsskyddslagen gör att OSL även gäller privata företag.
- → CER- och NIS 2-direktivens exakta förhållande till svensk lagstiftning är under utredning.
- → CER-direktivet behandlar allt kontinuitetsarbete för samhällskritiska verksamheter medan NIS/NIS 2-direktiven inriktar sig mot de it-miljöer som dessa verksamheter är beroende av.

6.1 Säkerhetsskyddslagen och NIS

Säkerhetsskyddslagen[21] och NIS-lagen[22] har ett tydligt definierat förhållande till varandra. Lagstiftarna är tydliga med att en verksamhet som omfattas av säkerhetsskyddslagen är undantagen från tillämpning av NIS-lagen (8 § NIS-lagen). Samtliga organisationer behöver alltså ta ställning till om de verksamheter man bedriver träffas av säkerhetsskyddslagen i första hand och om de träffas av NIS-lagen i andra hand. En organisation kan träffas av båda lagstiftningarna men en enskild verksamhet inom organisationen kan det inte.

NIS-lagen gäller för leverantörer inom sektorerna:

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvård
- Leverans och distribution av dricksvatten
- Digital infrastruktur

Vilka leverantörer som mer specifikt omfattas framgår av Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2021:9). Utöver dessa omfattas vissa tillhandahållare av digitala tjänster såsom molntjänster, digitala marknadsplatser och digitala sökmotorer. De leverantörer som träffas ska i sin tur identifiera vilka delar av verksamheten som är samhällsviktiga i syfte att skydda de nätverk och informationssystem som de samhällsviktiga verksamheterna är beroende av.

Säkerhetsskyddslagen i sin tur är tillämplig[23] för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet, så kallad säkerhetskänslig verksamhet. Vidare gäller att den som bedriver säkerhetskänslig verksamhet ska göra en säkerhetsskyddsanalys för att utreda behovet av säkerhetsskydd[24]. Säkerhetsskyddsanalysen ger således svar på vilka eller vilken del (om någon) av verksamheten som omfattas av säkerhets-

21. Säkerhetsskyddslag 2018:585.
22. NIS-lag 2018:1174.
23. 1 kap. 1 § säkerhetsskyddslagen, 2018:585.
24. Säkerhetsskyddsförordning 2021:995.

skyddslagen och vilka säkerhetsskyddsåtgärder som ska vidtas för denna del av verksamheten. Den egna bedömningen i säkerhetsskyddsanalysen om vilken del av verksamheten som är säkerhetskänslig ger samtidigt svar på vilken del av verksamheten som undantas från NIS-lagens tillämpningsområde.

Begreppet verksamhet som återkommer ovan kan föra tankarna till att det är en hel verksamhetsgren som ska undantas från tillämpning av NIS-lagen. Så kan det vara men det behöver inte vara så.

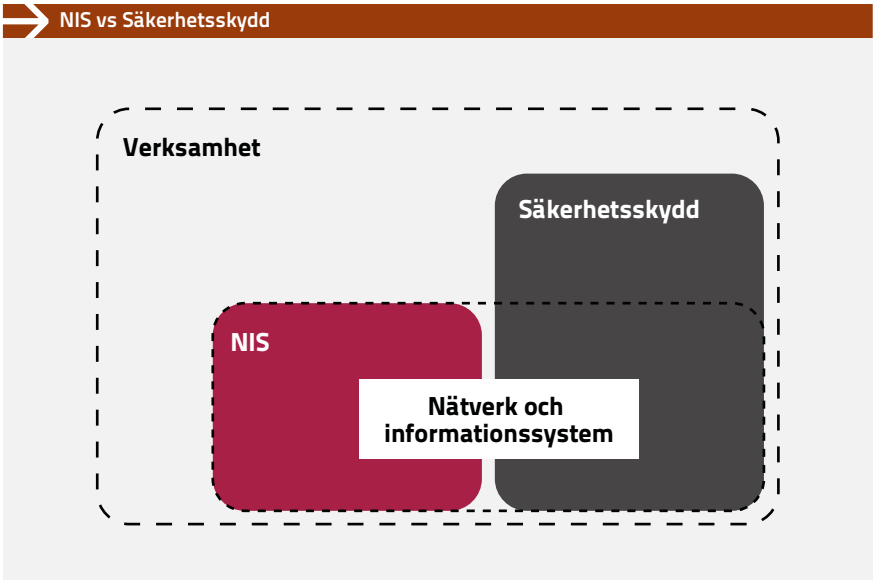
En säkerhetsskyddsanalys av en enskild verksamhet kan resultera i att denna kan delas upp i en delverksamhet som omfattas av säkerhetsskydd och en annan delverksamhet som inte omfattas av säkerhetsskydd.

Det är då endast de delar av verksamheten som omfattas av säkerhetsskyddslagen, det vill säga de delar som identifierats i säkerhetsskyddsanalysen, som undantas från NIS-lagens krav. För den övriga verksamheten ska NIS-lagen tillämpas.

I förhållande till verksamheter som anses vara samhällsviktiga enligt NIS-lagen behöver man vara särskilt noggrann med bedömningen då det kan ligga nära till hands att sådan samhällsviktig verksamhet också kan vara av betydelse för Sveriges säkerhet. Därför är det viktigt för verksamhetsutövaren att ha god kännedom om båda regelverken och ha gjort en säkerhetsskyddsanalys. Att exempelvis rapportera en incident som inträffat i ett nätverk eller informationssystem till tillsynsmyndigheten enligt 18 § NIS-lagen när den egentligen skulle ha anmälts till Säkerhetspolisen enligt 2 kap. 4 § 2 p säkerhetsskyddsförordningen[25] kan i sig innebära en säkerhetsskyddsincident.

Nedan är en illustration ett komplicerat scenario där de två regleringarna träffar olika delar av organisationens nätverk och informationssystem. Regleringarna gäller parallellt för olika delar av de nätverk och informationssystem som den samhällsviktiga tjänsten är beroende av. Delar som omfattas av säkerhetsskyddslagen är undantagna från NIS-regleringen medan NIS-regleringen gäller för de delar som inte omfattas av säkerhetsskyddslagen. I denna situation uppstår ofta mer detaljerade gränsdragningsfrågor som behöver analyseras och bedömas ytterligare.

25. Säkerhetsskyddsförordning 2021:995.



FIGUR 3 ▪ Källa: MSB, NIS-regleringen och säkerhetsskyddslagen.

För mer detaljer om de omnämnda lagstiftningarna se kapitel 2 – *Säkerhetsskyddslagen*, kapitel 3 – *Metodik och vägledning för genomförandet av en säkerhetsskyddsanalys* samt kapitel 5 – *NIS 2-direktivet*.

6.2 Säkerhetsskyddslagen och CER/NIS 2

I NIS2-direktivet och CER-direktivet betonas att direktiven inte påverkar medlemsstaternas ansvar för att skydda sin nationella säkerhet. Offentliga förvaltningar som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet eller försvar är i sin helhet undantagna från direktivens tillämpningsområde. När det gäller andra aktörer har medlemsstaterna möjlighet att besluta att särskilda entiteter med verksamhet på de aktuella områdena ska vara undantagna från skyldigheter enligt direktivet

Sveriges regering har via ett kommittédirektiv[26] beslutat om en statlig offentlig utredning där en särskild utredare ska föreslå de anpassningar av svensk rätt som är nödvändiga för att NIS 2-direktivet och CER-direktivet ska kunna genomföras. Utredaren ska bland annat:

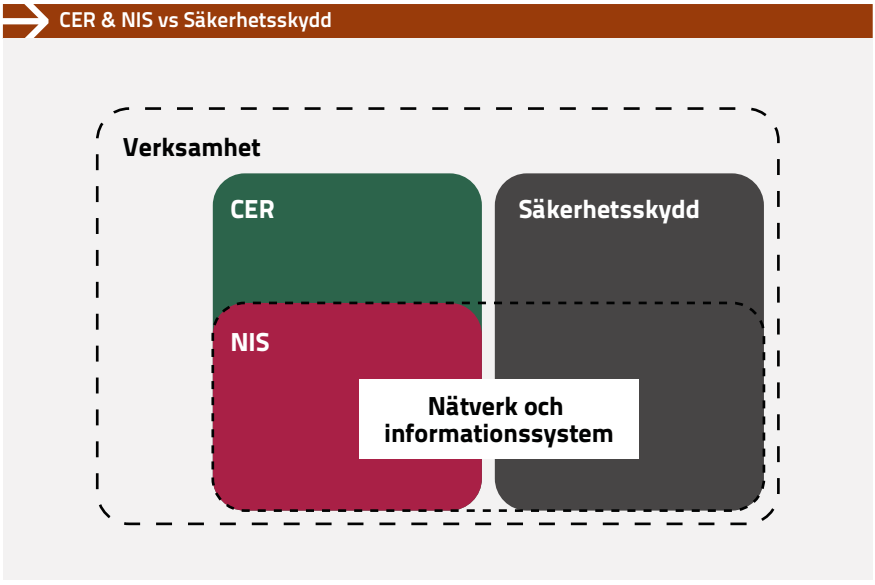
26. Kommittédirektiv 2023:30.

- Ta ställning till om kommuner ska omfattas av regleringen.
- Analysera hur den nya regleringen ska fungera vid sidan av säkerhetsskyddslagen och föreslå de ändringar som behövs för en mer sammanhållen systematik mellan regelverken.
- Föreslå hur identifieringen av och krav på entiteter som omfattas av NIS 2-direktivet respektive CER-direktivet ska regleras.
- Föreslå hur rollfördelningen mellan svenska myndigheter ska se ut med avseende på de olika uppgifter och ansvarsområden som föreskrivs i NIS2-direktivet och CER-direktivet.
- Ta ställning till om det behövs ett starkare och mer omfattande sekretesskydd för uppgifter som kan komma att behandlas enligt direktiven.
- Lämna förslag till nödvändiga författningsändringar.

I kommittédirektivets uppmaningar till utredaren noterar man att både CER- och NIS 2-direktiven ger medlemsstaterna rätt att fatta beslut om att flertalet av dessa direktivs bestämmelser inte ska vara tillämpliga på särskilda kritiska entiteter som bedriver verksamhet inom områden relaterade till nationell, allmän säkerhet eller försvar. Detta förfarande saknar motsvarighet i svensk rätt och man ålägger därför utredaren att analysera hur direktivens möjlighet att undanta specifika aktörer ska genomföras i svensk rätt.

Vissa kritiska entiteter skulle med ovanstående inriktning, precis som även är fallet med den befintliga NIS-lagen, ha delar av sin verksamhet som omfattas av NIS 2-direktivets eller CER-direktivets tillämpningsområde samtidigt som andra delar av verksamheten undantas och i stället omfattas av säkerhetsskyddslagen. Kommittédirektivet pekar därför ut behovet av att analysera hur säkerhetsskyddslagens systematik och terminologi i praktiken ska fungera vid sidan om de i svensk rätt införlivade direktiven. Utredaren ges även rätt att föreslå de ändringar i säkerhetsskyddsregleringen som man bedömer behövs för att uppnå en sådan sammanhållen terminologi och systematik mellan regelverken.

Nedan är en illustration av ett scenario där en organisation har samhällsviktig verksamhet enligt definitionerna i både NIS 2- och CER-direktiven samt att den träffas av säkerhetsskyddslagen i vissa delar av verksamheten. Säkerhetsskyddslagstiftningen kommer då att undantas de andra lagstiftningarna där den är tillämplig och CER-direktivet hänvisar samtliga föreskrifter som rör nätverk och informationssystem till NIS-regelverken.



FIGUR 4

6.3 Säkerhetsskyddslagen och OSL

Enskild verksamhet omfattas vanligtvis inte av offentlighets- och sekretesslagstiftningen (OSL). Inom ramen för säkerhetsskydd ska dock privat verksamhet göra en sekretessbedömning som om man omfattas av OSL.

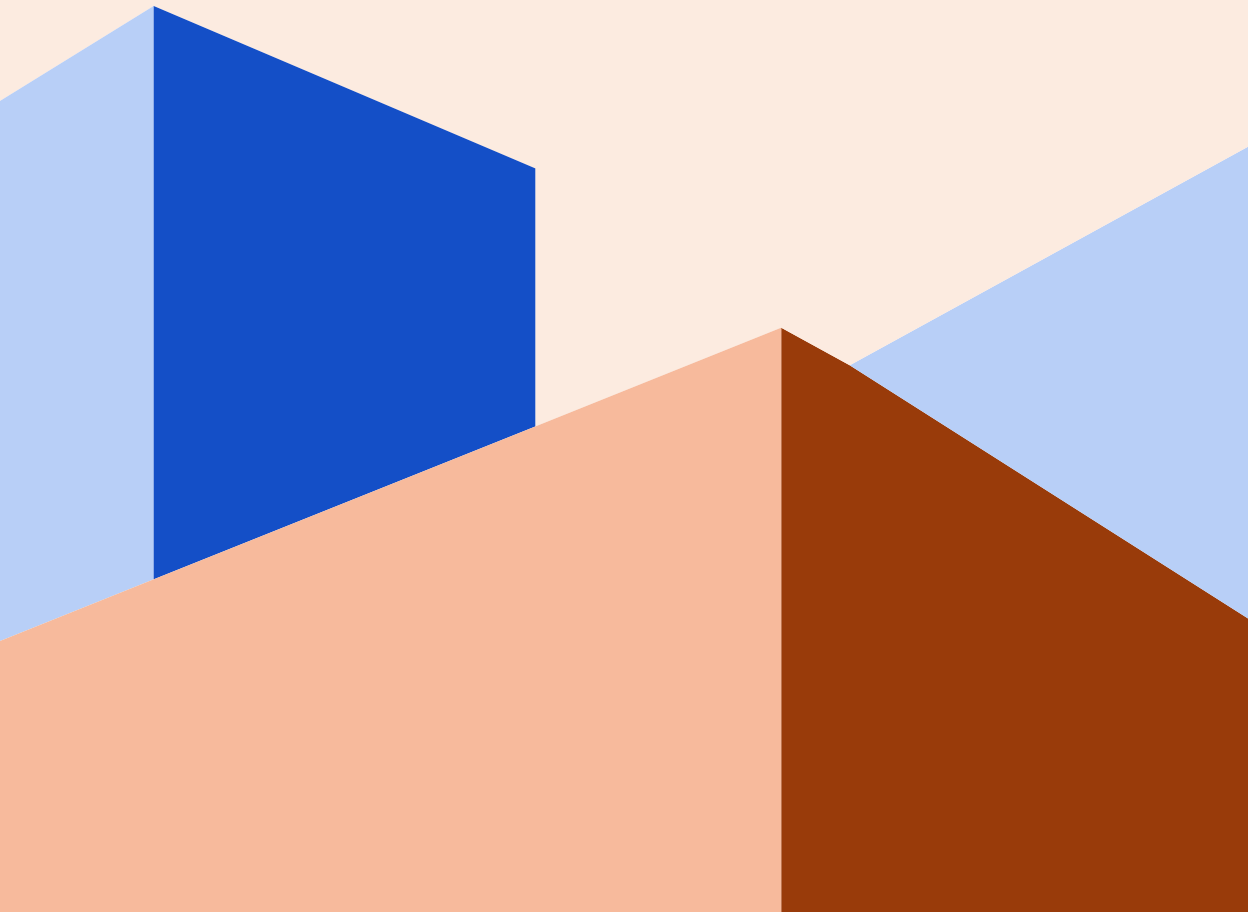
Detta innebär att i arbetet med att ta fram en säkerhetsskyddsanalys kan det komma att samlas in och dokumenteras uppgifter som kan skada Sveriges säkerhet om de röjs. Om man i arbetet med att ta fram en säkerhetsskyddsanalys gör bedömningen att ens verksamhet bedriver säkerhetskänslig verksamhet medför detta att verksamheten automatiskt omfattas av säkerhetsskyddslagstiftningen. Med detta följer i sin tur att skyddsvärda uppgifter ska bedömas och klassificeras i enlighet med OSL och att de särskilda hanteringsreglerna kopplade till den lagstiftningen gäller.

6.4 NIS 2 och CER

CER- och NIS-direktiven kompletterar varandra då NIS-direktivet reglerar det systematiska informationssäkerhetsarbetet även i samhällsviktig verksamhet som identifieras under CER-direktivet. Både CER- och NIS-regelverkens syfte och fokus ligger på motståndskraft och kontinuitet. De har som ändamål att leverantörer av samhällsviktiga tjänster har förmåga att både fortsatt leverera tjänsterna under påfrestningar och mindre avbrott samt att snabbt och effektivt kunna återhämta sig från större avbrott.
Skillnaden dem emellan är att CER-direktivet omfattar samtliga skyddsåtgärder som krävs för att säkerställa motståndskraften av all samhällsviktig verksamhet medan de båda NIS-direktiven begränsar sig till skydd av de nätverk, it-tjänster och it-komponenter som de samhällsviktiga tjänsterna är beroende av. Detta medför att CER-direktivet adderar krav på omfattningen av vilka verksamhetsaspekter man behöver ta hänsyn till samt vilka risker mot verksamheterna man behöver identifiera och hantera. Det tillkommer alltså via CER-direktivet exempelvis krav på ytterligare hantering av katastrof- och klimatpåverkan samt specifika åtgärder inom fysisk säkerhet personalsäkerhet.

För mer detaljer om lagstiftningarna se kapitel 4 – *CER-direktivet* samt kapitel 5 – *NIS 2-direktivet*.

7



Utmaningar med att förhålla sig till CER och NIS

EU-direktiven CER-direktivet[27] och NIS-direktiven[28] betonar ett par punkter som direkt eller indirekt leder till att organisationer (så kallade entiteter i direktiven) i många fall behöver göra betydande investeringar samt ofta omfattande justeringar av sitt arbetssätt.

Vägledning från MSB i hur man ska förhålla sig till CER-direktivet och NIS 2-direktivet kommer att tillhandahållas efter att de har implementerats i svensk lag och MSB har fått det uppdraget. Vägledning för det i Sverige redan implementerade NIS-direktivet står till viss grad att finna. Regeringen har i sin förordning[29] gett MSB rätt att skriva och publicera föreskrifter om vilka som ska omfattas av NIS-lagen, föreskrifter om vad som räknas som en betydande störning, föreskrifter om systematiskt och riskbaserat informationssäkerhetsarbete samt föreskrifter om incidentrapportering. I deras föreskrifter ingår även allmänna råd kopplat till kravställningarna i föreskrifterna och består av nedanstående dokument[30]:

- Anmälan och identifiering av leverantörer av samhällsviktiga tjänster.
- Informationssäkerhet för leverantörer av samhällsviktiga tjänster.
- Rapportering av incidenter för leverantörer av samhällsviktiga tjänster.
- Rapportering av incidenter för leverantörer av digitala tjänster.
- Frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet.

27. (EU) 2022:2557.
28. (EU) 2016:1148 respektive (EU) 2022:2555.
29. Förordning om informationssäkerhet för samhällsviktiga och digitala tjänster, 2018:1175.
30. MSBFS 2018:7–11.

En organisation som bedriver någon form av samhällsviktig tjänst, enligt de definitioner som MSB föreskriver, behöver i någon form ta sig igenom ett antal steg som översiktligt beskrivs nedan. Några av dem är sannolikt enklare att genomföra, medan andra kräver att verksamheten gör större förändringar för att anpassa sina processer, sin personalstyrka och sin teknikflora. Stora organisationer vars komplexitet är omfattande och som inte har hunnit etablera ett moget arbetssätt inom kontinuitet och informationssäkerhetsarbete har de största utmaningarna framför sig.

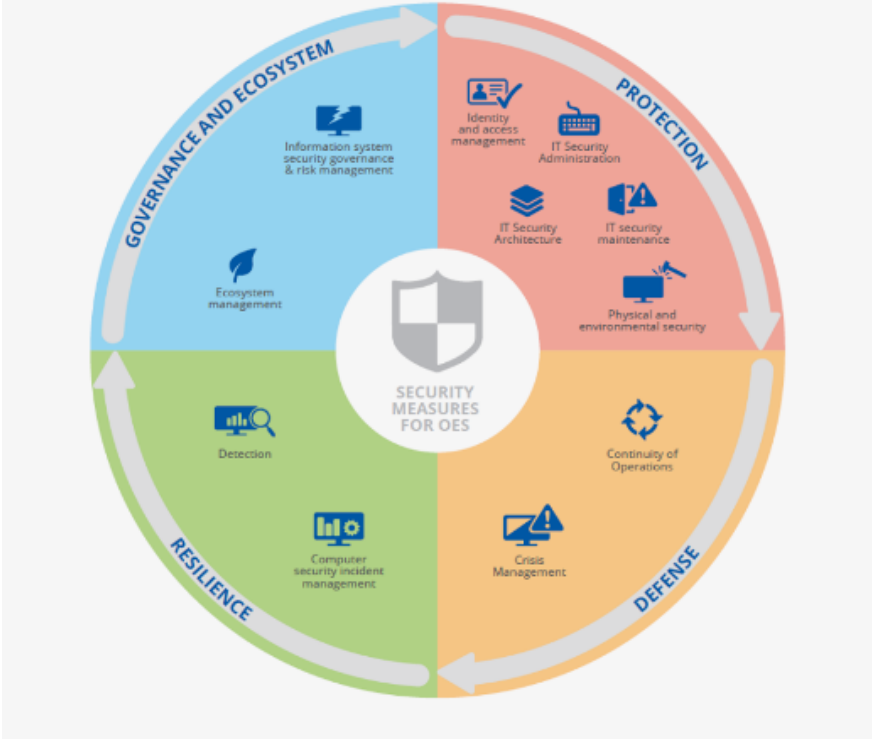
→ VIKTIGT ATT TÄNKA PÅ FÖR ATT ANPASSA VERKSAMHETEN TILL CER OCH NIS!

För att kunna anpassa verksamheten till de regulatoriska krav som kommer från CER- respektive NIS 2-direktiven så behöver följande punkter stegvis adresseras:

1. Identifiera berörd verksamhet som leverantör av samhällsviktig tjänst och anmäla detta till aktuell tillsynsmyndighet.
2. Identifiera vilka delar av verksamheten som bedriver samhällsviktiga tjänster samt, exakt vilka beroenden som dessa verksamhetsdelar har i form av nätverk och informationssystem (i fallet för NIS) samt alla andra former av beroenden inklusive personalsäkerhetsfrågor (i fallet för CER). Att organisationen har kunskap om detta är fundamentalt för att kunna bedöma riskerna i nästa steg.
3. Bedriv riskanalysarbete för samtliga risker som kan drabba den samhällsviktiga verksamheten och vidta nödvändiga åtgärder. Här ska samtliga risker beaktas för att möta CER-direktivet och specifikt de risker som kan drabba de kritiska it-miljöerna för att möta NIS-/NIS 2-direktiven.
4. Säkerställ tillräckliga säkerhetsåtgärder. De beslutade åtgärderna får inte understiga de specifika krav som återfinns i MSB:s och tillsynsmyndigheternas föreskrifter.

5. Säkerställ att organisationen har tillräckligt effektiva processer och rutiner för att förhindra och upptäcka, rapportera, hantera, återhämta sig från och utvärdera incidenter.
6. Bygg en organisation för, och öva kontinuitet. Att planera och träna för tänkbara avbrott i den samhällsviktiga leveransen är vitalt för att kunna absorbera, anpassa sig till och återhämta sig från incidenter.
7. Bedriv regelbunden uppföljning för att uppnå ständiga förbättringar som en del av systematiken.

ENISA:s vägledning



FIGUR 5 ▪ Källa: ENISAs Guidelines on assessing DSP security and OES compliance with the NISD security requirements.

7.1 Administrativa utmaningar

De lagar, regler och föreskrifter som implementerar NIS-direktivet i Sverige kräver, som en förutsättning för att kunna säkra leveransen av de samhällsviktiga tjänsterna, en fullständig visibilitet och dokumentation över både de samhällsviktiga tjänsterna i sig samt alla de it-tjänster och komponenter som tjänsterna är beroende av. Detsamma kommer att gälla för NIS 2- och CER-direktivens införlivande i svensk lagstiftning, där CER dessutom inte enbart fokuserar på it-miljöerna utan samtliga verksamhetsberoenden. Detta ställer nya krav på en organisation som anpassar sig till dessa regelverk.

Allra minst behöver en ny utredning som beskriver exakt vilka delar av verksamheten som bedriver samhällsviktiga tjänster genomföras och dokumenteras. Därefter behöver en inventering genomföras över samtliga processer, tjänster och it-komponenter som de samhällsviktiga tjänsterna är beroende av. Detta ställer höga krav på organisationens inventering och dokumentation genom hela organisationen, genom hela it-arkitekturen och genom de inkluderade it-komponenternas hela livscykel. Enbart en organisation med hög mognadsgrad i sina administrativa processer och rutiner kan förväntas ha all denna information lättillgängligt sedan tidigare.

För att kunna bedriva den kravställda systematiska identifieringen och hanteringen av risker som kan äventyra leveransen av de samhällsviktiga tjänsterna ställs uttryckliga krav på ett fullgott ledningssystem för informationssäkerhet (LIS) och utvecklade riskhanteringsprocesser. I denna fråga specificerar inte lagstiftarna noggrannare än så hur ledningssystemet ska se ut utan lämnar det till varje organisation att anpassa det till dess förutsättningar.

MSB nämner i sina föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster att "varje leverantör ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 om ledningssystem för informationssäkerhet eller motsvarande".

– [MSBFS 2018:8].

Certifiering mot de standarder som omnämns i föreskrifterna är inte ett uttryckligt krav men det krävs implementering och förvaltning av ett ledningssystem för informationssäkerhet som tar hänsyn till samtliga relevanta aspekter av standarderna. Att implementera ett nytt ledningssystem är något som tar tid och stort arbete för en organisation som inte redan har ett sådant på plats.

7.2 Tekniska utmaningar

För att nå och hålla den nivå på systematiskt informationssäkerhetsarbete som krävs av en organisation som levererar samhällsviktiga tjänster krävs förutom administrativ ordning och reda en teknisk infrastruktur som möjliggör detta. Detta inkluderar både nödvändiga stödsystem för administration och processer samt lämplig arkitektur för it-miljöer och eventuell annan teknik. De tekniska säkerhetskontrollerna bör implementeras som en följd av den interna riskhanteringsprocessen och tillkomma efter beslut baserade på kostnad och effektivitet. De lagar, regler och föreskrifter som är framtagna avser att addera en miniminivå till dessa processer och beslut.

För de flesta, men framför allt för något större organisationer, krävs någon form av stödsystem för inventering av nätverk, system och it-komponenter för att löpande kontroll av it-miljöerna ska vara genomförbart i praktiken. Ofta sker detta i en databas som i it-termer benämns *configuration management database* (CMDB).

Även andra nödvändiga processer är i behov av stödsystem som organisationen behöver implementera, använda sig av och förvalta. Främsta exemplen på verktyg som underlättar efterlevnad av CER- och NIS-direktiven är de som behövs för incidenthantering och rapportering, avvikelsedetektering samt regelbundna kontroller av högre behörigheter.

Till detta kommer vissa tekniska säkerhetskontroller som föreskrifterna ställer specifika krav på. De ger riktlinjer för hantering inom ett antal områden som anses extra viktiga. Inga krav uttrycks på teknik i form av hårdvara eller mjukvara men det krävs att organisationen har säkerställt hantering av dessa områden. Tekniklösningar ska utredas för deras effektivitet i att minimera risker mot de samhällsviktiga tjänsterna och implementeras där så är lämpligt.

Detta kräver motiverade beslut om tekniklösningar för minst nedanstående områden:

- Nätverkssegmentering
- Härdning
- Kryptering
- Skydd mot skadlig kod
- Loggning
- Detektering av avvikelser
- Autentiserings- och behörighetskontroller
- Backup
- Redundans

För mogna organisationer som sedan tidigare har etablerat ett systematiskt informationssäkerhetsarbete är dessa områden sannolikt redan till stor grad införlivade i it-säkerhetsarbetet och dess arkitektur. Andra organisationer kan komma att ställas inför signifikanta investeringar i tid och resurser för att justera sin arkitektur samt implementera och förvalta nya säkerhetskontroller.

7.3 Fysisk säkerhet och personalsäkerhet

Kraven i NIS-direktiven ställer implicita krav på fysisk säkerhet i syfte att säkra access till samhällsviktiga it-miljöer. CER-direktivet tar detta område ett steg längre med ett uttryckt fokus på både *åtgärder för katastrofriskreducering och klimatanpassning*[31] samt fysiskt intrångsskydd i form av *till exempelvis stängsel, barriärer, verktyg och rutiner för övervakning av områdesgränser, detektionsutrustning och åtkomstkontroller*[32].

Nytt i CER-direktivet är dessutom specifika krav på personalsäkerhet och bakgrundskontroller. Eu-lagstiftarna ägnar ett helt eget kapitel[33] åt att specificera minimikrav på sådan hantering. Detta medför en högt satt lägstanivå på dessa aspekter av kritiska entiteters rekryteringsprocesser.

31. Artikel 13, kap. 1a, (EU) 2022/2557.
32. Artikel 13, kap. 1b, (EU) 2022/2557.
33. Artikel 14, (EU) 2022/2557.

Tydliga krav ställs alltså på ett helhetsperspektiv i sitt informationssäkerhets- och riskhanteringsarbete för att kunna tillfullo identifiera och hantera samtliga risker som kan störa tillhandahållandet av de samhällsviktiga tjänsterna.

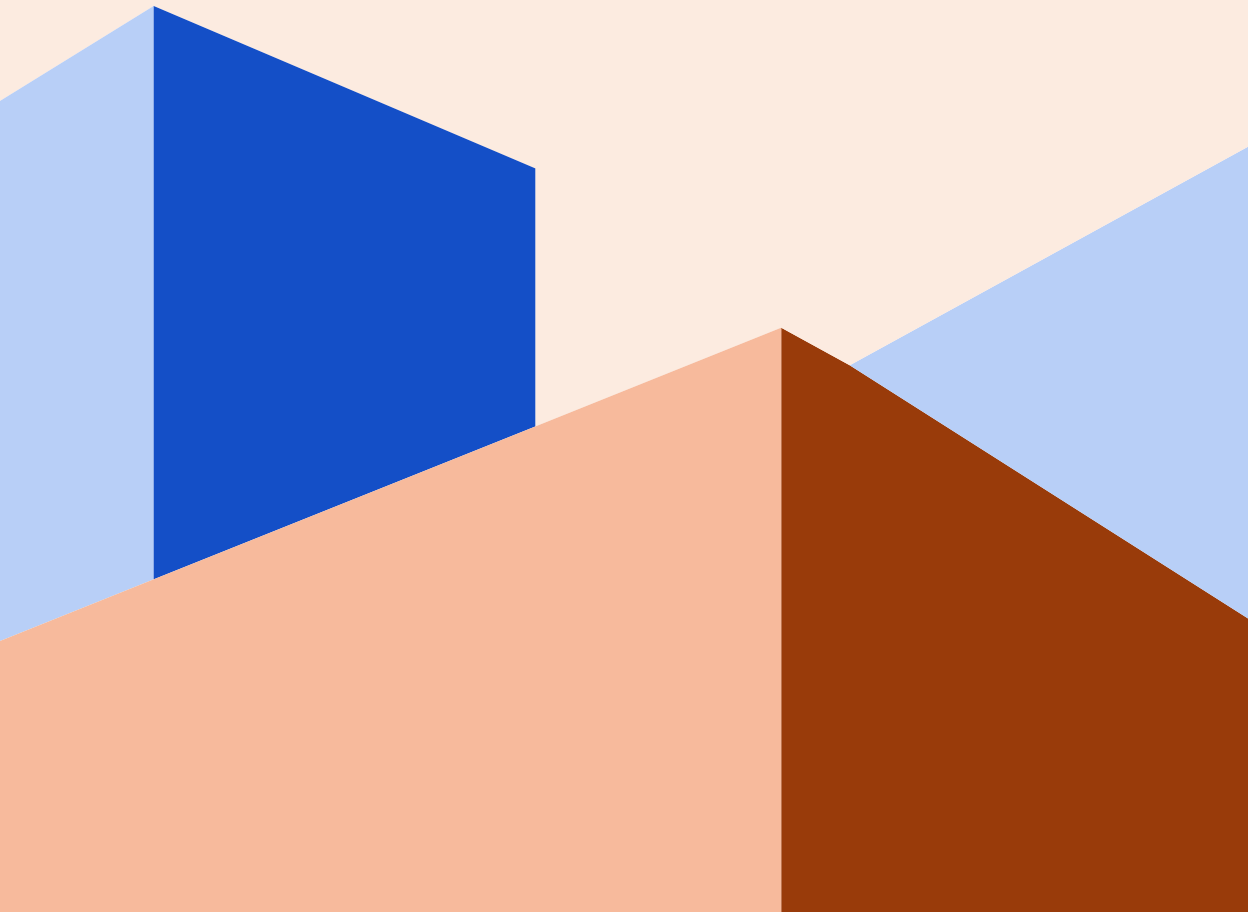
7.4 Organisatoriska utmaningar

Samtliga ovanstående utmaningar som uppstår för leverantörer av samhällsviktiga tjänster kräver en bakomliggande organisation som är byggd för att hantera dem.

Allra viktigast är insikt, deltagande och kontinuerligt stöd från organisationens högsta ledning. De behöver ta ägandeskap över och skapa förutsättningar för att verksamhetens informationssäkerhetsprogram håller önskad nivå och är kapabelt till att möta de regulatoriska kraven. Detta inkluderar dokumenterade roll- och ansvarsbeskrivningar, processer och hanteringsregler för samtliga relaterade arbetsområden där följande är fokusområden:

- Personalutbildning och säkerhetsmedvetenhet
- Visibilitet, spårbarhet och dokumentation
- Systematiskt riskhanteringsarbete
- Säkerhetsuppdateringar
- Incidentdetektering, -hantering och -rapportering
- Kontinuitetsplanering och -hantering
- Träning och övningar
- Systematiskt uppföljningsarbete

8



Aggregerade och ackumulerade informations-mängder

När man bedömer hot och konsekvenser behöver man även ta hänsyn till effekterna av påverkan eller obehörig åtkomst till samlad information då dessa effekter inte nödvändigtvis får samma konsekvensnivå, eller att de ens ökar linjärt med antalet. Det är även möjligt att helt nya konsekvenser kan uppstå.

Detta innefattar även säkerhetsskyddsklassificerad information. Om enskilda uppgifter som saknar säkerhetsskyddsklass eller är indelade i en av säkerhetsskyddsklasserna begränsat hemlig, konfidentiell eller hemlig samlas, kan det i vissa fall medföra att en högre säkerhetsskyddsklass ska tillämpas på uppgiftssamlingen. Så är fallet om den aggregerade eller ackumulerade informationen gör att en antagonist kan dra andra, helt nya slutsatser av uppgiftssamlingen än av varje enskild uppgift[34], exempelvis:

- Stora mängder information lagras i systemet (ackumulering).
- Flera olika informationsmängder som när de sammanförs skapar känsligare information vilket innebär ett högre skyddsbehov (aggregering).

34. 4 kap. 6 § Säkerhetspolisens föreskrifter (PMFS 2019:2) om säkerhetsskydd.

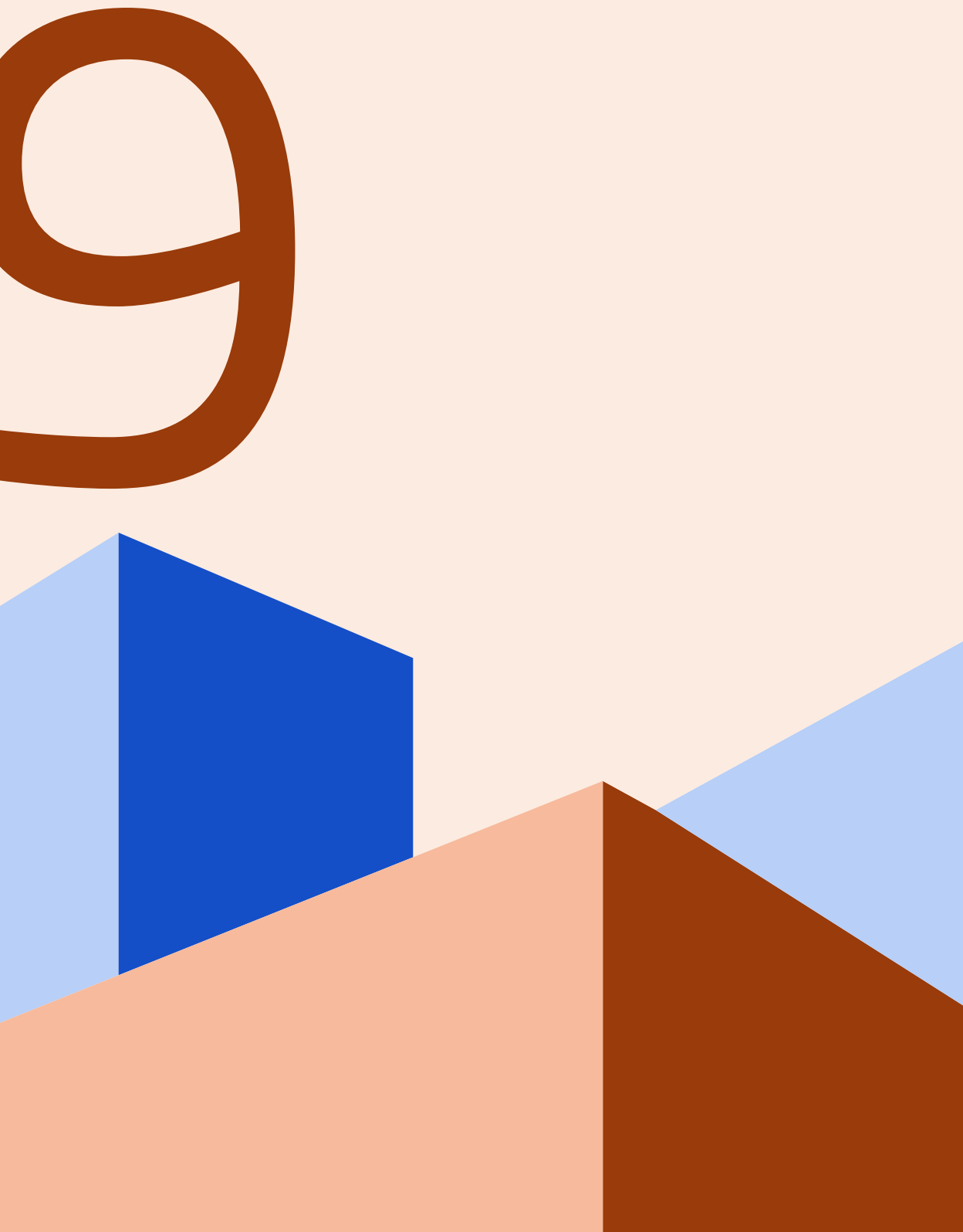
→ BEGREPP OCH FÖRTYDLIGANDEN

Informationsmängd
Innebär en gruppering av information, exempelvis i form av ett dokument, en databas eller liknande. En informationsmängd innehåller en eller flera informationstyper. En informationsmängd utgör minsta möjliga meningsfulla del, till exempel ska en pdf-fil inte delas upp i dess olika informationstyper utan ses som en informationsmängd. En informationstillgång som klassificeras (klassificeringsobjekt) innehåller normalt ett flertal informationsmängder.

Informationstyp
Innebär information av ett visst slag. Man kan välja att definiera en informationstyp som en informationsmängd och klassificera den. Vilka informationstyper en organisation väljer att definiera som en informationsmängd och klassificera beror på organisationens behov. Att identifiera informationstyper som är viktiga kan underlätta klassificeringen, till exempel när en viss typ av information är spridd i stora delar av organisationen, som personuppgifter, eller är av särskild betydelse för organisationen. Exempel på informationstyper som kan vara av särskild betydelse för en organisation är kundregister, ekonomisk redovisning, riskanalyser, källkod, ritningar, forskningsresultat eller liknande beroende på vilken verksamhet som bedrivs. Informationstyper som finns på många ställen i er organisation eller som är särskilt viktiga för hela organisationen kan klassificeras organisationsgemensamt, för att undvika att olika verksamheter lägger tid på att klassificera samma informationstyp flera gånger.

Aggregerade uppgifter
Betyder att flertalet olika typer av uppgifter samlas.

Ackumulerade uppgifter
Betyder en ökad volym av samma typ av uppgifter. I båda fallen skapas det i och med detta nya informationsmängder med nya skyddsvärden.



Risk, riskhantering och riskanalys

Med väldigt få undantag har alla organisationer behov av att kunna förhålla sig till och hantera möjliga skador och förluster inom sin verksamhet. Skador och förluster som i värsta fall kan påverka hela organisationens framgång och överlevnad. Organisationens förmåga att systematiskt kunna prioritera, balansera och förebygga möjliga skador av olika karaktär och storlek utgör kärnan i organisationens riskhantering.

Riskhantering omfattar olika aspekter av en organisations verksamhet och kan beskrivas som organisationens förmåga att kunna tillämpa ett riskbaserat angreppssätt i syfte att:

1. **Förebygga skador:** I en verksamhet finns det alltid en risk för skador på människor, egendom och miljö. Det kan vara olyckor, naturkatastrofer, brand, stöld eller andra incidenter. Genom att genomföra en effektiv riskhantering kan verksamheten identifiera potentiella faror och vidta åtgärder för att minimera risken för skador. Det kan innebära att utarbeta säkerhetsföreskrifter, implementera förebyggande åtgärder, tillhandahålla nödvändig utbildning och utrustning för personalen samt säkerställa att det finns en plan för att hantera eventuella skador om de inträffar. Genom att minska skador kan organisationen undvika produktionsavbrott, rättsliga konsekvenser och kostsamma skadestånd.
2. **Uppfylla lag- och avtalskrav:** Lagar, föreskrifter och avtal är viktiga inom alla verksamheter och reglerar olika aspekter av verksamhetens funktion. Genom att bedöma risker ökar medvetenheten om organisationens förutsättningar att uppfylla de tillämpliga lagar, föreskrifter och avtal som gäller för verksamheten, därmed förbättras organisationens förmåga att undvika rättsliga påföljder, sanktioner, böter och förlorat förtroende från kunder och intressenter.

3. **Skydda tillgångar:** Genom att bedöma risker kan verksamheten skydda sina tillgångar, inklusive fysisk egendom, immateriell egendom, finansiella tillgångar och personal.
4. **Minska osäkerheter:** Riskhantering hjälper till att identifiera och analysera osäkerheter och hot som kan påverka verksamheten. Genom att förstå och hantera dessa risker kan företaget fatta mer informerade beslut och minimera oväntade negativa konsekvenser.
5. **Förbättra effektivitet:** Genom att identifiera och hantera risker kan verksamheten förbättra sin effektivitet och sina möjligheter. Genom att ta risker på ett kontrollerat sätt kan organisationen bättre optimera sina resurser, hitta nya möjligheter och driva tillväxt.
6. **Minska kostnader:** Genom att förebygga skador och incidenter kan företaget minska kostnader för reparationer.

Gemensamt för ovanstående ändamål är att riskhantering omfattar alla de steg och aktiviteter som vidtas; från att identifiera och värdera de olika hot som verksamheten är exponerade mot och de risker som hoten genererar till att följa upp att valda riskreducerande åtgärder är implementerade i verksamheten och är effektiva.

Fortsättningsvis beskrivs i detta avsnitt riskhantering sett till informationssäkerhet och det systematiska arbete som bland annat föreskrivs i den internationella standarden ISO IEC 27001. Standarden ISO27001 betraktar riskhanteringsarbetet ur aspekterna ”riskbedömning” och ”riskbehandling”. Standarden fokuserar på riskhanteringens centrala betydelse för det systematiska informationssäkerhetsarbetet och i det som benämns ”ledningssystem för informationssäkerhet” och som vanligen förkortas LIS.

SAMMANFATTNING

Ett systematiskt arbete med riskhantering är nödvändigt för att kunna prioritera och fatta beslut kring eventuella åtgärder avsedda att hantera risker mot organisationer | organisationers risker.

Ett systematiskt riskarbete innebär att:

1. Tillse förutsättningar för varje steg nedan.
2. Identifiera och värda hot.
3. Formulera risker.
4. Bedöma risker.
5. Behandla risker, exempelvis genom att vidta riskreducerande åtgärder.
6. Följa upp riskåtgärder för implementation och effektivitet.

Några viktiga saker att tänka på för att bedriva ett sådant arbete är att:

- Tillse ett stöd från ledningen för att ge arbetet en ärlig chans att lyckas.
- Ta fram en tydlig metodik.
- Tillse att metodiken innehåller tydliga definitioner av begrepp, värden, skalor och bedömningsgrunder.

Tydlighet, eftertanke och fokus på vad man försöker åstadkomma är således nyckelorden.

9.1 Om den valda riskmetodiken i denna vägledning

Den riskmetodik man väljer behöver vara väl valt på det sättet att det förhåller sig till de olika regel- respektive ramverk som beskriver hur riskhantering ska utföras. För läsaren av denna vägledning är det därmed fördelaktigt att känna till hur den valda riskmetodiken förhåller sig till några av de mer framträdande regel- och ramverken.

Ur ett regelverksperspektiv bedöms huvudsakligen nedanstående MSB föreskrifter vara de centrala för målgruppen av denna vägledning:

- MSBFS2015:4 MSB:s föreskrifter om landstings risk- och sårbarhetsanalyser
- MSBFS2015:5 MSB:s föreskrifter om kommuners risk- och sårbarhetsanalyser
- MSBFS2020:6 MSB:s föreskrifter om informationssäkerhet för statliga myndigheter

Såväl MSBFS2015:4 som MSBFS2015:5 definierar begreppet risk som ”en sammanvägning av sannolikheten för att en händelse ska inträffa och de konsekvenser händelsen kan leda till”[35] i övrigt anges helt enkelt att arbetet med risk- och sårbarhetsanalys ska anpassas till de egna behoven och till övriga befintliga förutsättningar. MSBFS2020:6 är betydligt mer detaljerad i sina krav på bland annat riskhantering jämfört med de tidigare två och anger att arbetet exempelvis ska omfatta att ”identifiera, analysera och värdera risker för sin information” samt ”utifrån genomförd informationsklassning och riskbedömning identifiera behov av och införa ändamålsenliga och proportionella säkerhetsåtgärder”[36].

Den valda riskmetodiken i denna vägledning överensstämmer helt med vad som anges i ovan nämnda föreskrifter i att definiera innebörden av begreppet risk. Riskmetodiken svarar även upp mot de nyare föreskrifterna och allmänna råden i MSBFS2020:6.

Utöver föreskrifter så finns även ett antal ramverk och standarder som omfattar riskhantering. Bland dessa anses nedanstående standarder vara viktiga för målgruppen av denna vägledning:

- SS-ISO 31000 Riskhantering – Vägledning.
- SS-EN ISO/IEC 27001 Ledningssystem för informationssäkerhet.

Såväl SS-ISO 31000 som SS-EN ISO/IEC 27001 beskriver att riskhantering omfattar riskbedömning, riskbehandling och riskuppföljning. Standarderna beskriver även olika aspekter och faktorer som bör omfattas såsom roller och ansvar, att riskanalyser ska leda till konsekventa och jämförbara resultat samt val av lämpliga säkerhetsåtgärder.

35. 2§ MSB:s föreskrifter om landstings risk- och sårbarhetsanalyser (MSBFS 2015:4).
36. 6§ MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

Den valda riskmetodiken som finns i denna vägledning överensstämmer helt med vad som anges i ovan nämnda standarder sett till hur risker betraktas respektive värderas.

9.2 Begreppet risk

Innan riskanalyser och riskanalysarbetet beskrivs på lite djupare nivå behöver begreppet risk förtydligas, inte minst för att bättre förstå exempelvis innebörden av att tillämpa ett riskbaserat angreppssätt.

→ FALLGROPAR ATT UNDVIKA AVSEENDE BEGREPPET RISK

Begreppet risk används frekvent. Tyvärr används det ofta utan att reflektera så mycket över vad som avses och vad begreppet innebär. Detta leder ofta till att risken blir otydlig. Ett par fallgropar är viktiga att känna till för att inte riskformuleringen ska bli otydlig och oavsiktligt försvåra kommunikationen mellan berörda roller eller efterlevnaden av exempelvis de regelverk som nämnts tidigare i detta dokument.

- → Begreppet risk uttrycks ibland felaktigt som en konsekvens (risken är att vi drabbas av sanktioner).
- → Begreppet risk uttrycks ibland felaktigt som en sårbarhet (risken är att it-systemet inte är uppdaterat).
- → Begreppet risk uttrycks ibland felaktigt som en allmän oro (risken är att digitaliseringen går för fort).
- → Begreppet risk uttrycks ibland med övergripande och generella ord (risken är internt läckage av viktig information).

I detta dokument avses med begreppet risk en tydlig riskformulering som byggs upp på ett ordnat sätt med hjälp av några andra centrala begrepp; hothändelse, sannolikhet och (skade)konsekvens.

För att underlätta diskussioner och dialoger kring risker och riskhantering är det rekommenderat och lämpligt att använda en enhetlig riskformulering som byggs upp med hjälp av dessa tre begrepp för att skapa tydliga riskformuleringar (begreppen inom hakparentes ersätts med de respektive värden som gäller för den aktuella situationen).

"Risk för att [Hothändelse]. På årsbasis bedöms risken inträffa [Sannolikhet] med en total skadeverkan motsvarande [Skadekonsekvens]"

Lite förenklat kan sägas att denna riskformulering beskriver hur ofta en negativ händelse inträffar och hur stor skada som då bedöms uppstå.

9.3 Riskanalyser

Riskanalys utgör det metodiska arbetet med att granska och värdera gällande förutsättningar och omständigheter för att därigenom komma fram till ett ställningstagande och en rekommendation gällande hantering av en möjlig skada. Riskanalyser är därmed ett viktigt verktyg i arbetet med intern styrning och kontroll.

Riskanalys genomförs vanligen i samband med att förändringar sker eller planeras att ske för en verksamhet, systemlösning etc. Riskanalys bör även göras vid förändringar i den omgivande miljön sett till andra aktörer och händelser i omvärlden för att komma fram till om detta kan leda till en förändrad hotbild och därmed till förändrade risknivåer.

Den valda metoden för riskanalysen behöver kunna anpassas efter den aktuella situationen och framförallt verksamhetens betydelse, komplexitet och prioritet. Oavsett metodens utformning måste det dock säkerställas att riskanalysen genomförs på ett sätt som resulterar i att upprepade analyser och bedömningar genererar konsekventa, korrekta och jämförbara resultat. Detta innebär att metoden för riskanalys ska vara så stabil att samma resultat uppnås givet ingående parametrar och förutsättningar oavsett vilka personer som deltar i analysen.

Även i detta sammanhang är det viktigt att använda entydiga begrepp och tydliga beskrivningar, att analysera hot samt bedöma grad av skada och uppskattad sannolikhet för ett visst hot.

9.4 Viktiga förutsättningar för riskanalysarbetet

Vid riskanalys, precis som i många andra aspekter av en verksamhet, är det grundläggande att ha ledningens stöd, att ha tydligt utsedda roller med ansvarsområden samt att arbeta systematisk.

Ytterligare förutsättningar som är viktiga att ha på plats vid riskanalys beskrivs nedan.

9.4.1 Tydligt analysobjekt

Det sammanhang eller den situation där risker ska analyseras behöver vara tydligt sett till såväl omfattning som vilken tidsperiod som avses. Analysobjektet kan exempelvis avse en viss process, en upphandling, ett utvecklingsarbete eller mottaglighet för ett visst angrepp. Ju tydligare analysobjektet definieras desto mer underlättas riskanalysarbetet vilket i sin tur gör att beslutsunderlaget blir tydligt.

Det är även viktigt att den tidsperiod som analysen avser klart anges eftersom detta kan ha mycket stor inverkan på sannolikheten att en risk infaller. I normalfallet brukar ett verksamhetsår avses (aktuellt eller kommande) men även andra tidsperioder kan vara möjliga.

Utifrån ett tydligt beslutsunderlag underlättas beslut om riskacceptans och val av eventuella riskreducerande åtgärder. Att basera en riskanalys på tydligt inramade frågeställningar och förutsättningar, istället för en generell fråga av typen ”finns det några risker?”, medför en större chans att uppnå nödvändig tydlighet i det resulterande beslutsunderlaget.

9.4.2 Tydliga begrepp

Ett enhetligt synsätt på hur risker bedöms och behandlas är också en starkt bidragande faktor till att uppnå konsekventa, korrekta och jämförbara resultat. Med tydliga begrepp avses att alla som är berörda av riskanalysen och riskanalysens resultat ska förstå vad de begrepp som används betyder och hur de används (respektive inte ska användas). Tydligheten innebär att begrepp som används, såsom hothändelse, sannolikhet och skadekonsekvens behöver vara konkreta och ska kunna följas upp på ett objektivt sätt även av någon som inte aktivt deltagit i analysarbetet.

ATT TÄNKA PÅ FÖR ATT UPPNÅ TYDLIGHET

Behovet av tydlighet innebär att **nedanstående aktivt ska undvikas**:

- Undvik att enbart använda verbala subjektiva begrepp såsom allvarligt, betydande, lindrigt, där dessa inte konkretiseras på mätbara sätt.
- Undvik att använda själva begreppet som förklaring till begreppet (exempelvis genom att definiera "Allvarlig skada" med orden "En skada som är allvarlig").
- Undvik att använda begrepp i skalor som inte konkretiseras på ett utvärderingsbart sätt utan som bara beskriver en allmän storleksindelning (som exempelvis Låg, Medel, Hög eller 1,2,3).

Genom tydliga begrepp underlättas analys och kommunikation av såväl ingående faktorer som identifierade risker. Tydligheten innebär även att analysresultatet blir ett bra beslutsunderlag för beslut om riskacceptans och eventuella riskreducerande åtgärder.

9.4.3 Tydliga enheter och uppskattningar

Tydliga enheter och uppskattningar innebär att enheter behöver uttryckas i objektiva och mätbara mängder samt på ett transparent sätt. Genom att göra detta underlättas kommunikation och ständiga förbättringar av gjorda uppskattningar vilket i sin tur resulterar i bättre riskanalyser.

När det gäller att uttrycka mängder på ett tydligt sätt behöver strävan vara att ange dessa i form av realistiska intervall istället för enstaka värden. Genom att använda intervall uppnås två fördelar, dels förbättras möjligheterna att hamna rätt i bedömningen och dels blir intervallets omfattning en tydlig indikator på hur säker bedömningen är. Ju större osäkerhet desto större intervall. För att ytterligare öka kvaliteten och rimligheten i riskanalysen, och därmed i den formulerade risken, kan man även bedöma det mest troliga värdet inom den identifierade risken. Det mest troliga värdet behöver inte vara medelvärdet av intervallet!

För att öka användbarheten eftersträvas mängder som är lätta att förhålla sig till hos de som ska använda riskanalysens resultat, av denna anledning är ekonomiska värden och frekvenser att föredra framför subjektiva

värdeord såsom exempelvis ”inte obetydlig konsekvens” eller ”ofta”. Nära kopplat till att kunna mäta och uppskatta mängder är att använda en enhetlig tidshorisont. Vanligen används tidsintervallet ett år men även andra intervall kan användas, det viktigt är att aktuellt tidsintervall kommuniceras och förstås av de som ska använda riskanalysen.

Exempel på bedömningsgrunder/skalsteg

Sannolikhet	Konsekvens (skada)
0,02≤0,1 ggr/år (Mkt låg)	0≤100 tkr (Ingen-Ringa)
<0,1≤1 ggr/år (Låg)	>100≤1 000 tkr (Måttlig)
>1≤10 ggr/år (Måttlig)	>1 000 ≤ 10 000 tkr (Allvarlig)
>10≤100 ggr/år (Hög)	> 10 000 tkr ≤100 000 tkr (Mycket allvarlig)

TABELL 1 ▪ Genom att såväl sannolikhet som konsekvens anges med ”stängda” intervall ges varje skalsteg ett minvärde och ett maxvärde. Skalorna behöver anpassas för respektive organisation och vara gemensamma för hela organisationen. Ovanstående skalor används för exempel i detta kapitel och i bilagan.

Ytterligare en enhet som behöver lyftas fram pga sin betydelse för att uppnå god kvalitet på riskanalyser är konsekvens. Med konsekvens avses i detta sammanhang den skada i form av ekonomiska förluster som uppstår då en hothändelse realiseras. Det är inte rimligt att kunna göra en uttömmande uppskattning av den ekonomiska förlusten men genom att ha ett systematiskt sätt för att uttrycka förluster och uppskattningar underlättas såväl kommunikation som ständiga förbättringar. Denna vägledning rekommenderar att standarden FAIR[37] nyttjas för att beskriva de förluster som bedöms uppstå. Använd kategorierna som en checklista för att fånga upp relevanta förluster, det är inte nödvändigt att alla kategorier används i alla situationer.

37. Standarden FAIR tillhandahålls genom The Open Group. Standarden är gratis och är åtkomlig via https://www.opengroup.org/open-fair.

ATT TÄNKA PÅ NÄR DET GÄLLER TYDLIGA VÄRDEN OCH MÄNGDER VID RISKFORMULERING

En inte ovanlig (miss)uppfattning när det gäller riskformulering är att det är svårt att göra konkreta uppskattning av sannolikhet och konsekvens och att detta helt enkelt inte går att göra eftersom vi inte kan veta alla detaljer.

Ett intressant fenomen när det gäller att skapa tydliga risker är att det uppfattade initiala behovet av detaljer egentligen inte behöver vara så stort utan att det räcker med att "lite grovt" – men med eftertanke – göra bedömningarna i intervallform (innebär alltså inte att man ska skjuta från höften). Eftersom man förklarar vad bedömningarna baseras på och gör det transparent bjuder man automatiskt in andra personer till att bidra till ständiga förbättringar mot succesivt ökad tydlighet.

Om förbättringarna "i värsta fall" skulle utebli så är vi i alla fall tydliga gentemot beslutsfattaren om beslutsunderlagets aktuella "grovkornighet".

KATEGORIER AV SKADOR I FORM KOSTNADER ENLIGT STANDARDEN FAIR

Enligt standarden FAIR kan 6 kategorier av kostnader uppstå (i standarden benämnda "förluster"). Dessa kostnader delas även upp i två grupper – primära respektive sekundära – beroende på när och hur de uppstår relaterat till ett visst skeende (inträffad hothändelse). Primära kostnader uppstår och drabbar organisationen och dess primära intressenter direkt pga händelsen medan sekundära kostnader uppstår som en följd av de primära kostnaderna (genom att sekundära intressenter engagerar sig).

Dessa är:

1. **Produktivitet** (Productivity):
   - Definieras som kostnader som uppstår pga en operativ oförmåga att leverera produkter eller tjänster.
   - Utgör normalt en primär kostnad.
   - Innefattar exempelvis är uteblivna intäkter och förlorade lönekostnader.

2. **Hantering** (Response):
   - Definieras som kostnader som uppstår på grund av en händelses hantering.
   - Kan utgöra både primär och sekundär kostnad.
   - Primära kostnader innefattar exempelvis kostnad för incident-hanterings team, kostnad för forensik/utredning, kostnad för genomförda interna möten (ledningsmöten, samverkansmöten, intern och extern kommunikation etc).
   - Sekundära kostnader innefattar exempelvis kundkontakt, kundvård och kundstödjande åtgärder.
3. **Ersättning** (Replacement):
   - Definieras som kostnader som uppstår pga att en organisation måste ersätta eller reparera kapital- och/eller personaltillgångar.
   - Utgör normalt en primär kostnad.
   - Innefattar exempelvis ersättningsinvesteringar/-upphandling av ny tillgång, kostnader för nyanställning (jobbannonsering, intervjuer, utbildning plus förlorad produktivitet fram tills den nyanställde kommer igång).
4. **Konkurrensfördel** (Competitive Advantage):
   - Definieras som kostnader som uppstår pga att immateriell egendom eller andra viktiga konkurrensskillnader äventyras eller skadas.
   - Utgör normalt en sekundär kostnad.
   - Innefattar exempelvis förlorade affärshemligheter, information om sammanslagningar och uppköp, information marknadsplaner/strategier.
5. **Böter och sanktioner** (Fines and Judgements):
   - Definieras som kostnader som uppstår pga att böter eller sanktioner tas ut mot organisationen genom rättsliga eller avtalsmässiga åtgärder/processer.
   - Utgör normalt en sekundär kostnad.
   - Innefattar exempelvis sanktionsavgifter från myndigheter, civilrättsliga respektive affärsmässiga stämningar och böter.
6. **Förtroende** (Reputation):
   - Definieras som kostnader som uppstår pga att (ur ett externt intressentperspektiv) en organisations värde har minskat och/eller att dess ansvar har ökat.
   - Utgör normalt en sekundär kostnad.
   - Innefattar exempelvis reducerad marknadsandel, försämrad tillväxt, ökade kapitalkostnader, förtroendebyggande åtgärder, ökade rekryteringskostnader.

9.4.4 Tydliga och gemensamma bedömningsgrunder

Med bedömningsgrunder avses de olika kriterier, skalor och ”skalsteg” som olika avvägningar och bedömningar baseras på. Det är mycket viktigt att bedömningsgrunderna är anpassade till den egna organisationen och inte är en allmänt hållen generell konstruktion som exempelvis är hämtad efter lite snabbt sökande på internet. Använd skalor med tydliga och stängda intervall, dvs undvik skalsteg av typen ”mindre än” respektive ”mer än”. Det är även mycket viktigt att bedömningsgrunderna är accepterade och godkända av den ansvariga ledningen och tillämpas inom hela organisationen.

9.4.5 Riskvärde och riskacceptans

Riskvärde och riskacceptans tillhör ovan nämnda bedömningsgrunder men ges här ytterligare förtydliganden.

Riskvärde syftar till att vara ett stöd vid bedömning och behandling av risker sett till dessas allvarlighetsgrad och anges vanligen som ett numeriskt värde. Riskvärdets storlek för en viss risk är vanligen en funktion av riskens nivå på sannolikhet och riskens nivå på skadekonsekvens. Skalan för riskvärde kan variera hos olika organisationer och påverkas vanligen av de skalor som används för sannolikhet och konsekvens innebärande allt från 1–3 till 1–25. Det kan även konstateras att ju bättre en organisation blir på att uttrycka risker i form av ekonomiska skador desto mindre betydelse får begreppet riskvärde.

Några aspekter som är särskilt viktiga att tänka på när det gäller hur metoden för riskvärde utformas och används är:

- **Använd tydliga och konkreta intervall** för riskvärde där intervallens undre och övre gräns uttrycks i absoluta värden. Undvik att uttrycka intervallen i endast beskrivande ord eller genom att använda procentuella gränsdragningar (tex procent av budget) då detta inte ger jämförbara resultat.
- **Tillämpa en komplett tabell för riskvärden**. Metoden för att identifiera riskvärde behöver möjliggöra att alla skalsteg ska kunna användas. Att räkna ut riskvärdet genom att enbart multiplicera en viss nivå sannolikhet med en viss nivå för konsekvens är därför olämpligt eftersom vissa värden inte kommer att kunna användas. Istället bör en tabell eller koordinatsystem med samtliga riskvärden som funktion av olika nivåer för sannolikhets och konsekvens tillämpas.

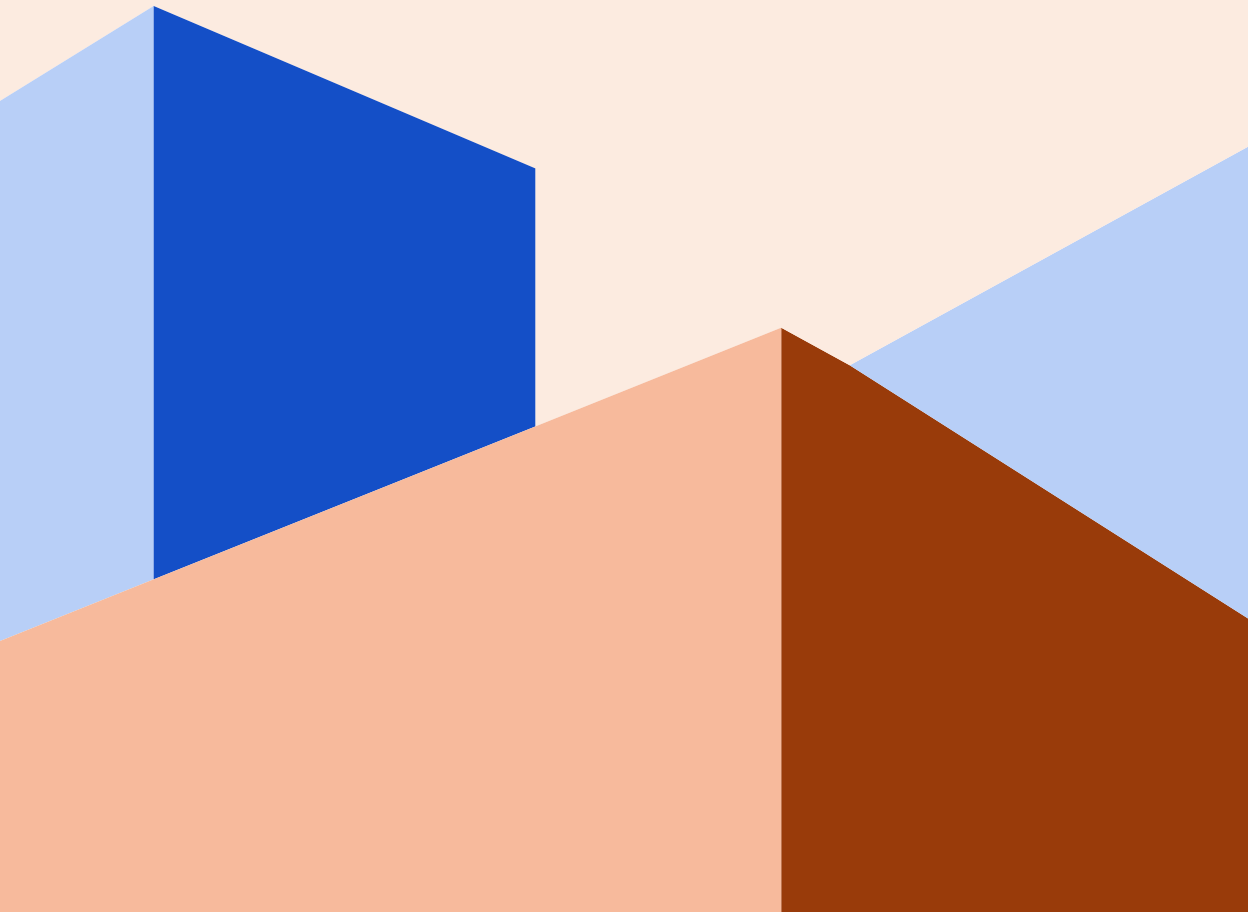
- **Reflektera över utfallet**. Vid såväl utformning som vid tillämpning av riskvärde för bedömning och behandling av risker behöver reflektion ske över vad det erhållna riskvärdet de facto innebär. Analysera till exempel vad den underliggande risken innebär och om detta motsvarar det erhållna riskvärdet. Beroende på de olika intervall och den detaljgrad som finns hos underliggande skalor (för främst sannolikhet och konsekvens) kan två risker med samma riskvärde visa sig ha sinsemellan mycket stor variation.

Riskacceptans är begreppet som utrycker vilka risker som en organisation kan acceptera och vilka risker som ej accepteras och därför behöver behandlas. I syfte att utgöra ett beslutsstöd är en vanlig metod att använda en tabell där olika former av riskacceptans kopplas till olika nivåer av riskvärde.

Några aspekter som är särskilt viktiga att tänka på när det gäller utformning och användning av en sådan tabell för riskacceptans är:

- Inkludera all nödvändig information. För ej acceptabla risker som kräver åtgärder behöver tabellen för att besluta om riskacceptans omfatta såväl det bedömda riskvärdet innan behandling som det målsatta riskvärdet efter behandlingen.
- Förankra riskacceptansen inom organisationen. Speglar den valda tabellen för riskacceptans organisationens verkliga riskaptit? När det gäller att bedöma vilka risker som är acceptabla eller ej lägger organisationer och verksamheter vanligen olika vikt på sannolikheten att en hothändelse inträffar jämfört med de skadekonsekvenser som bedöms uppstå. För att spegla riskaptiten på ett korrekt sätt behöver därför metoden för riskacceptans tillåtas vara asymmetrisk genom att exempelvis lägga större vikt på konsekvens än på sannolikhet.
- Använd normerande slutsatser istället för rekommendationer. Beskrivning av åtgärder som kopplas till olika riskvärden behöver beskrivas i bestämd form genom att använda ord såsom ”ska” och ”måste” istället för ord så som ”bör” och ”kan”.

10



Tillämpning av det systematiska riskanalysarbetet

I detta kapitel beskrivs de centrala aspekterna när det gäller att tillämpa ett systematiskt riskanalysarbete på ett effektivt och långsiktigt hållbart sätt. Varje aspekt beskrivs med vägledande instruktioner och rådgivning.

10.1 Utformning av riskanalysarbetet

Det är ledningens ansvar att all riskhantering utformas på lämpligt sätt för att uppfylla de syften och mål med riskanalysarbetet som omnämns i kapitel 9 ovan.

På en övergripande nivå är det även ledningens ansvar att se till att riskanalysarbetet ges förutsättningar att kunna bedrivas och producera lämpliga underlag som stöd för det riskbaserade angreppsättet. Vid utformningen riskanalysarbetet behöver hänsyn tas till bland annat verksamhetens förutsättningar, befintliga lednings- och organisationsstrukturer, roller och ansvar, processer, informationssystem och informationsflöden.

På mer verksamhetsnära nivå kan de funktioner och de roller som de facto deltar i riskanalysarbetet variera med hänsyn taget till det aktuella analysobjektet. Normalt är dock nedanstående roller de centrala:

- **Riskägare:** Med riskägare avses i detta fall den roll som har tillräckligt mandat för att besluta om en risk är acceptabel eller ej samt har mandat att prioritera resurser för riskens hantering. I en processorienterad verksamhet tilldelas denna roll vanligen respektive processägare, i en förvaltningsorienterad verksamhet tilldelas denna roll vanligen respektive förvaltningsansvarig och i andra fall kan riskägare vara en chef som är tillräckligt högt upp i organisationen för att ha dessa nödvändiga mandat.

- **Informationsägare:** Med informationsägare avses i detta fall den roll som ansvarar för att en viss informationstillgång värderas till rätt värde. Informationsägaren ansvarar även för att andra roller i verksamheten som behandlar informationstillgången behandlas på det sätt som motsvarar informationens värde.
- **Systemägare:** Med systemägare avses i detta fall den roll som ansvarar för ett it-system eller annan teknisk behandlingslösning och som har mandat att påverka lösningens utformning sett till bland annat teknisk utformning och säkerhetsåtgärder.
- **Ämnesexperter:** Med ämnesexperter avses roller som har god insikt i såväl analysobjektets funktion, dagliga arbete samt insikt och förståelse för verksamhetsmässiga förutsättningar och konsekvenser vid avvikelser och störningar. Detta kan exempelvis avse expertis från drift, ekonomi, marknadsföring, kommunikation och HR.

Vid utformning av riskanalysarbetet är det också viktigt med en skalbar metodik anpassad till den egna organisationen. Metodiken ska säkerställa att rätt underlag samlas in så att riskanalysen och dess resultat blir konsekventa, korrekta och jämförbara. Metodiken behöver även omfatta kontinuerlig granskning och utvärdering för att säkerställa dess funktion och därmed undvika felaktiga resultat.

10.2 Hot och hothändelser

Kärnan i att kunna formulera tydliga och relevanta risker är att ha identifierat de hot och de hothändelser som är troliga och rimliga sett till analysobjektet. Detta nämndes övergripande i relation till säkerhetskydd i kapitel 3.2 ovan.

Hothändelser uppstår som ett resultat av att någon (en aktör) medvetet eller omedvetet agerar på ett visst oönskat sätt. Det är med andra ord inte bara oönskade händelser i form av angrepp som behöver identifieras utan även de oönskade händelser som uppstår på grund av ett omedvetet ”felaktigt” eller ”olyckligt” agerande. De faktorer som bidrar till, eller möjliggör agerandet benämns som sårbarheter eller brister och kan exempelvis utgöras av bristfälliga arbetsrutiner, avsaknad av kompetens eller ineffektiva skyddsåtgärder.

Att identifiera och bedöma hothändelser är en viktig del i det systematiska arbetet med hotunderrättelser (eng. threat intelligence) som organisationer och verksamheter bör utföra för att skapa medvetenhet om organisationens hotmiljö så att lämpliga avhjälpande åtgärder kan vidtas.

Ett sätt för att underlätta arbetet med att identifiera och kommunicera hothändelser är att dessa händelser uttrycks i form av ett påstående såsom ”aktör X utför oönskad händelse Y”. För att en oönskad händelse ska anses vara en hothändelse så ska den innebära negativa följder för verksamheten/analysobjektet på grund av försämrad eller förlorad; konfidentialitet, riktighet och tillgänglighet hos i första hand informationstillgångar och i andra hand andra relaterade tillgångar.

Börja arbetet med att identifiera hothändelser genom att först identifiera oönskade händelser. Här är det lämpligt att kontakta den roll som är ansvarig för det aktuella analysobjektet eller de roller som har god inblick i analysobjektet för att utifrån deras erfarenheter och kunskaper påbörja kartläggning av oönskade händelser. För kartläggningen är det viktigt att välja ett samtalsformat som underlättar dialog och reflektioner för att på så sätt lättare kunna fånga upp eventuella sidospår och erfarenheter som kan visa sig vara värdefulla informationskällor antingen det gäller redan identifierade oönskade händelser, hothändelser eller indikatorer på nya händelser.

Under kartläggningen läggs fokus på att identifiera oönskade händelser, den aktör som direkt eller indirekt utför händelsen, de sårbarheter som underlättar eller möjliggör den oönskade händelsen samt den effekt som uppstår som resultat av händelsen.

→ METODIK FÖR ATT KARTLÄGGA OÖNSKADE HÄNDELSER (SOM GRUND FÖR HOTHÄNDELSER)

Exempel på några frågeställningar som kan användas som stöd för i arbetet att kartlägga oönskade händelser för att därigenom kunna identifiera hothändelser. Frågorna i sig är inte uttömmande utan bör ses mer som utgångspunkter för fördjupande frågeställningar.

1. Frågeställningar för att bedöma förekomst av troliga **oönskade händelser** inom den aktuella processen eller det scenario som ska analyseras:
   - Har oönskade händelser inträffat tidigare och om så – kan de bedömas inträffa igen?
   - Finns troliga oönskade händelser som ännu inte inträffat i verksamheten?

2. Frågeställningar för att bedöma **aktörer** för de oönskade händelserna enligt ovan:
   - Vilka aktörer är troligast i förhållande till verksamheten – interna eller externa aktörer?
   - Vilka aktörer har direkt respektive indirekt koppling till aktuell verksamhet och riskscenario?
3. Frågeställningar för att bedöma aktörens **intention** med sitt agerande:
   - Kan aktören gynnas av ett medvetet agerande?
   - Kan aktören anses agera omedvetet på grund av någon form av brist eller sårbarhet.
4. Frågeställningar för att bedöma förekomst av eventuella **sårbarheter och brister** som möjliggör eller underlättar för den oönskade händelsen att inträffa:
   - Vanligen hittas dessa sårbarheter och brister när en oönskad händelse har identifierats och som svar på frågan "på grund av vad kan denna oönskade händelse inträffa?"
   - Finns information om tidigare incidenter och störningar kopplat till analysobjektet eller till analysobjektets omgivning. Detta kan gälla incidenter och störningar som inträffat inom den egna verksamheten likväl som hos andra verksamheter.

Denna kartläggning av hot och hothändelser behöver dokumenteras. Minst följande punkter behöver dokumenteras för respektive identifierad hothändelse:

- ➔ Aktuellt analysobjekt
- ➔ Agerande/skeende
- ➔ Aktör
- ➔ Aktörens intention
- ➔ Sårbarheter
- ➔ Drabbad tillgång/effekt/skada

Ovanstående information dokumenteras lämpligen i en tabellform för att därigenom utgöra början till en hotförteckning. Hotförteckningar kan med fördel ligga till grund för erfarenhetsutbyte inom och mellan olika analysobjekt eller organisationer kopplat till att succesivt kunna förbättra hotbedömning och hotunderrättelser inom såväl egna verksamheten som i närliggande verksamheter.

Förutom själva agerandet och aktören är de identifierade sårbarheterna (eller bristerna) viktiga att dokumentera och gärna detaljera i detta steg. Motivet till detta är att det vanligen är åtgärdande av sårbarheter som bidrar till riskreducering och genom att ha dokumenterat underliggande resonemang och eventuella exempel så underlättas detta arbete.

De oönskade händelser som bedöms leda till negativa följder för verksamheten och dess analysobjekt på grund av försämrad konfidentialitet, riktighet och tillgänglighet tas vidare i riskanalysarbetet i form av en hothändelse. Hothändelsen byggs upp genom att ange aktuell aktör, dennes intention samt aktuellt agerande (dvs den oönskade händelsen)

→ SKILLNAD MELLAN OÖNSKAD HÄNDELSE OCH HOTHÄNDELSE

Kärnan i riskformulering är att identifiera ett negativt skeende samt hur ofta detta sker och med vilka skadliga konsekvenser. I detta kommer såväl "oönskade händelser" som "hothändelser" att behöva beaktas fast ur olika aspekter. Det är viktigt att förstå skillnaden mellan dessa händelser och hur de spelar in vid formulerande av risk. Nedanstående beskrivs ett scenario i syfte att förtydliga skillnaden.

Scenario: Tillträdesskydd
En dörr till ett maskinrum lämnas olåst trots att dörren, enligt gällande bestämmelser, alltid ska vara låst för att förhindra personskada, stöld och sabotage. Att dörren lämnas olåst sker ofta, minst en gång per dag under året.

Är detta en oönskad händelse?
Ja, att lämna dörren olåst måste ses som en oönskad händelse som bryter mot bestämmelserna och KAN leda till skador, kostnader och förluster. Denna händelse dokumenteras i analysprocessen och om möjligt identifieras bakomliggande orsaker till denna händelse (dvs sårbarheter).

Är detta en hothändelse?
Nej, inte uppenbart. Den olåsta dörren innebär ju inte med automatik att något negativt de facto inträffar alla gånger som dörren lämnas olåst. Det är heller inte känt vilken aktör som kan utnyttja detta och i vilket syfte.

Kan händelsen komma att utgöra grund för en hothändelse?
Ja, i analysen görs bedömningen att negativa effekter inträffar en gång var annan månad som följd av den olåsta dörren. I analysen identifieras kriminella som den aktör som troligen kan utnyttja den olåsta dörren i syfte att stjäla verktyg eller att sabotera motordelar. Dessa konsekvenser kan därefter kostnadsbedömas sett till de skador som bedöms uppstå. Bakomliggande information för detta kan hämtas från källor inom egna organisationen, från andra organisationer såsom försäkringsbolag eller från trender i omvärlden.

Blir det en risk?
Ja, detta blir en risk. Dock används inte den ursprungliga oönskade händelsen (med dess höga sannolikhet och otydliga konsekvenser) utan det är den identifierade hothändelsen (med betydligt lägre sannolikhet och tydliga konsekvenser) som utgör grunden till risken. Skillnaden blir än tydligare om vi lägger in respektive typ av händelse i riskformeln: "Risk för att [Hothändelse]. På årsbasis bedöms risken inträffa [Sannolikhet] med en total skadeverkan motsvarande [Skadekonsekvens]"

- ➔ Med oönskad händelse som grund: "Risk för att dörren lämnas olåst. På årsbasis bedöms risken inträffa 365 gånger med en total skadeverkan på personskada, stöld eller sabotage"
- ➔ Med hothändelse som grund: "Risken är att kriminella kommer in i maskinrummet och stjäl eller saboterar motordelar. På årsbasis bedöms risken inträffa 6 ggr/år med en total skadeverkan på 50–150 tKr"

Vilken av ovanstående riskformuleringar som utgör bäst beslutsunderlag kan kännas uppenbart.

Nedanstående figur exemplifierar några hothändelser i ett fiktivt fall gällande hot och riskbedömning inom luftbehandling. Hothändelserna har i sin tur identifierats genom att oönskade händelser först har kartlagts och därefter analyserats. På efterföljande sidor byggs detta fiktiva fall på för att till slut sammanfattas i en riskförteckning.

Exempel på bedömningsgrunder/skalsteg

Hothändelse ID	Hotkategori	Hothändelse (aktör+ ev intention+agerande)
H-001	Hanteringsfel	Tekniker anger felaktiga styrvärden för ventilation
H-002	Angrepp	Tekniker medvetet anger felaktiga styrvärden för ventilation
H-003	Angrepp	Ransomware gör att styrning av ventilation inte är möjlig
H-004	Tekniskt fel	Sensordata för luftkvalitet kommer inte fram till styrsystemet

TABELL 2 ▪ Förklaring: Fyra hothändelser har identifierats för analysobjektet Luftbehandling. För att underlätta spårbarhet ges varje hothändelse ett ID. För senare sammanställningar och statistik kategoriseras varje hothändelse. Denna hotbedömning görs genom att följa metodiken för att kartlägga oönskade händelser. Resultatet blir en hotförteckning som succesivt kan byggas på och förvaltas.

10.3 Riskbedömning

Riskbedömning omfattar att identifiera, formulera samt bedöma om en risk är acceptabel eller inte.

En tydligt formulerad risk omfattar en hothändelse i kombination med den bedömda sannolikheten för att hothändelsen ska inträffa samt den bedömda skadan som hothändelsen orsakar. För att lättare uppnå den önskade tydligheten rekommenderas att använda den formel för riskformulering som beskrevs i början av detta avsnitt där utgångspunkten är de hothändelser som kartlagts och dokumenterats i organisationens hotförteckning. Som en repetition återfinns den nedan.

”Risk för att [Hothändelse]. På årsbasis bedöms risken inträffa [Sannolikhet] med en total skadeverkan motsvarande [Skadekonsekvens]”

Att bedöma hothändelsers sannolikhet och konsekvenser (för att utifrån detta kunna identifiera risker) kan göras på olika sätt. I nedanstående exempel bedöms sannolikheterna för alla hothändelser i ett första steg och därefter bedöms konsekvenserna för alla hothändelser, det finns inget som hindrar omvänd ordning alternativt att identifiera sannolikhet och konsekvens per hothändelse.

10.3.1 Bedöm sannolikhet

Sannolikheten för att hothändelser inträffar inom den aktuella analystiden (vanligen årsbasis) bedöms i två delsteg. Först bedöms det rimliga intervallet för sannolikhet (valbara rimliga intervall ska återfinnas bland bedömningskriterierna och gälla för hela organisationen), sedan när ett rimligt intervall har identifierats görs en precisering inom intervallet av det mest troliga värdet. Det är viktigt att bedömningarna baseras på befintlig kunskap såsom erfarenhet, ämneskunskap och omvärldsbevakning samt att underliggande motiveringar av sannolikheten dokumenteras.

Nedanstående figur exemplifierar det fortsatta arbetet med det fiktiva fallet gällande hot och riskbedömning inom luftbehandling. I detta steg bedöms hur ofta respektive identifierad hothändelse inträffar. Genom att, med eftertanke, först identifiera ett rimligt intervall och därefter, med samma eftertanke, identifiera det mest troliga utfallet så läggs grunden för att kunna använda olika former av trepunkts-estimat. Trepunkts-estimat är en etablerad metod för att öka kvaliteten i bedömningar. Genom att beskriva bakgrunden till gjorda bedömningar så skapas en transparens och därmed läggs grunden för att, i dialog, kunna förbättra gjorda bedömningar. För att ytterligare öka kvaliteten vid trepunkts-estimat kan intervallens storlek behöva anpassas till rimliga värden.

Exempel på bedömning av sannolikhet för hothändelser inom analysobjektet Luftbehandling

Hothändelse ID	Hothändelse (aktör+ ev intention+agerande)	Sannolikhet intervall (drop-down)	Mest troligt sannolikhet (ggr per år)	Motivering sannolikhet
H-001	Tekniker anger felaktiga styrvärden för ventilation	>1 & ≤10 ggr per år (Måttlig)	2	Bedömning görs sett till tidigare historik från incidenter och störningar. Bedömningen är relativt säker.
H-002	Tekniker medvetet anger felaktiga styrvärden för ventilation.	<0,1 & ≤1 ggr/år (Låg)	0,3	Bedömning görs sett till stor andel leverantörer och tidigare händelser i omvärlden. Bedömningen är relativt osäker.
H-003	Ransomware gör att styrning av ventilation inte är möjlig	<0,1 & ≤1 ggr/år (Låg)	0,4	Bedömningen görs sett till tidigare händelser i branschen och i omvärlden. Bedömningen är relativt osäker.
H-004	Sensordata för luftkvalitet kommer inte fram till styrsystemet	>1 & ≤10 ggr/år (Låg)	6	Bedömningen görs sett till tidigare historik från incidenter och störningar. Bedömningen är relativt säker.

TABELL 3 ▪ Hothändelserna från föregående figur har här försetts med sannolikhetsbedömningar vilka dessutom motiveras/beskrivs.

10.3.2 Bedöm konsekvens (skada)

Metoden för att bedöma konsekvens pga inträffade hothändelser följer samma tillvägagångssätt som för sannolikhet, dvs först identifieras ett rimligt intervall och därefter bedöms det mest troliga värdet inom detta intervall. Observera att bedömningen ska avse respektive skadetillfälle. För ge en så god bedömning av skador som möjligt kan med fördel skadekategorierna i standarden FAIR nyttjas. På samma sätt som vid bedömning av sannolikhet är det viktigt att bedömningar av skadekonsekvens baseras på befintlig kunskap, erfarenhet, ämneskunskap och omvärldsbevakning samt att underliggande motiveringar av skadekonsekvens dokumenteras.

Nedanstående figur exemplifierar det fortsatta arbetet med det fiktiva fallet gällande hot och riskbedömning inom luftbehandling. I detta steg bedöms hur vilken skada i form av kostnad som uppstår när respektive identifierad hothändelse inträffar. Arbetet följer samma mönster som föregående steg när det gäller att identifiera intervall respektive det mest troliga utfallet. På samma sätt som för bedömda sannolikheter beskrivs bakgrunden till gjorda bedömningar för att skapas transparens och kunna förbättra gjorda bedömningar.

Exempel på bedömning av konsekvens/skada för hothändelser inom analysobjektet Luftbehandling

Hot-händelse ID	Hothändelse (aktör + ev intention + agerande)	Konsekvensnivå intervall (drop-down)	Mest trolig konse-kvens (tkr)	Motivering konsekvens
H-001	Tekniker anger felaktiga styrvärden för ventilation	>100≤1 000 tkr (Låg)	800	Bedömning baseras på kostnader orsakade av omarbeten, återställningsarbete respektive avbrott i verksamheten. **Bedömning:** Hanteringskostnad 800 tkr.
H-002	Tekniker medvetet anger felaktiga styrvärden för ventilation	>5 000≤20 000 tkr (Allvarlig)	7 000	Bedömning baseras på kostnader orsakade av sanktionsavgifter, omarbeten, återställningsarbete, stilleståndsersättning respektive avbrott i verksamheten. **Bedömning:** Produktivitetskostnad 2 500 tkr, hanteringskostnad 1 000 tkr, böter & sanktioner 3 500 tkr.
H-003	Ransomware gör att styrning av ventilation inte är möjlig	>5 000≤20 000 tkr (Allvarlig)	12 000	Bedömning baseras på kostnader orsakade av sanktionsavgifter, omarbeten, återställningsarbete, inköp, stilleståndsersättning respektive avbrott i verksamheten. **Bedömning:** Produktivitetskostnad 2 500 tkr, hanteringskostnad 4 000 tkr, ersättningskostnad 2 000 tkr, böter & sanktioner 3 500 tkr.
H-004	Sensordata för luftkvalitet kommer inte fram till styrsystemet	>1 000≤5 000 tkr (Måttlig)	2 000	Bedömning baseras på kostnader orsakade av omarbeten respektive återställningsarbete. **Bedömning:** Hanteringskostnad 2 000 tkr.

TABELL 4 ▪ Hothändelserna från föregående figur har här försetts med sannolikhetsbedömningar vilka dessutom motiveras/beskrivs.

10.3.3 Formulera risker

Identifiering och formulering av en risk sker genom att ersätta begreppen inom hakparentes med konkreta och mätbara värden, vilka erhålls som resultaten från bedömning av sannolikhet respektive konsekvens. Nedanstående arbetsgång rekommenderas för detta ändamål där utgångspunkten är den generella riskformuleringen *"Risk för att [Hothändelse]. På årsbasis bedöms risken inträffa [Sannolikhet] med en total skadeverkan motsvarande [Skadekonsekvens]"*:

1. **Ersätt** [Hothändelse] **med faktisk hothändelse** från hotförteckningen.
2. **Ersätt** [Sannolikhet] **med det mest troliga antal tillfällen** på årsbasis,
3. **Ersätt [Skadekonsekvens] med det totala skadebeloppet** uttryckt i ekonomiska termer. Det totala skadebeloppet erhålls genom att multiplicera värdet för mest trolig sannolikhet med värdet för mest trolig konsekvens/skada.

Genom att följa stegen 1–3 tas en riskformulering fram på ett systematiskt och tydligt sätt. Genom att underliggande resonemang och motiveringar dokumenteras blir grunderna för den aktuella riskformuleringen transparenta vilket i sin tur underlättar dialoger och kontinuerliga förbättringar.

Nedanstående figur exemplifierar det avslutande arbetet med det fiktiva fallet gällande hot och riskbedömning inom luftbehandling. I detta steg skapas riskformuleringar som sedan blir underlag för riskbeslut och prioriteringar.

Exempel formulering av risker inom analysobjektet Luftbehandling

Risk ID	Hothän-delse ID	Hothändelse (aktör+ ev intention+agerande)	Mest troligt sannolikhet (ggr per år)	Mest trolig konse-kvens (tkr)	Riskformulering
R-001	H-001	Tekniker anger felaktiga styrvärden för ventilation	2	800	Risk för att tekniker anger felaktiga styrvärden för ventilation. På årsbasis bedöms risken inträffa 2 ggr med total skadeverkan motsvarande 1 600 tkr.
R-002	H-002	Tekniker medvetet anger felaktiga styrvärden för ventilation.	0,3	7 000	Risk för att tekniker medvetet anger felaktiga styrvärden för ventilation. På årsbasis bedöms risken inträffa 0,3 ggr med total skadeverkan motsvarande 2 100 tkr.
R-003	H-003	Ransomware gör att styrning av ventilation inte är möjlig	0,4	12 000	Risk för att ransomware gör att styrning av ventilation inte är möjlig. På årsbasis bedöms risken inträffa 0,4 ggr med total skadeverkan motsvarande 4 800 tkr.
R-004	H-004	Sensordata för luftkvalitet kommer inte fram till styr-systemet	6	2 000	Risk för att sensordata för luftkvalitet kommer inte fram till styrsystemet. På årsbasis bedöms risken inträffa 6 ggr med total skadeverkan motsvarande 120 000 tkr.

TABELL 5 ▪ Hothändelserna från föregående figur har här försetts med sannolikhetsbedömningar vilka dessutom motiveras/beskrivs.

Om det finns ytterligare behov av att kunna sortera och filtrera riskformuleringar kan det vara lämpligt att förse dessa med ett riskvärde. Riskvärdet kan ge ett visst stöd under riskbedömningen men här är rimligen riskens totala skadeverkan till mer nytta när det gäller bedömning av en risk. Respektive risk behöver tilldelas en riskägare som kan fatta riskacceptansbeslut, dvs huruvida den aktuella risken anses vara acceptabel eller inte. Det är riskägaren som godkänner framtagna riskhanteringsplaner för de risker som inte är acceptabla och som anger vilket riskvärde som är acceptabelt.

→ VIKTIGT GÄLLANDE FORMULERADE RISKERS BEDÖMDA SANNOLIKHET OCH SKADEKONSEKVENS!

Vid bedömning är det viktigt att komma ihåg att de **angivna värdena i riskformuleringen representerar intervall** av kombinationen sannolikhet och skadekonsekvens för en viss hothändelse, de angivna värdena ska därför inte betraktas som en "absolut" sanning.

I ett fortsatt arbete bör såväl intervallen som de mest troliga värdena förfinas – här finns dessutom etablerade metoder och verktyg att ta hjälp av.

På samma sätt som för hotförteckningar kan riskförteckningar ligga till grund för erfarenhetsutbyte inom och mellan olika analysobjekt och organisationer. Förutom att dokumentera riskformuleringen med den aktuella hothändelsen och den totala skadeverkan, riskvärdet och riskägaren är det mycket viktigt att även dokumentera och gärna detaljera de underliggande resonemang och eventuella exempel som framkommit under arbetet med riskformuleringen.

10.4 Riskbehandling

Riskbehandling innebär att välja lämpliga alternativ för de risker som bedöms vara oacceptabla sett till bedömda skadekonsekvenser och förluster. Huvudalternativen vid riskbehandling är att acceptera, undvika, reducera eller transferera risken.

I denna vägledning beskrivs riskbehandling genom att reducera risken. Reducering sker genom att identifiera och föreslå lämpliga och proportionerliga säkerhetsåtgärder. Med åtgärder som är "lämpliga och proportionerliga" avses att åtgärdernas kostnader och omfattning ska vara i balans med den skada som ska reduceras.

Åtgärdernas implementation beskrivs i en riskbehandlingsplan som ska godkännas av den aktuella riskägaren. Riskbehandlingsplanen ska även beskriva de risker som bedöms kvarstå när åtgärderna väl har implementerats. Val av säkerhetsåtgärder behöver ske med omsorg och sett till den riskreducerande effekt som ska uppnås, här är det väsentligt att den efterfrågade effekten anges tydligt vilket lämpligen görs genom konkreta säkerhetsmål i form av hur mycket skadekonsekvensen ska reduceras eller vilket riskvärde som ska uppnås.

I vissa fall kan det även vara nödvändigt att kombinera flera säkerhetsåtgärder för att uppnå den eftersträvade riskreduceringen samtidigt som det då även behöver säkerställas att de olika åtgärderna kan samverkan, dvs är kompatibla med varandra, för att uppnå den önskade funktionen. I andra fall kan man förlita sig på den omgivande miljön och de säkerhetsåtgärder som finns naturligt i den omgivande miljön, som exempelvis fysiska eller personella skyddsegenskaper.

Notera! Ju tydligare säkerhetsmålen uttrycks desto mer underlättas arbetet med att kunna visa sambandet mellan de säkerhetsåtgärder som väljs och hur dessa bedöms kunna reducera den aktuella risken. Det motsatta (som ska undvikas) är att dåliga val av säkerhetsåtgärder leder till ineffektiva åtgärder och/eller ej ändamålsenliga och därmed olämpligt dyra lösningar.

Ansvaret för att behandling av aktuella risker sker genom lämpliga åtgärder åligger riskägaren även om förvaltningen av valda åtgärder vanligen delegeras.

Nedan ges en övergripande beskrivning av tillvägagångssättet vid riskhantering genom riskreducering:

1. **Säkerställ att den aktuella riskformuleringen är korrekt och relevant**
2. **Identifiera och beskriv de säkerhetsåtgärder som är möjliga** att använda vid riskreducering. Det kan gälla redan befintliga säkerhetsåtgärder eller åtgärder som kan tillföras.
3. **Identifiera och beskriv de säkerhetsåtgärder som är lämpliga** och proportionerliga för att uppnå beslutad acceptabel risknivå för den risk som ska reduceras. Notera skillnaden mellan att en åtgärd är möjlig kontra att den är lämplig, för att vara lämplig ska:
   - Kostnaden för åtgärden vara proportionerlig med värdet hos det som ska skyddas.
   - Det ska vara möjligt att resonera sig fram till på vilket sätt åtgärden bidrar till riskreducering. Som stöd för att verifiera detta är det lämpligt att gå tillbaka och analysera de sårbarheter och brister som dokumenterades i samband med kartläggningen av den underliggande hothändelsen. Givet att sårbarheterna och bristerna har beskrivits på ett tydligt sätt underlättas denna verifiering avsevärt genom att den effekt som ska uppnås framgår tydligare.
4. **Dokumentera respektive lämplig säkerhetsåtgärd** genom att ange:
   - Allmän information om åtgärden såsom åtgärdens benämning, omfattning, eventuella avgränsningar, förslag på åtgärdsansvarig.
   - Åtgärdens förmåga att reducera riskens sannolikhet och/eller dess skadekonsekvens.
   - Bedömd kostnad för anskaffning respektive förvaltning av åtgärden.
   - Tidsförhållanden, planer och uppföljning av åtgärden.

Den identifierade åtgärderna för respektive risk sammanställs sett till aggregerade effekter, kostnader och tidsförhållanden; och presenteras därefter för riskägaren för prioritering och beslut.

Notera! Val av säkerhetsåtgärder bör inte ske mekaniskt utan ske genom att analysera och bedöma vilka säkerhetsåtgärder som ger den bästa effekten.

En riskhanteringsplan skapas sedan utifrån samtliga erhållna prioriteringar och beslut. Planen i sig ska godkännas av respektive riskägare

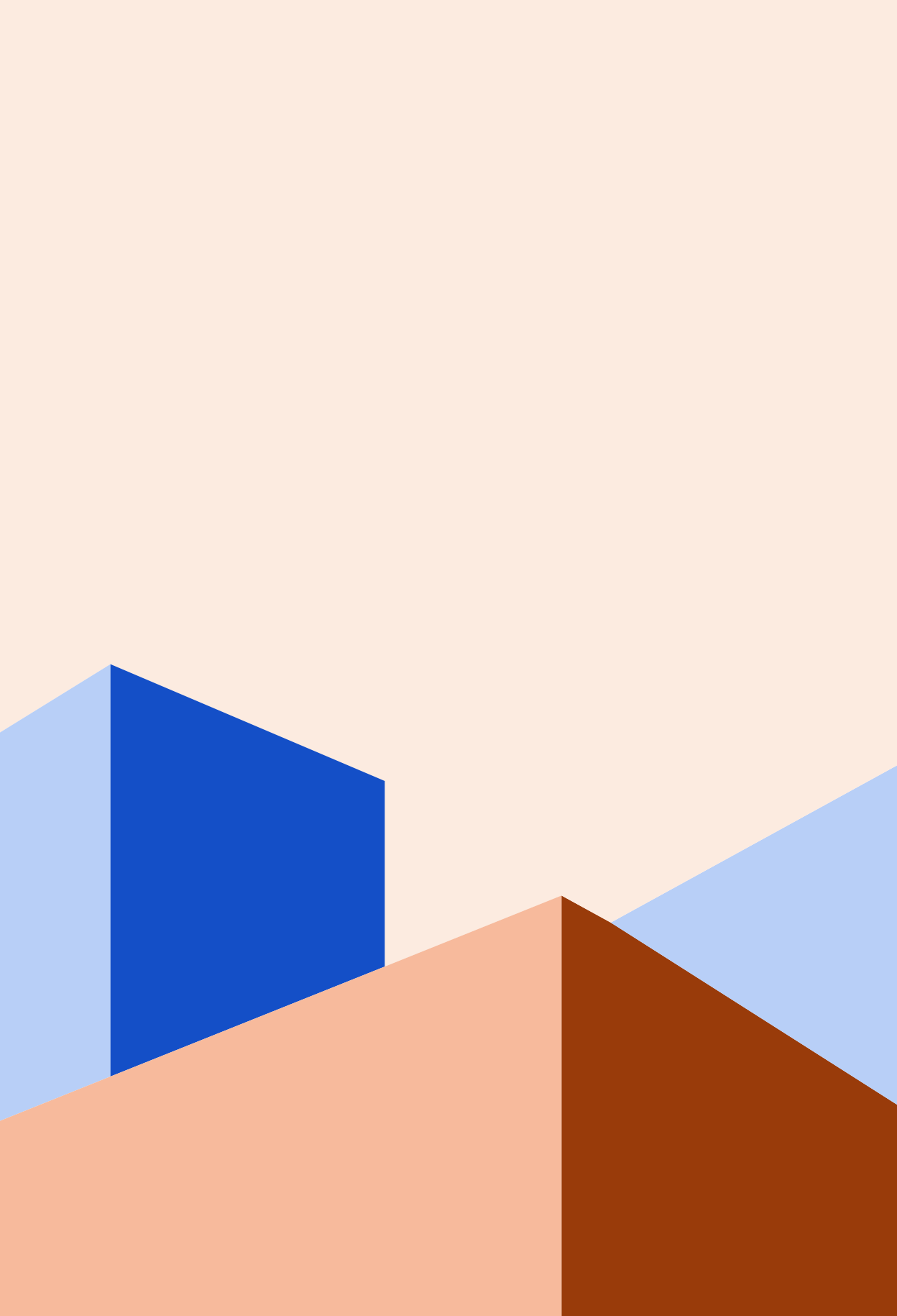
10.5 Riskuppföljning

Riskuppföljning innebär att succesivt och systematiskt utvärdera de beslutade säkerhetsåtgärderna sett dels till åtgärdernas införande och dels till åtgärdernas effektivitet när det kommer till riskreducering.

Respektive riskägare ansvarar för att behandlade risker följs upp.

Följande åtgärder utförs under riskuppföljningen för varje risk som är under behandling:

1. Följ upp att planerade säkerhetsåtgärder är implementerade enligt riskhanteringsplanen.
2. Följ upp att implementerade säkerhetsåtgärder är effektiva i enlighet med riskhanteringsbeslutet.
3. Utvärdera effekten av de implementerade åtgärderna och säkerställ att kvarvarande risker ligger inom det intervall som framgår av riskhanteringsplanen och fattat beslut.



Epilog

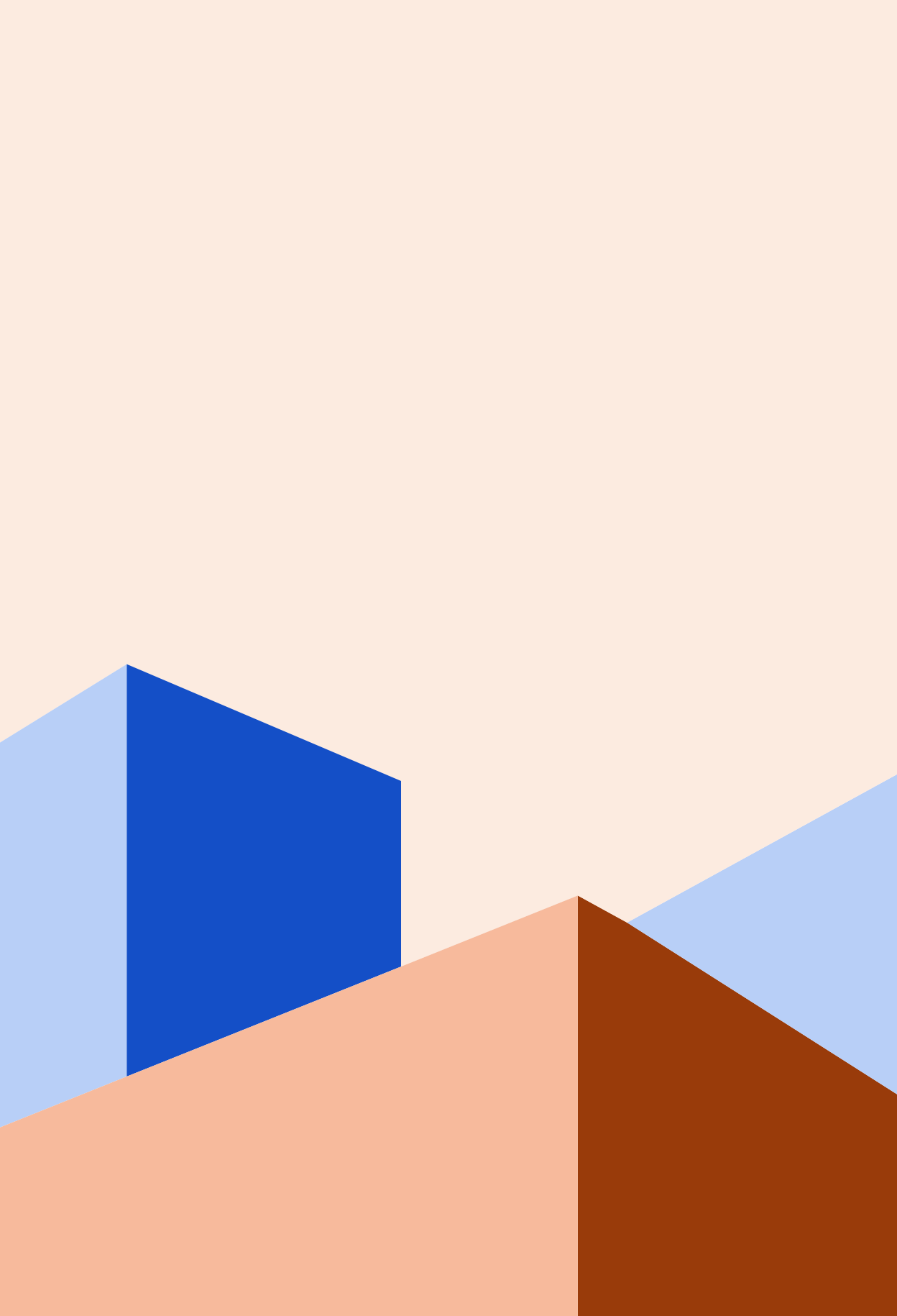
Sammanfattningsvis är vägen framåt tydlig. Rekommendationer, lagar, föreskrifter och ramverk pekar åt samma håll. Ett effektivt ledningssystem för informationssäkerhet som är hållbart över tid tar hänsyn till rådande och kommande regelverk, har sin grund i riskhantering och är enbart effektivt om det har en inbyggd systematik som fungerar för verksamheten och efterlevs. Med ett fokus på eftertanke om vad det är man vill uppnå, planering om hur detta ska ske och uppföljning av ifall detta inträffade så har man samtliga hörnstenar på plats. Som en summering lämnas läsaren med följande slutord och uppmaningar:

- ➔ Skaffa er en överskådlig men tillräcklig inblick i vad rådande och kommande regelverk innebär.
- ➔ Underskatta inte den noggrannhet och arbetsinsats som krävs vid hantering av säkerhetsskyddsrelaterade frågor.
- ➔ En betydande del av regulatoriska krav på informationssäkerhet hanteras via ett systematiskt riskbaserat arbetssätt.
- ➔ Noggrannhet och eftertanke i allt från modeller, indata, definitioner till metodik är nödvändigt för att säkerställa att man får ut det värde man vill ha ur riskhanteringsarbetet.

Framöver behöver arbetet inom dessa områden fortsätta, förhoppningsvis på det systematiska sätt som rekommenderas. Detta dokument lämnar läsaren med en grundläggande förståelse för regelverken säkerhetsskyddslagen, NIS/NIS 2 och CER; plus en introduktion och vägledning i systematiskt riskhanteringsarbete inklusive dess förutsättningar. En nyfiken läsare har däremot sannolikt även fortsatt ett antal kvarstående frågeställningar som behöver fångas upp i vidare skrifter.

Ett par punkter har särskilt identifierats som lämplig vidareutveckling av detta material:

- **Behov av ett metodstöd för att navigera informationssäkerhetsregleringslandskapet.** EU framstår som drivande i mycket av den reglering som kommer på cybersäkerhets- och informationssäkerhetsområdet. Samtliga nya EU-regleringar använder en liknande modell för hur den typen av reglering utformas. Grunden i modellen är i alla dessa fall en form av ett systematiskt och riskbaserat informationssäkerhetsarbete. Att ha, och arbeta enligt ett ledningssystem för informationssäkerhet (LIS) som både inkluderar ett systematiskt riskbaserat informationssäkerhetsarbete samt en metodik för bevakning av och kompensationer för aktuell lagstiftning skapar därför sannolikt goda förutsättningar för att hantera såväl dagens som morgondagens krav.
- **Behov av vidare vägledning i arbetet att identifiera och utvärdera de mest effektiva åtgärderna som reducerar de risker som har kartlagts och bedömts.** Ett centralt element som ofta omnämns i regulatoriska kravställningar är att riskreducerande åtgärder ska var proportionella, det vill säga att aktuellt behov ska vara i balans med åtgärdernas resursåtgång och tillförd nytta. Eftersom innebörden av ordet proportionella ofta inte förklaras ingående nog för att uppnå önskad tydlighet och systematik för den aktuella organisationen finns ett behov av konkreta förklaringar och vägledningar. Detta blir speciellt viktigt när det gäller möjligheten att kunna utvärdera ifall åtgärden är tillräcklig eller om den behöver kompletteras eller ersättas med annan åtgärd.
- **Behov av förvaltning av denna typ av dokument.** Då omvärlden utgör ett rörligt mål så ska detta dokument ses som ett levande material som är i behov av förvaltning och löpande uppdateringar. En process för dokumenthantering och -förvaltning behöver därför säkerställas där dokument av detta slag kan ingå.



Bilaga 1 – Exempel på olika fall

Våra byggnader blir allt mer smarta och den byggda miljön spelar också en viktig roll i den smarta staden där allt fler funktioner samverkar. Vi pratar om digitala tvillingar av både byggnader och städer där digital representation av det fysiska och där tvillingen visar både hur det ser ut och hur byggnaden/staden mår och presterar.

Den smarta staden ställer krav på bland annat tillgång till data vilket medför att både personer och organisationer måste vara beredda att dela med sig av information. Att avgöra vilken data vi är beredda att dela med oss av bottnar i kunskap och analyser av vilken data vi hanterar och hur våra byggnader är uppbyggda.

En smart byggnad innebär att den genom sina tekniska system och sensorteknik sitter på en massa data. Data som är användbar ur ett drift- och förvaltningsperspektiv, dels som enskild byggnad, dels som del i ett fastighetsbestånd i vilket man kan samköra data och dela system och därmed få bättre överblick och en effektivare skötsel.

Genom sensorteknik kan man reglera skalskydd och larm, se över nyttjandegrad och optimera schemaläggning och koppla drift, underhåll, städning och leveranser till en optimal tidpunkt. Ur ett hållbarhetsperspektiv kan man kalibrera luft, värme och kyla och på så vis skapa ett idealt inomhusklimat med lägre klimatpåverkan.

En förutsättning är att samla och dela data men att avgöra vilken data vi är beredda att dela med oss av bottnar i kunskap och analyser av vilken data vi hanterar och hur våra byggnader är uppbyggda.

I den fortsatta skrivningen applicerar vi metodiken från de tidigare kapitlen på några praktiska exempel för att påvisa hur offentliga byggnader med avancerade system är berörda av olika lagstiftningar och vilka områden som behöver hanteras.

Det första steget är att klargöra huruvida verksamheten träffas av säkerhetsskyddslagstiftningen (se kapitel 2 och 3) och till vilken grad. För att mer detaljerat bedöma hur man ska hantera sina anläggningar/byggnader behöver man också fundera kring lämpliga analysobjekt och hur detaljerat man ska studera sin anläggning. Ett sätt är att utgå från anläggningens uppbyggnad dvs olika byggdelar och tekniska system och med det som grund fundera kring skyddsvärden, hot, sårbarheter och säkerhetsskyddsåtgärder.

När analysen är genomförd är det tydligt vilka eventuella delar som träffas av säkerhetsskydd och av det följer att säkerhetsskyddslagstiftningen ska tillämpas medan andra delar kanske träffas av andra delar av OSL, CER (se kapitel 4) NIS (se kapitel 5) och personuppgiftslagstiftningen där ett sedvanligt informations- och cybersäkerhetsarbete ska tillämpas och där riskhantering är en mycket central för det arbetet (se kapitel 9 och 10 och 11).

Analys av vårdbyggnad/sjukhus

En säkerhetsanalys för en sjukhusbyggnad visar med största sannolikhet att man till större del inte träffas av säkerhetsskyddslagen men att det ändå finns ett antal anläggningar och system som behöver skyddas.

Verksamhetsbeskrivning

Sjukhus är generellt att betrakta som samhällsviktig verksamhet och omfattas av hälso- och sjukvårdssektorn i både CER-direktivet och NIS 2-direktivet. Vissa delar av verksamheten kan även träffas av säkerhetsskyddslagen.

Skyddsvärden och analysobjekt

För en sjukvårdsbyggnad finns det ett antal analysobjekt som är skyddsvärda och där en analys bör göras vad konsekvensen är av en eventuell händelse. Ingående analysobjekt och en bedömning av vilka objekt som är sårbara kan se ut enligt följande:

Exempel på skyddsvärden Vårdbyggnad

Analysobjekt		Potentiell sårbarhet för cyberhot
Mark och utemiljö	Mark	-
	Parkeringstjänster	Ja
	Karttjänster	Ja
Byggnadskonstruktion	Stomme	-
	Skalskydd	-
Lokaler	Planlösning	Ja
	Lokalanvändning	Ja
	Karttjänster	Ja
Gas och luft	Medicinska gaser	Ja
	Tryckluft	-
Vatten	Rent vatten	Ja
Avlopp och avfall	Avlopp	Ja
	Avfall	-
Kyla och värme	Kyla	Ja
	Värme	Ja
Luftbehandling	Luftkvalitet	Ja
Elkraft	Normalkraft	Ja
	Reservkraft	Ja
	Avbrottsfri kraft	Ja
Automation	Övervakning	Ja
	Styrning	Ja
Information och kommunikation	Positionering	Ja
	Kommunikation	Ja
Transport	Hissar, rulltrappor	Ja
	Lyftar	Ja
Säkerhet och skydd	Passagesystem	Ja
	Brandlarm, utrymningslarm	Ja
Belysning och dagsljus	Belysningsstyrning	Ja
Verksamhetsutrustning		Ja
Administrativa it-system		Ja

TABELL 1

Sårbarheter/brister
För sårbarheter/brister se sammanställning under 3.

Säkerhetsåtgärder
För säkerhetsåtgärder, se sammanställning under 3.

Riskanalys
För arbete med riskanalys, se kapitel 9 och 10 samt bilaga med exempel.

Analys av skola

Den smarta skolan har beskrivits i skriften Digitalisering i lärmiljöer från Offentliga fastigheter 2020. I den skriften beskrivs den smarta byggnaden och hur den påverkas av och kan samverka med verksamhetens digitalisering.

Smarta byggnader utrustade med sensorteknik är kostnadseffektiva och kan generera data som när den analyseras kan förutse drift och underhåll samt anpassa installationer optimalt.

I skolan kan sensortekniken dels underlätta administration, närvarohantering och skydd, dels analysera den specifika lärsituationen och aktiviteten på en given plats i ett givet rum i byggnaden. I undervisningen kan man lära sig av byggnaden i realtid.

Verksamhetsbeskrivning
En skola bedöms normalt inte vara berörd av något av regelverken i denna skrift, dock finns hothändelser även här vilket gör att metodiken ändå är relevant.

Skyddsvärden/analysobjekt:
För en skolbyggnad finns det med förmodligen färre analysobjekt som kan tänkas vara utsatta för cyberhot men det är viktigt att göra bedömningen i varje enskilt fall eftersom en eventuell händelse naturligtvis får konsekvenser för verksamheten. De analysobjekt som bedöms vara mest sårbara framgår nedan:

Exempel på skyddsvärden Skolbyggnad

Analysobjekt		Potentiell sårbarhet för cyberhot
Mark och utemiljö	Mark	-
	Parkeringstjänster	-
	Karttjänster	-
Byggnadskonstruktion	Stomme	-
	Skalskydd	-
Lokaler	Planlösning	-
	Lokalanvändning	-
	Karttjänster	-
Vatten	Rent vatten	-
Avlopp och avfall	Avlopp	-
	Avfall	-
Kyla och värme	Kyla	-
	Värme	-
Luftbehandling	Luftkvalitet	-
Elkraft	Normalkraft	Ja
Automation	Övervakning	Ja
	Styrning	Ja
Information och kommunikation	Positionering	-
	Kommunikation	-
Transport	Hissar	-
Säkerhet och skydd	Passagesystem	Ja
	Brandlarm, utrymningslarm	Ja
Belysning och dagsljus	Belysning	-
Verksamhetsutrustning		-
Administrativa it-system		-
Belysning och dagsljus	Belysningsstyrning	Ja
Verksamhetsutrustning		Ja
Administrativa it-system		Ja

TABELL 2

Sårbarheter/brister
För sårbarheter/brister se sammanställning under 3.

Säkerhetsåtgärder
För säkerhetsåtgärder, se sammanställning under 3.

Riskanalys
För arbete med riskanalys, se kapitel 9 och 10 samt bilaga med exempel.

Analys av anläggning/byggnad där verksamheten träffas av säkerhetsskyddslagen

En säkerhetsskyddsanalys för en anläggning eller byggnad där verksamheten träffas av säkerhetsskyddslagen beskrivs inte närmre i denna skrift. De analysobjekt i form av system och funktioner som behöver skyddas är med största sannolikhet de samma som för övriga byggnader varför sammanställningen i kapitel 3 kan användas som input till analysen.

Verksamhetsbeskrivning
Verksamheten som nyttjar anläggningen/byggnaden betraktas som säkerhetskänslig och omfattas av säkerhetsskyddslagen.

Skyddsvärden och analysobjekt
För en anläggning eller byggnad där verksamheten träffas av säkerhetsskyddslagen är det troligt att de flesta system är skyddsvärda även om hotbilden kan se annorlunda ut beroende på utformningen av anläggningen. Ingående analysobjekt och en bedömning av vilka objekt som är sårbara kan se ut enligt följande:

Exempel på skyddsvärden för anläggning där verksamheten träffas av säkerhetsskyddslagen

Analysobjekt		Potentiell sårbarhet för cyberhot
Mark och utemiljö	Mark	-
	Parkeringstjänster	Ja
	Karttjänster	Ja
Byggnadskonstruktion	Stomme	Ja
	Skalskydd	Ja

Lokaler	Planlösning	Ja
	Lokalanvändning	Ja
	Karttjänster	Ja
Gas och luft	Medicinska gaser	Ja
	Tryckluft	-
Vatten	Rent vatten	Ja
Avlopp och avfall	Avlopp	Ja
	Avfall	-
Kyla och värme	Kyla	Ja
	Värme	Ja
Luftbehandling	Luftkvalitet	Ja
Elkraft	Normalkraft	Ja
	Reservkraft	Ja
	Avbrottsfri kraft	Ja
Automation	Övervakning	Ja
	Styrning	Ja
Information och kommunikation	Positionering	Ja
	Kommunikation	Ja
Transport	Hissar, Rulltrappor	Ja
Säkerhet och skydd	Passagesystem	Ja
	Brandlarm, utrymningslarm	Ja
Belysning och dagsljus	Belysningsstyrning	Ja
Verksamhetsutrustning		Ja
Administrativa it-system		Ja

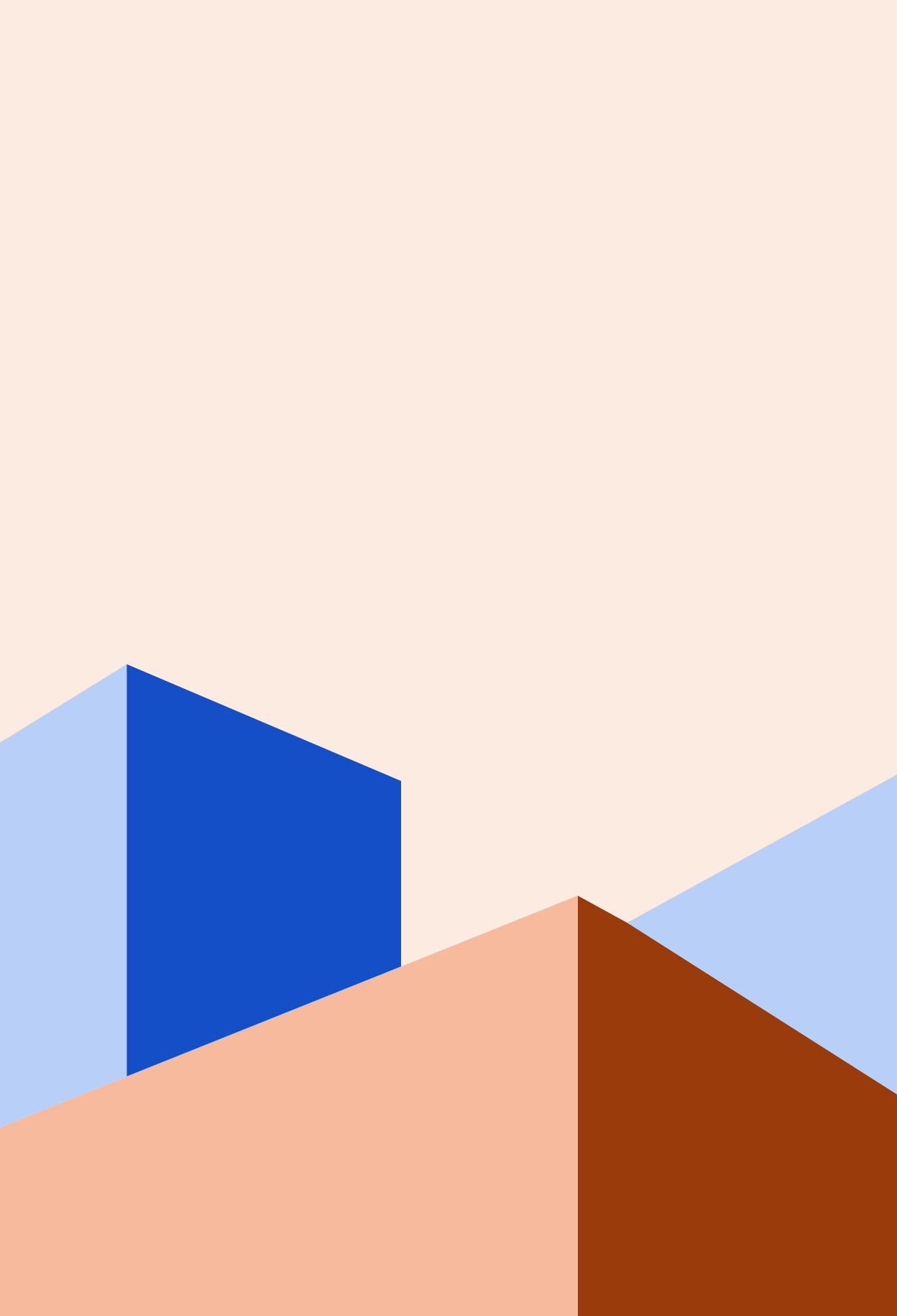
TABELL 3

Sårbarheter/brister

För sårbarheter/brister se sammanställning under kap 3.

Säkerhetsskyddsåtgärder

För säkerhetsskyddsåtgärder, se sammanställning under kap 4.



Bilaga 2 – Exempel på hot och riskanalyser

I denna bilaga ges ytterligare exempel på tillämpningen av det systematiska riskanalysarbetet som beskrivs i kapitel 10 ovan. Samma metodik, bedömningsgrunder och skalor används mm.

I nedanstående exempel följs arbetet med hot- respektive riskanalys för analysobjektet Transportsystem.

Hot och hothändelser

Arbetet med att identifiera aktuella hothändelser har föregåtts av ett arbete med att kartlägga och analysera vilka oönskade händelser som inträffat eller troligen skulle kunna inträffa inom analysobjektet Transportsystem.

I detta fall blir resultatet att tre hothändelser identifieras sett till aktuell aktör, dennes intention samt hur aktören agerar. Som nämndes i kapitel 10 är det viktigt att skapa tydliga riskformuleringar och grunden för denna tydlighet läggs redan på stadiet där hothändelser identifieras. Fördelen med att tydligt identifiera exempelvis den aktuella aktören är att det underlättar senare steg i arbetet, såsom att identifiera lämpliga skyddsåtgärder.

Exempel på hotbedömning inom analysobjektet Transportsystem

Hothändelse ID	Hotkategori	Hothändelse (aktör+ ev intention+agerande)
H-005	Hanteringsfel	Driftstopp då leverantören ej säkerhetsuppdaterat hissens övervakningssystem.
H-006	Angrepp	Kriminella modifierar byggnadens tillträdesbegränsningar via hissens övervakningssystem.
H-007	Angrepp	Tekniker medvetet sprider känslig styrinformation via molntjänst.

TABELL 1

För att underlätta framtida sammanställningar väljer man att kategorisera respektive hothändelse, detta kan senare nyttjas för att identifiera trender eller för att underlätta prioritering av åtgärder.

För att underlätta spårbarhet i analysarbetet ges varje hothändelse ett ID.

Resultatet blir en hotförteckning som succesivt kan byggas på och förvaltas.

Riskbedömning

Som nämndes i kapitel 10 omfattar riskbedömning att identifiera, formulera samt bedöma om en risk är acceptabel eller inte. För att riskbedömningen ska ske på ett enhetligt sätt är det viktigt att risken är tydligt formulerad.

Utifrån den grundläggande riskformuleringen ”Risk för att [Hothändelse]. På årsbasis bedöms risken inträffa [Sannolikhet] med en total skadeverkan motsvarande [Skadekonsekvens]” innebär det fortsatta arbetet att identifiera och uttrycka [Sannolikhet] respektive [Skadekonsekvens] på ett tydligt sätt. Begreppet [Hothändelse] identifierades i avsnittet ovan.

Bedöm sannolikhet

Sannolikheten för respektive hothändelse bedöms genom att först identifiera det troliga intervallet och därefter att inom det aktuella intervallet identifiera vad det mest troliga utfallet är. För hothändelse H-005 identifieras att sannolikheten för händelsens inträffande är 1–10 gånger per år där det mest troliga utfallet är 3 gånger per år. Vad detta resultat baseras på anges i kolumnen ”Motivering sannolikhet”. Genom att dessa input dokumenteras blir bedömningsarbetet transparent och andra personer/roller kan ges möjlighet att kommentera och diskutera korrektheten hos värdena och därigenom stödja i förbättringsarbetet.

Exempel på bedömning av sannolikhet för hothändelser inom analysobjektet Transportsystem

Hothändelse ID	Hothändelse (aktör+ ev intention+agerande)	Sannolikhet intervall (drop-down)	Mest troligt sannolikhet (ggr per år)	Motivering sannolikhet
H-005	Driftstopp då leverantören ej säkerhetsuppdaterat hissens övervakningssystem.	>1 ≤10 ggr per år (Måttlig)	3	Bedömning görs sett till tidigare historik från incidenter och störningar. Bedömningen är relativt säker.
H-006	Kriminella modifierar byggnadens tillträdesbegränsningar via hissens övervakningssystem.	<0,1 ≤1 ggr/år (Låg)	0,5	Bedömning görs sett till trender i omvärlden och ökad publicitet kring sårbarheter i SCADA-system. Bedömningen är relativt säker.
H-007	Tekniker medvetet sprider känslig styrinformation via molntjänst.	<0,1 ≤1 ggr/år (Låg)	0,3	Bedömningen görs sett till tidigare händelser i branschen. Bedömningen är relativt osäker.

TABELL 3

Bedöm konsekvens (skada)

Bedömning av konsekvens sker med samma metodik som bedömning av sannolikhet. Konsekvensen för respektive hothändelse bedöms genom att först identifiera det troliga intervallet och därefter att inom det aktuella intervallet identifiera vad det mest troliga utfallet är. För hothändelse H-005 identifieras att konsekvensen för händelsens inträffande till intervallet 100 tKr–1.000 tKr per händelse där den mest troliga skadan är 600 tKr. Vad detta resultat baseras på anges i kolumnen ”Motivering konsekvens”. För att underlätta framtagandet av ingångsvärden för skador kan de skador som beskrevs i kapitel 9.4.3 användas som en checklista.

Exempel på bedömning av konsekvens/skada för hothändelser inom analysobjektet Transportsystem

Hot-händelse ID	Hothändelse (aktör + ev intention + agerande)	Konsekvensnivå intervall (drop-down)	Mest trolig konse-kvens (tkr)	Motivering konsekvens
H-005	Driftstopp då leverantören ej säkerhetsupp-daterat his-sens övervak-ningssystem.	>100≤1 000 tkr (Låg)	600	Bedömning baseras på kostnader or-sakade av omarbeten, återställnings-arbete respektive avbrott i verksam-heten. **Bedömning:** Hanteringskostnad 600 tkr.
H-006	Kriminella modifierar byggnadens tillträdesbe-gränsningar via hissens övervaknings-system.	>5 000≤20 000 tkr (Allvarlig)	9 500	Bedömning baseras på kostnader orsakade av forensiska arbeten, återställningsarbete, stilleståndser-sättning respektive avbrott i verksam-heten. **Bedömning:** Produktivitetskost-nad 2 500 tkr, hanteringskostnad 5 000 tkr, ersättningskostnad 2 000 tkr.
H-007	Tekniker med-vetet sprider känslig styrin-formation via molntjänst.	>5 000≤20 000 tkr (Allvarlig)	6 000	Bedömning baseras på kostnader orsakade av sanktionsavgifter, omar-beten, återställningsarbete, stille-ståndsersättning respektive avbrott i verksamheten. **Bedömning:** Produk-tivitetskostnad 500 tkr, hanterings-kostnad 2 500 kr, böter & sanktioner 2 000 tkr.

TABELL 4

Formulera risker

Efter att alla ingående delar identifierats sätts dessa samman i riskfor-muleringar. Nedanstående figur visar en vy som innehåller de 6 kolumn-rubrikerna. Det är naturligtvis fullt möjligt och lämpligt att även ha de tidigare kolumnerna tillgängliga om man under bedömningen vill gräva lite djupare kring någon del. Det kan även vara lämpligt att lyfta fram skadan/kostnaden för en enstaka händelse, dvs att som komplement till den förde-lade kostnaden på årsbasis även visa kostnaden för en enstaka händelse.

Genom detta skapas en riskförteckning över de aktuella riskerna. Denna riskförteckning kan med fördel expanderas till en hel organisation om detta är möjligt och lämpligt. För att möjliggöra ett effektivt och uthålligt riskar-bete är det viktigt att riskförteckningen förvaltas och hålls uppdaterad.

Exempel formulering av risker inom analysobjektet Luftbehandling

Risk ID	Hothän-delse ID	Hothändelse (aktör+ ev intention+agerande)	Mest troligt sannolikhet (ggr per år)	Mest trolig konse-kvens (tkr)	Riskformulering
R-005	H-005	Driftstopp då leverantören ej säkerhetsupp-daterat hissens övervakningssys-tem.	3	600	Risk för att driftstopp då leverantören ej säker-hetsuppdaterat hissens övervakningssystemet. På årsbasis bedöms risken inträffa 3 ggr med total skadeverkan motsvarande 1 800 tkr.
R-006	H-006	Kriminella modifierar byggnadens tillträ-desbegränsningar via hissens övervak-ningssystem.	0,5	9 500	Risk för att kriminella modifierar byggnadens tillträdesbegränsningar via hissens övervakningssys-tem. På årsbasis bedöms risken inträffa 0,5 ggr med total skadeverkan motsva-rande 4 750 tkr.
R-007	H-007	Tekniker medvetet sprider känslig styrinformation via molntjänst.	0,3	6 000	Risk för att tekniker med-vetet sprider känslig styr-information via molntjänst. På årsbasis bedöms risken inträffa 0,3 ggr med total skadeverkan motsvarande 1 800 tkr.

TABELL 5

Sammanställd riskförteckning

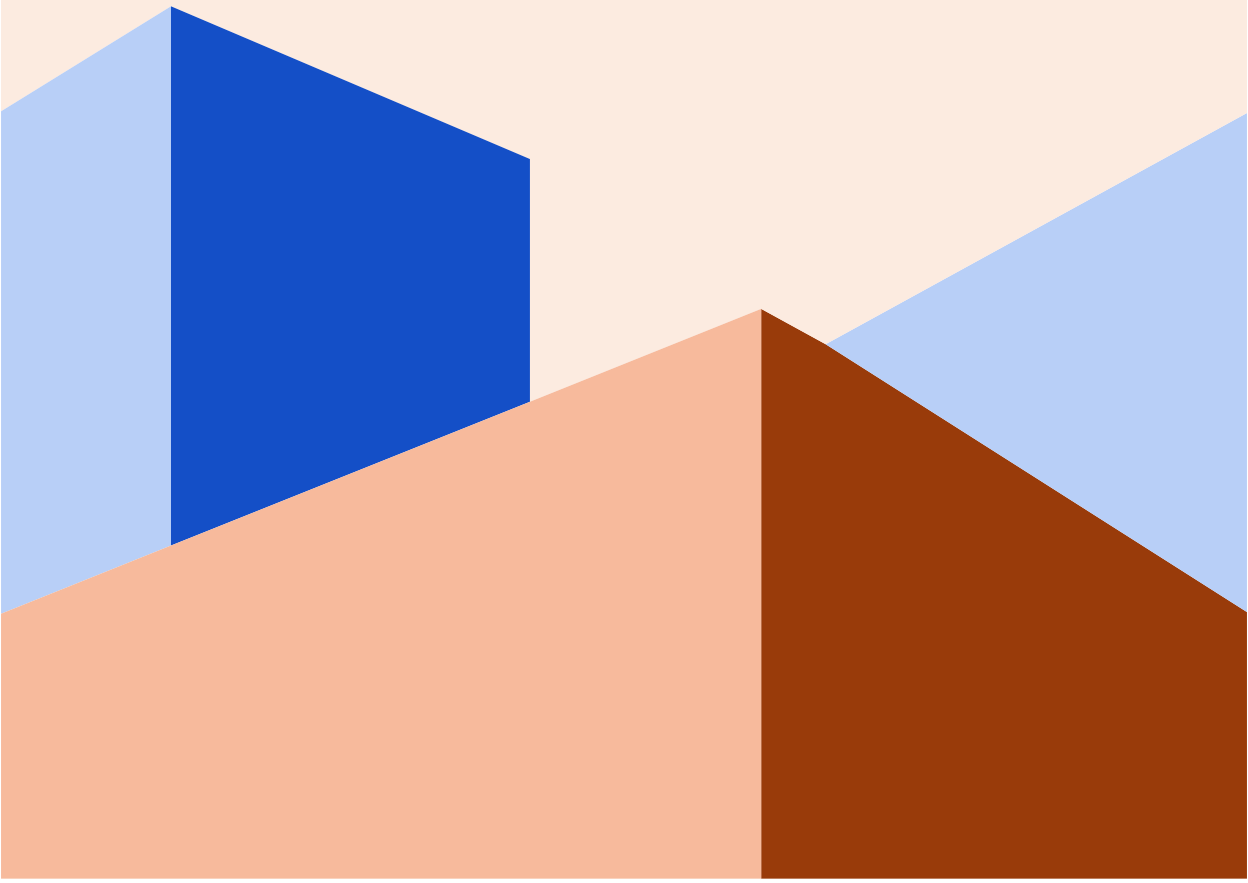
Nedanstående riskförteckning omfattar risker för analysobjekt Luft-behandling (enligt kap 10) respektive analysobjekt Transportsystem.

I denna riskförteckning har kolumnen ”Årlig skadeverkan” tillförts, genom detta kan alla risker filtreras från exempelvis högsta till lägsta skade-verkan. Genom detta kan riskbedömning och prioritering underlättas men även värdering av lämpliga åtgärders kostnader för de risker som ej kan accepteras.

Exempel på sammanställd riskförteckning för Luftbehandling resp Transportsystem

Risk ID	Hothändelse (aktör + ev intention + agerande)	Mest troligt sannolikhet (ggr per år)	Mest trolig konse-kvens (tkr)	Riskformulering
R-001	Tekniker anger felaktiga styrvärden för ventilation	2	800	Risk för att tekniker anger felaktiga styrvärden för ventilation. På årsbasis bedöms risken inträffa 2 ggr med total skadeverkan motsvarande 1 600 tkr.
R-002	Tekniker medvetet anger felaktiga styrvärden för ven-tilation	0,3	7 000	Risk för att tekniker medvetet anger felaktiga styrvärden för ventilation. På årsbasis bedöms risken inträffa 0,3 ggr med total skadeverkan motsvarande 2 100 tkr.
R-003	Ransomware gör att styrning av ventila-tion inte är möjlig	0,4	12 000	Risk för att ransomware gör att styr-ning av ventilation inte är möjlig. På årsbasis bedöms risken inträffa 0,4 ggr med total skadeverkan motsvarande 4 800 tkr.
R-004	Sensordata för luftkvalitet kommer inte fram till styr-systemet	6	2 000	Risk för att sensordata för luftkvalitet kommer inte fram till styrsystemet. På årsbasis bedöms risken inträffa 6 ggr med total skadeverkan motsvarande 12 000 tkr.
R-005	Driftstopp då leverantören ej säkerhetsupp-daterat hissens övervakningssys-tem.	3	600	Risk för att driftstopp då leverantö-ren ej säkerhetsuppdaterat hissens övervakningssystem. På årsbasis bedöms risken inträffa 3 ggr med total skadeverkan motsvarande 1 800 tkr.
R-006	Kriminella mo-difierar byggna-dens tillträdes-begränsningar via hissens övervak-ningssystem.	0,5	9 500	Risk för att kriminella modifierar byggnadens tillträdesbegränsningar via hissens övervakningssystem. På årsbasis bedöms risken inträffa 0,5 ggr med total skadeverkan motsva-rande 4 750 tkr.
R-007	Tekniker medvetet sprider känslig styrinformation via molntjänst.	0,3	6 000	Risk för att tekniker medvetet sprider känslig styrinformation via moln-tjänst. På årsbasis bedöms risken inträffa 0,3 ggr med total skadever-kan motsvarande 1 800 tkr.

TABELL 6



ISBN: 978-91-8047-198-5
www.offentligafastigheter.se

OFFENTLIGA
FASTIGHETER