Myndigheten för civilt försvar

Co-funded by the European Union

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Temarapport

Metodik för strategisk cybersäkerhetsanalys

Första utgåvan: Samlade lärdomar från åtta år av it-incidentrapportering

Metodik för strategisk cybersäkerhetsanalys

Myndigheten för civilt försvar
651 81 Karlstad

Enhet: Enheten för strategisk cybersäkerhet

Foto omslag: Myndigheten för civilt försvar, Melker Dahlstrand
Text: CS-SC-SA
Tryck: Ljunbergs tryckeri
Produktion: Advant

Publikationsnummer: MCF0171 – juni 2026
ISBN-nummer: 978-91-7927-772-7

Förord

Den strategiska cybersäkerhetsanalysen etablerades först på dåvarande Myndigheten för samhällsskydd och beredskap 2014. Den informationsteknologiska utvecklingens betydelse för samhällsutvecklingen hade länge varit tydlig, och det var hög tid att samlat börja bevaka, analysera och bedöma utvecklingen och dess olika konsekvenser.

Jag började på myndigheten i augusti det året. Det mesta var nytt, och mycket skulle byggas från grunden. Vi bedrev omvärldsbevakning, arbetade med egna analyser och stöttade i myndighetens olika analysverksamheter.

Vi testade olika befintliga analysmetodiker men fann ofta att de bara delvis var ändamålsenliga. Ofta krävdes det att vi, åtminstone i delar, utvecklade egna sätt att bedriva den analys som behövdes.

Efter några år beslutade regeringen om att införa it-incidentrapportering för statliga myndigheter. Vikten av en analysmetodik som kunde användas för att säkerställa att användbar, entydig och relevant information först kom in och sedan kunde vidareutnyttjas för att svara på viktiga frågor eller ligga till grund för andra satsningar ökade bara.

Samtidigt innebar inflödet av information att sätt att systematisera informationen successivt växte fram i form av begrepps- och kriterieutveckling, och så vidare.

Sedermera beslutades och implementerades NIS-direktivet i Sverige, varpå incidentrapporteringen utvidgades till en betydligt större krets. Nya sorters information tillkom också, vilket i sin tur innebar ytterligare metodutveckling.

När jag nu läser den föreliggande rapporten och ser tillbaka på de snart 12 år som jag har följt den successiva utvecklingen av den strategiska cybersäkerhetsanalysen, och de snart 8 år som vi har utvecklat vår metodik för att bättre förstå och skapa nytta utifrån den data vi mottar, är jag stolt över vad vi har åstadkommit. Det vi tar fram med hjälp av vår metodik har blivit allt bättre, och vi har idag stort gehör i EU-kretsen när vi diskuterar metodfrågor.

Jag vill tacka såväl alla er som har rapporterat incidenter till oss genom åren, och alla er som jag har bedrivit den här utvecklingen tillsammans med. Tack vare er är vi nu väl satta att från och med den 1 juli i år fortsätta vårt viktiga arbete hos FRA och inom Nationellt cybersäkerhetscenter.

Stockholm, 2026-06-26

Johan Turell
Chef, Enheten för strategisk cybersäkerhet

Innehåll

Ordlista

Aktör
En enhet med förmåga att agera och med egna mål eller intressen.

Allriskperspektivet
Synsätt där alla typer av orsaker till incidenter beaktas, inklusive angrepp, misstag, systemfel och naturhändelser.

Angrepp
Avsiktligt antagonistiskt handlande som kan orsaka incidenter.

Attityd
En aktörs inställning till objekt, sakförhållanden eller händelser (önskvärda eller oönskade).

Begreppssystem
Strukturerad uppsättning begrepp och deras inbördes relationer.

Brist
Avsaknad som bidrar till att oönskade händelser kan uppstå.

Chans
En möjlig önskad händelse.

Cyberhot
Hot som interagerar med informationssystem och kan orsaka incidenter i sådana system.

Cyberkrishantering
Hantering av samhälleliga konsekvenser av it incidenter.

Cybersäkerhetsincident
En oönskad händelse inom cybersäkerhetsområdet.

Cybersäkerhetstriaden (KRT)
Samlingsbegrepp för konfidentialitet, riktighet och tillgänglighet.

Digital leveranskedja
Det nätverk av system, leverantörer och tjänster som möjliggör leverans av digitala produkter eller tjänster.

Domän
Analysnivå, exempelvis it-miljö, organisation eller samhälle.

Effektivitet (åtgärder)
Bedömning av hur väl en åtgärd reducerar risk eller konsekvens.

Faktisk incident
Incident där skada orsakas eller nytta förhindras för den drabbade aktören, eller där nytta orsakas eller skada förhindras för en antagonist.

Framgång
En inträffad önskad händelse.

Framgångsfaktor
Objekt eller förhållanden som orsakar eller bidrar till önskade händelser.

Fullständighet (åtgärder)
Bedömning av om åtgärder sammantaget hanterar hela problemet.

Förhindrande kausalitet
Samband där en händelse leder till att en annan händelse uteblir.

Hinder
Objekt eller förhållanden som förhindrar eller motverkar önskade händelser.

Hot
Objekt eller förhållanden som orsakar eller bidrar till incidenter.

Hotbild
Samlad bild av potentiella hot och deras utveckling.

Händelse
Tidsperiod under vilken ett objekt eller sakförhållande existerar eller förändras.

IT incidenthantering
Operativ hantering av incidenter i it miljö.

IT miljö
Den samlade mängden informationssystem en organisation använder.

Incident
En inträffad oönskad händelse.

Indirekt framgång
Utebliven oönskad händelse.

Indirekt incident
Utebliven förväntad önskad händelse.

Informationssystem
System för att samla in, lagra och distribuera information.

Kausalitet
Samband mellan orsak och verkan.

Kausalt flöde
Kedja av händelser där en påverkar en annan.

Komponent
Del av en mekanism.

Konfidentialitet
Information är endast tillgänglig för behöriga.

Konsekvensanalys
Analys av effekter av incident eller risk.

Kontext
Den avgränsade situation inom vilken en analys sker.

Lägesbild
Samlad bild av aktuella incidenter och risker.

Lämplighet (åtgärder)
Bedömning av genomförbarhet.

Mekanism
Objekt eller system som orsakar eller förhindrar händelser.

Misstag
Oavsiktligt mänskligt handlande.

Monoberoende
Många aktörer beroende av samma resurs.

Naturhändelse
Icke mänsklig händelse, till exempel brand.

Normalbild
Beskrivning av vad som är normalt över tid.

Objekt
Något som existerar och har egenskaper.

Orsakande kausalitet
Samband där en händelse leder till en annan.

Orsaksanalys
Varför en incident uppstår.

Primitiva begrepp
Begrepp som inte definieras vidare.

Redogörelse
Strukturerad beskrivning av analysens avgränsning.

Redundans
Alternativa resurser som kan ersätta varandra.

Resiliens
Förmåga att återhämta sig efter störning.

Riktighet
Information är korrekt och inte manipulerad.

Risk
Möjlig oönskad händelse.

Robusthet
Förmåga att motstå störningar.

Sakförhållande
Ett objekts egenskap eller tillstånd.

Samhällspåverkan
Konsekvenser som påverkar samhälleliga funktioner.

Samhällsviktig funktion
Funktion nödvändig för samhället.

Samhällsviktig infrastruktur
Infrastruktur som stöder samhällsviktiga funktioner.

Samhällsviktig tjänst
Tjänst avgörande för samhället.

Sammanställd analys
Samlad analys av orsaker och konsekvenser.

Skydd
Åtgärder eller objekt som motverkar incidenter.

Strategisk cybersäkerhetsanalys
Metodik för systematisk analys av risker och incidenter.

Störning
Konsekvens där funktion inte upprätthålls.

Systemfel
Fel eller brister i tekniska system.

Sårbarhet
Avsaknad av skydd som möjliggör incident.

Sårbarhetsanalys
Identifiering av sårbarheter.

Säkerhetshändelse
Samlingsbegrepp för incidenter och risker.

Tillgänglighet
Information och tjänster finns vid behov.

Trigger (utlösande händelse)
Händelse som aktiverar en mekanism.

Värde (nytta/skada)
Positiv eller negativ effekt för en aktör.

Åtgärdsanalys
Analys av möjliga åtgärder.

Öppning
Avsaknad som möjliggör incidenter.

Foto: Myndigheten för civilt försvar, Melker Dahlstrand

Kapitel 1

Om rapporten

Om rapporten

Denna rapport sammanfattar stora delar av den utveckling av analysmetodik som har genomförts inom ramen för den strategiska cybersäkerhetsanalysen under den tid som den har bedrivits hos Myndigheten för civilt försvar. Delar av den utvecklade metodiken har successivt presenterats i tidigare temarapporter men har sedermera vidareutvecklats. Rapporten är en vägledning som är tänkt att ges ut i nya utgåvor i framtiden, i takt med att den strategiska cybersäkerhetsanalysens metodik fortsätter att utvecklas.

Innehållet riktar sig främst till personer med strategiska och operativa roller i cybersäkerhetsarbetet. Det omfattar analytiker, verksamhetsutvecklare, strateger inom it och säkerhet, CISO-funktioner samt andra nyckelroller inom säkerhet och verksamhetsstöd. Även beslutsfattare som behöver förstå området har nytta av rapporten.

Den strategiska cybersäkerhetsanalysens metodik genomsyrar det strategiska arbetet med cybersäkerhet i många olika sammanhang. Metodiken används i den kontinuerliga hanteringen av inkomna incidentrapporter. Den tillämpas vid framtagande av års-, tema-, och andra rapporter. Den används för att avgränsa inom vilka områden nya stödinsatser och utlysningar inom forskning, innovation och kompetensförsörjning ska tas fram. Den har även använts vid framtagningen av föreskrifter.

Utanför myndigheten har metodiken exempelvis också implementerats i den verktygslåda för säkerhet i digitala leveranskedjor som EU-kommissionen och medlemsstaterna har tagit fram i syfte att stärka och harmonisera insatser för att identifiera, bedöma och hantera risker kopplade till digitala leveranskedjor. Metodiken används också i andra arbeten på EU-nivå, såsom i gemensamt arbete inom ramen för EU:s cyberkrishanteringsnätverk, EU-CyCLONe.

Rapporten är en vägledning och kan därför läsas och tillägnas på olika sätt. Den är tänkt att kunna användas som ett utbildningsmaterial och ett uppslagsverk för analytiker om vad strategisk cybersäkerhetsanalys är, och hur strategisk cybersäkerhetsanalys går till. Den är inte tänkt att utgöra en vägledning om hur resultatet av analyser, bedömningar eller värderingar ska uttryckas eller kommuniceras för en extern publik. Rapporten går att läsa från början till slut, men beroende på behov kan andra sätt läsa den på vara mer lämpliga. Om rapporten exempelvis ska användas som stöd i en utbildningsinsats så kan det vara bättre

att inleda läsningen med delar ur kapitlen Analys och bedömning av orsak och verkan respektive Bedömningar.

Rapporten kommer att ges ut i nya utgåvor i takt med att substantiell utveckling av metodiken görs. Rapporten innehåller inte heller all metodik som har utvecklats inom ramen för den strategiska cybersäkerhetsanalysen sedan den etablerades på myndigheten 2014. Ett noterbart exempel är Cybersäkerhetskollen, vars modell och metodik finns beskrivna separat.

Rapporten är den femte i en serie av temarapporter. De tidigare rapporterna är:

- Hoten mot de digitala leveranskedjorna[1] (november 2021)
- Ändringar som både hotar och skyddar[2] (december 2022)
- Cyberangrepp mot samhällsviktiga informationssystem[3] (januari 2024)
- It-incidenters påverkan[4] (juni 2025).

Rapporten har tagits fram med stöd av medel från EU inom ramen för ENIAC-projektet (The Enhanced NIS2 Implementation And Cooperation Project).

Not 1. MSB. Hoten mot de digitala leveranskedjorna: 50 rekommendationer för att stärka samhällssäkerheten. Stockholm: MSB, 2021. Länk: https://rib.msb.se/filer/pdf/29829.pdf.

Not 2. MSB. Ändringar som både hotar och skyddar: 20 rekommendationer för säkrare ändringar i våra informationssystem. Stockholm: MSB, 2022. Länk: https://rib.msb.se/filer/pdf/30193.pdf.

Not 3. MSB. Cyberangrepp mot samhällsviktiga informationssystem – 25 rekommendationer för stärkt skydd mot cyberangrepp. Stockholm: MSB, 2024. Länk: https://rib.msb.se/filer/pdf/30558.pdf.

Not 4. MSB. It-incidenters påverkan – Ramverk för bedömning av påverkan på it-miljö, verksamhet och samhälle. Stockholm: MSB, 2025. Länk: https://rib.msb.se/filer/pdf/31096.pdf.

Foto: Myndigheten för civilt försvar, Melker Dahlstrand

Kapitel 2

Om den strategiska cybersäkerhetsanalysen

Om den strategiska cybersäkerhetsanalysen

Den strategiska cybersäkerhetsanalysen syftar till att förklara hur organisationer och samhället beror, påverkas och utvecklas av den informationsteknologiska utvecklingen.

Centrala uppgifter för den strategiska cybersäkerhetsanalysen är därför att möjliggöra en djupare förståelse av:

- Vad som händer när nya teknologier först upprättas, därefter upptas allt bredare och till slut ersätter andra teknologier.
- Hur nya risker uppstår och gamla risker förändras när samhället förändras som en följd av den informationsteknologiska utvecklingen.
- Vilka konsekvenser som uppstår eller kan förväntas uppstå för organisationer och samhället när risker realiseras och incidenter inträffar, och varför.
- Hur händelser som påverkar informationsteknologi, information, tjänster, människor, organisationer och samhället kan bedömas och klassificeras.
- Hur risker strategiskt kan förebyggas och hur förmåga kan byggas för att återställa skada som uppstår när risker ändå realiseras.

Den strategiska cybersäkerhetsanalysen måste vara användbar för de som ska motta dess resultat. När analysen ska användas för att förebygga risker eller bygga förmåga så avgränsas analysen typiskt sett till att beskriva *vad* problemet är, samt *vad* och *vilka* strategiska insatser som skulle kunna åtgärda problemet. För att sedan faktiskt lösa problemet krävs en ytterligare analys av *hur* de insatserna bör utformas för att vara effektiva. Den som tillämpar den strategiska cybersäkerhets-analysen behöver därför, för att nå resultat, säkerställa att den som tar emot resultatet har en förståelse för analysens metodik och därigenom kan använda resultatet som en inramning i arbetet med att designa och genomföra åtgärderna.

Den strategiska cybersäkerhetsanalysen tillämpas inom många olika sammanhang, såsom: riskanalyser och riskbedömningar, incidentanalyser och incidentbedöm-ningar, inriktningar, framtagande av åtgärdsplaner, övningar, cyberkrishantering och utveckling av forsknings-, innovations och kompetensförsörjningsinitiativ. Den strategiska cybersäkerhetsanalysen kommer därutöver att i växande grad behöva kunna användas för att göra förutsägelser och prognoser.

Den strategiska cybersäkerhetsanalysen skiljer på *analys* och *bedömning*. Analys handlar om att avgöra hur världen faktiskt är beskaffad. Bedömning handlar om att utifrån tillgänglig information på ett rationellt sätt komma fram till en beskrivning av hur analytikern *tror* att världen är beskaffad. Därutöver omfattar också den strategiska cybersäkerhetsanalysen *värdering*, främst i form av att den behöver kunna användas för att på strukturerat sätt avgöra hur allvarliga oönskade händelser inom dess omfång är.

Den strategiska cybersäkerhetsanalysen i korthet

För att möjliggöra en systematisk och fördjupad strategisk cybersäkerhetsanalys har en metodik utvecklats som består av tre centrala delar. Den första delen är ett strukturerat språkbruk, i form av begrepp och begreppssystem, för att möjliggöra analys. Den andra delen är en metodik för att beskriva och förklara förhållanden och händelser i omvärlden, och hur de beror av varandra genom kausala relationer. Den tredje delen är en metodik för att bedöma och klassificera händelser. De tre delarna presenteras, i den ordningen, i varsitt kommande kapitel. Här sammanfattas innehållet.

Begrepp och begreppssystem

Begreppssystemet tar sin utgångspunkt i några primitiva begrepp. Med ”primitiv” avses här något som inte definieras, utan bara beskrivs – och som sedan används för att definiera andra saker.

Utifrån de primitiva begreppen sätts sedan ett antal begreppssystem upp för att dela in och förklara olika typer av händelser och deras relation till olika objekt. I begreppssystemen ingår ett antal begrepp som definieras och begreppens relationer till varandra tydliggörs.

Med stöd av begreppssystemen utvecklas sedan taxonomier för säkerhetshändelser respektive faktiska incidenter och faktiska risker, begrepp som spelar en central roll i den strategiska cybersäkerhetsanalysens bedömningar.

Slutligen inkluderar den här delen av metodiken ett antal andra begrepp som också spelar en central roll för den strategiska cybersäkerhetsanalysens område och tillämpning:

- konfidentialitet, riktighet och tillgänglighet
- robusthet, resiliens och redundans
- cybersäkerhet
- allriskperspektivet
- monoberoenden

Analys och bedömning av orsak och verkan

Orsak och verkan är centralt i den strategiska cybersäkerhetsanalysen. Den här delen av metodiken tar därför sin utgångspunkt i hur orsak och verkan kan modelleras. Begreppet kausalitet (som beskriver orsak och verkan) introduceras, och med stöd av det definieras sedan begreppen *mekanism* respektive *komponent* som spelar centrala roller i representationen av orsak- och verkansrelationer.

Med stöd av de etablerade begreppen representeras dels incidenters respektive orsaker och verkningar, och riskers respektive orsaker och verkningar. Utifrån sådana representationer kan först sårbarheter analyseras, och sedan olika åtgärder för att hantera incidenter och risker identifieras. För att säkerställa att rätt åtgärder väljs genomgår de tre test: Ett för lämplighet, ett för effektivitet och ett för fullständighet.

Slutligen visas hur alla incidenter respektive risker är säkerhetshändelser, och hur säkerhetshändelser kan analyseras för att avgöra om incidenten eller risken också en är en faktisk incident eller en faktisk risk. Analysen ger en inledande förståelse för det ramverk för bedömning av säkerhetshändelser och faktiska incidenter respektive faktiska risker som utvecklas i den strategiska cybersäkerhetsanalysens tredje del.

Bedömning och värdering

Att kunna bedöma händelser (oavsett om de är incidenter eller risker) är också en central del av den strategiska cybersäkerhetsanalysen.

För att en bedömning ska vara möjlig (och, i förlängningen, tydlig) krävs det att det dels är tydligt *vad den ska handla om* (dess fokus) och att det dels är tydligt *vad den inte ska handla om* (dess avgränsning). Kombinationen av relevanta fokus och nödvändiga avgränsningar kallas för en redogörelse. Redogörelser görs åtminstone med avseende på i vilken domän en bedömning ska göras (it-miljö, verksamhet/organisation, samhälle), vilken incident eller risk som ska bedömas samt den tidsperiod som bedömningen avser.

Med stöd av redogörelser kan händelser bedömas. Det görs först genom att identifiera och bedöma den eller de typer av säkerhetshändelser en viss händelse utgör. Utifrån de gjorda bedömningarna bedöms därefter huruvida, och i så fall vilka, faktiska incidenter eller faktiska risker respektive typ av säkerhetshändelse utgör. Förfarandet görs för respektive domän som ska bedömas. Utifrån bedömningen av händelsen i samtliga domäner, de typer av säkerhetshändelser den utgör inom respektive domän och de (om några) typer av faktiska incidenter eller faktiska risker de typerna av säkerhetshändelser utgör kan sedan en samlad bedömning göras.

Det är också, slutligen, centralt att kunna bedöma orsaker till incidenter respektive risker. Orsaker (egentligen det som kallas för ”triggers” eller ”trigger-händelser”) delas typiskt in i kategorierna *angrepp, misstag, systemfel*, *naturhändelser* och *övrigt*. För att avgöra vilken kategori det är som gäller finns ett antal kriterier.

Foto: Myndigheten för civilt försvar, Melker Dahlstrand.

Kapitel 3

Begrepp och begreppssystem

Begrepp och begreppssystem

I detta kapitel presenteras den första delen i den strategiska cybersäkerhetsanalysens metodik. Kapitlet behandlar centrala begrepp som behövs för att förstå och kunna tillämpa metodiken för strategisk cybersäkerhetsanalys, samt relationerna mellan de begreppen. Kapitlet innehåller inte alla begrepp som förekommer i metodiken.

Fundamentala begrepp

I detta avsnitt presenteras fundamentala begrepp som ligger till grund för dels utvecklingen av andra begrepp, men också för utvecklingen av metodik som förekommer i senare kapitel.

Primitiva begrepp

I detta delavsnitt presenteras de sex primitiva begrepp (det vill säga begrepp som inte definieras utan endast beskrivs) som ligger till grund för alla andra begrepp som senare utvecklas:

Objekt: Sådant som finns och har egenskaper. Tiden ett objekt finns eller har en viss egenskap utgör en händelse (se Händelser nedan i detta avsnitt). Objekt kan bestå av andra objekt. Objekt kan vara *aktiva* respektive *passiva* i särskilda bemärkelser. Solen är ett exempel på ett aktivt objekt i bemärkelserna att den på egen hand avger ljus och värme. Månen är ett inaktivt objekt i samma bemärkelser. Två kategorier av objekt som är av särskild betydelse för den strategiska cybersäkerhetsanalysens metodik är mekanismer och komponenter (se avsnittet Mekanismer och komponenter nedan).

Sakförhållanden: De egenskaper som enskilda objekt har. När ett sakförhållande uppstår eller upphör så *förändras* det objekt som fick eller blev av med egenskapen/sakförhållandet.

Händelser: Den tid som enskilda objekt eller sakförhållanden är fallet. Händelser kan *uppstå*, *pågå* och *upphöra*. Konceptuellt kan händelser *inträffa* eller *utebli*, respektive vara *möjliga* eller *omöjliga*. Att en händelse är möjlig kan representeras av att den kan beskrivas som havande en sannolikhet som är högre än noll. Att en händelse är omöjlig kan representeras av att den kan beskrivas som havande en sannolikhet som är noll. En möjlig händelse som inträffar *realiseras*.

Aktör: En enhet med förmåga att agera och med egen vilja och intressen. Exempel kan vara en individ, en organisation eller en stat. Aktörer kan *förvänta* sig, respektive *inte förvänta* sig, att händelser ska inträffa.

Attityd: Den attityd, om någon, som en given aktör har till objekt, sakförhållanden och händelser. Aktörer kan antingen ha attityden att något är önskvärt eller oönskvärt. Aktörer kan också sakna attityd till objekt, sakförhållanden och händelser och de är då, utifrån aktörens perspektiv, varken önskvärda eller oönskvärda.

Värde: Det finns två typer av värde, positivt värde som kallas för *nytta* och negativt värde som kallas för *skada*. Nytta och skada är varandras motsatser. Ett sätt att uttrycka det på är att skada innebär negativ nytta, och att negativ skada innebär nytta. Att något innebär nytta för en aktör gör det önskvärt för aktören. Att något innebär skada för en aktör gör det oönskvärt för aktören. I vissa fall kan något innebära skada först och (övervägande) nytta sedan. Den sammanvägda uppfattningen beskrivs som att något ligger i en aktörs intresse (se delavsnittet Faktiska incidenter och faktiska risker i avsnittet Typer av incidenter och risker nedan). Objekt och sakförhållanden kan ha positivt värde (vara nyttiga) respektive negativt värde (vara skadliga). Händelser kan medföra positivt värde (göra nytta) och negativt värde (göra skada).

Begrepp för övergripande händelsekategorier

I detta delavsnitt definieras de fyra övergripande händelsekategorier som den strategiska cybersäkerhetsanalysen använder sig av. Samtidigt presenteras det begreppssystem som ligger till grund för idén om att incidenter och risker är två sidor av samma mynt. Begreppen definieras med stöd av de primitiva begrepp som presenterades i delavsnittet Primitiva begrepp ovan och genom att varje möjlig kombination namnges.

Tabell 1. Övergripande händelsekategorier

Övergripande händelse-kategorier	… har inträffat kallas för en/ett…	… kan inträffa (är möjlig) kallas för en/ett…
En önskad händelse som…	Framgång	Chans
En oönskad händelse som…	Incident	Risk

Not: Framgångar och chanser, respektive incidenter och risker, är två sidor av samma mynt. Alla framgångar är chanser, och alla incidenter är risker (det som har inträffat kan ju inträffa). Det omvända gäller däremot inte – det är inte fallet att alla chanser realiseras och blir till framgångar, och det är inte heller fallet att alla risker realiseras och blir till incidenter. På motsvarande sätt är framgångar och incidenter, respektive chanser och risker, varandras motsatser.

Begrepp för objekt och avsaknad av objekt

I detta delavsnitt definieras de fyra övergripande begreppen för objekt, respektive de fyra övergripande begreppen för avsaknad av objekt, som den strategiska cybersäkerhetsanalysen använder sig av. Begreppen definieras med stöd av de primitiva begrepp som presenterades i delavsnittet Primitiva begrepp och de händelsebegrepp som definierades i delavsnittet Begrepp för händelser (tabell 1 ovan) ovan.

Tabell 2. Övergripande objektkategorier

Övergripande objektkategorier	… framgång kallas för en/ett…	… incident kallas för en/ett…
Objekt som orsakar, eller bidrar till att orsaka, en…	Framgångsfaktor	Hot
Objekt som förhindrar, eller bidrar till att förhindra, en…	Hinder	Skydd
Avsaknad av objekt som orsakar, eller bidrar till att orsaka, en…	Brist	Lugn
Avsaknad av objekt som förhindrar, eller bidrar till att förhindra, en…	Öppning	Sårbarhet

Not: ”Objekt som orsakar” respektive ”objekt som förhindrar” indikerar att objektet är en *mekanism*. ”Objekt som bidrar till att orsaka” respektive ”objekt som bidrar till att förhindra” indikerar att objektet är en *komponent*. Se avsnittet Mekanismer och komponenter nedan.

Händelser som inträffar respektive uteblir

I detta delavsnitt görs en liten utvikning avseende en vanligt förekommande sammanblandning av händelser som inträffar respektive uteblir. Distinktionen som görs här bygger nyttjar följande begreppsbildning från delavsnittet Primitiva begrepp ovan:

Händelser: Den tid som enskilda objekt eller sakförhållanden är fallet. Händelser kan *uppstå*, *pågå* och *upphöra*. Konceptuellt kan händelser *inträffa* eller *utebli*, respektive vara *möjliga* eller *omöjliga*. Att en händelse är möjlig kan representeras av att den kan beskrivas som havande en sannolikhet som är högre än noll. Att en händelse är omöjlig kan representeras av att den kan beskrivas som havande en sannolikhet som är noll. En möjlig händelse som inträffar *realiseras*.

Definitionen av begreppet ”hot” i tabell 2 i det föregående delavsnittet är ”objekt som orsakar, eller bidrar till att orsaka, en incident. Definitionen av begreppet ”incident” i tabell 1 i delavsnittet Begrepp för övergripande händelsekategorier är ”en oönskad händelse som har inträffat”. En händelse är i sin tur (se föregående stycke) den tid som enskilda objekt eller sakförhållanden är fallet. Ett hot är därför ett objekt som orsakar, eller bidrar till att orsaka, att ett objekt eller ett sakförhållande som är oönskat är fallet under en viss tid.

En incident är därför något som uppstår, inte något som (enbart) uteblir.[5] Detta är en viktig distinktion då incidenter ofta resulterar i att något som aktörer är vana vid tillhandahålls, eller kan tillhandahållas, inte längre tillhandahålls/levereras eller inte längre kan tillhandahållas/levereras – det vill säga att *framgångar* (se tabell 2 i det föregående delavsnittet) uteblir. Det är vanligt att uppfatta att själva den uteblivna framgången *i sig* också är en incident. Men, utifrån ovan analys av definitionerna av hot respektive händelser är uteblivna framgångar *inte* incidenter eftersom inget som aktören har eller som finns hos aktören har tagit skada.

Samtidigt är det rimligt att en förväntad leverans som uteblir ändå räknas som något oönskat. Utebliven leverans av något som är önskat och förväntat spelar en avgörande roll inom säkerhet i digitala leveranskedjor (se delavsnittet En not om digitala leveranskedjor i det nästföljande avsnittet). För att omhänderta denna omständighet kan tabell 1 i delavsnittet Begrepp för övergripande händelse-kategorier ovan utökas enligt följande:

Tabell 3. Övergripande händelsekategorier

Övergripande händelsekategorier	… har inträffat kallas för en/ ett…	… har uteblivit, men förväntats, kallas för en/ett	… kan inträffa (är möjlig) kallas för en/ett…
En önskad händelse som…	Framgång	Indirekt incident[6]	Chans
En oönskad händelse som…	Incident	Indirekt framgång	Risk

Med tilläggen av *indirekt incident* respektive *indirekt framgång* kan uteblivna händelser också representeras på sätt som förefaller motsvara vanliga intuitioner.

En not om sårbarheter

I detta delavsnitt görs en liten utvikning med anledning av att begreppet ”sårbarhet” definieras som det gör i delavsnittet Begrepp för objekt respektive avsaknad av objekt.

Begreppet ”sårbarhet” är centralt i stora delar av säkerhetslitteraturen, såväl som i praktiken för de som arbetar med säkerhet. Det finns minst tre sätt som begreppet förstås, och det kan i vissa sammanhang vara oklart vad som avses. De tre olika sätten att förstå sårbarhet på är:

Not 5. En incident är till exempel därför att en aktörs mejlsystem slutar att fungera – och det kan ju leda till att ett mejl som någon har skickat till mejlsystemet inte kommer till användare av mejlsystemet. Men om aktören A:s mejlsystem har slutat att fungera och det resulterar i att aktören B inte mottar ett mejl som någon hos A försöker skicka så räknas det inte som en incident hos B då det inträffade enbart innebär att en händelse uteblir hos B (att mejlet kommer fram).

Not 6. Ett exempel på indirekta incidenter är digitala leveranskedjor av typ 1 (utebliven leverans av det som skulle levereras). Se delavsnittet En not om digitala leveranskedjeincidenter i det nästföljande avsnittet.

1. **En sårbarhet är en avsaknad av något som hade kunnat förhindra en oönskad händelse.** *Avsaknaden av en brandvägg* mellan en filyta där känslig information lagras och internet kan förstås som en sårbarhet utifrån det här synsättet.
2. **En sårbarhet är en mekanism som kan användas på ett sätt som resulterar i en oönskad händelse.** En filyta där känslig information lagras kan förstås som en sårbarhet utifrån det här synsättet.
3. **En sårbarhet är *kombinationen* av en mekanism som kan användas på ett sätt som resulterar i en oönskad händelse och avsaknaden av något som förhindrar att mekanismen används på ett sådant sätt.** En filyta där känslig information lagras som är ansluten till internet utan att det finns en brandvägg mellan filytan och internet kan förstås som en sårbarhet utifrån det här synsättet.

Det är viktigt att det är tydligt vilken definition som används. Om mekanismen *i sig* definieras som sårbarheten, då följer det att informationssystem som har mekanismen är sårbara oavsett vilka skydd de har. Om avsaknaden av skydd definieras som sårbarheten så kan olika informationssystem som alla har mekanismen i vissa fall räknas som sårbara, och i andra fall inte, beroende på vilka skydd de har. I den här rapporten åsyftas den första betydelsen när sårbarheter nämns.

Det förekommer också att man talar om att ett informationssystem är sårbart. Ibland avses då att det finns en sårbarhet som innebär att det saknas ett skydd som skulle kunna förhindra, eller att det finns en mekanism som skulle kunna möjliggöra, att informationssystemet självt skulle kunna ta skada. Ibland avses istället att organisationen som har informationssystemet, eller någon annan, skulle kunna ta skada genom att något görs med eller i informationssystemet.

Kategorisering av händelser utifrån begreppssystemet

I detta delavsnitt kategoriseras händelser där de fyra typerna av objekt som definierades i delavsnittet Begrepp för objekt och avsaknad av objekt ovan. Kategorierna utgörs av de sex typer av övergripande händelser som definierades i delavsnittet Händelser som inträffar respektive uteblir (tabell 3) ovan.

Tabell 4. Händelsers relation till övergripande händelsekategorier

Händelse	Klassificering
1. När det har uppstått en/ett…	… så är det en…
Framgångsfaktor	Framgång
Skydd	Framgång
Hot	Incident
Hinder	Incident

Händelse	Klassificering
2. När det förväntades att en/ett…	… skulle uppstå men den/det har uteblivit så är det en…
Framgångsfaktor	Indirekt incident
Skydd	Indirekt incident
Hot	Indirekt framgång
Hinder	Indirekt framgång
3. När det skulle kunna uppstå en/ett…	… så är det en…
Framgångsfaktor	Chans
Skydd	Chans
Hot	Risk
Hinder	Risk
4. När en/ett…	… har upphört så är det en…
Framgångsfaktor	Incident
Skydd	Incident
Hot	Framgång
Hinder	Framgång
5. När det förväntades att en/ett…	… skulle upphöra men den/det har förblivit så är det en…
Framgångsfaktor	Indirekt framgång
Skydd	Indirekt framgång
Hot	Indirekt incident
Hinder	Indirekt incident
5. När en/ett…	… skulle kunna upphöra så är det en…
Framgångsfaktor	Risk
Skydd	Risk
Hot	Chans
Hinder	Chans

Not: I vissa fall kan framgångsfaktorer eller skydd som upphör göra det för att någon väljer att ta bort dem/låta dem upphöra. Enligt vissa regelverk och i vissa praktiska sammanhang skulle det inte räknas som en incident – men det avgörande här är att något som har värde för någon upphör – varför densamme förfogar över mindre värde, vilket per definition är en oönskad händelse.

Typer av incidenter och risker

I detta avsnitt introduceras begreppen ”säkerhetshändelse” respektive ”faktisk incident” och ”faktisk risk”. Begreppen är centrala för bedömningar inom ramen för den strategiska cybersäkerhetsanalysens metodik. Begreppens innehåll definieras med stöd av den begreppsutveckling som gjordes i det föregående avsnittet.

Säkerhetshändelser

I detta delavsnitt förklaras begreppet ”säkerhetshändelse”. Sådana händelser som är säkerhetshändelser listas. Begreppet definieras med stöd av klassificeringen som gjordes i det föregående avsnittets sista delavsnitt Kategorisering av händelser utifrån begreppssystemet.

I det delavsnittet (tabell 4) listas vissa händelser som incidenter respektive risker. De händelserna kallas inom den strategiska cybersäkerhetsanalysens metodik samlat för säkerhetshändelser. Följande är därmed *säkerhetshändelser*:

Tabell 5. Alla händelser som är säkerhetshändelser

Incidenter	Indirekta incidenter	Risker
När det har uppstått ett hot	När en förväntad framgångsfaktor har uteblivit	När det skulle kunna uppstå ett hot
När ett skydd har upphört	När ett förväntat skydd har uteblivit	När ett skydd skulle kunna upphöra
När en framgångsfaktor har upphört	När det förväntades att ett hot skulle upphöra men det förblev	När en framgångsfaktor skulle kunna upphöra
När det har uppstått ett hinder	När det förväntades att ett hinder skulle upphöra men det förblev	När det skulle kunna uppstå ett hinder

Faktiska incidenter och faktiska risker

I detta delavsnitt förklaras begreppen ”faktisk incident” och ”faktisk risk”. Sådana händelser som är faktiska incidenter respektive faktiska risker listas. Begreppen definieras med stöd av de begrepp som beskrevs i delavsnittet Primitiva begrepp i det föregående avsnittet.

Precis som i tidigare avsnitt och delavsnitt så genereras begreppsuppsättningen genom att kombinera begrepp och utifrån den samlade mängden kombinationer klassificera en del av de kombinationerna, i detta fall som faktiska incidenter respektive faktiska risker.

Tabell 6. Faktiska incidenter/risker respektive framgångar/chanser

Vad	Vem/vilka	Intresse	Klassificering
När nytta eller skada orsakas			
Skada orsakas…	…för aktören, eller för andra,…	…på ett sätt som inte ligger i aktörens intresse.	Faktisk incident/ risk
Skada orsakas…	…för aktören, eller för andra,…	…på ett sätt som ligger i aktörens intresse.	Varken faktisk incident/risk eller faktisk framgång/ chans
Skada orsakas…	…för aktörens antagonister, eller för andra,…	…på ett sätt som inte ligger i aktörens intresse.	Varken faktisk incident/risk eller faktisk framgång/ chans
Skada orsakas…	…för aktörens antagonister, eller för andra,…	…på ett sätt som ligger i aktörens intresse.	Faktisk framgång/ chans
Nytta orsakas…	…för aktören, eller för andra,…	…på ett sätt som inte ligger i aktörens intresse.	Varken faktisk incident/risk eller faktisk framgång/ chans
Nytta orsakas…	…för aktören, eller för andra,…	…på ett sätt som ligger i aktörens intresse.	Faktisk framgång/ chans
Nytta orsakas…	…för aktörens antagonister, eller för andra,…	…på ett sätt som inte ligger i aktörens intresse.	Faktisk incident/ risk
Nytta orsakas…	…för aktörens antagonister, eller för andra,…	…på ett sätt som ligger i aktörens intresse.	Varken faktisk incident/risk eller faktisk framgång/ chans

Vad	Vem/vilka	Intresse	Klassificering
När nytta eller skada förhindras			
Skada förhindras…	…för aktören, eller för andra,…	… på ett sätt som inte ligger i aktörens intresse.	Varken faktisk incident/risk eller faktisk framgång/chans
Skada förhindras…	…för aktören, eller för andra,…	… på ett sätt som ligger i aktörens intresse.	Faktisk framgång/chans
Skada förhindras…	…för aktörens antagonister, eller för andra,…	… på ett sätt som inte ligger i aktörens intresse.	Faktisk incident/risk
Skada förhindras…	…för aktörens antagonister, eller för andra,…	… på ett sätt som ligger i aktörens intresse.	Varken faktisk incident/risk eller faktisk framgång/chans
Nytta förhindras…	…för aktören, eller för andra,…	… på ett sätt som inte ligger i aktörens intresse.	Faktisk incident/risk
Nytta förhindras…	…för aktören, eller för andra,…	… på ett sätt som ligger i aktörens intresse.	Varken faktisk incident/risk eller faktisk framgång/chans
Nytta förhindras…	…för aktörens antagonister, eller för andra,…	… på ett sätt som inte ligger i aktörens intresse.	Varken faktisk incident/risk eller faktisk framgång/chans
Nytta förhindras…	…för aktörens antagonister, eller för andra,…	… på ett sätt som ligger i aktörens intresse.	Faktisk framgång/chans

Totalt sett finns det därmed fyra faktiska incidenter respektive faktiska risker:

1. **Skada orsakas:** Skada orsakas för aktören, eller för andra, på ett sätt som inte ligger i aktörens intresse.
2. **Skada förhindras:** Skada förhindras för aktörens antagonister, eller för andra, på ett sätt som inte ligger i aktörens intresse.
3. **Nytta förhindras:** Nytta förhindras för aktören, eller för andra, på ett sätt som inte ligger i aktörens intresse.
4. **Nytta orsakas:** Nytta orsakas för aktörens antagonister, eller för andra, på ett sätt som inte ligger i aktörens intresse.

I delavsnittet Angrepp, i kapitlet Analys och bedömning av orsak och verkan nedan, presenteras en motsvarande uppsättning kategorier som är mer antagonistiskt betonade (det vill säga mer handlar om hur syftet respektive effekten av ett angrepp kan förstås):

1. **Skada orsakas:** Orsaka skada hos den aktör som angreppet genomförs gentemot, eller gentemot andra, via den aktör som angreppet genomförs gentemot.
2. **Nytta förhindras:** Förhindra nytta för den aktör som angreppet genomförs gentemot, eller för andra, via den aktör som angreppet genomförs gentemot.
3. **Nytta orsakas:** Orsaka nytta hos den aktör som genomför angreppet, eller hos andra, via den aktör som genomför angreppet.
4. **Skada förhindras:** Förhindra skada hos den aktör som genomför angreppet, eller hos andra, via den aktör som genomför angreppet.

De båda uppsättningarna av faktiska incidenter respektive faktiska risker ovan är designade för att passa utifrån ett allriskperspektiv (se delavsnittet Allriskperspektivet i det nästföljande avsnittet), respektive utifrån ett antagonismbetonat perspektiv och för att det ska gå att klassificera incidenter respektive risker på sätt som är säkerhetspolitiskt relevanta. Med ”säkerhetspolitiskt relevant” avses här att aktörer som har en antagonistisk relation till varandra (och som eventuellt opererar i ”gråzonen”) kan förväntas agera på sätt som maximerar den egna maktpositionen visavi andra aktörer. Det kan de göra på de ovan listade fyra sätten.

Se delavsnittet Introduktion till bedömning av säkerhetshändelser och faktiska incidenter/risker i kapitlet Bedömning och värderingnedan för en förklaring av hur säkerhetshändelser relaterar till faktiska incidenter respektive faktiska risker, och därigenom hur skada och nytta relateras till de sorters händelser (och därigenom de sorters objekt) som definierades i det föregående avsnittet.

En not om digitala leveranskedjeincidenter

I detta delavsnitt förklaras vad en incident i den digital leveranskedja är (se delavsnittet Digitala leveranskedjor och digitala produkter i avsnittet Övriga begrepp som är centrala för den strategiska cybersäkerhetsanalysen nedan). Sådana incidenter skiljer sig ifrån övriga incidenter på så vis att medan övriga incidenter inträffar hos och drabbar samma aktör eller organisation, så inträffar digitala leveranskedjeincidenter hos en organisation och drabbar såväl den som andra organisationer (sådana organisationer som är *mottagare av en digital tjänst* ifrån den organisation som har incidenten).

En incident i en digital leveranskedja definierades i Hoten mot de digitala leveranskedjorna[7] som:

1. *En händelse där något som:*
   a. *ska levereras i den digitala leveranskedjan (en framgångsfaktor eller ett skydd) inte levereras[8], eller*
   b. *inte ska levereras i den digitala leveranskedjan (ett hot eller ett hinder) ändå levereras, och*
2. *Där händelsen resulterar i antingen en oplanerad negativ påverkan eller en oönskad avsaknad av positiv påverkan på informationssystems, eller informationen i informationssystems, konfidentialitet, riktighet eller tillgänglighet.*

För att fullt ut fungera med den utveckling som har gjorts av den strategiska cybersäkerhetsanalysens metodik sedan dess definieras nu sådana incidenter enligt följande:

1. *En händelse där något som:*
   a. *ska levereras i den digitala leveranskedjan (en framgångsfaktor eller ett skydd) inte levereras (det vill säga uteblir), eller*
   b. *inte ska levereras i den digitala leveranskedjan (ett hot eller ett hinder) ändå levereras, och*
2. *Där händelsen resulterar i antingen en inträffad oönskade händelse eller en utebliven önskad händelse med avseende på informationssystems, eller informationen i informationssystems, konfidentialitet, riktighet eller tillgänglighet.*

Övriga begrepp som är centrala för den strategiska cybersäkerhetsanalysen

I detta avsnitt introduceras slutligen ytterligare begrepp som ofta används inom den strategiska cybersäkerhetsanalysens metodik, och som är nödvändiga att känna till för den som ska bedriva strategisk analys inom cybersäkerhetsområdet.

Konfidentialitet, riktighet och tillgänglighet

I detta delavsnitt förklaras begreppen konfidentialitet, riktighet och tillgänglighet. De tre begreppen (ofta kallade för ”cybersäkerhetstriaden”) är centrala för förståelsen av cybersäkerhetsområdet.

De tre begreppen konfidentialitet, riktighet och tillgänglighet är förmodligen några av de viktigaste inom hela cybersäkerhetsområdet. Det är utifrån de tre begreppen som cybersäkerhet förstås och analyseras. Ett vanligt språkbruk är att tala om att ett informationssystem, ett nätverk eller en informationsmängd ska

Not 7. MSB. Hoten mot de digitala leveranskedjorna: 50 rekommendationer för att stärka samhällssäkerheten. Stockholm: MSB, 2021. Länk: https://rib.msb.se/filer/pdf/29829.pdf.

Not 8. En händelse där något som ska levereras i den digitala leveranskedjan inte levereras är ett exempel på en indirekt incident, se avsnittet Fundamentala begrepp, delavsnittet Händelser som inträffar respektive uteblir ovan.

ha *rätt nivå* av konfidentialitet, riktighet respektive tillgänglighet. Det kan förstås som att:

Ett informationssystem, ett nätverk eller en informationsmängd har rätt nivå av:

- konfidentialitet om det är otillgängligt för obehöriga användare
- riktighet om det fungerar på det och endast det sätt som det ska respektive innehåller det och endast det som det ska
- tillgänglighet om det är tillgängligt för behöriga användare

Konfidentialitet och tillgänglighet är i många avseenden varandras motsatser. För att förstå de tre begreppen mer ingående kan man lista olika händelser som medför att informationssystem, nätverk eller en informationsmängd får fel nivå av konfidentialitet, riktighet och tillgänglighet. Nedbrytningen blir olika för informationssystem och nätverk å ena sidan, och informationsmängder å andra sidan.

Tabell 7. KRT-triaden för informationssystem

Konfidentialitet	Riktighet	Tillgänglighet
Behöriga användare har fått för höga behörigheter till informationssystem	Konfigurationer har lagts till i informationssystem	Behöriga användare har fått för låga behörigheter till informationssystem
Tillgång för obehöriga kan upprättas till informationssystem	Konfigurationer har ändrats i informations-system	Tillgång för behöriga användare kan inte upprättas till informationssystem
Obehöriga har tillgång till informationssystem	Konfigurationer har tagits bort i informationssystem	Avbrott har uppstått i behöriga användares befintliga tillgång till informationssystem
Information kan tas emot från obehöriga användare i informationssystem	Konfigurationer i infor-mationssystem har gjorts otillförlitliga	Information kan inte tas emot från behöriga använ-dare i informationssystem
Information från obehöriga användare kan behandlas i informationssystem	Informationssystemet utför inte uppgifter det ska utföra	Information från behöriga användare kan inte behandlas i informationssystem
Information från obehöriga användare kan skickas i informationssystem	Informationssystemet utför uppgifter det inte ska utföra	Information från behöriga användare kan inte skickas i informationssystem
Uppgifter utförs på obehörigas begäran i informationssystem	Informationssystemet utför inte uppgifter det är konfigurerat att utföra	Uppgifter utförs inte på behöriga användares begäran i informationssystem
Informationssystemet kan konfigureras av obehöri-ga användare	Informationssystemet utför uppgifter det inte är konfigurerat att utföra	Informationssystemet kan inte konfigureras av behöriga användare

En motsvarande nedbrytning av de tre begreppen för informationsmängder kan istället se ut som följer:

Tabell 8. Ibid

Konfidentialitet	Riktighet	Tillgänglighet
Behöriga användare har fått för höga behörigheter till informationsmängder	Information har lagts till i informationsmängder	Behöriga användare har fått för låga behörigheter till informationsmängder
Tillgång för obehöriga kan upprättas till informationsmängder	Information har ändrats i informationsmängder	Tillgång för behöriga användare kan inte upprättas till informationsmängder
Obehöriga har tillgång till informationsmängder	Information har tagits bort i informationsmängder	Avbrott har uppstått i behöriga användares befintliga tillgång till informationsmängder
-	Information har gjorts otillförlitlig i informationsmängder	-

Robusthet, resiliens och redundans

I detta delavsnitt förklaras begreppen robusthet, resiliens och redundans. De tre begreppen är centrala för förståelsen av vad säkerhet är och betyder, såväl som för bedömning av incidenter och risker och för att strategiskt välja åtgärder.

Robusthet

Intuitivt kan robusthet förstås som att objekt är robusta om de kan blockera hot och därför inte ta skada.

I den strategiska cybersäkerhetsanalysens metodik kan objekt vara robusta om de har skydd (som blockerar hot, varför skada inte orsakas – se avsnittet Faktiska incidenter och faktiska risker ovan respektive Analys av säkerhetshändelser och faktiska incidenter/risker nedan).

Exempel: En bil är robust om den har ett starkt chassi (ett skydd) som gör att den tål kollisioner (den första bemärkelsen ovan).

Resiliens

Intuitivt kan resiliens förstås som att objekt är resilienta om de kan återställa sig efter att ha tagit skada från hot de inte har kunnat blockera.

I den strategiska cybersäkerhetsanalysens metodik är objekt resilienta om de har framgångsfaktorer eller skydd som kan ersätta skadade framgångsfaktorer eller skydd, respektive om de har framgångsfaktorer som orsakar att objekt som har tagit skada (framgångsfaktorer eller skydd) återställs eller att nya motsvarande objekt uppstår.

Exempel: En bil som är utrustad med ett extrahjul kan få ett skadat hjul ersatt med extrahjulet och kan därigenom fortfarande köras.

Redundans

Intuitivt kan redundans förstås som att objekt är redundanta om det finns flera objekt med samma egenskaper och de kan ersätta varandra.

I den strategiska cybersäkerhetsanalysens metodik är objekt redundanta om de har samma framgångsfaktorer och skydd.

Exempel: Om det finns två bilar som båda är anpassade för körning i svår terräng och enbart en behövs så är den andra bilen redundant. En bil som inte är anpassad för körning i svår terräng kan enbart delvis vara redundant i förhållande till en bil som *är* anpassad till körning i svår terräng. Skälet till det är att båda bilarna kan köras på en vanlig väg (varför den ena kan ersätta den andra), men att bara den ena kan köras i svår terräng.

Tillämpning av de tre begreppen i cybersäkerhetssammanhang

I cybersäkerhetssammanhang förstås säkerhet för exempelvis en informationsmängd utifrån konfidentialitet, riktighet och tillgänglighet. Olika aktörer har olika behov av konfidentialitet, riktighet och tillgänglighet för olika informationsmängder i olika kontexter.

I en viss kontext är en viss informationsmängd robust för en viss aktör om den informationsmängden har den nivå av konfidentialitet, riktighet respektive tillgänglighet som den aktören behöver, och om den informationsmängden är skyddad så att hot inte kan förändra de nivåerna av konfidentialitet, riktighet respektive tillgänglighet.

På motsvarande sätt är en viss informationsmängd resilient för en viss aktör om den informationsmängdens nivå av konfidentialitet, riktighet respektive tillgänglighet, efter att ha tagit skada från ett hot som inte kunde blockeras, kan återställas till den nivå av konfidentialitet, riktighet respektive tillgänglighet som aktören behöver att informationsmängden har.

Slutligen är den informationsmängden redundant om det finns en kopia av informationsmängden som kan ersätta den om den skulle ta skada och inte kan återställas.

Cybersäkerhet

I detta delavsnitt presenteras ett sätt beskriva vad cybersäkerhet är och som bygger på begreppen som förklarats i de två föregående delavsnitten Konfidentialitet, riktighet och tillgänglighet, respektive Robusthet, resiliens och redundans.

Informationssystem, nätverk respektive informationsmängder kan anses vara *cybersäkra* om:

1. De har rätt nivå av konfidentialitet, riktighet och tillgänglighet.
2. De nivåerna är robusta och resilienta.
3. Det finns fler informationssystem, nätverk respektive informationsmängder med samma egenskaper som också uppfyller 1 och 2.

Vid sidan av begreppet cybersäkerhet betyder så är det också viktigt att känna till de fyra delområden som området ofta, inom ramen för den strategiska cybersäkerhetsanalysen, bryts ner i:

- **Informationssäkerhet:** Avser skydd av information.
- **It-säkerhet:** Avser skydd av it-system och deras funktionalitet.
- **Ot-säkerhet:** Avser skydd av ot-system[9] och deras funktionalitet.
- **Säkerhet i digitala leveranskedjor:** Avser skydd av organisationers nyttjande av information, mjukvara, hårdvara eller tjänster som levereras av andra organisationer.

Relationen mellan säkerhetshändelser och KRT-triaden

I detta delavsnitt förklaras relationen mellan säkerhetshändelser, som spelar en central roll i den strategiska cybersäkerhetsanalysens metodik, och KRT-triaden som är central inom cybersäkerhetsområdet i allmänhet.

Som framgår av det föregående delavsnittet så kan informationssystem, nätverk respektive informationsmängder anses vara *cybersäkra* om:

1. De har rätt nivå av konfidentialitet, riktighet och tillgänglighet.
2. De nivåerna är robusta och resilienta.
3. Det finns fler informationssystem, nätverk respektive informationsmängder med samma egenskaper som också uppfyller 1 och 2.

Säkerhetshändelser kan inverka på alla de tre ovanstående punkterna. Om informationssystem slutar att fungera (en säkerhetshändelse av typen framgångsfaktor upphör) och det inte finns andra informationssystem som har samma slags funktion (orsakar samma slags önskade händelser) så påverkas både informationssystemets riktighet och tillgänglighet (se tabell 7 i delavsnittet Konfidentialitet, riktighet och tillgänglighet ovan). Om en av flera brandväggar slutar att fungera

---

Not 9. Ot-system är en kortform för system för operativ teknik. Ett relaterat begrepp är ”cyberfysiska system”. Det handlar om sådan teknik som styr och upprätthåller fysiska processer (dammar, trafikledning, och så vidare.). Sådana system förekommer ofta exempelvis inom industrin.

(en säkerhetshändelse av typen skydd upphör) så minskar robustheten i nivån av konfidentialitet.

På motsvarande sätt kan förändringar avseende nivån av konfidentialitet, riktighet och tillgänglighet innebära att olika sorters säkerhetshändelser har skett. Om ett informationssystem blir otillgängligt för behöriga användare så kan det antingen innebära att informationssystemet har upphört att fungera (en säkerhetshändelse av typen ”framgångsfaktor upphör”) eller att informationssystemet har blivit blockerat (en säkerhetshändelse av typen ”hinder uppstår”).

Lägesbild, hotbild och normalbild

I detta delavsnitt presenteras tre begrepp som beskriver resultat som den strategiska cybersäkerhetsanalysen typiskt sett förväntas leverera.

En *lägesbild* är en bild av läget, ofta med avseende på en eller alla incidenter och/eller risker inom ramen för en *redogörelse* (se avsnittet Modellering av kontext i kapitlet Bedömning och värdering nedan).

En *hotbild* är en bild av de företeelser som kan orsaka att risker realiseras inom ramen för en redogörelse.

En *normalbild* är en bild av vad som är normalt som genereras utifrån en jämförelse av flera tidsmässigt separata lägesbilder. En *månadsvis* normalbild med avseende på en viss typ av incident kan exempelvis genereras genom att jämföra lägesbilder (med avseende på hur många gånger den typen av incident har inträffat respektive hur allvarlig respektive inträffad instans av den incidenten var) för varje månad under ett år.

Allriskperspektivet

I detta delavsnitt presenteras ett begrepp som är mycket viktigt för att förstå skillnaden i synen på vad som ska och inte ska inkluderas inom cybersäkerhetsområdet.

Allriskperspektivet är ett begrepp som beskriver ett sätt att ta sig an säkerhetsfrågor som innebär att alla oönskade händelser ska förebyggas och hanteras, och att alla orsaker till att oönskade händelser inträffar ska förebyggas och hanteras. Detta innebär att såväl angrepp som misstag, systemfel, naturhändelser och andra händelser alla utgör relevanta händelser att analysera, bedöma och förebygga.

Cybersäkerhet utifrån allriskperspektivet är förhållandevis ovanligt utanför EU. Det vanliga utanför EU är att cybersäkerhet endast handlar om att förebygga och hantera antagonistiska orsaker (angrepp). Andra orsaker till oönskade händelser i och kring informationssystem, nätverk respektive informationsmängder anses i sådana sammanhang inte ingå i cybersäkerhetsämnet.

Digitala leveranskedjor och digitala produkter

I detta delavsnitt presenteras ett begrepp som är centralt för att förstå hur enskilda incidenter kan resultera i kaskadeffekter som på olika sätt resulterar i störningar på samhällsnivå.

I Hoten mot de digitala leveranskedjorna[10] definierades en *digital leveranskedja* som följer:

> De tjänster och infrastrukturer som levererar eller möjliggör leverans av digitala produkter vilka används för att upprätta, upprätthålla, utveckla eller återställa en verksamhets informationshantering och informationssystem.

En *digital produkt* definieras i samma publikation som:

> En informationsmängd (som kan upprättas, lagras och bearbetas i informationssystem), mjukvara, hårdvara eller en tjänst (som upprätthålls, utvecklas och tillhandahålls via informationssystem).

I senare arbeten har digitala leveranskedjor istället definierats som:

> Det nät av leverantörer, tjänster, system och underleverantörer som tillsammans möjliggör en digital tjänst eller produkt.

Monoberoenden

I detta delavsnitt presenteras ett begrepp som är mycket viktigt för att förstå varför incidenter i digitala leveranskedjor kan hota samhället mycket mer än incidenter hos enskilda organisationer.

För att förstå vad ett monoberoende är krävs det att man först förstår vad ett beroende är. Ett beroende kan definieras som:

1. Något som en aktör har eller använder.
2. Något som aktören behöver ha eller använda.
3. Något som aktören inte kan ersätta eller har några alternativ till.

Ett monoberoende råder när många organisationer, exempelvis alla eller de flesta organisationer i ett land, eller inom en sektor, har ett beroende till samma digitala produkt (information, mjukvara, hårdvara eller tjänst).

Not 10. MSB. Hoten mot de digitala leveranskedjorna: 50 rekommendationer för att stärka samhällssäkerheten. Stockholm: MSB, 2021. Länk: https://rib.msb.se/filer/pdf/29829.pdf.

It-incidenthantering och cyberkrishantering

I detta delavsnitt presenteras två begrepp som är centrala för att förstå hur den strategiska cybersäkerhetsanalysen bidrar till operativ hantering.

It-incidenthantering består i att hantera, respektive stödja hanteringen, av it-incidenter. Hanteringen är koncentrerad till det som händer i domänen it-miljö, men berör delvis också det som händer i domänen organisations-/verksamhetsnivå (se delavsnittet Redogörelse för domän i kapitlet Bedömning och värdering nedan) samt kommunikation om det som händer i de domänerna.

Cyberkrishantering består i att hantera, respektive stödja hanteringen, av störningar och andra konsekvenser av it-incidenter. Hanteringen berör delvis det som händer i domänen organisations-/verksamhetsnivå, men är koncentrerad till det som händer i domänen samhällsnivå (se delavsnittet Redogörelse för domän i kapitlet Bedömning och värdering nedan) samt kommunikation om det som händer i de domänerna.

Medan it-incidenthantering koncentreras till att stödja den eller de som har en it-incident (och att informera andra om den it-incident) så handlar cyberkrishantering om att stödja den eller de som drabbas av effekterna av en it-incident. Uppdelningen kan förklaras med stöd av följande exempel:

Exempel: Incident i dricksvattenverk

En incident inträffar i it-systemet som styr filtreringen i ett vattenverk. Incidenten innebär att filtreringen avstannar. Vattenverket fortsätter att pumpa vatten. Orenat vatten sprids därför i det kommunala dricksvattennätet. Människor i området dricker av vattnet, och några blir sjuka.

I det här exemplet är *incidenten* den oönskade händelse som har inträffat i it-systemet som styr filtreringen i vattenverket. Förekomsten av kontaminerat vatten är en *störning i en samhällsviktig tjänst*. Människor som har insjuknat på grund av att de har druckit det kontaminerade vattnet är en *följdverkan* av en störning i en samhällsviktig tjänst.

De tre problemen (felet i filtreringssystemet, det kontaminerade vattnet och de förgiftade personerna) särskiljs då de utgör olika fenomen, som kräver olika typer av expertis för att hanteras.

Samtidigt förutsätter en effektiv hantering av följdverkan att de som arbetar med följdverkan är koordinerade med de som hanterar störningen. Om störningen kan hanteras snabbt så krävs kanske inte några omfattande åtgärder (såsom att flytta patienter med särskilda vårdbehov, begränsa restaurangverksamhet, och så vidare.), men om den kommer att ta lång tid att hantera så kanske sådana åtgärder krävs. På motsvarande sätt förutsätter en effektiv hantering av störningen att de som arbetar med störningen är koordinerade med de som hanterar incidenten. Om incidenten kan åtgärdas på kort tid så kan kanske vissa mer omfattande åtgärder undvikas, men om den tar lång tid att hantera så kanske mer omfattande åtgärder krävs.

Den strategiska cybersäkerhetsanalysens roll i cyberkrishanteringen handlar här om att analysera it-incidenten och omsätta analysen i information som underlättar och gör hanteringen av störningen respektive följdverkan mer effektiv. Några exempel på det kan bestå i att bedriva riskanalys för att identifiera möjliga ytterligare konsekvenser som inte tidigare har förutsetts, respektive att prognosticera hur lång tid hanteringen av it-incidenten kan tänkas ta, och därför vilka åtgärder som är mer eller mindre lämpliga.

Exempel: Incident i system där personuppgifter lagras

Ett intrång sker hos en leverantör av HR-tjänster. Under intrånget exfiltreras personuppgifterna som är lagrade i de HR-tjänster som leverantören tillhandahåller. Intrånget följs av att ransomware installeras i leverantörens it-miljö, varpå HR-tjänsten slutar att fungera.

I den del av it-incidenthanteringen som handlar om att ge stöd så går stödet bland annat ut på att forensiskt analysera systemen för att förstå hur intrånget genomfördes, och om att återställa system och informationsmängder som har infekterats med ransomware.

I den del av cyberkrishanteringen som handlar om att ge stöd så går stödet bland annat ut på att samla, och samlat ge ut stöd till de som drabbas av effekterna av intrånget respektive ransomwareangreppet. Det kan bestå i att samla råd och stöd för de som har fått skyddade personuppgifter röjda, eller de som kanske inte får ut sina löner i tid.

Den strategiska cybersäkerhetsanalysens roll i cyberkrishanteringen handlar här om att analysera it-incidenten och omsätta analysen i information som underlättar och gör hanteringen av störningen respektive följdverkan mer effektiv. Några exempel på det kan bestå i att bedriva riskanalys för att identifiera möjliga ytterliga konsekvenser som inte tidigare har förutsetts (såsom att identifiera att det kanske finns skyddade personuppgifter lagrade i tjänsten, och att röjandet av dem kan resultera i en förändrad hotbild mot de individer vars personuppgifter det är), respektive att prognosticera hur lång tid hanteringen av it-incidenten kan tänkas ta, och därför vilka åtgärder som är mer eller mindre lämpliga.

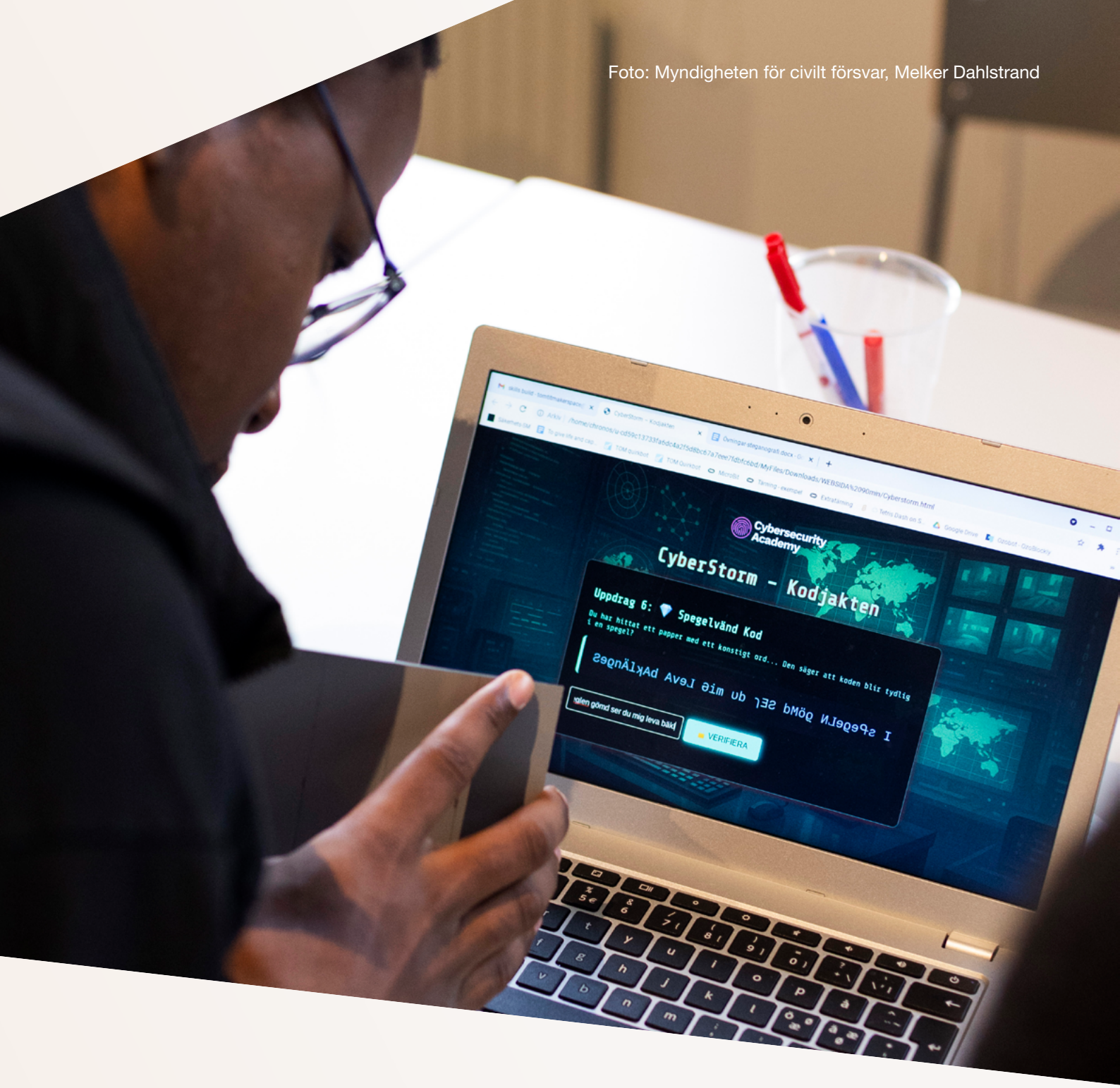

Foto: Myndigheten för civilt försvar, Melker Dahlstrand

Kapitel 4

Analys och bedömning av orsak och verkan

Analys och bedömning av orsak och verkan

I detta kapitel presenteras den andra delen i den strategiska cybersäkerhetsanalysens metodik. Kapitlet behandlar hur orsak och verkan (kausalitet) kan förstås, och tillämpar sedan den förståelsen tillsammans med den strategiska cybersäkerhetsanalysens begrepp för att strukturerat beskriva, analysera och bedöma incidenter och risker, bedöma orsaker till incidenter samt identifiera sårbarheter och åtgärder.

Kort om analys och bedömningar

I detta avsnitt redovisas centrala kunskapsteoretiska utgångspunkter för hur bedömningar ska göras.

Som noterades i kapitlet Om den strategiska cybersäkerhetsanalysen så skiljer man inom metodiken på *analys* och *bedömning*. Analys handlar om att avgöra hur världen faktiskt är beskaffad. Bedömning handlar om att utifrån tillgänglig information på ett rationellt sätt komma fram till en beskrivning av hur analytikern *tror* att världen är beskaffad.

Många gånger saknas tillräcklig information för att det ska vara helt säkert hur världen är beskaffad. I sådana lägen får istället bedömningar göras – och för att de ska kunna göras på ett rationellt sätt krävs det att den som ska göra bedömningen har en välgrundad uppfattning om tillförlitligheten i den information som finns tillgänglig.

Det finns tre centrala delar i att värdera information. Den ena är källkritik. Den strategiska cybersäkerhetsanalysen nyttjar Natos Admirality-system, se Bilaga: Källvärdering för mer information nedan. Den andra delen är argumentationsanalys. Oavsett om informationen kommer ifrån en i alla delar tillförlitlig källa eller inte måste eventuella argument som framförs analyseras och värderas. Den tredje delen handlar om att göra antaganden. Det ska alltid vara tydligt när ett antagande görs och varför just det antagandet görs (inklusive varför det antagandet, snarare än något annat antagande, görs).

Modellering av orsak och verkan

I detta avsnitt beskrivs hur kausalitet (orsak och verkan) övergripande kan förstås, och hur den förståelsen kan omsättas och modelleras på ett sätt som möjliggör analys av såväl orsaker till som konsekvenser av incidenter.

Kausalitet

I detta delavsnitt förklaras kausalitet (orsak och verkan) övergripande. Förklaringen ligger dels till grund för definitionerna av vad en mekanism respektive en komponent är i det nästföljande delavsnittet, och är dels central för förståelsen av innehållet i stora delar av de nästföljande avsnitten.

Kausalitet är det som gör att en viss händelse inträffar (ett objekt eller ett sakförhållande uppstår eller upphör, se avsnittet Primitiva begrepp ovan), respektive inte inträffar, som en verkan[11] (konsekvens) av en annan inträffad händelse. Det finns två typer av kausalitet; orsakande och förhindrande.

Endast det som finns (objekt) kan ha kausal effekt (verkan). Sårbarheter och brister, såväl som öppningar och lugn (se Begrepp för objekt och avsaknad av objekt ovan), kan därför inte orsaka något.[12]

Orsakande kausalitet: Fenomenet att vissa inträffade händelser med regelbundenhet[13] uppstår som en verkan (konsekvens) för att en viss, eller vissa, händelse(r) har inträffat.

Exempel: Om någon släpper ett objekt (en händelse) och det inte finns något mellan objektet och marken så kolliderar objektet med marken (en annan händelse). Kollisionen sker för att objektet släpptes, och det sker med regelbundenhet.

Förhindrande kausalitet: Fenomenet att vissa händelser med regelbundenhet *uteblir* som en verkan (konsekvens) av att en viss, eller vissa, händelse(r) har inträffat, *för* att en viss, eller vissa, händelse(r) har inträffat.

Exempel: Om någon släpper ett objekt (en händelse) och marken har täckts för (en händelse) marken så kolliderar inte objektet med marken (en utebliven händelse). Kollisionen med marken, som annars skulle ha inträffat, uteblir för att en annan händelse (att marken täcktes för) har inträffat innan objektet släpptes. Kollisionen uteblir därför med regelbundenhet.

Not 11. Därav uttrycket ”orsak och verkan”.

Not 12. Det är vanligt att rapportörer i sina incidentrapporter exempelvis skriver att okunskap var orsaken till att en medarbetare gjorde något. Det är inkorrekt. Det är möjligt att den medarbetaren hade agerat annorlunda om den hade haft mer kunskap, men det faktum att den inte hade den kunskapen kan inte vara orsaken till att den gjorde som den gjorde. Orsaken måste istället vara något annat. Detta är viktigt, för det är bara när den egentliga orsaken är känd som det blir möjligt att avgöra om mer kunskap hos medarbetaren hade lett till att medarbetaren hade valt att göra på något annat sätt än den gjorde.

Not 13. I bemärkelsen ”bundet av regler”, snarare än ”ofta”. Sådana regler kan bestå i naturlagar (som gravitationen) eller andra varaktiga fenomen.

Mekanismer och komponenter

I detta delavsnitt definieras mekanismer och komponenter. Genom att förstå mekanismer och komponenter så kan man representera kausala flöden och därför förstå hur en händelse orsakade en annan – något som är helt centralt för att kunna analysera incidenters orsaker respektive konsekvenser.

En *mekanism* är ett objekt, eller en samling av objekt (*komponenter*), som givet att en specifik typ av händelse (en *trigger*) sker

1. (förutsatt att inget annat förhindrar det) orsakar, eller
2. (förutsatt att inget annat orsakar det) förhindrar,

att en annan specifik typ av händelse sker. Detta kallas för mekanismens *funktion* och det är detta som *definierar* mekanismen. Exempelvis definieras ett ur av dess funktion, det vill säga att visa tiden.

Mekanismer består av en begränsad uppsättning komponenter som är ordnade på särskilda sätt. Komponenter är typer av objekt som behöver ingå i ett större objekt eller i samlingar av objekt för att det större objektet eller samlingen av objekt ska kunna orsaka, eller förhindra, den specifika typ av händelse som definierar mekanismen. Komponenter *bidrar* därför till att orsaka, eller förhindra, den specifika typ av händelse som definierar en specifik mekanism.

En *inkomplett mekanism* är ett objekt eller en samling objekt där minst en av en specifik typ av mekanisms komponenter saknas.

Mekanismer kan vara komponenter i andra mekanismer.

Ett exempel på en mekanism

Ett ur är en samling av objekt (urets komponenter, se bild) som, givet att ström tillförs eller att uret aktiveras på annat sätt (triggern) och givet att inget i eller omkring uret förhindrar det, orsakar att en tim- och en minutvisare med en specifik frekvens förflyttar sig runt en urtavla och därigenom visar en tidsangivelse (urets funktion).

Det som definierar den uppsättning saker som vi samlat kallar för ett ur är att de, om de ordnas på ett visst sätt och om man sätter i ett batteri med ström eller på annat sätt aktiverar uret, orsakar att urets visare rör på sig på urtavlan.

Urets komponenter, såsom dess visare och dess batteri, bidrar till att orsaka en tidsangivelse visas i uret.

Ett ur utan visare är ett inkomplett ur.

Ett ur kan vara en beståndsdel i en annan mekanism, till exempel en dator.

Automatik och mänskligt handlande

I detta delavsnitt görs en kort metodologisk utvikning om i vilken utsträckning människor kan förstås som mekanismer, något som är viktigt för representationer av kausala flöden där mänskligt handlande spelar en roll.

I den strategiska cybersäkerhetsanalysens metodik görs en skillnad på sådant som sker med automatik (det vill säga det som sker när en trigger-händelse aktiverar en mekanisms olika komponenter, varpå den händelse som det är mekanismens funktion att orsaka, orsakas) och sådant som sker genom att människor agerar och reagerar.

Människor är inte mekanismer i den bemärkelse som beskrivs i avsnittet Mekanismer och komponenter ovan (om samma slags trigger-händelse sker vid flera olika tidpunkter så kan en och samma människa vid varje givet sådant tillfälle välja vilken reaktion, om någon, som den vidtar i respons till triggerhändelsen). Människors agerande sker med andra ord inte med automatik.

Människor kan dock vara komponenter i en mekanism. En avstängd klocka kommer inte att kontinuerligt visa tiden om den inte först aktiveras, och aktiveringen kan ju utföras av en människa.

För mer information om hur mänskligt handlande kan förstås i förhållande till mekanismer och händelser, se avsnittet Skillnaden mellan konsekvenser och följder senare i kapitlet.

Analys och bedömning av incidenters orsaker och verkan

I detta avsnitt beskrivs hur incidenters orsaker och verkan kan analyseras och bedömas. Att analysera incidenter är en central del i arbetet med strategisk cybersäkerhetsanalys. I arbetet ingår att försöka förstå hur och varför en incident orsakades, samt vilka konsekvenser den orsakade, och hur och varför den orsakade de konsekvenserna.

Analys och bedömning av incidenters orsaker

I detta delavsnitt beskrivs hur incidenters orsaker kan representeras och förklaras genom mekanismer. Förklaringen återanvänds sedan i delavsnittet Sammanställd orsaks- och konsekvensanalys nedan.

Beskrivningar och förklaringar av orsak och verkan görs genom att beskriva den händelse som har inträffat, den mekanism som händelsen orsakades utifrån och den trigger som aktiverade mekanismen (se avsnittet Mekanismer och komponenter ovan).

När en incidents orsak ska beskrivas, förstås eller undersökas så anges därför incidenten (händelsen), hotet (mekanismen) och dess ingående komponenter och triggern. Beskrivningen görs typiskt sett i list- eller tabellformat enligt nedan.[14]

Utifrån den uppställda beskrivningen kan sedan det kausala flödet beskrivas.

Tabell 9. Mekanism för att förklara hur en incident kunde orsakas

Incidenten: Konfidentiell information exponeras
Orsaken till att incidenten inträffade (Hotet):
(3) **Komponent:** En internettjänst I som fritt tillhandahåller information på internet
(2) **Komponent:** En publiceringsfunktion F som automatiskt tar information från en databas och publicerar den i internettjänsten
(1) **Komponent och trigger:** En medarbetare lägger konfidentiell information i databasen

Not: Mekanismen (hotet) består av tre komponenter – medarbetaren, publiceringsfunktionen F och internettjänsten I.

Det kausala flödet: När konfidentiell information läggs i databasen (1) så tar F automatiskt den informationen och lägger den I (2), varpå informationen fritt finns tillgänglig att nå på internet (3).

Analys och bedömning av incidenters konsekvenser

I detta delavsnitt beskrivs hur incidenters konsekvenser kan representeras och förklaras genom mekanismer. Förklaringen återanvänds sedan i delavsnittet Sammanställd orsaks- och konsekvensanalys nedan.

Konsekvenser av en inträffad incident är händelser som har orsakats av den incidenten. Beskrivningar och förklaringar av hur och varför en viss konsekvens (i form av en ny incident) har kunnat orsakas av en incident görs därför på exakt samma sätt som beskrivningen och förklaringen av incidentens orsak. Det kan uppstå ett antal olika konsekvenser av incident, och de kan alla var för sig analyseras i varsin uppställning.

Not 14. Om incidentens orsak ska undersökas så kan det vara fallet att viss information som är nödvändig för att förstå mekanismen saknas. Det är också möjligt att information saknas om triggern. I sådana fall anges det som är känt, varpå uppställningen i listan eller tabellen kan användas för vidare efterforskningar.

Tabell 10. Mekanism för att förklara hur en incident kunde orsakas

En konsekvens av att incidenten inträffade (en ny incident): Konfidentiell information skickas till obehöriga
Orsaken till att konsekvensen av incidenten inträffade:
(6) **Komponent:** En spridningsfunktion P som sprider informationen den får av S i ett automatiserat utskick (såsom ett nyhetsbrev) till alla som har anslutit sig till P
(5) **Komponent:** En scrapingtjänst S som kopierar informationen i internettjänsten och delar den med en spridningsfunktion P
(4) **Komponent och trigger:** Internettjänsten I tillhandahåller den konfidentiella informationen

Not: Mekanismen (hotet) består av tre komponenter – internettjänsten I, scrapingtjänsten S och spridningsfunktionen P.

Det kausala flödet: I börjar tillhandahålla den konfidentiella informationen (4), S kopierar informationen i I och delar den med P (5), P skickar informationen till alla som har anslutit sig till P (6). Den nya incidenten har nu orsakats.

Sammanställd orsaks- och konsekvensanalys

I detta delavsnitt beskrivs hur beskrivningar av incidenters orsaker respektive incidenters konsekvenser kan kombineras för att därigenom förklara längre och mer komplexa händelseförlopp.

En fullständig analys av en incident inkluderar bl.a. en orsaksbeskrivning av incidenten, samt en beskrivning av vilka konsekvenser incidenten orsakade, och hur de kunde uppstå. En sådan analys kan sammanställas genom att respektive uppställning kopplas samman, med den ursprungliga incidenten först (till vänster), och alla de identifierade och analyserade konsekvensernas respektive uppställningar till höger om den.

Tabell 11. Sammanställd orsaks- och konsekvensanalys

Den ursprungliga incidenten: Konfidentiell information exponeras	Den nya incidenten: Konfidentiell information skickas till obehöriga
Orsaken till att incidenten inträffade (Hotet):	Orsaken till att konsekvensen av incidenten inträffade (Hotet):
(3) **Komponent:** En internettjänst I som fritt tillhandahåller information på internet	(6) **Komponent:** En spridningsfunktion P som sprider informationen den får av S i ett automatiserat utskick (såsom ett nyhetsbrev) till alla som har anslutit sig till P
(2) **Komponent:** En publiceringsfunktion F som automatiskt tar information från en databas och publicerar den i internettjänsten	(5) **Komponent:** En scrapingtjänst S som kopierar informationen i internettjänsten och delar den med en spridningsfunktion P
(1) **Komponent och trigger:** En medarbetare lägger konfidentiell information i databasen	(4) **Komponent och trigger:** Internet-tjänsten I tillhandahåller den konfiden-tiella informationen

Det kausala flödet: När konfidentiell information läggs i databasen (1) så tar F automatiskt den informationen och lägger den I (2), varpå informationen fritt finns tillgänglig att nå på internet (3). Den ursprungliga incidenten har nu orsakats. I börjar tillhandahålla den konfidentiella informationen (4), S kopierar informationen i I och delar den med P (5), P skickar informationen till alla som har anslutit sig till P (6). Den nya incidenten har nu orsakats.

Analys och bedömning av riskers orsaker och verkan

I detta avsnitt beskrivs hur riskers orsaker och verkan kan analyseras och bedömas. Att analysera och bedöma risker är också en central del i arbetet med strategisk cybersäkerhetsanalys. Som noteras i delavsnittet Begrepp för händelser i det föregående kapitlet så är framgångar och chanser, respektive incidenter och risker, två sidor av samma mynt. Analys av risker kan därför, med vissa variationer som beskrivs nedan, göras med samma metodik som används för att analysera incidenter.

Analys och bedömning av riskers orsaker

I detta delavsnitt beskrivs hur riskers orsaker kan representeras och förklaras genom mekanismer. Förklaringen återanvänds sedan i delavsnittet Sammanställd orsaks- och konsekvensanalys nedan.

En given möjlig händelse kan typiskt sätt orsakas på många olika sätt. Skillnaden mellan analyser av incidenters orsaker respektive analyser av riskers orsaker består därför i att analysen av en incidents orsak endast beskriver *en* mekanism (den mekanism som aktiverades och orsakade incidenten) och *en* trigger (den trigger

som aktiverade mekanismen varpå incidenten orsakades) medan analysen av en risks orsak(er) typiskt kommer att behöva bestå av flera olika mekanismer med varsina triggers. Precis vilka mekanismer och vilka triggers som aktuella i ett givet fall kommer att avgöras av kontexten som risken ska analyseras i. Samma mekanism kan dessutom ha olika triggers, vilket nedan exempel visar:

Tabell 12. Analys av flera orsaker till samma risk

Risken: Konfidentiell information exponeras	
Orsak 1 till att risken inträffar (Hot):	Orsak 2 till att risken inträffar (Hot):
(3) **Komponent:** En internettjänst I som fritt tillhandahåller information på internet	(6) **Komponent:** En internettjänst I som fritt tillhandahåller information på internet
(2) **Komponent:** En publicerings-funktion F som automatiskt tar information från en databas och publicerar den i internettjänsten	(5) **Komponent:** En publicerings-funktion F som automatiskt tar information från en databas och publicerar den i internettjänsten
(1) **Komponent och trigger:** En medarbetare lägger konfidentiell information i databasen	(4) **Komponent och trigger:** En tekniker omkonfigurerar F så att F hämtar information ifrån en annan databas och den databasen innehåller konfidentiell information

Det kausala flödet: När konfidentiell information läggs i databasen (1) så tar F automatiskt den informationen och lägger den I (2), varpå informationen fritt finns tillgänglig att nå på internet (3). Risken har nu realiserats på det första sättet. Efter att F har omkonfigurerats till att ta information ifrån en annan databas som innehåller konfidentiell information (4) så tar F automatiskt den informationen och lägger den i I (5), varpå informationen fritt finns tillgänglig att nå på internet (6). Risken har nu realiserats på det andra sättet.

Analys och bedömning av riskers konsekvenser

I detta delavsnitt beskrivs hur riskers konsekvenser kan representeras och förklaras genom mekanismer. Förklaringen återanvänds sedan i delavsnittet Sammanställd orsaks- och konsekvensanalys nedan.

En inträffad händelse kan orsaka många olika ytterligare händelser. Om händelsen inträffar i en viss kontext kan en viss uppsättning ytterligare händelser orsakas, om händelsen inträffar i en annan kontext kan eventuellt en annan uppsättning ytterligare händelser orsakas.

Skillnaden mellan analys och bedömning av incidenters konsekvenser respektive riskers konsekvenser är därför att medan kontexten är given när en incident ska analyseras (incidenten inträffade i ett visst sammanhang, på en viss plats, vid en viss tid, hos en viss organisation, och så vidare.) så behöver den definieras när en risk ska analyseras. En ytterligare skillnad är att incidenters konsekvenser inte

kan variera. Det som hände, hände. En risk som realiseras vid ett tillfälle kan ha en viss uppsättning konsekvenser och om samma risk sedan realiseras vid ett annat tillfälle så kan den ha en annan uppsättning konsekvenser – även om kontexten i flera avseenden är definierad (såsom att den inträffar inom samma organisation i båda fallen).

Individuella konsekvenser av att risken realiseras listas kolumnvis med samma metodik som i andra avsnitt enligt nedan:

Tabell 13. Analys av flera konsekvenser av samma risk

Risken: Konfidentiell information exponeras	
Konsekvens 1 (en ny risk) av att risken realiseras: Konfidentiell information skickas till obehöriga	Konsekvens 2 (en ny risk) av att risken realiseras: Omvärlden informeras om att informationen som har exponerats är konfidentiell
(9) **Komponent:** En spridningsfunktion P som sprider informationen den får av S i ett automatiserat utskick (såsom ett nyhetsbrev) till alla som har anslutit sig till P	(12) **Komponent:** En AI-tjänst A som analyserar informationen den får av C och därefter ställer samman och publicerar en analys på en nyhetssida i vilken det framgår att informationen som nu finns på I är konfidentiell
(8) **Komponent:** En scrapingtjänst S som kopierar informationen i internet-tjänsten och delar den med en spridningsfunktion P	(11) **Komponent:** En scrapingtjänst C som kopierar informationen i internet-tjänsten och delar den med en AI-tjänst A som bevakar och analyserar nyheter
(7) **Komponent och trigger:** Internettjänsten I tillhandahåller den konfidentiella informationen	(10) **Komponent och trigger:** Internettjänsten I tillhandahåller den konfidentiella informationen

Det kausala flödet: I börjar tillhandahålla den konfidentiella informationen (7), S kopierar informationen i I och delar den med P (8), P skickar informationen till alla som har anslutit sig till P (9). Konsekvens 1 av att risken realiseras nu också. I börjar tillhandahålla den konfidentiella informationen (10), C kopierar informationen i I och delar med A (11), A analyserar informationen, och ställer samman och publicerar en analys i vilken det framgår att den information som tillhandahålls i I är konfidentiell. Konsekvens 2 av att risken realiseras nu också.

Sammanställd orsaks- och konsekvensanalys

I detta delavsnitt beskrivs hur beskrivningar av incidenters orsaker respektive incidenters konsekvenser kan kombineras för att därigenom förklara längre och mer komplexa händelseförlopp.

En fullständig analys av en risk inkluderar bl.a. en beskrivning av riskens olika möjliga orsaker, samt en beskrivning av vilka konsekvenser risken skulle kunna få i den definierade kontexten, och hur de kan uppstå. En sådan analys kan sammanställas genom att respektive uppställning kopplas samman, med de olika sätt risken kan realiseras först (till vänster), och alla de identifierade och analyserade möjliga konsekvenserna av att risken realiseras till höger om dem.

Tabell 14. Sammanställd orsaks- och konsekvensanalys

Risken: Konfidentiell information exponeras			
Orsak 1 till att risken inträffar (Hot):	Orsak 2 till att risken inträffar (Hot):	Konsekvens 1 (en ny risk) av att risken realiseras: Konfidentiell information skickas till obehöriga	Konsekvens 2 (en ny risk) av att risken realiseras: Omvärlden informeras om att informationen som har exponerats är konfidentiell
(3) **Komponent:** En internettjänst I som fritt tillhandahåller information på internet	(6) **Komponent:** En internettjänst I som fritt tillhandahåller information på internet	(9) **Komponent:** En spridningsfunktion P som sprider informationen den får av S i ett automatiserat utskick (såsom ett nyhetsbrev) till alla som har anslutit sig till P	(12) **Komponent:** En AI-tjänst A som analyserar informationen den får av C och därefter ställer samman och publicerar en analys på en nyhetssida i vilken det framgår att informationen som nu finns på I är konfidentiell
(2) **Komponent:** En publiceringsfunktion F som automatiskt tar information från en databas och publicerar den i internettjänsten	(5) **Komponent:** En publiceringsfunktion F som automatiskt tar information från en databas och publicerar den i internettjänsten	(8) **Komponent:** En scrapingtjänst S som kopierar informationen i internettjänsten och delar den med en spridningsfunktion P	(11) **Komponent:** En scrapingtjänst C som kopierar informationen i internettjänsten och delar den med en AI-tjänst A som bevakar och analyserar nyheter
(1) **Komponent och trigger:** En medarbetare lägger konfidentiell information i databasen	(4) **Komponent och trigger:** En tekniker omkonfigurerar F så att F hämtar information ifrån en annan databas och den databasen innehåller konfidentiell information	(7) **Komponent och trigger:** Internettjänsten I tillhandahåller den konfidentiella informationen	(10) **Komponent och trigger:** Internettjänsten I tillhandahåller den konfidentiella informationen

En not om sannolikhet

I detta delavsnitt görs en utvikning om hur begreppet ”sannolikhet” kan förstås.

Inom vetenskaplig och analytisk praxis används olika tolkningar av sannolikhet. Två centrala perspektiv är *frekventistisk sannolikhet* och *epistemisk sannolikhet*. Den ena, som kan kallas för *frekventistisk sannolikhet* handlar om hur ofta, eller hur många gånger, vissa typer av händelser inträffar under ett visst tidsintervall. Mer precist avses den relativa frekvens med vilken en viss typ av händelse inträffar vid upprepade observationer under jämförbara förhållanden, typiskt sett över ett stort antal fall. Den andra, som kan kallas för *epistemisk* (kunskapsteoretisk) *sannolikhet* handlar om hur troligt ett visst påstående om hur världen är beskaffad är. Epistemisk sannolikhet avser därmed graden av osäkerhet eller tillit till ett påstående, givet tillgänglig information och kunskap.

Vid källvärdering (se Bilaga: Källvärdering nedan) och bedömningar av uppgifters tillförlitlighet tillämpas i huvudsak epistemisk sannolikhet, då dessa moment syftar till att värdera kunskap under osäkerhet. Inom exempelvis riskanalys då man bedömer att man har tillräckliga och relevanta data kan frekventistisk sannolikhet användas för att uppskatta hur ofta en typ av händelser inträffar.

Analys och bedömning av riskers förväntade skada

I detta delavsnitt görs en utvikning om hur riskers förväntade skada kan analyseras, bedömas och representeras. Medan analys av incidenter och risker har stora likheter i många avseenden så är en noterbar skillnad hur pass mycket mer komplext det är att avgöra skada av risker än det är av incidenter.

I avsnittet Begrepp för händelser ovan definieras risk som en oönskad händelse som kan inträffa (är möjlig). ”Kan inträffa” ska här förstås som att det kan variera hur många gånger risken kommer att inträffa.

Analys av risker och incidenter skiljer sig på så vis att en incident är en händelse som har inträffat. Analys, bedömning och klassificering av en incident görs därför mot bakgrund av det som har inträffat vid ett visst tillfälle. Analys, bedömning och klassificering av en risk görs istället mot en fastlagd tidslinje (se avsnitt Redogörelse för den tidsperiod som ska avhandlas nedan) under vilken risken eventuellt kan inträffa fler än en gång. Givet en tillräckligt lång tidsperiod kan därför en analys av risken som beskrivs i avsnitten ovan behöva utgå ifrån att det som beskrivs inträffar fler än en gång. En rigorös analys av risken går igenom varje sätt som risken kan realiseras på (de blåmarkerade kolumnerna i sammanställningen ovan) för att avgöra hur många gånger, och när, under den definierade tidsperioden som risken kommer att realiseras på just det sättet.[15] En kontroll görs också för att säkerställa att ingen dubbelräkning görs, det vill säga för att säkerställa att om risken realiseras på ett visst sätt och samtidigt på ett annat sätt så räknas detta endast en gång. En bedömning av risken måste utifrån

Not 15. En bedömning om frekventistisk sannolikhet görs alltså. Se delavsnittet En not om sannolikhet ovan.

den sammanställning som uppstår värdera den samlade skada som uppstår som ett resultat av att man lägger samman skadan som uppstår vid enskilda tillfällen.

I exemplet i tabell 14 i delavsnittet Sammanställd orsaks- och konsekvensanalys ovan kanske risken under ett kalenderår realiseras fyra gånger genom orsak 1, och ytterligare en gång genom orsak 2. En bedömning av risken sett till ett kalenderår blir då att risken totalt sätt kommer att realiseras fem gånger.

En *mindre* rigorös bedömning av skadan som risken förväntas medföra under kalenderåret kan göras utifrån en uppskattad eller konstaterad genomsnittlig skada vid varje tillfälle som risken realiseras. Den samlade skadan som risken medför under kalenderåret kan då beräknas genom att multiplicera antalet gånger risken kommer att realiseras med den skada risken medför varje gång den realiseras. Om skadan som risken genomsnittligt medför anges med s så skulle skadan som risken som beskrivs i exemplet ovan medför vara $5s$.

En *mer* rigorös bedömning av skadan som risken förväntas medföra under kalenderåret görs istället genom att först avgöra hur många gånger och när risken kommer att realiseras under kalenderåret. För varje identifierat tillfälle analyseras sedan skadan som skulle uppstå vid just det tillfället, inkluderat den skada som skulle uppstå genom de konsekvenser (se konsekvens 1 respektive konsekvens 2 i tabell 14 i delavsnittet Sammanställd orsaks- och konsekvensanalys ovan) som skulle uppstå vid just det tillfället (som tidigare har noterats så kanske en viss konsekvens enbart uppstår givet en viss kontext – och den kontexten kanske inte är fallet varje gång risken realiseras). I exemplet ovan skulle den samlade skadan som risken medför under kalenderåret då beräknas genom $s1 + s2 + s3 + s4 + s5$, där $s1$ är skadan vid det första tillfället risken realiseras, $s2$ är skadan vid det andra tillfället risken realiseras, och så vidare.

Skillnaden mellan konsekvenser och följder

I detta avsnitt görs en kort utvikning om skillnaden mellan sådana händelser som sker med automatik när något händer (konsekvenser) och sådana händelser som sker när människor reagerar på inträffade händelser (följder).

I exemplen i tidigare avsnitt beskrivs konsekvenser. Det är händelser som uppstår med automatik när trigger-händelser aktiverar mekanismer. Som framgår av avsnittet Automatik och mänskligt handlande ovan så räknas inte människor som mekanismer eftersom människor kan välja hur de agerar när en trigger-händelse inträffar, varför det en människa gör som respons på en trigger-händelse kan skilja sig åt från en gång till en annan.

När incidenter sker respektive när risker realiseras så reagerar människor. Ibland kan reaktionen i sig utgöra, eller leda till, att ytterligare incidenter inträffar eller att ytterligare risker realiseras. Då människor inte är mekanismer och deras reaktioner inte är automatiska responser som alltid ser likadana ut så utgör deras reaktioner inte *konsekvenser*. Incidenter respektive realiserade risker som har uppstått som ett resultat av en eller flera människors reaktioner på en tidigare incident eller realiserad benämns istället som *följder*.

Sårbarhetsanalys

I detta avsnitt presenteras ett centralt försteg i arbetet med att identifiera åtgärder. En central del i den strategiska cybersäkerhetsanalysen är att identifiera hur risker kan förebyggas och incidenter kan förhindras från att inträffa igen. Sårbarhet råder när ett skydd, som, om det fanns, skulle kunna förhindra att en risk realiseras. Identifierade sårbarheter kan med metodiken omsättas i lämpliga skyddsåtgärder. Detta avsnitt bör läsas i kombination med delavsnittet En not om sårbarheter i det föregående kapitlet.

En *mekanism* är ett objekt, eller en samling av objekt (*komponenter*), som givet att en specifik typ av händelse (en *trigger*) sker

1. (förutsatt att inget annat förhindrar det) orsakar, eller
2. (förutsatt att inget annat orsakar det) förhindrar,

att en annan specifik typ av händelse sker. Detta kallas för mekanismens *funktion*.

Hot är mekanismer, och det följer därför att ett sätt att hantera hot på är att identifiera sårbarheter (avsaknader av skydd) som, om de ersattes med skydd, skulle innebära att hotet inte längre kan orsaka en oönskad händelse.[16] Skydden som saknas förhindrar, eller bidrar till att förhindra, att komponenter i en mekanism tillsammans kan orsaka den oönskade händelsen. Det går typiskt sett att identifiera ett stort antal avsaknader för varje mekanism som ska analyseras. Nedan ges några exempel.

Not 16. Notera att begreppet ”sårbarhet” inte alltid används på just detta. Se avsnittet En not om sårbarheter ovan för mer om detta.

Tabell 15. Sårbarhetsanalys

Incidenten: Konfidentiell information exponeras
Orsaken till att incidenten inträffade (Hotet):
(3) **Komponent:** En internettjänst I som fritt tillhandahåller information på internet
(2) **Komponent:** En publiceringsfunktion F som automatiskt tar information från en databas och publicerar den i internettjänsten
(1) **Komponent och trigger:** En medarbetare lägger konfidentiell information i databasen
Avsaknad av skydd som hade kunnat förhindra att incidenten inträffade (sårbarheter):
(1*a) Avsaknad av kunskap bland medarbetarna om hur skyddsvärd information och databasen ska hanteras
(1*b) Avsaknad av funktion som blockerar tillägg i databasen utan godkännande från informationsägare
(2*) Avsaknad av kontroll i funktionen att informationsägaren har godkänt att den nya informationen publiceras

Not: (1*a) beskriver här att en avsaknad av skydd har identifierats med koppling till (1). Om medarbetarna hade information hur skyddsvärd information och databasen ska hanteras så kanske de skulle avstå ifrån att lägga konfidentiell information där. (1*b) beskriver en ytterligare avsaknad av skydd som har identifierats med koppling till (1). Om tillägg i databasen inte kunde genomföras utan att informationsägaren godkänner det först så skulle kanske informationsägaren avstått från att godkänna tillägg som innebär att konfidentiell information läggs in där. (2*) beskriver en avsaknad av skydd som har identifierats med koppling till (2). Om det krävdes godkännande av informationsägaren för att information som F hämtar ifrån databasen ska kunna publiceras i I så skulle kanske informationsägaren avstått från att just konfidentiell information publiceras i I.

Analys och bedömning av åtgärder för att förebygga risk och hantera incidenter

I detta avsnitt presenteras en trestegsmetod som syftar till att säkerställa att åtgärder, inklusive de som identifieras med stöd av sårbarhetsanalysen i det föregående avsnittet, är lämpliga, effektiva och fullständiga sett till det som skulle uppnås. Det är genom analysen som presenteras här som den strategiska cybersäkerhetsanalysen kan användas för att inrikta arbete med åtgärder som utförs av professioner som har ansvar för att närmare designa och genomföra åtgärder.

Det finns tre typer av åtgärder som kan vidtas för att förhindra att en oönskad händelse inträffar:

- **Borttagande:** Endast det som finns (objekt) kan ha kausal verkan (se avsnittet Kausalitet ovan). Om hotet som orsakar den oönskade händelsen upphör att existera så kommer därför inte den oönskade händelse att orsakas (såvida det inte finns fler hot som orsakar samma slags oönskade händelse).

- **Förändring:** Om mekanismen som utgör hotet förändras, det vill säga om minst en komponent i mekanismen som utgör hotet upphör att existera eller förändras så blir mekanismen inkomplett (se avsnittet Mekanismer och komponenter ovan) varför den oönskade händelse som mekanismen annars skulle ha orsakat inte orsakas (såvida det inte finns fler hot som orsakar samma slags oönskade händelse).
- **Blockering:** Om mekanismen som utgör hotet blockeras, det vill säga om mekanismen tillförs ett objekt som blockerar minst en komponent i mekanismen från att fylla sin funktion, så kommer inte den oönskade händelse som mekanismen annars skulle ha orsakat att orsakas (såvida det inte finns fler hot som orsakar samma slags oönskade händelse).

I analysen av åtgärder ingår att värdera åtgärdstyperna utifrån följande principiella utgångspunkter:

- **Lämplighet:** Vilka åtgärder kan genomföras och är acceptabla att genomföra givet nödvändiga hänsyn (såsom alternativkostnader, ekonomiska resonemang, och så vidare).
- **Effektivitet:** För respektive komponent i hotet avgöra vilken eller vilka sorts/er åtgärd/er som skulle vara mest effektiv/a med avseende på att förhindra att den oönskade händelsen inträffar.
- **Fullständighet:** Vilka åtgärder eller kombinationer av åtgärder som behövs för att i tillräckligt hög utsträckning säkerställa att den oönskade händelsen inte kan ske, eller inte kan ske lika ofta.
- Utifrån p. 1–3 sammanställa den mest optimala uppsättningen åtgärder.

Om man tillämpar ovanstående resonemang på incidenten som har analyserats i tidigare avsnitt så uppstår följande möjligheter:

Tabell 16. Första steget i åtgärdsanalysen – uppställning av handlingsalternativ

Incidenten: Konfidentiell information exponeras
Orsaken till att incidenten inträffade (Hotet):
(3) **Komponent:** En internettjänst I som fritt tillhandahåller information på internet **Handlingsalternativ:** Ingen, ta bort, förändra, blockera.
(2) **Komponent:** En publiceringsfunktion F som automatiskt tar information från en databas och publicerar den i internettjänsten **Handlingsalternativ:** Ingen, ta bort, förändra, blockera.
(1) **Trigger:** En medarbetare lägger konfidentiell information i databasen **Handlingsalternativ:** Ingen, ta bort, förändra, blockera.

Incidenten: Konfidentiell information exponeras
Avsaknad av skydd som hade kunnat förhindra att incidenten inträffade (sårbarheter):
(1*a) Avsaknad av kunskap bland medarbetarna om hur skyddsvärd information och databasen ska hanteras
(1*b) Avsaknad av funktion som blockerar tillägg i databasen utan godkännande från informationsägare
(2*) Avsaknad av kontroll i funktionen att informationsägaren har godkänt att den nya informationen publiceras

Not: För varje komponent i hotet finns fyra handlingsalternativ: Att inte göra något, att ta bort komponenten, att förändra komponenten eller att blockera komponenten.

Åtgärders lämplighet

I detta delavsnitt presenteras det första av de tre testen för åtgärder: Lämplighetsprincipen. Vid tillämpning av lämplighetsprincipen på exemplet från avsnittets inledning ovan kanske resultatet blir som följer:

Tabell 17. Andra steget i åtgärdsanalysen – test av åtgärders lämplighet

Incidenten: Konfidentiell information exponeras
Orsaken till att incidenten inträffade (Hotet):
(3) **Komponent:** En internettjänst I som fritt tillhandahåller information på internet **Handlingsalternativ:** Ingen, ~~ta bort~~, ~~förändra~~, ~~blockera~~.
(2) **Komponent:** En publiceringsfunktion F som automatiskt tar information från en databas och publicerar den i internettjänsten **Handlingsalternativ:** Ingen, ~~ta bort~~, ~~förändra~~, blockera.
(1) **Trigger:** En medarbetare lägger konfidentiell information i databasen **Handlingsalternativ:** Ingen, ta bort, förändra, blockera.
Avsaknad av skydd som hade kunnat förhindra att incidenten inträffade (sårbarheter):
(1*a) Avsaknad av kunskap bland medarbetarna om hur skyddsvärd information och databasen ska hanteras
(1*b) Avsaknad av funktion som blockerar tillägg i databasen utan godkännande från informationsägare
(2*) Avsaknad av kontroll i funktionen att informationsägaren har godkänt att den nya informationen publiceras

Not: Handlingsalternativ som ~~överstrukits~~ bedöms i exemplet inte utgöra lämpliga åtgärder i förhållande till komponenten de står under. Exempelvis är alla åtgärdstyperna överstrukna under (3). I det här exemplet skulle det kunna vara för att internettjänsten är ett företags primära inkomstkälla. Om den tas bort så kommer företaget inte att överleva. Motsvarande kanske även gäller för en blockering. En förändring av internettjänsten kanske hade varit möjlig, men skulle exempelvis kunna vara mycket teknisk komplex, och därför olämplig av det skälet.

Exemplet illustrerar något viktigt: Mekanismer som orsakar att händelser sker kan vara både hot och framgångsfaktorer på samma gång. I exemplet tjänar företaget pengar på internettjänsten, och intresse för internettjänsten skapas genom att den successivt försörjs med information enligt det förfarande som beskrivs i uppställningen. Så länge som *rätt* information läggs i databasen så är det inte något problem för företaget att information automatiskt publiceras i internettjänsten.

På motsvarande sätt kan mekanismer som förhindrar att händelser sker vara både hinder och skydd på samma gång.

Åtgärders effektivitet

I detta delavsnitt presenteras det andra av de tre testen för åtgärder: Effektivitetsprincipen. Om man tillämpar effektivitetsprincipen ovan på de handlingsalternativ som återstår i uppställningen från det föregående delavsnittet efter att olämpliga handlingsalternativ har sållats bort så kanske resultatet blir följande:

Tabell 18. Tredje steget i åtgärdsanalysen – test av åtgärders effektivitet

Incidenten: Konfidentiell information exponeras
Orsaken till att incidenten inträffade (Hotet):
(3) **Komponent:** En internettjänst I som fritt tillhandahåller information på internet **Handlingsalternativ:** Ingen, ~~ta bort~~, ~~förändra~~, ~~blockera~~.
(2) **Komponent:** En publiceringsfunktion F som automatiskt tar information från en databas och publicerar den i internettjänsten **Handlingsalternativ:** Ingen, ~~ta bort~~, ~~förändra~~, blockera.
(1) **Trigger:** En medarbetare lägger konfidentiell information i databasen **Handlingsalternativ:** Ingen, ta bort, förändra, blockera.
Avsaknad av skydd som hade kunnat förhindra att incidenten inträffade (sårbarheter):
(1*a) Avsaknad av kunskap bland medarbetarna om hur skyddsvärd information och databasen ska hanteras
(1*b) Avsaknad av funktion som blockerar tillägg i databasen utan godkännande från informationsägare
(2*) Avsaknad av kontroll i funktionen att informationsägaren har godkänt att den nya informationen publiceras

Not: Handlingsalternativ som understrukits bedöms i exemplet utgöra effektiva åtgärder i förhållande till komponenten de står under. Om både understrukna och inte understrukna typer av åtgärder finns kvar att välja efter att lämplighetsprincipen har tillämpats så väljs företrädesvis de understrukna typerna av åtgärder. I det här fallet har åtgärdstypen ”förändra” under (1) inte understrukits. I det här exemplet skulle det kunna vara för att företaget har en stor personalomsättning och att varje enskild medarbetare endast då och då arbetar med konfidentiell information och databasen. Det skulle innebära att det blir dyrt att åtgärda sårbarheten (1*a) genom att arrangera utbildningar då det är många som ska utbildas, och att utbildningen kanske inte blir effektiv då medarbetarna inte kommer att öva på att arbeta på rätt sätt, och att därigenom repetera sina kunskaper, så ofta.

Åtgärders fullständighet

I detta delavsnitt presenteras det tredje av de tre testen för åtgärder: Fullständighetsprincipen. Om man rensar uppställningen från det föregående delavsnittet så att endast sådana åtgärder som anses vara lämpliga att genomföra listas så kan man slutligen göra en samlad bedömning utifrån fullständighetsprincipen:

Tabell 19. Fjärde steget i åtgärdsanalysen – test av åtgärders fullständighet

Incidenten: Konfidentiell information exponeras
Orsaken till att incidenten inträffade (Hotet):
(3) **Komponent:** En internettjänst I som fritt tillhandahåller information på internet **Handlingsalternativ:** Ingen.
(2) **Komponent:** En publiceringsfunktion F som automatiskt tar information från en databas och publicerar den i internettjänsten **Handlingsalternativ:** Blockera.
(1) **Trigger:** En medarbetare lägger konfidentiell information i databasen **Handlingsalternativ:** Ta bort, förändra, blockera.
Avsaknad av skydd som hade kunnat förhindra att incidenten inträffade (sårbarheter):
(1*a) Avsaknad av kunskap bland medarbetarna om hur skyddsvärd information och databasen ska hanteras
(1*b) Avsaknad av funktion som blockerar tillägg i databasen utan godkännande från informationsägare
(2*) Avsaknad av kontroll i funktionen att informationsägaren har godkänt att den nya informationen publiceras

Not: I sådana fall där ingen av åtgärdstyperna ta bort, förändra eller blockera anses lämpliga blir valet automatiskt ingen åtgärd.

Åtgärden *blockera* under (2) kan genomföras genom att sådan kontroll som saknas enligt (2*) införs. Åtgärden *ta bort* under (1) kan genomföras genom att vissa medarbetare inte längre tillåts arbeta med konfidentiell information eller hantera databasen. Åtgärden *blockera* under (1) kan genomföras genom att en sådan funktion som saknas enligt (1*b) införs.

I den totala uppsättningen åtgärder som återstår efter lämplighetstestet har tre av fyra åtgärdstyper bedömts klara effektivitetstestet, varför det är motiverat att först analysera om de tre effektiva åtgärderna samlat klarat fullständighetstestet, det vill säga att avgöra om de tillsammans ger ett tillräckligt skydd. De möjliga utfallen är:

1. Tillsammans utgör de tre åtgärderna ett tillräckligt skydd.
2. Tillsammans utgör de tre åtgärderna inte ett tillräckligt skydd.
3. Ett tillräckligt skydd kan uppnås utan att alla de tre åtgärderna behöver genomföras.

Om utfallet blir som i 1 ovan så utgör de tre åtgärderna de som ska föreslås. Om utfallet blir som i 2 ovan så får antingen den kvarstående, mindre effektiva, åtgärden läggas till i uppsättningen, varpå ett nytt fullständighetstest görs, eller så får ett arbete vidtas med att identifiera ytterligare åtgärder och sedan göra om analysen igen, eller så får det accepteras att endast ett otillräckligt skydd kan införas. Om utfallet blir som i 3 ovan så får antingen olika kombinationer av några av de identifierade åtgärderna analyseras utifrån lämplighet, varpå den mest optimala kombinationen väljs, eller så får det accepteras att fler åtgärder än som behövs införs.

Bedömning av incidenters och riskers orsaker

I detta avsnitt presenteras de kriterier som den strategiska cybersäkerhetsanalysen följs för att avgöra vad för typ av triggerhändelse det är som orsakar en oönskad händelse. Triggerhändelser delas in i angrepp, misstag, systemfel, naturhändelser och övriga händelser. I takt med att det säkerhetspolitiska läget i omvärlden har förvärrats har behovet av att kunna avgöra om inträffade händelser har eller inte har orsakats av angrepp ökat. Många gånger kommer inte tillräckliga fakta att finns tillgängliga för att fastställa vilken kategori som är den korrekta, varför först antaganden och därefter bedömningar måste göras istället.

Som framgår av avsnittet Mekanismer och komponenter ovan så orsakas händelser av att mekanismer vars funktion det är att, om de aktiveras genom att en trigger-händelse inträffar, orsaka sådana händelser. Att ange en faktor som en orsak till en händelse kan därför vara vanskligt. Även om vissa fakta, såsom att trigger-händelsen var resultatet av mänskligt handlande, så räcker inte det i sig för att avgöra om det handlandet var ett misstag eller ett angrepp.

I det här avsnittet beskrivs hur kategorierna angrepp, misstag, systemfel och naturhändelse ska förstås, vilka fakta som behövs för att fastslå att trigger-händelsen kan kategoriseras på ett visst sätt – och därigenom vilka antaganden som måste göras om sådana fakta inte finns tillgängliga och inte kan inhämtas.

Angrepp

Detta avsnitt syftar till att introducera de kriterier som behöver mötas för att en triggerhändelse ska kunna bedömas vara ett angrepp. Avsnittet omfattar också kriterier och analysstöd som kan användas för att bilda hypoteser om en angripares syfte, respektive för att avgöra om ett angrepp var lyckat eller inte. Med stöd av kriterierna görs också en kort utvikning om hur begreppet ”cyberhot” kan förstås. Avsnittet är hämtat, med vissa justeringar, ifrån rapporten Cyberangrepp mot samhällsviktiga informationssystem.[17]

Kriterier för att bedöma att en händelse är ett angrepp

En triggerhändelse i form av en mänsklig handling som orsakar en incident i domänen it-miljö (se delavsnittet Redogörelse för domän i det nästföljande kapitlet) räknas alltså som ett angrepp om:

1. aktören som utför handlingen inte har rätt att utföra handlingen (*legalitetsvillkoret*),
2. handlingen resulterar i en interaktion, konfigurering, installation/sparande, avinstallation/raderande eller överbelastning i något av målets informationssystem, eller i informationssystem som aktören som drabbas av handlingen nyttjar (*praktikvillkoret*),
3. handlingen resulterar i minst en för målet oönskad konsekvens i termer av konfidentialitet, riktighet eller tillgänglighet i aktören som drabbas av handlingens informationssystem, i informationssystem som målet nyttjar, eller information som finns i sådana informationssystem (*incidentvillkoret*), och
4. aktören som utför handlingen utför den i antagonistiskt syfte (*uppsåtsvillkoret*), det vill säga aktören utför handlingen i syfte att:
    a. Orsaka skada hos den aktör som angreppet genomförs gentemot, eller gentemot andra, via den aktör som angreppet genomförs gentemot.
    b. Förhindra nytta för den aktör som angreppet genomförs gentemot, eller för andra, via den aktör som angreppet genomförs gentemot.
    c. Orsaka nytta hos den aktör som genomför angreppet, eller hos andra, via den aktör som genomför angreppet.
    d. Förhindra skada hos den aktör som genomför angreppet, eller hos andra, via den aktör som genomför angreppet.[18]

Not 17. MSB. Cyberangrepp mot samhällsviktiga informationssystem – 25 rekommendationer för stärkt skydd mot cyberangrepp. Stockholm: MSB, 2024. Länk: https://rib.msb.se/filer/pdf/30558.pdf.

Not 18. Notera att de fyra villkoren här är en antagonistiskt fokuserad variant av definitionerna av faktisk incident som först presenteras i delavsnittet Faktiska incidenter och faktiska risker i kapitlet Begrepp och begreppssystem ovan.

Legalitetsvillkoret uppfylls när angriparen saknar en legal rätt att utföra en handling inom ramen för interaktionen. Obehöriga ska begränsas att ta del av eller göra ändringar i informationssystem med hjälp av tekniska säkerhetslösningar för åtkomstkontroll och autentisering. Om informationssystemets komponenter saknar adekvat skydd kan det dock finnas flera sätt för en angripare att ta del av, ändra eller blockera tillgången till information utan en legal rätt att vidta sådana åtgärder. I vissa fall kan angripare dessutom upptäcka sätt att ta sig förbi de skydd som finns. I de fall där hotet kommer inifrån den egna organisationen eller där angriparen lyckats tillskansa sig giltiga inloggningsuppgifter på annat sätt, och därmed har teknisk tillgång, är exempel på scenarion där angriparen har teknisk behörighet, men saknar legal rätt. Legalitetsvillkoret möjliggör, exempelvis, en åtskillnad mellan cyberangrepp och penetrationstest.

Praktikvillkoret uppfylls när interaktionen mellan angriparen och målet utgör en eller flera händelser. En händelse inom sammanhanget innebär att angriparens handlande, inom ramen för interaktionen, måste ha resulterat i att något upphört, uppstått eller ändrats inom målets it-miljö. Händelsen kan till exempel bestå i att skadlig kod installerats, att digitala informationstillgångar har raderats, att information har kopierats eller att it-komponenter har konfigurerats om.

Incidentvillkoret uppfylls när interaktionen mellan angriparen och målet resulterat i en eller flera incidenter i målets informationssystem. För att kunna förstås som ett cyberangrepp måste händelsen ha orsakat it-miljöpåverkan. It-miljöpåverkan kan inom sammanhanget bestå i att ett informationssystems eller relaterad infrastrukturs tillgänglighet, riktighet eller konfidentialitet äventyras, förändras eller upphör. Ett cyberangrepp kan exempelvis resultera i att informationstillgångar eller informationssystem blir otillgängliga för målet eller blir tillgängliga för en obehörig part, alternativt att konfigurationer eller informationstillgångar obehörigen manipuleras. Konsekvensvillkoret innebär att händelser som uppstått i samband med interaktionen mellan angriparen och målet, men som inte resulterat i någon negativ påverkan för målet, inte förstås som ett cyberangrepp i sammanhanget. Ett sådant händelseförlopp bör istället förstås som ett misslyckat cyberangreppsförsök.

Uppsåtsvillkoret uppfylls när angriparen i ett antagonistiskt syfte initierar interaktionen med målet. I delavsnittet Angriparens syfte nedan förtydligas att angriparen kan ha flera övergripande motiv till att utföra cyberangreppet. Oavsett syfte så är ett antagonistiskt uppsåt fundamentalt för att en interaktion som uppfyller resterande villkor ska kunna klassas som ett cyberangrepp snarare än ett misstag. Detta då it-incidenter som uppstår som en konsekvens av ett misstag, både på grund av okunskap eller oaktsamhet, i praktiken kan resultera i samma typer av händelseförlopp som ett angrepp. Om en individ som saknar behörighet konfigurerar en it-komponent med konsekvensen att delar av ett informationssystem blir otillgängligt, men samtidigt saknar ett antagonistiskt syfte, utgör handlingen ett misstag och inte ett cyberangrepp.

Angriparens syfte

Angriparen har alltid ett syfte med att utföra ett cyberangrepp mot målet. Angriparens övergripande syfte styr både vilken typ av aktör som kan vara ett potentiellt mål för angreppet och vilka typer av angreppsmetoder som angriparen kommer använda för att nå måluppfyllelse. Som tidigare specificerats kan målet utgöra en individ eller organisation. Om angriparens syfte är att missgynna en stat eller gynna en annan stat kan flera organisationer som på ett eller annat sätt bidrar till samhällets funktionalitet utgöra mål för angriparen.

Målet för cyberangreppet behöver inte vara den angriparen huvudsakligen vill påverka. Det finns även situationer då en aktör kan bli ett mål för ett angrepp på grund av att angriparen vill påverka användare av målets tjänster. Detta återspeglas i de fyra kategorierna av uppsåt som beskrivs punkt 4 (uppsåtsvillkoret) i det föregående delavsnittet.

Enligt uppsåtsvillkoret går det att dela in cyberangreppets uppsåt i olika typfall. Det kan handla om att:

Att *förhindra* nytta för målet eller hos andra via målet. Att nytta förhindras innebär att viss aktivitet eller produktion avstannar eller fördröjs. En angripare som önskar att nytta förhindras verkar efter målsättningen att organisationen som utgör målet inte ska kunna nyttja informationssystem och andra it-komponenter som möjliggör viss aktivitet eller produktion. Det kan handla om göra det svårt eller omöjligt för organisationen att nyttja centrala informationssystem, och därav påverka hela organisationen, eller enstaka tjänster. En angripares syfte kan också tänkas vara att förhindra nytta för andra individer, organisationer eller stater *via* målet för angreppet. Om syftet är att förhindra kommunikation för allmänheten så skulle målet för angreppet exempelvis kunna vara en telekomoperatör. Exempel på metoder som angriparen skulle kunna använda sig av i syfte att förhindra nytta inkluderar överbelastningsangrepp som försvårar eller omöjliggör transmissionen av legitim datatrafik till och från angripna nätverkskomponenter.

Att *orsaka skada* för målet eller hos andra via målet. En angripare som önskar att skada orsakas målet kan exempelvis verka för att kritiska informationstillgångar eller funktionalitet förstörs alternativt att känsliga informationstillgångar röjs. Skadan som angriparen ämnar orsaka kan vara av både materiell och immateriell art. Exempelvis skulle en angripares syfte kunna vara att orsaka både ekonomisk förlust eller mänskligt fysiskt och psykiskt lidande. Angriparen kan också ämna att orsaka skada för en individ, organisation eller stat via målet för angreppet. Om angriparens syfte är att orsaka skada för samhället i stort kan detta innebära att samhällsviktiga tjänster blir mål för angreppet. Cyberangrepp kan exempelvis utföras i syfte att skapa misstro bland användare av en angripen tjänst, såväl som leverantören av tjänsten. Det bör noteras att ett cyberangrepp som endast orsakar att nytta förhindras för målet kan leda till att skada orsakas för andra organisationer och allmänheten i nästa led. Om angriparen genom att utföra ett cyberangrepp exempelvis lyckas med att temporärt slå ut produktionen hos en elproducent kan det orsaka skada för både allmänheten och de organisationer som är beroende av eltillförseln. Metoder som angriparen skulle kunna använda sig av för att orsaka skada inkluderar skadlig kod såsom så kallade ”wiper-program” som vid exekvering raderar informationstillgångar i det informationssystem som har blivit infekterat.

Att *orsaka nytta* för angriparen eller hos andra som angriparen stödjer.
En angripare som ämnar gynna sig själv kommer att genomföra cyberangrepp för att amplifiera sin egen förmåga eller sitt välstånd. Det kan handla om att extrahera känsliga informationstillgångar från målet eller att tjäna pengar. Det kan också handla om cyberangrepp som utförs i syfte att införliva delar av den angripna it-miljön inom den egna produktionen. En angripare som ämnar orsaka nytta åt någon som angriparen stödjer på bekostnad av målet kan tänkas utföra underrättelseaktivitet som kan gynna denne. Exempel på angreppsmetoder som angriparen kan använda vändas i syfte att orsaka nytta åt sig själv eller någon den stödjer är att installera spionprogram eller ett program för kryptomining[19] inom målets it-miljö som kan användas för att extrahera känslig information respektive utvinna kryptovaluta. Även utpressningsprogram används i detta syfte. Angriparen kräver då målet på en lösensumma i utbyte mot krypteringsnycklar som kan dekryptera informationstillgångar som angriparen krypterat.

Att *förhindra skada* för angriparen eller andra som angriparen stödjer.
En angripare som vill förhindra motparten från att orsaka angriparen, eller andra som angriparen stödjer, skada kommer verka efter målsättningen att negativt påverka informationssystem eller informationstillgångar som skulle kunna användas till detta syfte. Aktörer som blir mål för dessa typer av angrepp har en förmåga att agera på ett sådant sätt som kan orsaka skada. Det kan exempelvis röra sig om institutioner som arbetar med brottsbekämpning eller nyhetspublicering. Om angriparen stödjer en statlig aktör eller beväpnad gruppering skulle det även kunna handla om att slå ut eller störa offensiv militär förmåga. Angreppsmetoder som angriparen kan tänkas nyttja i syfte att förhindra skada korrelerar ofta med metoder som skulle kunna användas för att förhindra nytta eller orsaka skada för ett mål. En angripare som vill förhindra publiceringen av viss information skulle exempelvis kunna installera en wiper inom målets informationssystem för att i förebyggande syfte radera information som identifierats som skadlig.

Not 19. Både spionprogram och kryptominers är exempel på skadlig programvara. Spionprogram kan används för att överföra information om exempelvis användaraktivitet från målet till angriparen. Kryptominers kan installeras på offrets dator i syfte att använda processorkraften till att utvinna kryptovaluta.

Antagonistiska cyberhot

Utifrån beskrivningen av cyberangrepp och antagonism (angriparens syfte) ovan går det att beskriva begreppet cyberhot. Ett *hot* definieras i denna rapport som något som orsakar, eller bidrar till att orsaka, en incident. Ett *cyberhot* är ett hot som på något sätt interagerar med ett informationssystem och kan orsaka en incident i ett sådant informationssystem. Med stöd av de resonemang som har förts i de två föregående avsnitten kan definitionen av hot preciseras och ramas in för att karakterisera att cyberhot på följande vis:

Ett cyberhot är ett hot som kan användas för att uppfylla praktikvillkoret och incidentvillkoret i beskrivningen av ett cyberangrepp ovan. Ett cyberhot är, med andra ord, något som genom, eller genom att bidra till, interaktion med, konfiguration av, installation/sparande i, avinstallation/raderande i eller överbelastning av ett informationssystem (*praktikvillkoret*) orsakar, eller bidrar till att orsaka, en oönskad konsekvens i termer av konfidentialitet, riktighet eller tillgänglighet i en organisations informationssystem, eller i informationssystem som organisationen nyttjar, eller information som finns i sådana informationssystem (*incidentvillkoret*), såvida inte åtgärder för att stoppa en sådan effekt vidtas.

Ett *antagonistiskt cyberhot* kan utifrån det föregående avsnittets resonemang förstås som ett cyberhot som används eller kan förväntas användas av en angripare i ett antagonistiskt syfte.

Ibland talas det om avancerade eller kvalificerade cyberhot. Ett sätt att förstå avancerade cyberhot är som en delmängd av sådana företeelser som ryms inom den föreslagna definitionen av cyberhot ovan. Ett första sätt att avgränsa sådana cyberhot är att ställa ett ytterligare villkor om att sådana cyberhot, såvida inte åtgärder vidtas för att stoppa dem, orsakar *faktiska incidenter*. En faktisk incident definieras i denna rapport som en inträffad oönskad händelse där:

1. *Skada orsakas* för organisationen, eller för andra organisationer, i konflikt med organisationens intresse.
2. *Skada förhindras* för organisationens antagonister, eller för andra organisationer, i konflikt med organisationens intresse.
3. *Nytta förhindras* för organisationen, eller för andra organisationer, i konflikt med organisationens intresse.
4. *Nytta orsakas* för organisationens antagonister, eller för andra organisationer, i konflikt med organisationens intresse.

Ett ytterligare sätt att avgränsa delmängden är att sätta som villkor att avancerade cyberhot ska ha en förmåga att övervinna eventuella motåtgärder som sätts in mot dem. Dels i fråga om upptäckt, och dels i fråga om hantering. Det finns tre sätt att oskadliggöra en företeelse som utgör ett hot: få företeelsens som utgör hotet att upphöra att existera (radera), att förändra företeelsen som utgör hotet så att företeelsen inte längre har hotande egenskaper (förändra) och att blockera hotet så att det som hotas inte kan påverkas av hotet.

Med utgångspunkt i ovan skulle därmed ett *avancerat cyberhot* kunna definieras som:

1. Ett cyberhot som orsakar, eller bidrar till att orsaka, en faktisk incident,
2. som har skydd mot försök att upptäcka, radera eller förändra det, och
3. som har funktioner som gör att skydd som sätts upp för att blockera cyberhotet blir helt eller delvis verkningslösa.

Lyckade och misslyckade cyberangrepp

Ett cyberangrepp kan ses som ”lyckat” utifrån angriparens synvinkel om syftet med angreppet uppfylls. Tabell 20 nedan beskriver hur måluppfyllelsen nås utifrån angriparens syfte att *orsaka skada* eller att *förhindra nytta* hos målet eller hos andra via målet, alternativt genom att *orsaka nytta* eller *förhindra skada* för sig själv, eller för andra för vilkas räkning angriparen genomför angreppet.

Den stora utmaningen gällande kategorisering av effekten av ett cyberangrepp är att information om effekterna eller påverkan av cyberangreppet av olika skäl sällan är tillgänglig eller offentlig. Detta innebär att vissa antaganden måste göras, vilket medför en viss grad av osäkerhet och subjektivitet.

Tabell 20. Bedömning av huruvida ett cyberangrepp är lyckat eller misslyckat

Övergripande syfte/effekt	Orsaka skada hos den som angrips, eller hos andra, via den som angrips	Förhindra nytta hos den som angrips, eller hos andra, via den som angrips	Orsaka nytta för den som angriper, eller för andra, för vilkas räkning angriparen genomför angreppet	Förhindra skada för den som angriper, eller för andra, för vilkas räkning angriparen genomför angreppet
Orsaka skada hos den som angrips, eller hos andra, via den som angrips	Måluppfyllelse	Påverkan, men inte måluppfyllelse	Påverkan, men inte måluppfyllelse	Påverkan, men inte måluppfyllelse
Förhindra nytta hos den som angrips, eller hos andra, via den som angrips	Påverkan, men inte måluppfyllelse	Måluppfyllelse	Påverkan, men inte måluppfyllelse	Påverkan, men inte måluppfyllelse
Orsaka nytta för den som angriper, eller för andra, för vilkas räkning angriparen genomför angreppet	Påverkan, men inte måluppfyllelse	Påverkan, men inte måluppfyllelse	Måluppfyllelse	Påverkan, men inte måluppfyllelse
Förhindra skada för den som angriper, eller för andra, för vilkas räkning angriparen genomför angreppet	Påverkan, men inte måluppfyllelse	Påverkan, men inte måluppfyllelse	Påverkan, men inte måluppfyllelse	Måluppfyllelse
Ingen	Misslyckande	Misslyckande	Misslyckande	Misslyckande

Med stöd av tabell 20 ovan kan ett *lyckat cyberangrepp* definieras som ett cyberangrepp där *måluppfyllelse uppnåtts* och utefter fyra kategorier:

1. **Lyckat vårdslöst cyberangrepp:** Alla former av påverkan är tillåtna.
2. **Lyckat kontrollerat cyberangrepp:** Enbart vissa specifika andra former av påverkan är tillåtna.
3. **Lyckat återhållsamt cyberangrepp:** Enbart ett visst antal andra former av påverkan är tillåtna.
4. **Lyckat precist cyberangrepp:** Ingen annan form av påverkan är tillåten.

Misstag

Detta avsnitt syftar till att introducera de kriterier som behöver mötas för att en triggerhändelse ska kunna bedömas vara ett misstag. Därutöver omfattar avsnittet också en kort utvikning om en av de vanligaste typerna av misstag (och som ofta resulterar i allvarliga incidenter).

Kriterier för att bedöma att en händelse är ett misstag

Detta delavsnitt presenterar de kriterier som ska uppfyllas för att en orsak till en incident eller en risk ska räknas som ett misstag.

Mänskligt handlande som orsakar incidenter eller att risker realiseras, och som uppfyller legalitetsvillkoret, praktikvillkoret och incidentvillkoret men inte uppsåtsvillkoret som listas i avsnittet Angrepp ovan räknas i den strategiska cybersäkerhetsanalysen som misstag. En triggerhändelse i form av en mänsklig handling som orsakar en incident i domänen it-miljö (se delavsnittet Redogörelse för domän i det nästföljande kapitlet) räknas alltså som ett misstag om:

1. Aktören som utför handlingen inte har rätt att utföra handlingen (*legalitetsvillkoret*),
2. Handlingen utgör ett utbyte av information som resulterar i en interaktion, konfigurering, installation/sparande, avinstallation/raderande eller överbelastning i något av målets informationssystem, eller i informationssystem som målet nyttjar (*praktikvillkoret*),
3. Handlingen resulterar i minst en för målet oönskad konsekvens i termer av konfidentialitet, riktighet eller tillgänglighet i målets informationssystem, i informationssystem som målet nyttjar, eller information som finns i sådana informationssystem (*incidentvillkoret*), och
4. Aktören som utför handlingen *inte* utför den i antagonistiskt syfte (*det omvända uppsåtsvillkoret*), det vill säga aktören utför inte handlingen i syfte att:
    a. orsaka skada hos den aktör som handlingen utförs hos eller gentemot, eller hos eller gentemot andra, via aktören,
    b. förhindra nytta hos aktören, eller hos eller gentemot andra aktörer, via aktören,
    c. orsaka nytta hos aktören, eller hos eller gentemot andra aktörer, som aktören stödjer,
    d. förhindra skada hos aktören, eller hos eller gentemot andra aktörer, som aktören stödjer.

Det är viktigt att förstå att detta medför att visst mänskligt handlande som i vardagliga sammanhang inte nödvändigtvis skulle räknas som ett misstag gör det enligt den strategiska cybersäkerhetsanalysens metodik. Ett exempel på det är att legalitetsvillkoret kräver att mänskligt handlande, för att räknas som angrepp, måste vara otillåtet, eller något som utföraren inte har rätt att utföra.

Mänskligt handlande som varken är angrepp eller misstag hör hemma i kategorin Övrigt, se delavsnittet Övrigt nedan.

Ändringshantering

Detta delavsnitt gör en kort utvikning om en av de vanligaste typerna av misstag, och som har resulterat i några av de mest allvarliga incidenterna.

En vanlig form av misstag som orsakar (utgör trigger-händelser) för incidenter är ändringshantering. Ändringshantering som av misstag orsakar incidenter är inte angrepp då det inte finns något antagonistiskt syfte (handlandet uppfyller därför inte uppsåtsvillkoret). Ändringshantering är typiskt sett, men inte alltid, också tillåtet, varför handlandet inte uppfyller legalitetsvillkoret.

Systemfel

Detta avsnitt syftar till att introducera de kriterier som behöver mötas för att en triggerhändelse ska kunna bedömas vara ett systemfel.

Trigger-händelser som inte är ett direkt resultat av mänskligt handlande (oavsett om det handlar om ett angrepp eller ett misstag) och som utspelar sig enbart i informationssystem och nätverk, eller i system som försörjer informationssystem och nätverk, räknas som systemfel.

Kriterier för att bedöma att en händelse är ett systemfel

Detta delavsnitt presenterar de kriterier som ska uppfyllas för att en orsak till en incident eller en risk ska räknas som ett systemfel. En triggerhändelse utgör ett systemfel om den orsakar en incident i domänen it-miljö (se delavsnittet Redogörelse för domän i det nästföljande kapitlet) och triggerhändelsen:

1. Inte utgörs av mänskligt handlande.
2. Inte utgörs av en naturhändelse.
3. Resulterar i en interaktion, konfigurering, installation/sparande, avinstallation/raderande eller överbelastning i något av målets informationssystem, eller i informationssystem som målet nyttjar (*praktikvillkoret*).
4. Resulterar i minst en för aktören oönskad konsekvens i termer av konfidentialitet, riktighet eller tillgänglighet i aktörens informationssystem, i informationssystem som aktören nyttjar, eller information som finns i sådana informationssystem (*incidentvillkoret*).

Exempel på systemfel kan vara uppkomna kompatibilitetsproblem, certifikat som går ut, autonoma AI-modeller interagerar med mekanismer på felaktiga sätt, och så vidare.

Naturhändelser

Detta avsnitt syftar till att introducera de kriterier som behöver mötas för att en triggerhändelse ska kunna bedömas vara ett systemfel.

Trigger-händelser som inte är ett direkt resultat av mänskligt handlande och som inte enbart utspelar sig i informationssystem och nätverk, eller i system som försörjer informationssystem och nätverk, räknas som naturhändelser.

Kriterier för att bedöma att en händelse är en naturhändelse

Detta delavsnitt presenterar de kriterier som ska uppfyllas för att en orsak till en incident eller en risk ska räknas som en naturhändelse. En triggerhändelse utgör en naturhändelse om den orsakar en incident i domänen it-miljö (se delavsnittet Redogörelse för domän i det nästföljande kapitlet) och triggerhändelsen:

1. Inte utgörs av mänskligt handlande.
2. Inte utgörs av ett systemfel.
3. Resulterar i en interaktion, konfigurering, installation/sparande, avinstallation/raderande eller överbelastning i något av målets informationssystem, eller i informationssystem som målet nyttjar (*praktikvillkoret*).
4. Resulterar i minst en för aktören oönskad konsekvens i termer av konfidentialitet, riktighet eller tillgänglighet i aktörens informationssystem, i informationssystem som aktören nyttjar, eller information som finns i sådana informationssystem (*incidentvillkoret*).
5. Består i händelser som inträffar som en följd av naturlagar, exempelvis i form av fysiska, kemiska eller biologiska förhållanden.

Exempel på naturhändelser är regn, stormar, värmeböljor, jordbävningar, iskyla, solstormar, blixtnedslag, översvämningar, meteoritnedslag, och så vidare. En fullständig lista över naturfenomen återfinns i United Nations Office for Disaster Risk Reduction (UNDRR)[20] definitions- och klassifikationslista.[21]

Not 20. FN:s organ för katastrofriskreducering.

Not 21. United Nations Office for Disaster Risk Reduction, & International Science Council. UNDRR–ISC Hazard Definition & Classification Review: 2025 Update of the Technical Report. Genéve, Schweiz: United Nations Office for Disaster Risk Reduction, Paris, Frankrike: International Science Council 2025. Länk: https://doi.org/10.24948/2025.04.

Övrigt

Detta avsnitt syftar till att introducera de kriterier som behöver mötas för att en triggerhändelse ska kunna bedömas vara en övrig händelse.

Kriterier för att bedöma att en händelse är en naturhändelse

Detta delavsnitt presenterar de kriterier som ska uppfyllas för att en orsak till en incident eller en risk ska räknas som en övrig händelse.

En triggerhändelse utgör en övrig händelse om den orsakar en incident i domänen it-miljö (se delavsnittet Redogörelse för domän i det nästföljande kapitlet) och triggerhändelsen:

1. Inte är ett angrepp eller ett misstag (se delavsnitten Angrepp respektive Misstag ovan).
2. Inte är ett systemfel (se delavsnittet Systemfel ovan).
3. Inte är en naturhändelse (se delavsnittet Naturhändelser ovan).
4. Resulterar i en interaktion, konfigurering, installation/sparande, avinstallation/raderande eller överbelastning i något av målets informationssystem, eller i informationssystem som målet nyttjar (*praktikvillkoret*).
5. Resulterar i minst en för aktören oönskad konsekvens i termer av konfidentialitet, riktighet eller tillgänglighet i aktörens informationssystem, i informationssystem som aktören nyttjar, eller information som finns i sådana informationssystem (*incidentvillkoret*).

Exempel på kategorier av övriga händelser är mänskligt handlande som (till skillnad från angrepp och misstag) aktören som utför handlingen *har* rätt att utföra (det omvända legalitetsvillkoret) och som i övrigt uppfyller villkoren ovan. Ett konkret exempel på en sådan händelse är om en leverantör av en tjänst stänger ner sin tjänst på grund av konkurs.

Foto: Myndigheten för civilt försvar, Mikael Svensson

Kapitel 5

Bedömning och värdering

Bedömning och värdering

I detta kapitel presenteras den tredje delen i den strategiska cybersäkerhetsanalysens metodik. Den här delen av metodiken handlar om hur förutsättningar skapas för att göra bedömningar och värderingar samt hur bedömning och värdering av händelser som säkerhetshändelser och faktiska incidenter eller faktiska risker ska göras.

Kort om bedömningar och värdering

I detta avsnitt presenteras några viktiga kunskapsteoretiska utgångspunkter när värdering ska göras.

Som noterades i kapitlet Om den strategiska cybersäkerhetsanalysen så skiljer man inom metodiken på *analys* och *bedömning*. Analys handlar om att avgöra hur världen faktiskt är beskaffad. Bedömning handlar om att utifrån tillgänglig information på ett rationellt sätt komma fram till en beskrivning av hur analytikern *tror* att världen är beskaffad. Därutöver omfattar också den strategiska cybersäkerhetsanalysen *värdering*, främst i form av att den behöver kunna användas för att på ett strukturerat sätt avgöra hur allvarliga oönskade händelser inom dess omfång är.

Medan analys och bedömning handlar om hur världen är beskaffad respektive vad som är rimligt att tro om hur världen är beskaffad så handlar värdering om att resonera normativt och att göra normativa omdömen (typiskt sett i form av att avgöra *hur allvarligt* eller *hur problematiskt* något är). Värderingen som utförs inom den strategiska cybersäkerhetsanalysen handlar främst om att avgöra allvarlighetsgraden hos oönskade händelser.

Ju ”tyngre” det normativa omdömet, desto starkare blir förväntan om att något ska göras. Det är därför viktigt att normativa omdömen baseras på en förutsägbar, strukturerad metodik.

Modellering av kontext

I detta avsnitt presenteras hur kontext kan modelleras för att skapa förutsättningar för bedömningar. I avsnittet Analys och bedömning av riskers konsekvenser ovan noterades att kontext är viktigt för att kunna analysera vilka konsekvenser som kan uppstå som en följd av att risker realiseras. Kontext är också avgörande för att kunna göra bedömningar. Det måste vara tydligt vad det är som ska bedömas eller klassificeras.

För att uppnå sådan tydlighet krävs två saker: En beskrivning av det som *ska* bedömas, och en beskrivning av det som *inte* ska bedömas – det vill säga en avgränsning. En kombination av en beskrivning och en avgränsning kallas för en *redogörelse*.

Den strategiska cybersäkerhetsanalysen delar typiskt sett in det som ska analyseras i tre domäner: It-miljö, verksamhet och samhälle. Händelser kan utspela sig inom alla tre domänerna, men måste utspela sig i åtminstone it-miljön för att vara inom omfånget för den strategiska cybersäkerhetsanalysen.

Inom ramen för domänindelningen görs, som minst, redogörelser av följande:

1. Den eller de it-miljöer, verksamhet(er) och/eller samhälle(n) som incidenten/erna eller risken/erna ska analyseras, bedömas och klassificeras inom.
2. Den eller de incident(er) eller risk(er) som ska analyseras, bedömas och klassificeras.
3. Den tidsperiod som incidenten/erna eller risken/erna ska analyseras, bedömas och klassificeras inom.

Kombinationen av de ovan nämnda redogörelserna utgör en *samlad redogörelse för kontexten*.

Redogörelse för domän

I detta delavsnitt presenteras konceptet ”domän”, en viktig del i alla kontextbeskrivningar som förutsätts för att bedömningar ska kunna göras inom den strategiska cybersäkerhetsanalysen. De tre domänerna är:

It-miljö: Den domän där sådana oönskade händelser som analyseras inom ramen för den strategiska cybersäkerhetsanalysen först uppstår. Domänen omfattar informationssystem, nätverk, digitala leveranskedjor, ot-system, och annan teknik. Inom domänen avgränsas det som ska bedömas typiskt till en it-miljö hos en enda organisation eller aktör, men det är inte nödvändigt att göra en sådan avgränsning. Exempel på sådant som kan ske i domänen och som kan utögra oönskade händelser är konfigurering, installation/sparande, avinstallation/raderande eller överbelastning. Vid bedömning av oönskade händelser inom den här domänen är det ofta avgörande om det finns tekniska resurser som kan ersätta sådana informationssystem eller annan teknik som har påverkats av en incident.

Organisation/verksamhet: Den domän där människor med stöd av it-miljön utför verksamhet. Domänen omfattar människor, arbetssätt, interna flöden, tjänster som tillhandahålls, och så vidare. Inom domänen avgränsas det som ska bedömas typiskt sett till verksamhet hos en enda organisation eller aktör (i taget), men det är inte nödvändigt att göra en sådan avgränsning. Vid bedömning av oönskade händelser inom den här domänen är det ofta avgörande om det alternativa arbetssätt som kan ersätta sådana arbetssätt som har påverkats av en incident.

Samhälle: Den domän där organisationer med stöd av sina it-miljöer och sina arbetssätt tillhandahåller sina tjänster. Domänen omfattar tjänster, infrastruktur, flöden mellan organisationer, och så vidare. Inom domänen avgränsas det som ska bedömas typiskt sett till en viss tjänst (som kan erbjudas av en enda, eller flera, organisationer), men det är inte nödvändigt att göra en sådan avgränsning. Vid bedömning av oönskade händelser inom denna domän är det ofta avgörande om en viss typ av tjänst tillhandahålls av en eller flera organisationer. Om endast en organisation erbjuder tjänsten och denna drabbas av en incident, blir tjänsten helt otillgänglig. Om däremot flera organisationer erbjuder samma typ av tjänst finns möjligheten att fortsatt använda tjänsten via en annan aktör. Det är därför centralt att bedöma om tjänsten kan ersättas av motsvarande tjänster från andra organisationer.

I en redogörelse måste det framgå vilken eller vilka domäner som inkluderas i bedömningen, och att alla andra inte ingår i bedömningen. På motsvarande sätt måste det framgå vilken eller vilka verksamhet(er), samt vilket eller vilka samhällen som inkluderas, och att resten inte inkluderas. Bedömningen eller klassificeringen görs sedan *enbart* på det som ingår i redogörelsen.

För att en oönskad händelse ska vara inom den strategiska cybersäkerhetsanalysens omfång krävs det att den, åtminstone, utspelar sig i domänen it-miljö. Om en oönskad händelse inte innebär att något oönskat sker i domänen it-miljö så kan den oönskade händelsen inte räknas som en cybersäkerhetsrelaterad incident.

Redogörelse för den incident eller den risk som analyseras

I detta delavsnitt preciseras vad som behöver klargöras i en redogörelse avseende den oönskade händelse som ska bedömas.

Incidenter och risker är händelser. Konsekvenser av incidenter respektive risker är också händelser. Incidenter/risker och deras respektive konsekvenser är dock *separata* händelser. I avsnittet Analys och bedömning av riskers orsaker och verkan i det föregående kapitlet ovan analyseras först risken att konfidentiell information exponeras. Två konsekvenser av risken att konfidentiell information exponeras analyseras också, dels att konfidentiell information skickas till obehöriga och dels att omvärlden informeras om att informationen som har exponerats är konfidentiell. Totalt sett är detta tre *separata* händelser. De måste därför analyseras, bedömas och klassificeras var för sig. En samlad bedömning av en incident eller risk och några eller samtliga av dess konsekvenser kan göras utifrån de individuella bedömningarna av incidenten/risken samt respektive konsekvens, se delavsnittet Samlade bedömningar av incidenter och deras konsekvenser och följder nedan.

Redogörelse för den tidsperiod som ska avhandlas

I detta delavsnitt preciseras vad som behöver klargöras i en redogörelse avseende den tidsperiod som ska bedömas. Medan den aktuella tidsperioden ofta är relativt tydlig för incidenter, så är den ofta inte det för risker.

Incidenter inträffar, pågår och avslutas under fastställda tidsperioder. Analyser och bedömningar av incidenter har därför givna tidsförhållanden att utgå ifrån. Risker har inte det. Att ha en lämplig fastlagd tidslinje att utgå ifrån är viktigt vid analys, bedömning och klassificering av risker av tre skäl:

1. **När en risk realiseras kan vara avgörande för vilka konsekvenser den får.** Om exempelvis löneutbetalningssystem fallerar precis innan löner ska betalas ut och avbrottet pågår vid löneutbetalningstillfället så är det allvarligare än om sådana system fallerar vid någon annan tidpunkt och hinner återställas innan löneutbetalningstillfället. Om risker kopplade till ett sådant system analyseras under en tidsperiod som inte inkluderar ett löneutbetalningstillfälle så kommer avgränsningen att resultera i att risken bedöms som mindre allvarlig.
2. **En risk kan realiseras flera gånger.** En viss risk kanske typiskt realiseras en gång i januari och tio gånger i juni. En analys, bedömning och klassificering av risken där tidsperioden endast är januari, respektive en där analysen bedömningen och klassificeringen endast är i juni respektive en där tidsperioden täcker hela året får alla olika bedömningar.
3. **Om risker ska jämföras med varandra så bör jämförelsen utgå ifrån en lämplig tidsperiod.** Om en viss risk typiskt sett realiseras två gånger i januari och sedan inte alls under resten av året, medan en annan risk realiseras en gång i månaden under hela året så bör de två riskerna, i typfallet, inte jämföras inom ramen för en tidsperiod som endast inkluderar januari.

Bedömning och värdering av incidenters och riskers allvarlighetsgrad

I detta avsnitt beskrivs hur incidenters och riskers allvarlighetsgrad kan bedömas med stöd av de redogörelser som har beskrivits i det föregående avsnittet. Bedömningen görs i en skala med stegen måttlig, betydande, allvarlig och kritisk och som beskriver hur mycket av en faktisk incident eller en faktisk risk händelsen utgör inom respektive domän. När en samlad redogörelse för kontexten är fastställd så är det tydligt vad som ska bedömas.

I detta avsnitt introduceras den strategiska cybersäkerhetsanalysens ramverk för bedömningar. Avsnittet omfattar fem delavsnitt. Det inleds med en introduktion till hur händelser kan analyseras och bedömas som säkerhetshändelser, och hur säkerhetshändelser kan analyseras och bedömas som faktiska incidenter respektive faktiska risker. Syftet är att presentera hur resonemangen kan föras på en intuitiv nivå, innan en mer precis genomgång av hur analysen och bedömningarna ska genomföras tar vid. Därefter följer en genomgång av hur bedömningens nivåer och kriterier kan tillämpas inom var och en av de tre domänerna som presenterades i det föregående avsnittet, först på säkerhetshändelser och därefter på faktiska incidenter respektive faktiska risker. Efter det redogörs för hur en och samma händelse kan bedömas i alla tre domänerna. Slutligen beskrivs hur en samlad bedömning av en incident och dess konsekvenser och följder kan göras.

Introduktion till bedömning och värdering av säkerhetshändelser och faktiska incidenter och risker

Detta delavsnitt syftar till att på ett intuitivt plan förklara hur bedömningar av säkerhetshändelser och faktiska incidenter respektive faktiska risker går till. En mer precis beskrivning av hur sådana bedömningar går till inleds i det efterföljande delavsnittet.

Enligt avsnittet Mekanismer och komponenter i kapitlet Analys och bedömning av orsak och verkan ovan är en *mekanism* ett objekt, eller en samling av objekt (*komponenter*), som givet att en specifik typ av händelse (en *trigger*) sker

1. (förutsatt att inget annat förhindrar det) orsakar, eller
2. (förutsatt att inget annat orsakar det) förhindrar,

att en annan specifik typ av händelse sker. Detta kallas för mekanismens *funktion*.

Hot är mekanismer, och det följer därför att ett sätt att hantera hot på är att identifiera sårbarheter (avsaknader av skydd) som, om de ersattes med skydd, skulle innebära att hotet inte längre kan orsaka en oönskad händelse. Skydden som saknas förhindrar, eller bidrar till att förhindra, att komponenter i en mekanism tillsammans kan orsaka den oönskade händelsen.

Så, huruvida ett hot gör någon reell skada från och med det att ett nytt hot uppstår beror på om det finns något skydd som förhindrar hotet från att orsaka den oönskade händelse som hotet annars skulle orsaka. Motsvarande gäller om

ett skydd som tidigare blockerade ett *hot upphör*. Att ett nytt hot uppstår eller att redan existerande hot som var blockerat slutar vara blockerat utgör de två sätt som hot uppstår kan inträffa på. Ett hot som har uppstått kommer i vissa fall att orsaka skada och i andra fall inte – beroende på om det finns skydd som blockerar hotet när det uppstår eller inte.[22] En händelse där hot uppstår och inte blockeras är både en säkerhetshändelse och en faktisk incident eller en faktisk risk. En händelse där hot uppstår men det blockeras är en säkerhetshändelse men inte en faktisk incident eller en faktisk risk (se avsnitten Säkerhetshändelser respektive Faktiska incidenter och faktiska risker ovan).

Exempel: Om skadlig kod installeras i ett informationssystem och det informationssystemet inte har programvara som upptäcker och blockerar sådan kod så kan den skadliga koden sprida sig och orsaka skada. Då har det uppstått både en säkerhetshändelse och en faktisk incident. Om informationssystemet däremot har sådan programvara varför den skadliga koden omedelbart åtgärdas så är det en säkerhetshändelse men inte en faktisk incident.

Ett liknande resonemang gäller om ett skydd upphör. Om ett *skydd upphör* och det finns ett hot som skyddet blockerade så inträffar den ytterligare säkerhetshändelsen *hot uppstår* (se ovan) omedelbart när säkerhetshändelsen skydd upphör inträffar. Om ett skydd upphör så är det i sig en faktisk incident eller en faktisk risk om skyddet som upphör gör det på oåterkalleligt eller långvarigt sätt. Om skyddet som upphör kan återupprättas eller endast temporärt är deaktiverat så utgör det inträffade en säkerhetshändelse men inte en faktisk incident.

Exempel: Om ett skydd mot wiperware oåterkalleligen deaktiveras samtidigt som ett wiperwareangrepp genomförs och inget annat skydd mot wiperware finns så kan wiperwareangreppet orsaka skada. Då har det uppstått två säkerhetshändelser som var för sig också är faktiska incidenter. Den ena säkerhetshändelsen består i deaktiveringen av skyddet, den andra består i att den sedan tidigare blockerade wiperwaren inte längre är blockerad och därför kan spridas. Den första säkerhetshändelsen utgör en faktisk incident av typen skada orsakas då skyddet är oåterkalleligen deaktiverat. Den andra säkerhetshändelsen utgör en faktisk incident av typerna skada orsakas (de filer som infekteras förstörs) och nytta förhindras (de filer som infekteras kan inte användas för att göra nytta). Om skyddet mot wiperware deaktiveras vid en tidpunkt när det inte sker ett wiperwareangrepp, eller om det pågår ett wiperwareangrepp men det finns ett annat skydd mot wiperware så har det endast uppstått en säkerhetshändelse och inte en faktisk incident.

Notera att det är skillnad på två typerna av säkerhetshändelser som exemplifieras ovan (*hot uppstår* respektive *skydd upphör*) både i termer av vad som händer, men också i termer av vad som kan göras åt respektive typ av händelse. Det uppståndna hotet kan antingen hanteras genom att ta bort eller förändra det, eller genom att upprätta ett skydd (som förhindrar samma sorts händelse som

Not 22. Detta gäller både om ett nytt hot uppstår och om ett skydd som blockerar ett redan existerande hot upphör. I det senare fallet kan det finnas ytterligare skydd som blockerar hotet, i det föregående fallet kan det finnas något skydd som blockerar hotet.

hotet orsakar) för att förbigå hindret. Att ett skydd upphör kan (i vissa fall åtminstone, såsom i exemplet ovan) hanteras genom att återställa det objekt som utgjorde skyddet men som har deaktiverats, eller genom att upprätta ett annat skydd som förhindrar samma sorts händelse som det skydd som upphörde gjorde.

På motsvarande sätt kan det att ett *hinder uppstår* innebära att en viss framgångsfaktor förhindras från att orsaka den önskade händelse som den annars skulle orsaka – men om det finns andra framgångsfaktorer som orsakar samma slags händelse så kanske den händelsen inträffar ändå, trots att hindret uppstod. En händelse där hinder uppstår och blockerar en framgångsfaktor och det inte finns någon annan framgångsfaktor som orsakar samma slags önskade händelse är en säkerhetshändelse och en faktisk incident eller en faktisk risk (åtminstone av typen nytta förhindras). En händelse där hinder uppstår och blockerar en framgångsfaktor men det finns en annan framgångsfaktor som orsakar samma slags händelse är inte en faktisk incident eller en faktisk risk. Den framgångsfaktor som inte blockeras *förbigår* hindret.

Exempel: Om en modul som blockerar nätverkstrafik installeras i en router och organisationen inte har någon annan router så kan modulen förhindra nytta (genom att internet inte längre går att nå). Då har det uppstått en säkerhetshändelse och en faktisk incident (av typen nytta förhindras). Om det istället finns fler routrar så att internet fortfarande går att nå så har det uppstått en säkerhetshändelse, men inte en faktisk incident.

Ett liknande resonemang gäller om en *framgångsfaktor upphör*. Om det finns andra framgångsfaktorer som orsakar samma slags önskade händelse så kommer den händelsen att orsakas även om en av framgångsfaktorerna inte längre finns. En händelse där en framgångsfaktor upphör och det inte finns någon annan framgångsfaktor som orsakar samma slags önskade händelse är en faktisk incident eller en faktisk risk.

Exempel: Om en router går sönder och organisationen inte har någon annan router så förhindras nytta (genom att internet inte längre går att nå). Då har det uppstått en säkerhetshändelse och en faktisk incident. Om det istället finns fler routrar så att internet fortfarande går att nå så har det uppstått en säkerhetshändelse, men inte en faktisk incident.

Notera att det är skillnad på två typerna av säkerhetshändelser som exemplifieras ovan (*hinder uppstår* respektive *framgångsfaktor upphör*) både i termer av vad som händer, men också i termer av vad som kan göras åt respektive typ av händelse. Det uppståndna hindret kan antingen hanteras genom att ta bort det, eller genom att nyttja en annan framgångsfaktor (som orsakar samma sorts händelse som den framgångsfaktor som hindret blockerar) för att förbigå hindret. Att en framgångsfaktor upphör kan (i vissa fall åtminstone, såsom i exemplet ovan) hanteras genom att återställa det objekt som utgjorde framgångsfaktorn men som har gått sönder, eller genom att upprätta en annan framgångsfaktor som orsakar samma sorts händelse som den framgångsfaktor som upphörde gjorde.

Alla faktiska incidenter respektive faktiska risker är säkerhetshändelser, men inte alla säkerhetshändelser är faktiska incidenter respektive faktiska risker.

Det finns fyra typer av faktiska incidenter respektive faktiska risker. Deras namn, vad de betyder och hur de kan förstås listas nedan:

1. **Skada orsakas:** skada orsakas för aktören, eller för andra, på ett sätt som inte ligger i aktörens intresse. Händelser där det uppstår skador, förstörelse eller oönskade och oåterkalleliga ändringar utgör exempel händelser som är faktiska incidenter eller faktiska risker av den här typen.
2. **Skada förhindras:** skada förhindras för aktörens antagonister, eller för andra, på ett sätt som inte ligger i aktörens intresse. Händelser där saker en organisation har eller gör (och som andra aktörer ser sig hotade av) hindras från att fungera, förstörs eller ändras utgör exempel på händelser som är faktiska incidenter eller faktiska risker av den här typen.
3. **Nytta förhindras:** nytta förhindras för aktören, eller för andra, på ett sätt som inte ligger i aktörens intresse. Händelser där saker en organisation har eller gör för sin egen nyttas skull hindras från att fungera, förstörs eller ändras utgör exempel på händelser som är faktiska incidenter eller faktiska risker av den här typen.
4. **Nytta orsakas:** nytta orsakas för aktörens antagonister, eller för andra, på ett sätt som inte ligger i aktörens intresse. Händelser där saker en organisation har eller gör kommer obehöriga till handa utgör exempel på händelser som är faktiska incidenter eller faktiska risker av den här typen.

Bedömning och värdering av säkerhetshändelser i en domän

Detta delavsnitt syftar till att (med stöd av den intuitiva förståelse som föregående avsnitt är tänkt att ge) inleda en mer precis beskrivning av hur bedömningar av säkerhetshändelser och faktiska incidenter respektive faktiska risker går till. Denna mer precisa förklaring fortsätter sedan i de nästföljande delavsnitten.

Det första steget i att fastställa klassificeringen av en incidents allvarlighetsgrad är att avgöra hur det inträffade inverkar på helheten inom redogörelsen. Det görs genom att först fastställa vad det är för säkerhetshändelse eller för säkerhetshändelser som har inträffat[23], och sedan, via tabell 21 nedan, vilken allvarlighetsgrad säkerhetshändelsen eller säkerhetshändelserna har.

Not 23. En och samma händelse kan utgöra flera olika typer av säkerhetshändelser samtidigt. Se exemplet med den brinnande datahallen senare i detta avsnitt. På motsvarande sätt kan en säkerhetshändelse utgöra flera olika typer av faktiska incidenter samtidigt. Se samma exempel.

Tabell 21. Bedömning av säkerhetshändelser

Hot uppstår	Skydd upphör	Hinder uppstår	Framgångsfaktor upphör
Kritisk nivå: Samtliga…	**Kritisk nivå:** Samtliga…	**Kritisk nivå:** Samtliga…	**Kritisk nivå:** Samtliga…
Allvarlig nivå: En majoritet, men inte alla,…	**Allvarlig nivå:** En majoritet, men inte alla,…	**Allvarlig nivå:** En majoritet, men inte alla,…	**Allvarlig nivå:** En majoritet, men inte alla,…
Betydande nivå: Upp till hälften, och minst ett,…	**Betydande nivå:** Upp till hälften, och minst ett,…	**Betydande nivå:** Upp till hälften, och minst ett,…	**Betydande nivå:** Upp till hälften, och minst ett,…
Måttlig nivå: Endast en…	**Måttlig nivå:** Endast en…	**Måttlig nivå:** Endast en…	**Måttlig nivå:** Endast en…
Noll-nivå: Inget…	**Noll-nivå:** Inget…	**Noll-nivå:** Ingen…	**Noll-nivå:** Ingen…
… av de skydd som förhindrar oönskade händelser av en viss typ, eller de framgångsfaktorer som orsakar önskade händelser av en viss typ hotas av hotet som har uppstått.	… av de skydd som förhindrar oönskade händelser av den typ som det upphörda skyddet förhindrade har upphört.	… av de framgångsfaktorer som orsakar önskade händelser av en viss typ blockeras av hindret som har uppstått.	… av de framgångsfaktorer som orsakar önskade händelser av den typ som den upphörda framgångsfaktorn orsakade har upphört.

Not: I vissa fall kommer flera av nivåerna under respektive säkerhetshändelse att vara sanna samtidigt. Då gäller den högre allvarlighetsgraden. Exempelvis, under ”framgångsfaktor upphör”, om det ursprungligen bara fanns två sådana framgångsfaktorer och den ena nu har upphört, då stämmer beskrivningarna för både ”måttlig” och ”betydande”. Då gäller ”betydande”. Säkerhetshändelser med allvarlighetsgraden ”måttlig” eller lägre räknas inte som faktiska incidenter.

Nedan följer ett exempel per typ av säkerhetshändelse. Samtliga exempel hör till domänen ”it-miljö”. Motsvarande exempel kan ges inom andra domäner.

Exempel 1 – Hot uppstår: Ransomware installeras i en organisations it-miljö. Händelsen är en säkerhetshändelse av typen ”hot uppstår”. En undersökning av det inträffade visar att ransomwareinfektionen hotar hela it-miljön. Givet att redogörelsen över det som ska bedömas handlar om it-miljöns segment så motsvarar detta nivån ”kritisk”. Säkerhetshändelsen kan alltså utgöra en faktisk incident.[24]

Not 24. Om ransomwareinfektionen har infekterat filer utgör samma händelse även säkerhetshändelsen ”framgångsfaktor upphör”. Båda säkerhetshändelserna bör då analyseras och bedömas, och en samlad bedömning av händelsen bör sedan beakta utfallet av båda bedömningarna.

Exempel 2 – Skydd upphör: Ett skydd mot ransomwareinfektioner deaktiveras. Händelsen är en säkerhetshändelse av typen ”skydd upphör”. En undersökning av it-miljön visar att det finns tre andra skydd mot ransomwareinfektioner. Givet att redogörelsen över det som ska bedömas handlar om it-miljön motsvarar detta nivån ”måttlig”. Säkerhetshändelsen kan alltså inte utgöra en faktisk incident.

Exempel 3 – Hinder uppstår: En ny regel som blockerar all nätverkstrafik sätts upp i en router. Händelsen är en säkerhetshändelse av typen ”hinder uppstår”. En undersökning av it-miljön visar att samtliga av organisationens mejlserver skickar och tar emot mejl enbart genom den routern, varför det inte längre går att skicka eller ta emot mejl. Givet att redogörelsen över det som ska bedömas handlar om mejlsystemet så motsvarar detta nivån ”kritisk”. Säkerhetshändelsen kan alltså utgöra en faktisk incident.

Exempel 4 – Framgångsfaktor upphör: En organisation nyttjar en leverantör för sitt it-stöd. Leverantörens datahall brinner ner. Händelsen är en säkerhetshändelse av typen ”framgångsfaktor upphör”. Leverantören har ingen annan datahall, och all mjukvara och alla tjänster som nyttjas av organisationen kördes ifrån datahallen. Organisationen lagrar dock sin data lokalt. Organisationen nyttjar inte någon annan tjänsteleverantör som kan erbjuda motsvarande mjukvara och tjänster. Givet att redogörelsen över det som ska bedömas handlar om it-miljön så motsvarar detta en allvarlighetsgrad för säkerhetshändelser på nivån ”kritisk”. Säkerhetshändelsen kan alltså utgöra en faktisk incident.

Bedömning och värdering av faktiska incidenter och faktiska risker i respektive domän

Detta delavsnitt syftar till att, i varsin av de tre domänerna, fortsätta den mer precisa beskrivning av hur bedömningar av säkerhetshändelser och faktiska incidenter respektive faktiska risker går till och som inleddes i det föregående delavsnittet. I det nästföljande avsnittet läggs bedömningen och värderingen av faktiska incidenter respektive faktiska risker inom respektive domän samman.

Givet att en säkerhetshändelse bedöms, som lägst, ha allvarlighetsgraden ”betydande” så är nästa steg att bedöma huruvida säkerhetshändelsen också är en faktisk incident eller en faktisk risk. En kontroll görs i kolumnen för den typ av säkerhetshändelse det handlar om, för vart och en av de fyra typerna av faktisk incident respektive risk.

Tabell 22. Bedömning av faktiska incidenter respektive faktiska risker

Hot uppstår	Skydd upphör	Hinder uppstår	Framgångsfaktor upphör
Faktisk incident eller faktisk risk: Skada orsakas Skada orsakas för aktören, eller för andra, på ett sätt som inte ligger i aktörens intresse.			
Kritisk nivå: Samtliga…	**Kritisk nivå:** Samtliga…	**Kritisk nivå:** -	**Kritisk nivå:** Samtliga…
Allvarlig nivå: En majoritet, men inte alla…	**Allvarlig nivå:** En majoritet, men inte alla…	**Allvarlig nivå:** -	**Allvarlig nivå:** En majoritet, men inte alla…
Betydande nivå: Upp till hälften, och minst ett…	**Betydande nivå:** Upp till hälften, och minst ett…	**Betydande nivå:** -	**Betydande nivå:** Upp till hälften, och minst ett…
Måttlig nivå: Endast en…	**Måttlig nivå:** Endast en…	**Måttlig nivå:** -	**Måttlig nivå:** Endast en…
Noll-nivå: Ingen…	**Noll-nivå:** Inget…	**Noll-nivå:** -	**Noll-nivå:** Ingen…
… av antingen de framgångsfaktorer som orsakar önskade händelser av en viss typ, eller de skydd som förhindrar oönskade händelser av en viss typ, har upphört.	… av de skydd som förhindrar oönskade händelser av en viss typ, har upphört.	Ej tillämpligt.	… av de framgångsfaktorer som orsakar önskade händelser av den typ som den upphörda framgångsfaktorn orsakade har upphört.
Faktisk incident eller faktisk risk: Skada förhindras Skada förhindras för aktörens antagonister, eller för andra, på ett sätt som inte ligger i aktörens intresse.			
Kritisk nivå: Samtliga…	**Kritisk nivå:** -	**Kritisk nivå:** Samtliga…	**Kritisk nivå:** Samtliga…
Allvarlig nivå: En majoritet, men inte alla…	**Allvarlig nivå:** -	**Allvarlig nivå:** En majoritet, men inte alla…	**Allvarlig nivå:** En majoritet, men inte alla…
Betydande nivå: Upp till hälften, och minst ett…	**Betydande nivå:** -	**Betydande nivå:** Upp till hälften, och minst ett…	**Betydande nivå:** Upp till hälften, och minst ett…
Måttlig nivå: Endast en…	**Måttlig nivå:** -	**Måttlig nivå:** Endast en…	**Måttlig nivå:** Endast en…
Noll-nivå: Inget…	**Noll-nivå:** -	**Noll-nivå:** Inget…	**Noll-nivå:** Ingen…
… av de objekt som enligt aktörens antagonister utgör hot har upphört.	Ej tillämpligt.	… av de objekt som enligt aktörens antagonister utgör hot har blockerats.	… av de framgångsfaktorer som enligt aktörens antagonister utgör hot har upphört.

Hot uppstår	Skydd upphör	Hinder uppstår	Framgångsfaktor upphör
Faktisk incident eller faktisk risk: Nytta förhindras Nytta förhindras för aktören, eller för andra, på ett sätt som inte ligger i aktörens intresse.			
Kritisk nivå: Samtliga…	**Kritisk nivå:** -	**Kritisk nivå:** Samtliga…	**Kritisk nivå:** Samtliga…
Allvarlig nivå: En majoritet, men inte alla…	**Allvarlig nivå:** -	**Allvarlig nivå:** En majoritet, men inte alla…	**Allvarlig nivå:** En majoritet, men inte alla…
Betydande nivå: Upp till hälften, och minst ett…	**Betydande nivå:** -	**Betydande nivå:** Upp till hälften, och minst ett…	**Betydande nivå:** Upp till hälften, och minst ett…
Måttlig nivå: Endast en…	**Måttlig nivå:** -	**Måttlig nivå:** Endast en…	**Måttlig nivå:** Endast en…
Noll-nivå: Ingen…	**Noll-nivå:** -	**Noll-nivå:** Ingen…	**Noll-nivå:** Ingen…
… av de framgångs-faktorer som orsakar önskade händelser av en viss typ har upphört.	Ej tillämpligt.	… av de framgångs-faktorer som orsakar önskade händelser av en viss typ har blockerats.	… av de framgångs-faktorer som orsakar önskade händelser av en viss typ har upphört.
Faktisk incident eller faktisk risk: Nytta orsakas Nytta orsakas för aktörens antagonister, eller för andra, på ett sätt som inte ligger i aktörens intresse.			
Kritisk nivå: Samtliga…	**Kritisk nivå:** -	**Kritisk nivå:** -	**Kritisk nivå:** -
Allvarlig nivå: En majoritet, men inte alla…	**Allvarlig nivå:** -	**Allvarlig nivå:** -	**Allvarlig nivå:** -
Betydande nivå: Upp till hälften, och minst ett…	**Betydande nivå:** -	**Betydande nivå:** -	**Betydande nivå:** -
Måttlig nivå: Endast en…	**Måttlig nivå:** -	**Måttlig nivå:** -	**Måttlig nivå:** -
Noll-nivå: Inget…	**Noll-nivå:** -	**Noll-nivå:** -	**Noll-nivå:** -
… av de objekt som enligt aktörens antagonister utgör framgångsfaktorer eller skydd har uppstått hos aktörens antagonister.	Ej tillämpligt.	Ej tillämpligt.	Ej tillämpligt.

Not: Angående kolumnen under ”skydd upphör”: Om det sedan tidigare fanns ett hot som blockerades av enbart det skydd som upphör så inträffar säkerhetshändelsen ”hot uppstår” samtidigt som skydd upphör. Samma slags analys och bedömning av den händelsen måste därför också göras.

Med stöd av tabell 22 ovan kan exemplen från ovan nu analyseras och bedömas enligt följande:

Exempel 1: Hot uppstår

Ransomware installeras i en organisations it-miljö. Händelsen är en säkerhetshändelse av typen ”hot uppstår”. En undersökning av det inträffade visar att ransomwareinfektionen hotar hela it-miljön. Givet att redogörelsen över det som ska bedömas handlar om it-miljöns segment så motsvarar detta en allvarlighetsgrad för säkerhetshändelser på nivån ”kritisk”. En vidare undersökning visar att:

Tabell 23. Bedömning av faktisk incident eller faktisk risk i it-miljödomänen för säkerhetshändelsen hot uppstår

#	Beskrivning	Faktisk incident
1	Infektionen har bland annat slagit ut hela mejlsystemet och merparten av lagringsytorna. Hela mejlsystemet är utslaget och det finns inte något alternativt sätt att mejla.[25]	Skada orsakas – kritisk nivå
2	Information saknas för att avgöra vem som står bakom ransomwareangreppet och om den som stod bakom det, eller en uppdragsgivare till den som stod bakom det, såg sig hotad av något som organisationen har eller gör. Organisationen är en offentlig organisation som inte bedriver verksamhet i konkurrens med andra organisationer, varför det saknas skäl att tro att något som organisationen har eller gör i övrigt utgör ett hot mot andra organisationer.	Skada förhindras – går inte att avgöra
3	Mejlsystemet ligger nere och det finns inte något alternativt sätt att mejla.	Nytta förhindras – kritisk nivå
4	Den skadliga koden har endast som funktion att infektera filer och system med ransomware. Inget förs ut till angriparen, och därför får inte heller angriparen, eller en uppdragsgivare till angriparen, något som kan vara till nytta för den.[26]	Nytta orsakas – ingen nivå

Not 25. Regeln säger ju att ”/…/ antingen de framgångsfaktorer som orsakar önskade händelser av en viss typ, eller de skydd som förhindrar oönskade händelser av en viss typ, har upphört”. I det här fallet är det visat att samtliga framgångsfaktorer som gör att man kan mejla har upphört, och då blir nivån ”kritisk”.

Not 26. Beslutsfattare inom organisationen kan ju i ett senare skede bestämma sig för att betala en lösensumma för att få tillgång till en dekrypteringsnyckel. När de gör det orsakas nytta för angriparen eller angriparens uppdragsgivare. Beslutet att göra det är dock inte en del av själva incidenten, utan en reaktion på (en följd av) incidenten (som i sig är en incident). Se avsnittet Skillnaden mellan konsekvenser och följder ovan.

Samma händelse sett ur ett verksamhets- eller organisationsperspektiv kan med hjälp av tabell 22 ovan bedömas enligt följande:

Tabell 24. Bedömning av faktisk incident eller faktisk risk i verksamhets-/organisationsdomänen för säkerhetshändelsen hot uppstår

#	Beskrivning	Faktisk incident
1	Infektionen har slagit ut merparten av organisationens möjligheter att kommunicera genom text. Mobiltelefoner kan dock fortfarande användas, och det går att smsa.	Skada orsakas – allvarlig nivå
2	Samma som i tabell 23.	Skada förhindras – går inte att avgöra
3	Infektionen har slagit ut merparten av organisationens möjligheter att kommunicera genom text. Mobiltelefoner kan dock fortfarande användas, inklusive för att smsa.	Nytta förhindras – allvarlig nivå
4	Samma som i tabell 23.	Nytta orsakas – ingen nivå

Samma händelse sett ur ett samhällsperspektiv kan med hjälp av tabell 22 ovan bedömas enligt följande:

Tabell 25. Bedömning av faktisk incident eller faktisk risk i samhällsnivådomänen för säkerhetshändelsen hot uppstår

#	Beskrivning	Faktisk incident
1	Organisationen är en av fyra som tillhandahåller en viss typ av tjänst.[27]	Skada orsakas – betydande nivå
2	Samma som i tabell 23.	Skada förhindras – går inte att avgöra
3	Organisationen är en av fyra som tillhandahåller en viss typ av tjänst.	Nytta förhindras – betydande nivå
4	Samma som i tabell 23.	Nytta orsakas – ingen nivå

Not 27. Inom ramen för redogörelsen.

Exempel 2: Skydd upphör

Ett skydd mot ransomwareinfektioner deaktiveras. Händelsen är en säkerhetshändelse av typen ”skydd upphör”. En undersökning av it-miljön visar att det finns tre andra skydd mot ransomwareinfektioner. Givet att redogörelsen över det som ska bedömas handlar om it-miljön motsvarar detta en allvarlighetsgrad för säkerhetshändelser på nivån ”måttlig”. Säkerhetshändelsen kan alltså inte utgöra en faktisk incident. Ingen vidare undersökning behövs.

Exempel 3: Hinder uppstår

En ny regel som blockerar all nätverkstrafik sätts upp i en router. Händelsen är en säkerhetshändelse av typen ”hinder uppstår”. En undersökning av it-miljön visar att samtliga av organisationens mejlserver skickar och tar emot mejl enbart genom den routern, varför det inte längre går att skicka eller ta emot mejl. Givet att redogörelsen över det som ska bedömas handlar om mejlsystemet så motsvarar detta en allvarlighetsgrad för säkerhetshändelser på nivån ”kritisk”. Säkerhetshändelsen kan alltså utgöra en faktisk incident. En vidare undersökning visar att:

Tabell 26. Bedömning av faktisk incident eller faktisk risk i it-miljödomänen för säkerhetshändelsen hinder uppstår

#	Beskrivning	Faktisk incident
1	Säkerhetshändelser av typen ”hinder uppstår” kan definitionsmässigt inte utgöra faktiska incidenter av typen ”skada orsakas”.	Skada orsakas – ingen nivå
2	Organisationen är ett privat företag. Företaget varken har eller gör, eller planerar att ha eller göra, något som tydligt hotar dess antagonister.	Skada förhindras – går inte att avgöra
3	Samtliga av organisationens mejlservrar är blockerade.	Nytta förhindras – kritisk nivå
4	Säkerhetshändelser av typen ”hinder uppstår” kan definitionsmässigt inte utgöra faktiska incidenter av typen ”nytta orsakas”.	Nytta orsakas – ingen nivå

Samma händelse sett ur ett verksamhets- eller organisationsperspektiv kan med hjälp av tabell 22 ovan bedömas enligt följande:

Tabell 27. Bedömning av faktisk incident eller faktisk risk i verksamhets-/organisationsdomänen för säkerhetshändelsen hinder uppstår

#	Beskrivning	Faktisk incident
1	Infektionen har slagit ut merparten av organisationens möjligheter att kommunicera genom text. Mobiltelefoner kan dock fortfarande användas, och det går att smsa.	Skada orsakas – allvarlig nivå
2	Samma som i tabell 26.	Skada förhindras – går inte att avgöra
3	Infektionen har slagit ut merparten av organisationens möjligheter att kommunicera genom text. Mobiltelefoner kan dock fortfarande användas, och det går att smsa.	Nytta förhindras – allvarlig nivå
4	Samma som i tabell 26.	Nytta orsakas – ingen nivå

Samma händelse sett ur ett samhällsperspektiv kan med hjälp av tabell 22 ovan bedömas enligt följande:

Tabell 28. Bedömning av faktisk incident eller faktisk risk i samhällsnivådomänen för säkerhetshändelsen hinder uppstår

#	Beskrivning	Faktisk incident
1	Organisationen är en av fyra som tillhandahåller en viss typ av tjänst.[28]	Skada orsakas – betydande nivå
2	Samma som i tabell 26.	Skada förhindras – går inte att avgöra
3	Organisationen är en av fyra som tillhandahåller en viss typ av tjänst.	Nytta förhindras – betydande nivå
4	Samma som i tabell 26.	Nytta orsakas – ingen nivå

Exempel 4: Framgångsfaktor upphör

En organisation nyttjar en leverantör för sitt it-stöd. Leverantörens datahall brinner ner. Händelsen är en säkerhetshändelse av typen ”framgångsfaktor upphör”. Leverantören har ingen annan datahall, och all mjukvara och alla tjänster som nyttjas av organisationen kördes ifrån datahallen. Organisationen lagrar dock sin data lokalt. Organisationen nyttjar inte någon annan tjänsteleverantör som kan erbjuda motsvarande mjukvara och tjänster. Givet att redogörelsen över det som ska bedömas handlar om it-miljön så motsvarar detta en allvarlighetsgrad för säkerhetshändelser på nivån ”kritisk”. Säkerhetshändelsen kan alltså utgöra en faktisk incident. En vidare undersökning visar att:

Not 28. Inom ramen för redogörelsen.

Tabell 29. Bedömning av faktisk incident eller faktisk risk i it-miljödomänen för säkerhetshändelsen framgångsfaktor upphör

#	Beskrivning	Faktisk incident
1	Inget i organisationens egen it-miljö har tagit någon skada.	Skada orsakas – ingen nivå
2	Branden har totalförstört datahallen och det saknas därför förutsättningar för att avgöra om något som fanns eller något som utfördes i den utgjorde ett hot mot någon annan organisation.	Skada förhindras – går inte att avgöra
3	Organisationen har ingen annan datahall, och all mjukvara och alla tjänster som nyttjas inom organisationens it-miljö kördes ifrån datahallen.	Nytta förhindras – kritisk nivå
4	Branden har enbart skapat något av värde för någon annan.[29]	Nytta orsakas – ingen nivå

Samma händelse sett ur ett verksamhets- eller organisationsperspektiv kan med hjälp av tabell 22 ovan bedömas enligt följande:

Tabell 30. Bedömning av faktisk incident eller faktisk risk i verksamhets-/organisationsdomänen för säkerhetshändelsen framgångsfaktor upphör

#	Beskrivning	Faktisk incident
1	Organisationens tillgångar, inklusive dess information, är oförändrade.	Skada orsakas – ingen nivå
2	Samma som i tabell 29.	Skada förhindras – går inte att avgöra
3	Organisationens tjänster kan inte tillhandahållas med icke-digitala medel. Tjänsterna som kördes från leverantörens datahall utgjorde komponenter i organisationens produktion.	Nytta förhindras – kritisk nivå
4	Samma som i tabell 29.	Nytta orsakas – ingen nivå

Not 29. Det är möjligt att något har skett innan branden uppstod som orsakade nytta för någon av organisationens antagonister, men det är i.s.f. en separat händelse som ska analyseras och bedömas separat.

Samma händelse sett ur ett samhällsperspektiv kan med hjälp av tabell 22 ovan bedömas enligt följande:

Tabell 31. Bedömning av faktisk incident eller faktisk risk i samhällsnivådomänen för säkerhetshändelsen framgångsfaktor upphör

#	Beskrivning	Faktisk incident
1	Tjänsterna som organisationen tillhandahåller har inte i sig tagit skada.	Skada orsakas – ingen nivå
2	Samma som i tabell 29.	Skada förhindras – går inte att avgöra
3	Det finns bara två organisationer som tillhandahåller den typ av tjänst som organisationen tillhandahåller.[30]	Nytta förhindras – betydande nivå
4	Samma som i tabell 29.	Nytta orsakas – ingen nivå

Bedömning och värdering i de tre domänerna

Detta delavsnitt syftar till att fortsätta den mer precisa beskrivningen av hur bedömningar av säkerhetshändelser och faktiska incidenter respektive faktiska risker går till genom att visa hur sådana bedömningar som genomfördes i de två föregående avsnitten kan göras för en och samma händelse i samtliga domäner och sedan läggas samman. Det sista delavsnittet i avsnittet visar sedan hur samlade bedömningar kan göras av flera händelser som var för sig har bedömts på det sätt som presenteras i detta delavsnitt.

En sammanställning av hur en och samma händelse bedöms inom de tre domänerna (i detta fall exemplet med branden i en datahall ifrån det föregående delavsnittet – men denna gång från leverantören som äger datahallens perspektiv) kan se ut som följer:

Not 30. Inom ramen för redogörelsen.

Tabell 32. Bedömning av händelser i de tre domänerna vid ett exempel med brand i datahall

Säkerhetshändelse:		**Hot uppstår**			
Påverkan	Ingen	Måttlig	Betydande	Allvarlig	Kritisk
It-miljö					
Säkerhets-händelsen:	-	-	-	-	Kritisk
Skada orsakas	Ingen	-	-	-	-
Skada förhindras	Ej aktuellt	Ej aktuellt	Ej aktuellt	Ej aktuellt	Ej aktuellt
Nytta förhindras	-	-	-	-	Kritisk
Nytta orsakas	Ingen	-	-	-	-
Verksamhet/organisation					
Säkerhets-händelsen:	-	-	-	Allvarlig	-
Skada orsakas	Ingen	-	-	-	-
Skada förhindras	Ej aktuellt	Ej aktuellt	Ej aktuellt	Ej aktuellt	Ej aktuellt
Nytta förhindras	-	-	-	Allvarlig	-
Nytta orsakas	Ingen	-	-	-	-
Samhälle					
Säkerhets-händelsen:	-	-	Betydande	-	-
Skada orsakas	Ingen	-	-	-	-
Skada förhindras	Ej aktuellt	Ej aktuellt	Ej aktuellt	Ej aktuellt	Ej aktuellt
Nytta förhindras	-	-	Betydande	-	-
Nytta orsakas	Ingen	-	-	-	-

Säkerhetshändelse:		**Framgångsfaktor upphör**			
Påverkan	Ingen	Måttlig	Betydande	Allvarlig	Kritisk
It-miljö					
Säkerhets-händelsen:	-	-	-	-	Kritisk
Skada orsakas	Ingen	-	-	-	-
Skada förhindras	Ej aktuellt	Ej aktuellt	Ej aktuellt	Ej aktuellt	Ej aktuellt
Nytta förhindras	-	-	-	-	Kritisk
Nytta orsakas	Ingen	-	-	-	-
Verksamhet/organisation					
Säkerhets-händelsen:	-	-	-	Allvarlig	-
Skada orsakas	Ingen	-	-	-	-
Skada förhindras	Ej aktuellt	Ej aktuellt	Ej aktuellt	Ej aktuellt	Ej aktuellt
Nytta förhindras	-	-	-	Allvarlig	-
Nytta orsakas	Ingen	-	-	-	-
Samhälle					
Säkerhets-händelsen:	-	Måttlig	-	-	-
Skada orsakas	Ingen	-	-	-	-
Skada förhindras	Ej aktuellt	Ej aktuellt	Ej aktuellt	Ej aktuellt	Ej aktuellt
Nytta förhindras	-	Måttlig	-	-	-
Nytta orsakas	Ingen	-	-	-	-

Not: Själva branden är ju ett hot som har uppstått, medan det som brinner (och därför går sönder) är utrustningen i datahallen, vilket innebär att framgångsfaktorer upphör. I det här fallet resulterar det i en exakt överensstämmelse mellan bedömningarna av huruvida respektive säkerhetshändelse är en faktisk incident, och med vilken allvarlighetsgrad – men det måste inte alltid vara fallet. Viktigt att notera är också att branden i datahallen, för leverantören, resulterar i *två* säkerhetshändelser (hot uppstår och framgångsfaktor upphör) som var för sig utgör faktiska incidenter eller faktiska risker – medan samma brand för organisationer som nyttjar tjänster ifrån leverantören enbart utgör *en* säkerhetshändelse (framgångsfaktor upphör) som i sin tur utgör faktiska incidenter eller faktiska risker. Skälet till det är att inget av det (de objekt) som tillhör organisationen (snarare än leverantören) upphör, eller förändras. Det inträffade utgör därför en *indirekt incident* för organisationen (se delavsnittet Händelser som inträffar respektive uteblir i kapitlet Begrepp och begreppssystem ovan).

I tabell 32 ovan bedöms exemplet med branden i datahallen i domänen it-miljö som en säkerhetshändelse av typerna hot uppstår och framgångsfaktor upphör, båda på kritisk nivå. Händelsen utgör samtidigt en faktisk incident eller en faktisk risk av typerna skada orsakas och nytta förhindras, båda på kritisk nivå. Organisationen har ingen annan datahall, så händelsen är ett hårt slag mot organisationen i den domänen.

På motsvarande sätt bedöms branden i datahallen i domänen organisation/verksamhet utgöra en säkerhetshändelse av typerna hot uppstår och framgångsfaktor upphör, båda på allvarlig nivå. Händelsen utgör samtidigt en faktisk incident av typerna skada orsakas och nytta förhindras, båda på allvarlig nivå. Avsaknaden av it-stöd reducerar organisationens effektivitet kraftigt, men organisationens personal kan fortfarande sköta några uppgifter på egen hand.

Slutligen bedöms branden i datahallen i domänen samhälle utgöra en säkerhetshändelse av typerna hot uppstår och framgångsfaktor upphör, båda på måttlig nivå. Händelsen utgör samtidigt en faktisk incident av typerna skada orsakas och nytta förhindras, båda på måttlig nivå. Det finns fyra andra organisationer inom den angivna redogörelsen som bedriver sådan verksamhet som den drabbade organisationen gör.

Samlade bedömningar av incidenter och deras konsekvenser och följder

Detta delavsnitt avslutar avsnittet och syftar till att visa hur flera händelser, som var för sig har bedömts på de sätt som förevisats i de föregående tre delavsnitten kan läggas samman till en samlad bedömning.

I många fall när en större incident har inträffat handlar det egentligen om flera incidenter som har skett vid ungefär samma tillfälle. I exemplet ovan kanske branden föregicks av att inbrott där viss utrustning stals, varpå den som bröt sig in satte eld på datahallen. Det kan också vara så att incidenter får konsekvenser i form av nya incidenter (se avsnittet Redogörelse för den incident eller den risk som analyseras ovan), och att människors reaktioner på incidenter resulterar i följder (se avsnittet Skillnaden mellan konsekvenser och följder ovan). Vid större incidenter förväntas ofta den inträffade helheten bedömas. Det kan göras genom att identifiera samtliga av de separata händelser som har inträffat, samtliga av de typer av säkerhetshändelser som de separata händelserna utgör i samtliga domäner och samtliga av de typer av faktiska incidenter som samtliga av de typerna av säkerhetshändelserna utgör.

När så många bedömningar görs så kommer utfallet många gånger resultera i att olika säkerhetshändelser, och genom dem, olika faktiska incidenter, bedöms olika. I exemplet med datahallen i det föregående avsnittet skulle exempelvis bedömningen av de faktiska incidenterna eller faktiska riskerna ”skada orsakas” och ”nytta förhindras” under säkerhetshändelsen ”hot uppstår” kunnat bedömas som allvarliga, medan de motsvarande faktiska incidenterna eller faktiska riskerna under säkerhetshändelsen ”framgångsfaktor upphör” hade kunnat bedömas som kritiska. Om en samlad bedömning av incidenten ska göras så gäller i sådana fall *den högre allvarlighetsgraden*. I det fallet skulle därför den samlade bedömningen av den inträffade faktiska incidenten vara ”kritisk”.

Kapitel 6

Referenser

Referenser

1. Hoten mot de digitala leveranskedjorna (MSB, 2021)

Titel: *Hoten mot de digitala leveranskedjorna: 50 rekommendationer för att stärka samhällssäkerheten*

Utgivare: MSB

År: 2021

Länk: https://rib.msb.se/filer/pdf/29829.pdf

2. Ändringar som både hotar och skyddar (MSB, 2022)

Titel: *Ändringar som både hotar och skyddar: 20 rekommendationer för säkrare ändringar i våra informationssystem*

Utgivare: MSB

År: 2022

Länk: https://rib.msb.se/filer/pdf/30193.pdf

3. Cyberangrepp mot samhällsviktiga informationssystem (MSB, 2024)

Titel: *Cyberangrepp mot samhällsviktiga informationssystem – 25 rekommendationer för stärkt skydd mot cyberangrepp*

Utgivare: MSB

År: 2024

Länk: https://rib.msb.se/filer/pdf/30558.pdf

4. It-incidenters påverkan (MSB, 2025)

Titel: *It-incidenters påverkan – Ramverk för bedömning av påverkan på it-miljö, verksamhet och samhälle*

Utgivare: MSB

År: 2025

Länk: https://rib.msb.se/filer/pdf/31096.pdf

5. UNDRR–ISC Hazard Definition & Classification Review (UNDRR & ISC, 2025)

Titel: *UNDRR–ISC Hazard Definition & Classification Review: 2025 Update of the Technical Report*

Utgivare: United Nations Office for Disaster Risk Reduction (UNDRR) & International Science Council (ISC)

År: 2025

Plats: Genève, Schweiz & Paris, Frankrike

Länk: https://doi.org/10.24948/2025.04

Kapitel 7

Bilaga: Källvärdering

Bilaga: Källvärdering

Källvärdering görs inom den strategiska cybersäkerhetsanalysen med hjälp av Natos Admirality-system. I modellen bedöms en källa utifrån dels grundläggande trovärdighet och dels den information som källan bidrar med.[31]

Tillförlitlighet

En källa bedöms utifrån en värdering av dess tillförlitlighet:

A. **Fullständigt tillförlitlig:**
   Ingen tvekan om äkthet, trovärdighet eller kompetens; har en historik av fullständig tillförlitlighet.
B. **Vanligtvis tillförlitlig:**
   Kan finnas viss tvekan om äkthet, trovärdighet eller kompetens; har för det allra mesta lämnat korrekt information.
C. **Ganska tillförlitlig:**
   Tveksamheter kring äkthet, trovärdighet eller kompetens, men har tidigare lämnat korrekt information.
D. **Vanligen inte tillförlitlig:**
   Betydande tvekan om äkthet, trovärdighet eller kompetens, men har ändå lämnat korrekt information tidigare.
E. **Otillförlitlig:**
   Bristande äkthet, trovärdighet och kompetens; har en historik av felaktig information.
F. **Tillförlitlighet kan inte bedömas:**
   Det finns ingen grund för att bedöma källans tillförlitlighet.

Not 31. Det är alltså epistemisk sannolikhet som bedöms inom källvärderingen. Se delavsnittet En not om sannolikhet i avsnittet Analys och bedömning av riskers orsak och verkan i kapitlet Analys och bedömning av orsak och verkan ovan.

Trovärdighet

En uppgift bedöms utifrån graden av stöd den har ifrån andra källor:

1. Bekräftad av andra källor:
   Verifierad av andra oberoende källor; logisk i sig själv; överensstämmer med annan information i ämnet.
2. Troligen sann:
   Inte bekräftad; logisk i sig själv; överensstämmer med annan information i ämnet.
3. Möjligtvis sann:
   Inte bekräftad; rimligt logisk i sig själv; överensstämmer med viss annan information i ämnet.
4. Tveksam:
   Inte bekräftad; möjlig men inte logisk; det finns ingen annan information i ämnet.
5. Osannolik:
   Inte bekräftad; inte logisk i sig själv; motsägs av annan information i ämnet.
6. Sanningshalt kan inte bedömas:
   Det finns ingen grund för att bedöma uppgiftens riktighet.

Myndigheten
för civilt försvar

Co-funded by
the European Union

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

“Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or ECCC. Neither the European Union nor the granting authority can be held responsible for them.”