Myndigheten för samhällsskydd och beredskap

Co-funded by the European Union

It-incidenters påverkan

Ramverk för bedömning av påverkan på it-miljö, verksamhet och samhälle

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

Foto omslag: Johan Eklund
Foto: Alex & Martin Photographers, Johan Eklund, Melker Dahlstrand, Mikael Svensson
Tryck: Åtta45
Produktion: Advant

Publikationsnummer: MSB2600 – juni 2025
ISBN-nummer: 978-91-7927-635-5

Förord

Myndigheten för samhällsskydd och beredskap har under många år mottagit och analyserat it-incidentrapporter. Detta har möjliggjort en datadriven utveckling av våra kunskaper och våra metoder, som vi sedermera har presenterat i våra temarapporter om digital leveranskedjesäkerhet, ändringshantering och cyberangrepp. Jag vill tacka de organisationer som rapporterat it-incidenter till MSB.

It-incidentrapporteringen ger många insikter om *karaktären* hos de incidenter som inträffar i Sverige. Denna rapport fokuserar särskilt på variationen i incidenternas natur – hur olika de kan vara och vilka utmaningar som uppstår när de ska jämföras. Den utforskar även hur dessa utmaningar kan hanteras för att säkerställa en enhetlig bedömning och klassificering av alla it-incidenter enligt samma ramverk.

Ramverket som vi presenterar i denna rapport syftar till att skapa en konsekvent och jämförbar analys av it-incidenters påverkan på it-miljö, verksamhet och samhället. Rapporten innehåller även fallstudier för att illustrera exempel på tillämpning.

Arbetet är viktigt. Cybersäkerhetsområdets betydelse för samhällets motståndskraft växer, och i samma takt växer också behovet av att analytiskt kunna ringa in dels de mest frekventa incidenterna, dels de mest allvarliga incidenterna. Av samma skäl är det också viktigt att stärka förmågan att kommunicera om hur allvarligt läget är, om exempelvis en cyberkris skulle uppstå.

Arbetet är samtidigt inte färdigt. Vi ser fram emot att fortsätta utveckla våra metoder för att förstå, analysera och bedöma utvecklingen, och vi ser fram emot att fortsätta diskussionen med alla som vill bidra till utvecklingen av samhällets cybersäkerhet.

Stockholm, 2025-06-12

Johan Turell

Verksamhetschef, Strategisk cybersäkerhet,
Avdelningen för cybersäkerhet och samhällsviktiga kommunikationer, Myndigheten för samhällsskydd och beredskap

Innehåll

Begreppsförteckning

Här redovisas de begrepp som är centrala för förståelsen av rapporten. Se Bilaga 1 för en mer djupgående redogörelse av de begrepp som använts i rapporten för att analysera it-incidenter.

Faktisk incident: Typ av incident. En händelse där *nytta förhindras* eller *skada orsakas* för den drabbade organisationen eller *nytta orsakas* eller *skada förhindras* för en av organisationens konkurrenter (se Bilaga 1 för en mer djupgående redogörelse av begreppets innebörd).

Incident: En inträffad oönskad händelse. Vid it-incidentrapportering delas incidenters orsaker in enligt *mänskliga hot* (både antagonistiska hot i form av angrepp och icke-antagonistiska hot i form av misstag), *tekniska hot* (i form av systemfel) eller *naturhot* (det kan handla om exempelvis väderfenomen, jordbävningar och solstormar).

Informationssystem: System för att samla in, lagra, bearbeta och distribuera information för ett givet ändamål.

It-miljö: En samlad mängd informationssystem som används för att behandla information som organisationen ansvarar för. Organisationens it-miljö omfattar både informationssystem som hanteras internt och de som är utkontrakterade.

Konfidentialitet: En aspekt av informationssäkerhet som i korthet innebär att endast behöriga kan ta del av information.

Monoberoende: En organisation har ett monoberoende av exempelvis en tjänst när den är beroende av den tjänsten och det saknas alternativa tjänster att använda ifall den tjänst man redan använder upphör.

Redundans: Tillstånd då mer än ett medel finns för att upprätthålla ett givet funktionssätt för att säkerställa kontinuerlig drift.

Resiliens: Förmåga hos en organisation att stå emot störningar.

Risk: En möjlig oönskad händelse.

Robusthet: Ett systems eller verksamhets förmåga att stå emot, anpassa sig till och återhämta sig från störningar eller påfrestningar, vilket säkerställer dess funktionalitet under förändrade eller oförutsedda förhållanden.

Samhällsviktig funktion: En viktig samhällsfunktion är nödvändig för samhällets grundläggande behov, värden eller säkerhet. Dessa funktioner upprätthålls och säkerställs av samhällsviktiga verksamheter.

Samhällsviktig infrastruktur: Avser till exempel strukturer för tele- och datakommunikation, elproduktion och eldistribution, bank- och finanssystem, samt olika transportledningssystem.

Samhällsviktig tjänst: Tjänster som betraktas som viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet inom den Europeiska unionen.

Samhällspåverkan: Samhällspåverkan uppstår när en eller flera händelser medför konsekvenser som förändrar, eller förändrar förutsättningarna för, samhällsviktiga funktioner, tjänster eller grundläggande värden.

Störning: En konsekvens av en incident som innebär att en digital tjänst inte kan tillhandahållas på avsett sätt.

Sårbarhet: Avsaknad av något som förhindrar, eller bidrar till att förhindra, att en incident inträffar.

Säkerhetshändelse: Typ av incident. En händelse där ett hot uppstår, ett skydd upphör, sårbarhet(er) uppstår, framgångsfaktor(er) upphör, brist(er) uppstår eller hinder uppstår (se Bilaga 1 för en mer djupgående redogörelse av begreppen).

Tillgänglighet: En aspekt av informationssäkerhet som i korthet innebär att information är nåbar när behöriga efterfrågar den.

Utpressningsangrepp: Angrepp som innebär att utpressningsprogram används eller att känslig information stjäls med hot om publicering eller radering om inte lösensumma betalas eller annat krav uppfylls.

Sammanfattning

Sammanfattning

Rapporten syftar till att stärka samhällets gemensamma förmåga att förstå och bedöma konsekvenserna av it-incidenter. Genom att ta fram ett ramverk för analys och bedömning presenterar rapporten ett strukturerat och enhetligt sätt att undersöka och förstå incidenters påverkan på it-miljö, verksamhet och samhället.

Ramverket bygger på en distinktion mellan säkerhetshändelser, händelser där ett hot eller hinder uppstår, och faktiska incidenter, där nytta förhindras eller skada orsakas. Genom att analysera olika händelser utifrån en bestämd taxonomi möjliggörs ett nyanserat resonemang och bedömning av påverkan i samband med inträffade incidenter.

För att pröva ramverket analyseras fem fallstudier. Fallstudierna bygger på öppna källor och de drabbade verksamheternas egna analyser och omfattar:

1. Ett datumfel i nya betalsystem i Ica-butiker och Apotek Hjärtats apotek.
2. Ett utpressningsangrepp mot Svenska kyrkans administrativa system.
3. Ett utpressningsangrepp mot ett av Tietoevrys datacenter.
4. En felaktig uppdatering som distribuerades automatiskt av Crowdstrike.
5. En misslyckad automatisk påfyllning av flytande kväve till kryofrysarna på Karolinska Institutet, som orsakades av ett tidigare servicearbete.

Fallstudierna visar hur modellen kan tillämpas på inträffade händelser. Analyserna kompletteras med lärdomar kring ramverkets tillämpning på fallstudien. Fallstudierna visar på variation i påverkan men också återkommande mönster, särskilt när det kommer till de lärdomar som kan dras från analysen. Bland annat framkommer att en säkerhetshändelse kan pågå under lång tid innan förutsättningarna för en faktisk incident uppstår.

Ramverket är utvecklat baserat på MSB:s erfarenheter och kunskaper från att under många år mottagit och analyserat it-incidentrapporter. Tanken är att det ska användas av samhällsviktiga verksamheter såväl som leverantörer och andra aktörer för att få en gemensam terminologi och förståelse för konsekvenser. Eftersom både teknik och samhälle förändras över tid kommer även ramverket att behöva utvecklas och förfinas. Denna rapport är ett första steg mot en mer systematisk syn på it-incidenter och hur de påverkar it-miljö, verksamhet och samhället i stort.

Om rapporten

Om rapporten

Inom ramen för denna rapport presenteras kriterier för bedömning av de konsekvenser en it-incident kan orsaka, inklusive i vilken utsträckning en it-incident kan sägas orsaka samhällspåverkan. Avsaknaden av bedömningskriterier bidrar idag till spekulationer och godtyckliga bedömningar. Denna rapports huvudsakliga syfte är att presentera ett ramverk för bedömning så att branschen får ett gemensamt förhållningssätt till sakområdet.

En fördjupad förståelse av vilka it-incidenter som leder till samhällspåverkan är avgörande för att kunna stärka motståndskraften i det digitaliserade samhället. Genom att systematiskt analysera incidenter är det möjligt att identifiera mönster, sårbarheter och förebyggande åtgärder.

MSB har under många år mottagit och analyserat rapporter om it-incidenter. Arbetet har resulterat i värdefulla insikter om hur olika incidenter påverkar it-miljöer, verksamheter och samhället i stort. Erfarenheterna har också möjliggjort metodutveckling, driven av behovet att kunna systematisera, analysera och jämföra incidenter på ett enhetligt sätt. Den metodik som presenteras i denna rapport är ett resultat av detta arbete och syftar till att ge ett strukturerat ramverk för bedömning och klassificering av it-incidenters påverkan. I rapporten analyseras it-incidenters påverkan utifrån aspekterna it-miljöpåverkan, verksamhetspåverkan och ytterst samhällspåverkan.

Rapporten har tagits fram med stöd av medel från EU inom ramen för ENIAC-projektet (The Enhanced NIS2 Implementation And Cooperation Project). Den riktar sig främst till analytiker, verksamhetsutvecklare och strateger inom it-verksamhet men också säkerhetsfunktioner och verksamhetsstöd, såsom informationssäkerhetssamordnare, CISO[1] och motsvarande nyckelroller i informations- och cybersäkerhetsarbetet.

I kapitlet ”Om påverkan på olika nivåer” beskrivs vad som menas med påverkan på it-miljö, verksamhet respektive samhälle i relation till it-incidenter. En central del av rapporten är det ramverk för bedömning av påverkan som presenteras i

Not 1. Chief information security officer, CISO ansvarar för samordning av informationssäkerhetsarbetet i en organisation.

kapitlet ”Bedömning av it-incidenters påverkan”. Ramverket har utvecklats för att kunna ge en sammanhängande och konsekvent bedömning av incidenters konsekvenser. MSB bedömer att det är avgörande att ha ett väl genomarbetat ramverk för att det ska fylla sitt syfte. Klassificeringar av incidenter får ofta karaktären av en förenklad tolkning av en mer komplex verklighet. Det är därför viktigt att klassificeringar görs med hög precision, transparens och underbyggda resonemang, så att de både tål granskning och kan bemötas på ett korrekt sätt. I kapitlet ”Fallstudier” analyseras verkliga incidenter utifrån ramverket. Syftet med fallstudierna är att bedöma incidenters påverkan men också att pröva ramverket. I rapportens sista kapitel kopplas ramverket och fallstudierna ihop i ett slutord.

Om påverkan på olika nivåer

Om påverkan på olika nivåer

It-incidenter kan ha en negativ påverkan som sträcker sig bortom enskilda individer, företag och organisationer. De kan även påverka samhället, dess institutioner, grundläggande värden och funktioner. Genom att förstå denna påverkan kan det förebyggande arbetet förbättras och utvecklas för att stärka Sveriges motståndskraft.

Ramverkets grundläggande delar

Ramverkets delar presenteras i sin helhet i Bilaga 1. Det bygger på en logik kring säkerhetshändelser och faktiska incidenter. En säkerhetshändelse är en oönskad händelse som påverkar säkerheten i it-miljö, verksamhet eller samhälle. Den behöver inte leda till någon faktisk skada, särskilt inte om det finns skyddsåtgärder eller redundans på plats. En faktisk incident å andra sidan är en säkerhetshändelse som lett till konkret negativ påverkan – till exempel genom att en funktion slutar fungera eller att skada uppstår.

Tabell 1. Översikt över taxonomi för säkerhetshändelser och faktiska incidenter

Säkerhetshändelse	Beskrivning	Exempel	Möjlig incident
Hinder uppstår	Något blockerar en funktion från att fungera som avsett.	En felaktig nätverkskonfiguration gör att en molntjänst inte kan kommunicera med andra system.	Nytta förhindras/ Skada förhindras
Framgångsfaktor upphör	En viktig faktor som krävs för att upprätthålla en funktion slutar fungera.	Ett kritiskt back-up-system går offline, vilket gör att dataförlust inte kan återställas.	Nytta förhindras/ Skada förhindras

Säkerhetshändelse	Beskrivning	Exempel	Möjlig incident
Hot uppstår	En säkerhets-händelse innebär en ökad risk för negativ påverkan.	Ett cyberspionage avslöjar känsliga företagsdata för en konkurrent.	Skada orsakas/ Nytta orsakas
Skydd upphör	Ett skyddssystem som tidigare förhindrade oön-skade händelser slutar fungera.	En brandväggs-regel tas bort, vilket möjliggör ett externt cyber-angrepp.	Skada orsakas/ Nytta orsakas

Påverkan på it-miljö, verksamhet och samhälle

I denna rapport presenteras ett ramverk för att analysera och bedöma hur allvarliga incidenter är, utifrån deras påverkan på tre olika nivåer: it-miljönivå, verksamhetsnivå och samhällsnivå. Dessa nivåer påverkar, och påverkas av varandra. Ramverket tillämpar ett helhetsperspektiv där varje nivå kan förstås som en del av ett större sammanhang. Analysen omfattar därför inte bara påverkan inom en enskild nivå, utan också hur påverkan förhåller sig mellan nivåer.

- **It-miljönivån** omfattar en organisations samlade informationssystem – både de som ägs och de som hyrs, inklusive molntjänster som tillhanda-hålls av externa leverantörer. Detta utgör den tekniska infrastrukturen där många incidenter först uppstår.
- **Verksamhetsnivån** avser hela organisationens funktionalitet och verksamhet i stort. På denna nivå analyseras hur it-incidenten påverkar organisationens förmåga att leverera sina tjänster, fatta beslut och upprätthålla operativ kontinuitet.
- **Samhällsnivån** avser den nivå där organisationers tjänster tillsammans skapar samhällets funktionalitet. Exempelvis vård, energi, betalningar eller transport – inom ett geografiskt område. På denna nivå bedöms hur en incident påverkar samhällets möjligheter att tillhandahålla grundläggande tjänster till medborgare, företag och andra aktörer.

Påverkan från en it-incident kan uppstå på en eller flera av dessa nivåer och behöver inte vara lika allvarlig överallt. En incident kan exempelvis ha viss påverkan på en funktion inom en organisations it-miljö, samtidigt som dess påverkan på den övergripande verksamheten är hanterbar och dess effekter på samhällsnivån obefintliga. För att bedöma påverkan används en kombination av information om vilka funktioner som påverkats, i vilken omfattning påverkan skett samt om det finns alternativ eller redundans som mildrar konsekvenserna. Ramverket möjliggör en systematisk och nyanserad analys av en incident, även i komplexa situationer där olika delar påverkas på olika sätt och i olika omfattning.

Påverkan på it-miljö

It-miljöpåverkan avser den påverkan som en incident har på en organisations samlade informationssystem, oavsett om dessa är egenägda eller inhyrda. Det inkluderar exempelvis servrar, molntjänster, nätverk, databaser och terminaler. Kategorin fångar säkerhetshändelser som påverkar organisationens it-miljö negativt. Det kan handla om att tillgängligheten, konfidentialiteten eller riktigheten hos informationssystemen, eller den information som lagras och behandlas i dem, har äventyrats. En faktisk incident på denna nivå uppstår exempelvis när en beståndsdel i it-miljön slutar fungera som avsett, och kompensatoriska åtgärder, som säkerhetskopior, redundans eller alternativa system, inte är tillräckliga för att fullt ut upprätthålla funktionaliteten.

Påverkan på verksamhet

Verksamhetspåverkan avser hur en it-incident påverkar en organisations förmåga att bedriva sin verksamhet. Det innefattar kärnverksamhet såväl som administrativa och stödjande funktioner. Bedömningen på denna nivå fokuserar på incidentens konsekvenser för organisationens funktionalitet, beslutsförmåga eller leveranskapacitet, och i förlängningen även på ekonomiska värden eller andra centrala intressen för verksamheten och dess intressenter.

Verksamhetspåverkan innebär att en säkerhetshändelse orsakar eller bidrar till att orsaka en faktisk incident för den drabbade organisationen – eller för andra, genom organisationen. En faktisk incident på denna nivå kan bestå i att nytta förhindras alternativt att skada orsakas för organisationen eller dess uppdragsgivare och intressenter. Det kan även handla om att nytta orsakas eller skada förhindras för organisationens konkurrenter eller för andra, på ett sätt som inte ligger i organisationens intresse.

En påverkan på denna nivå är inte nödvändigtvis beroende av en föregående påverkan på it-miljön även om sådana samband ofta förekommer. Påverkan på verksamhet uppstår när det saknas alternativ eller reservlösningar för att upprätthålla verksamheten som avsett. Det kan handla om uteblivna leveranser, störningar i vårdkedjan, försenade beslut, men även förlust av kontroll och förtroendeskador. I analysen är det avgörande att identifiera vilken del av organisationens funktion som påverkas, hur allvarlig påverkan är och i vilken utsträckning verksamheten kan anpassa sig, fortsätta enligt alternativa arbetssätt eller återhämta sig inom rimlig tid.

Påverkan på samhälle

Samhällspåverkan uppstår när en eller flera händelser medför konsekvenser som förändrar samhällsviktiga funktioner, tjänster eller grundläggande värden samt dess förutsättningar. Samhällspåverkan kan vara både positiv och negativ. Denna rapport är dock avgränsad till negativ samhällspåverkan.

Samhällspåverkan kan delas in i direkt och indirekt påverkan. Direkt påverkan uppstår omedelbart som en följd av en incident – exempelvis när ett cyberangrepp slår ut en samhällsviktig tjänst, vilket leder till att människor inte kan ta ut pengar, sjukhus förlorar tillgång till patientjournaler eller transporter störs. Dessa konsekvenser sker per automatik utan ytterligare agerande från externa aktörer.

Indirekt påverkan uppstår däremot genom reaktioner och följdeffekter som incidenten medför. Det kan handla om hur samhället, myndigheter eller företag agerar för att hantera situationen, exempelvis genom krishantering, skärpta säkerhetsåtgärder eller förändrade regelverk. Indirekt påverkan kan också inkludera hur andra aktörer, såsom konkurrenter eller hotfulla aktörer, utnyttjar situationen för egna syften. Exempelvis kan ett företag stärka sin position på marknaden om en konkurrent drabbas av en omfattande driftstörning, eller så kan en incident påverka allmänhetens förtroende för digitala tjänster, vilket på sikt kan leda till förändrade beteenden och policybeslut.

En faktisk incident på samhällsnivå uppstår när påverkan är så pass omfattande att samhällsnyttan uteblir, hotas eller urholkas – och det saknas tillräcklig förmåga att kompensera eller återställa funktionalitet inom rimlig tid.

Att förstå både den direkta och indirekta påverkan av en incident är avgörande för att kunna bedöma dess fulla samhällseffekter. För att stärka samhällets motståndskraft krävs därför en helhetssyn där både omedelbara och efterföljande konsekvenser tas i beaktande.

It-incidenter som orsakar, eller bidrar till att orsaka, samhällspåverkan

It-incidenter som leder till samhällspåverkan uppstår sällan isolerat – de utgör ofta en del av en kedja där flera faktorer samverkar. En it-incident kan vara både utlösande faktor (en så kallad ”trigger”) eller förvärrande omständighet i en redan kritisk situation. Till exempel kan ett cyberangrepp mot ett elbolag under extremväder förvärra effekterna av strömavbrott.

Samhällspåverkan kan uppstå direkt, som när ett angrepp mot ett sjukhus slår ut journalsystem och påverkar vården. Det kan också uppstå indirekt, som när en it-störning fördröjer hanteringen av en pågående kris, exempelvis räddningstjänstens kommunikation vid en naturkatastrof.

Exempel: Samhällspåverkan

Ett exempel är cyberangreppet mot Synnovis i Storbritannien 2024. På kort sikt ställdes 800 operationer in på grund av uteblivna blodanalyser. På längre sikt bidrog incidenten till nationell blodbrist, i kombination med andra samhällsfaktorer. It-incidenten både orsakade och förvärrade samhällspåverkan.[2]

Not 2. BBC. *Blood stocks drop to ’unprecedentedly low levels’*. https://www.bbc.com/news/articles/cw4y2x2kn4ko (Hämtad 05/2024).

Enligt MSB:s ramverk uppstår faktisk samhällspåverkan antingen när *nytta förhindras* (en funktion slutar fungera) eller när *skada orsakas* (exempelvis läckta personuppgifter[3] eller personskador). Det vanligaste scenariot är att nytta förhindras, särskilt när system kopplade till samhällsviktiga funktioner drabbas. Faktorer som avgör om påverkan uppstår på samhällsnivå är ofta varaktigheten i störningen, om alternativa lösningar finns och hur många verksamheter eller människor som drabbas.

Robusthet och resiliens spelar en avgörande roll. Robusthet handlar om att motstå störningar, exempelvis genom redundanta system eller alternativa rutiner. Resiliens handlar om att återhämta sig snabbt, exempelvis genom fungerande incidenthantering och återställning. Den relativt låga frekvensen av it-incidenter som orsakar skada på samhällsnivå kan möjligen tillskrivas att många verksamheter har inbyggd robusthet och resiliens, vilket begränsar skadeverkningarna. Samtidigt är det viktigt att kontinuerligt utveckla och stärka dessa förmågor, eftersom hotlandskapet förändras och komplexiteten i digitala ekosystem ökar.

MSB:s tidigare analyser visar att monoberoenden – där många är beroende av en enda aktör – kan skapa stora konsekvenser vid incidenter. Men ofta finns alternativa aktörer, vilket minskar effekterna. Exempelvis kunde kunder i Sverige handla i andra butiker när Coops kassasystem låg nere 2021 till följd av it-angreppet mot Kaseya.[4]

Not 3. Läckta personuppgifter innebär inte bara en kränkning för den enskilde, utan påverkar även rätten till privatliv. Rätten till privatliv är en mänsklig rättighet och en grundläggande princip i ett demokratiskt samhälle.

Not 4. SVT. *It-attacken mot Coop – detta har hänt.* https://www.svt.se/nyheter/inrikes/it-attacken-mot-coop-detta-har-hant (Hämtad 05/2025).

Tabellen nedan exemplifierar händelser som skulle kunna uppstå till följd av en eller flera incidenter.

Tabell 2. Händelser som skulle kunna uppstå till följd av en eller flera incidenter

Nytta förhindras för samhället	Skada orsakas för samhället
It-incidenten orsakar eller bidrar till att orsaka: • en störning som orsakar att elförsörjningen till ett större antal hushåll och företag uteblir i flera dygn. • en störning som orsakar att ett signifikant ekonomiskt tillskott för samhället uteblir.	It-incidenten orsakar eller bidrar till att orsaka: • en störning som resulterar i ett antal döda eller skadade. • en störning som resulterar i en signifikant ekonomisk kostnad för samhället.

Skada förhindras för andra på bekostnad av samhället	Nytta orsakas för andra på bekostnad av samhället
It-incidenten orsakar eller bidrar till att orsaka: • att system som används för att försvara ett land militärt slås ut för att underlätta en förestående invasion. • att bevis för korruption förstörs.	It-incidenten orsakar eller bidrar till att orsaka: • att hemliga uppgifter om exempelvis totalförsvarsplanering hamnar i händerna på utländska aktörer. • att beslut fattas som gynnar andra aktörer, exempelvis angripare, på bekostnad av samhället intresse.

I exemplen framgår att ramverket skiljer på direkt kausalitet (orsakar) och indirekta konsekvenser (resulterar i). ”Orsakar” används när en it-incident direkt leder till en händelse, utan att ytterligare triggers krävs. ”Resulterar i” används när en incident bidrar till en konsekvens genom en indirekt effekt eller en kedja av händelser. Ett exempel som illustrerar skillnaden är när ett cyberangrepp som slår ut ett sjukhus it-system orsakar att patientjournaler blir otillgängliga, vilket i sin tur resulterar i försämrad vårdkvalitet och i vissa fall livshotande konsekvenser.

Bedömning av it-incidenters påverkan

Bedömning av it-incidenters påverkan

Introduktion

Ramverket för bedömning av påverkan tar sin utgångspunkt i att en it-incident har inträffat. Det innebär per definition att en *säkerhetshändelse* har inträffat i en organisations it-miljö. Säkerhetshändelsen i it-miljön *kan* i sin tur, men måste inte, utgöra en *faktisk incident* i it-miljön. It-incidenten kan också utgöra eller medföra en säkerhetshändelse i organisationens verksamhet, och den säkerhetshändelsen *kan* i sin tur, men måste inte, utgöra en faktisk incident i organisationens verksamhet. På motsvarande sätt kan händelsen också utgöra en säkerhetshändelse på samhällsnivå, och under vissa omständigheter *kan* den säkerhetshändelsen i sin tur utgöra en faktisk incident på samhällsnivå.

Figur 1. Illustration av hur it-incidenter, säkerhetshändelser och faktiska incidenter förhåller sig till varandra

Händelser som utgör säkerhetshändelser kan fördelas över ett spektrum över deras allvarlighetsgrad där ena änden utgörs av renodlade säkerhetshändelser som inte i någon bemärkelse liknar en faktisk incident, medan andra änden är renodlade faktiska incidenter. Det är genom att dela in spektrumet mellan de två extremerna som bedömningsklasser definieras i ramverket.

Modellen omfattar fyra bedömningsnivåer (*kritisk, allvarlig, betydande och måttlig*) som tillämpas för att bedöma påverkan på it-miljön, verksamhet och samhället.

Syftet med att använda bedömningsnivåerna är att på ett strukturerat sätt bedöma hur allvarligt läget är, utifrån den information som finns tillgänglig. Bedömningen sker först inom en avgränsad del av en viss nivå, exempelvis en specifik del av en organisations it-miljö eller en del av elförsörjningen i en kommun. Om det finns information om ytterligare delar på samma nivå – exempelvis en annan del av organisationens it-miljö eller en annan del av kommunens elförsörjning – kan även dessa bedömas.

Nedan följer en förenklad beskrivning av hur bedömningar av en it-incidents påverkan kan göras för respektive område:

Tabell 3. Tabellen visar hur påverkan av en it-incident kan variera mellan olika nivåer

Allvarlighetsgrad	It-miljö	Organisation	Samhälle
Kritisk	Kritisk		
Allvarlig		Allvarlig	
Betydande			Betydande
Måttlig			

Tabellen visar att den aktuella it-incidenten har bedömts som kritisk inom it-miljön, med allvarlig påverkan på organisationens verksamhet och med betydande samhällspåverkan. En sådan bedömning kan exempelvis grundas på ett scenario där en kommun utsätts för ett cyberangrepp som leder till att hela eller stora delar av kommunens it-miljö blir otillgänglig. Detta får, givet bristande kontinuitetsarbete, allvarliga konsekvenser för kommunens förutsättningar att bedriva sin verksamhet, vilken i sin tur riskerar leda till en betydande påverkan på samhället.

Viktigt att veta är att respektive bedömningsnivå innefattar ett större antal delar och områden. Om endast en del av en nivå har bedömts, exempelvis mejlservrarna inom en organisations it-miljö, kan klassificeringen för den delen indikera det samlade läget. Bedömningen av mejlservrar kan ge en indikation på den potentiella påverkan på hela it-miljön, på samma sätt som en analys av elförsörjningen i en kommun kan indikera bredare konsekvenser.[5]

För att det ska vara möjligt att göra en bedömning, och för att det ska vara möjligt för andra reproducera den bedömningen, behöver det som ska bedömas definieras och avgränsas. Avgränsningen består av fem delar:

1. Avgränsningar inom it-miljön, verksamhet eller samhället.
2. Avgränsning till interna förhållanden.
3. Avgränsning av incidenter.
4. Avgränsning mellan direkta konsekvenser och följdeffekter.
5. Avgränsning i tid.

De olika avgränsningarna beskrivs i de nästföljande avsnitten.

Not 5. Se avsnittet ”*Samlade bedömningar av påverkan på respektive nivå*” nedan.

Avgränsningar inom it-miljön, verksamhet eller samhället

Oavsett om det är påverkan på it-miljön, verksamhet eller samhället som ska bedömas, måste bedömningen göras inom en tydlig avgränsning på den aktuella nivån. Vissa organisationer har flera separata it-miljöer eller tydligt segmenterade system. Andra har flera avgränsade delar av verksamheten, såsom kommuner med olika förvaltningar eller företagskoncerner med flera dotterbolag. På samhällsnivå kan samhällsviktiga tjänster utföras av olika aktörer på olika geografiska nivåer – exempelvis dagligvaruhandel inom en kommun, transporter/infrastruktur inom en region, internetbanktjänster på nationell nivå eller molntjänster som verkar internationellt. Resiliens, redundans och geografisk spridning är avgörande faktorer för att bedöma vilken, om någon, påverkan en it-incident får på it-miljön, verksamheten eller samhället.

Om en samhällsviktig tjänst – exempelvis dricksvattenförsörjning – upphör att fungera i en kommun på grund av att it-systemet som upprätthåller tjänsten fallerar, kan påverkan bli allvarlig. Om dessutom förmågan att återställa tjänsten (resiliensen) är begränsad och återställningen därför tar lång tid, samt inga alternativa lösningar (redundans) finns inom kommunen, kan tjänstens nytta för samhället utebli under en längre period utan att kunna ersättas.

I en sådan situation kan påverkan på samhällets förmåga att tillhandahålla denna funktion i kommunen bedömas som allvarlig eller kritisk, särskilt om incidenten blir långvarig. Om tjänsten även var den enda i hela det geografiska området, påverkas funktionaliteten i större utsträckning. Däremot, om andra dricksvattenverk i det geografiska området kan understödja tjänsten via separata it-system, kan samhällspåverkan på regional nivå bedömas som delvis kritisk, medan bedömningen för den enskilda kommunen kvarstår som allvarlig eller kritisk.

När ramverket tillämpas ska det därför alltid framgå vad som bedöms. Exempelvis kan det anges att bedömningen gäller hela företaget X:s it-miljö, företaget Y:s webbproduktion eller dricksvattenförsörjningen i kommunen Z.

Avgränsning till interna förhållanden

Bedömningarna som görs i ramverket handlar om interna förhållanden i det som bedöms. När it-miljöpåverkan bedöms är det påverkan inom it-miljön som bedöms, exempelvis i form av i vilken utsträckning påverkan på mejlservrarnas funktionalitet har uppstått. När påverkan på organisationens verksamhet bedöms handlar det om möjligheten för organisationen att bedriva eller få till stånd sådan verksamhet som har drabbats av incidenten, såsom möjligheten att hantera och expediera inkommande kundordrar. När påverkan på samhället bedöms är det med avseende på samhällets möjlighet att fortsätta att möjliggöra eller tillhandahålla sådan funktionalitet som har störts, exempelvis genom att ge vård utan stöd av digitala journaler.

När ramverket tillämpas ska det därför framgå att det är de interna förhållandena inom den nivå och den avgränsade del av den valda nivån som bedöms.

Avgränsning av incidenter

En och samma incident kan orsaka, eller leda till, nya incidenter. I det här ramverket görs därför bedömningen för en incident i taget, och för en nivå i taget – det vill säga påverkan på antingen it-miljön, verksamheten eller samhället.

Om en incident i exempelvis it-miljön orsakar en störning i organisationens verksamhet, och den störningen i sin tur leder till konsekvenser för samhället, ska dessa bedömas som tre separata incidenter – en per nivå. På så sätt blir det tydligt vad som påverkar vad, och hur långtgående konsekvenserna är.

Exempel: En incident som orsakar nya incidenter

En incident inträffar i it-systemet som styr filtreringen i ett vattenverk. Incidenten innebär att filtreringen av dricksvatten upphör, samtidigt som vattenverket fortsätter att pumpa ut vatten till det kommunala vattennätet.

- Påverkan på it-miljönivå: Den ursprungliga incidenten är ett fel i styrsystemet – det är en faktisk incident i vattenverkets it-miljö.
- Påverkan på verksamhetsnivå: Eftersom it-incidenten leder till att orenat vatten distribueras, fungerar vattenverkets verksamhet inte längre som avsett. Det är en separat faktisk incident i vattenverkets verksamhet.
- Påverkan på samhällsnivå: Dricksvattenförsörjningen har fallerat. Det utgör en ytterligare faktisk incident, nu på samhällsnivå. En följdverkan av den incidenten är dessutom att människor i området dricker det kontaminerade vattnet och insjuknar.

Även om dessa tre händelser hänger ihop orsaksmässigt, ska de alltså analyseras separat. Det beror på att de utgör olika fenomen, med olika typer av påverkan och ofta kräver olika typer av åtgärder eller expertis. It-incidenten kan behöva lösas av tekniker, driftstörningen hanteras av vattenverkets personal och hälsoeffekterna kräver insatser från vård- och smittskyddsmyndigheter.

Effektiv incidenthantering kräver därför både samordning och tydlig ansvarsfördelning. De som arbetar med att hantera samhällseffekterna behöver information om hur verksamheten påverkas – och verksamhetsansvariga behöver i sin tur förstå orsaken till störningen i it-miljön.

När ramverket tillämpas ska det därför framgå vad det är för incident som analyseras och på vilken nivå, samt hur incidenten skiljs från eventuella följder av den ursprungliga incidenten.

Avgränsning mellan direkta konsekvenser och följdeffekter

I analysen av it-incidenters påverkan på it-miljö, verksamhet och samhälle är det viktigt att göra en distinktion mellan direkta konsekvenser av en incident och de effekter som följer av de reaktioner som incidenten utlöser. En reaktion är inte en automatisk följd av en händelse i sig, utan snarare en utlösande faktor för en ny kausal kedja.

Detta innebär att när en organisation reagerar på en incident – exempelvis genom att investera i ny utrustning eller återhämtning av system – är dessa åtgärder i sig en respons på incidenten. Samtidigt ger de också upphov till ytterligare konsekvenser, såsom ekonomiska kostnader, organisatoriska förändringar eller förändrad riskuppfattning.

Att analytiskt separera de direkta konsekvenserna av en incident från de följdeffekter som uppstår genom reaktioner är inte ett sätt att reducera betydelsen av reaktionerna eller deras kostnader. Tvärtom är det en viktig distinktion för att förstå både hur incidenter påverkar system på olika nivåer och hur reaktiva åtgärder kan forma cybersäkerhetsarbetet. Denna uppdelning gör det också möjligt att mer precist analysera berörda aktörers val och strategier och hur de påverkar incidentens långsiktiga effekter.

När ramverket tillämpas ska det därför framgå om det är incident eller en reaktion på en incident som bedöms.

Avgränsning i tid

Som det föregående avsnittets exempel visar kan tidsaspekten vara avgörande för hur incidenter, och incidenter de orsakar eller resulterar i, ska bedömas och hanteras. Hur länge en incident pågår är avgörande för bedömningen. Det gäller särskilt när incidenten hindrar it-miljön, verksamheten eller samhället från att skapa nytta.

Det är också möjligt att tidsaspekten inte spelar så stor roll. Om incidenten handlar om att ett intrång har skett kan det många gånger vara mindre betydelsefullt hur länge intrånget har pågått – det viktiga är då att information som skulle skyddas inte skyddas längre.

När ramverket tillämpas ska därför incidentens varaktighet framgå om det är nödvändigt för bedömningen.

Olika bedömningar på olika nivåer

En och samma incident kan bedömas olika på olika nivåer. En incident där utpressningsprogramvara har stängt ner en it-miljö kan resultera i att påverkan på it-miljönivå kan bedömas som kritisk. Om organisationens verksamhet kan bedrivas på andra sätt utan it-stöd, behöver incidenten inte nödvändigtvis ha en kritisk påverkan på verksamhetsnivån.

Det omvända kan också gälla. Om information har läckt ifrån en it-miljö kanske det inte nödvändigtvis orsakar, eller resulterar i, mer än måttlig påverkan på it-miljön – men det kan föranleda att organisationen behöver fatta beslut om stora ändringar i verksamheten.

Samlade bedömningar av påverkan på respektive nivå

Ramverket möjliggör klassificering och bedömning av incidenter på it-miljö-, verksamhets- och samhällsnivå inom avgränsade och definierade delar. Inom varje nivå görs en bedömning inom en avgränsning (se tidigare avsnitt i kapitlet ovan). Påverkan kan uppstå inom flera avgränsade delar på en och samma nivå. Exempelvis kan en och samma incident både påverka en organisations möjlighet att tillhandahålla webbtjänster och dess möjlighet att omhänderta kundordrar. Om incidenten gör att webbtjänsterna inte kan tillhandahållas alls medan vissa kundordrar fortfarande kan omhändertas, är påverkan olika inom olika delar av organisationens verksamhet. Den samlade bedömningen av påverkan på organisationens verksamhet tar då sin utgångspunkt i den avgränsade del av verksamheten som bedöms ha påverkats värst.

Exempelvis, om det är klarlagt att en it-incident har medfört att en viss organisations samtliga mejlservrar (en del av organisationens it-miljö) helt har slutat att fungera, och it-incidenten antingen redan har pågått länge (eller kommer att pågå länge) blir bedömningen att it-incidentens påverkan på den del av it-miljön som utgörs av mejlservrar är kritisk. Om det är okänt hur incidenten har påverkat övriga delar av it-miljön, säger ramverket, givet den information som finns tillgänglig, att påverkan på *hela* den organisationens it-miljö *som värst* är kritisk. Om det sedan framkommer vilken påverkan it-incidenten har haft på andra delar av samma organisations it-miljö aggregeras de olika bedömningarna, med utgångspunkt i den allvarligaste angivna bedömningsklassen. Om även de andra delarna av it-miljön har angetts vara drabbade av kritisk påverkan kvarstår bedömningen att påverkan på *hela den organisationen som värst är kritisk*. Om det visar sig att andra delar av samma organisations it-miljö inte har påverkats på ett lika allvarligt sätt blir den aggregerade bedömningsklassen för hela it-miljön som *värst delvis kritisk påverkan*.

På motsvarande sätt kan en och samma incident ha påverkan inom flera olika områden på samhällsnivå.

Exempel: Påverkan på flera nivåer

Cyberangreppet mot Kalix kommun i december 2021 illustrerar hur en enskild incident kan få flera olika typer av påverkan inom en kommuns egen verksamhet och på samhället i stort. Eftersom kommunen ansvarar för en rad viktiga tjänster och funktioner, resulterade angreppet i störningar på flera nivåer – från it-miljön, till den interna organisationens förmåga att bedriva sin verksamhet, samt i förlängningen påverkan på samhället.

It-miljöpåverkan. Angreppet mot Kalix kommun påverkade hela kommunens digitala infrastruktur.[6] Påverkade system låg nere i tre veckor, vilket innebar en omfattande påverkan på *hela* den tekniska miljön. Eftersom angreppet ledde till total nedstängning av systemen och krävde att samtliga datorer genomgick kontroller och säkerhetsuppdateringar, kan påverkan på *hela* it-miljön klassificeras som *kritisk* enligt bedömningsmodellen. Dock påbörjades återställningsarbetet relativt snabbt, vilket begränsade ytterligare spridning och långsiktig påverkan.

Verksamhetspåverkan. Cyberangreppet innebar en allvarlig påverkan på organisationens verksamhet, särskilt inom socialförvaltningen. Förvaltningens verksamhet fick gå över till manuella arbetssätt, inklusive dokumentation på papper, telefonsamordning och fysiska planeringstavlor. Trots dessa åtgärder drabbades socialförvaltningens verksamhet av störningar, såsom svårigheter att genomföra utbetalningar av ekonomiskt bistånd och hantera socialtjänstens ärenden. Tack vare tidigare krisövningar och kontinuitetsplaner kunde verksamheten dock hålla igång grundläggande funktioner. Påverkan på socialförvaltningens verksamhet bedöms som *betydande* enligt ramverket. Den samlade bedömningen för hela kommunens verksamhet är *som värst betydande* påverkan.

Samhällspåverkan. Socialtjänsten ansvarar för flera samhällsviktiga funktioner, såsom äldreomsorg, vård och omsorg samt ekonomiskt bistånd. Angreppet påverkade flera av dessa områden. Dock fungerade viktiga tjänster, såsom digitala lås och trygghetslarm, vilket mildrade effekten på de mest sårbara grupperna. Snabba åtgärder och möjligheten att använda alternativa arbetssätt gör att samhällspåverkan för funktionerna äldreomsorg, vård och omsorg samt ekonomiskt bistånd bedöms som *betydande*. Den samlade bedömningen för samhällspåverkan blir därför *som värst betydande* i det geografiska området som kommunen ansvarar för.

Not 6. Eftersom analysen av it-miljöpåverkan omfattar hela den digitala infrastrukturen är bedömningen samtidigt en samlad bedömning.

Tillämpning av ramverket i operativt arbete

Ramverket är designat så att det både ska kunna användas för långsiktig strategisk analys, och för bedömning av pågående incidenter i samband med operativ hantering, exempelvis i samband med cyberkrishantering.

Information om en pågående incident uppdateras ofta fortlöpande, vilket kan innebära att information tillkommer som gör att tidigare bedömningar måste omvärderas. I ett tidigare läge kanske påverkan inom en viss avgränsad del av en verksamheten bedömdes som *kritisk*, och bedömningen blev gränssättande för den samlade bedömningen av vilken påverkan en it-incident *som värst* har på organisationens samlade verksamhet. Med tillkommande information blir det kanske tydligt att påverkan inte var fullt så omfattande inom just den delen av verksamheten. Om det samtidigt tillkommer information om en annan avgränsad del av organisationens verksamhet som gör att den får bedömningsklassen *allvarligt* påverkad blir istället bedömningen av den delen av verksamheten gränssättande. Den samlade bedömningen av påverkan på organisationens samlade verksamhet går då från *som värst kritisk påverkan* till *som värst delvis allvarlig påverkan*.

Ett fiktivt exempel illustrerar tillämpning i operativt arbete:

En större offentlig verksamhet upptäcker en it-incident där deras dokumenthanteringstjänst har drabbats av en driftstörning. Incidenten gör att anställda inte kan komma åt dokument och system som krävs för det dagliga arbetet, vilket leder till förseningar i handläggningsprocesser. Vid denna tidpunkt är det oklart om andra system har påverkats. Påverkan bedöms som *betydande* för dokumenthanteringstjänsten i organisationens it-miljö och *som värst betydande* för hela organisationen.

Efter ytterligare analys visar det sig att flera databaser har blivit korrupta och att viktiga filer riskerar att gå förlorade. Återställningen kommer att kräva mer tid än initialt bedömt, och vissa avdelningar kan inte arbeta effektivt under tiden. Det står också klart att dokumenthanteringstjänsten har en mer central funktion än först antaget och att dess påverkan även stör andra administrativa processer. Incidenten omvärderas och klassificeras nu som *allvarlig* för den drabbade tjänsten och *som värst allvarlig* för organisationen.

Ytterligare undersökningar visar dock att flera andra viktiga system, såsom e-post samt ekonomi- och personalsystem, fortsätter att fungera normalt. Alternativa rutiner, såsom användning av äldre filkopior och utskrifter, har implementerats, vilket gör att påverkan på organisationens totala verksamhet blir mer hanterbar. Bedömningen justeras därför till att påverkan *som värst är delvis allvarlig* för hela organisationen, då vissa delar fungerar normalt medan andra fortfarande har störningar.

Händelsen illustrerar hur en it-incident kan omvärderas allteftersom ny information tillkommer och visar vikten av en stegvis bedömning för att fatta informerade beslut om hantering och skadebegränsning.

Bedömning av påverkan på it-miljön, verksamhet och samhälle

Nedan beskrivs exempel på it-incidenters påverkan utifrån ramverkets kriterier för påverkan. Exemplen i tabellerna underlättar bedömning av en it-incidents påverkan för respektive nivå.

Följande kriterier gäller för respektive påverkansnivå:

En it-incident har kritisk påverkan på (hela eller delar av) it-miljön, verksamheten eller samhället om (minst) en säkerhetshändelse har inträffat (d.v.s. ett hot har uppstått, ett skydd har upphört, en framgångsfaktor har upphört eller ett hinder har uppstått) och (minst) en faktisk incident har inträffat (skada har orsakats, skada har förhindrats, nytta har förhindrats eller nytta har orsakats).

En it-incident har allvarlig påverkan på (hela eller delar av) it-miljön, verksamheten eller samhället om it-incidenten inte har kritisk påverkan och (minst) en säkerhetshändelse har inträffat och det är mer korrekt att bedöma att (minst) en faktisk incident har inträffat än det är att bedöma att ingen faktisk incident har inträffat.

En it-incident har betydande påverkan på (hela eller delar av) it-miljön, verksamheten eller samhället om it-incidenten inte har allvarlig påverkan och (minst) en säkerhetshändelse har inträffat och det inte är mer korrekt att bedöma att enbart en (eller flera) säkerhetshändelse(r) har inträffat.

En it-incident har måttlig påverkan på (hela eller delar av) it-miljön, verksamheten eller samhället om it-incidenten inte har betydande påverkan.

En it-incident har ingen påverkan på (hela eller delar av) it-miljön, verksamheten eller samhället om it-incidenten inte har inneburit någon säkerhetshändelse med påverkan på it-miljö, verksamhet eller samhälle.

Bedömning av påverkan på it-miljö

Tabell 4. Översikt som visar exempel på möjliga händelser och påverkan på it-miljön

Säkerhetshändelse	Faktisk incident	Kritisk	Allvarlig	Betydande	Måttlig
Hot uppstår	**Skada orsakas, nytta förhindras**	Skadlig kod installeras och krypterar alla lagringsmedia.	Skadlig kod krypterar mer än hälften av lagringsmedia.	Skadlig kod krypterar mindre än hälften av lagringsmedia.	Skadlig kod installeras och krypterar enstaka lagringsmedia.
Skydd upphör	**Nytta förhindras, skada orsakas**	Alla brandväggar slutar att fungera.	Mer än hälften av brandväggarna slutar att fungera.	Mindre än hälften av brandväggarna slutar att fungera.	Mindre än hälften men fler än enstaka brand-väggar slutar fungera.
Framgångsfaktor upphör	**Nytta förhindras**	Alla servrar är otillgängliga.	Mer än hälften av servrarna är otillgängliga.	Mindre än hälften av servrarna är otillgängliga.	Mindre än hälften men fler än enstaka servrar är otillgängliga.
Hinder har uppstått	**Nytta förhindras**	Fullständig blockering i kommunikationslösningar.	Omfattande men inte fullständig blockering i kommunikationslösningar.	Delvis blockering i kommunikationslösningar.	Delvis blockering i kommunikationslösningar så att trafik inte kan flöda.

Bedömning av påverkan på organisationens verksamhet

Tabell 5. Översikt som visar exempel på möjliga händelser och påverkan på organisationens verksamhet

Säkerhetshändelse	Faktisk incident	Kritisk	Allvarlig	Betydande	Måttlig
Hot uppstår	**Skada orsakas, nytta förhindras**	Det installeras en wiper som gör att informationssystem som verksamheten använder för att upprätthålla en molntjänst som de tillhandahåller till sina kunder krypteras. Molntjänsten är helt nedstängd för alla användare.	Det installeras en wiper som gör att informationssystem som verksamheten använder för att upprätthålla en molntjänst som de tillhandahåller till sina kunder krypteras. Molntjänsten är helt nedstängd för mer än hälften, men inte alla, användare.	Det installeras en wiper som gör att informationssystem som verksamheten använder för att upprätthålla en molntjänst som de tillhandahåller till sina kunder krypteras. Molntjänsten är helt nedstängd för mindre än hälften, men fler än enstaka, användare.	Det installeras en wiper som gör att informationssystem som verksamheten använder för att upprätthålla en molntjänst som de tillhandahåller till sina kunder krypteras. Molntjänsten är helt nedstängd för enstaka användare.
Skydd upphör	**Nytta förhindras, skada orsakas**	Ett angrepp riktas mot ett centralt system för åtkomsthantering och avaktiverar multifaktorautentisering. Organisationens skydd mot intrång upphör helt.	Ett angrepp riktas mot ett centralt system för åtkomsthantering och avaktiverar multifaktorautentisering. Mer än hälften av organisationens tjänster är utan skydd.	Ett angrepp riktas mot ett centralt system för åtkomsthantering och avaktiverar multifaktorautentisering. Mindre än hälften av organisationens tjänster är utan skydd.	Ett angrepp riktas mot ett centralt system för åtkomsthantering och avaktiverar multifaktorautentisering. Enstaka tjänster är utan skydd.
Framgångsfaktor upphör	**Nytta förhindras**	All data raderas i de system som vanligtvis används i arbetet och kan inte återställas alls från andra källor. Uppdrag kan inte genomföras i tid.	All data raderas i de system som vanligtvis används i arbetet. Mindre än hälften kan återställas. Flera uppdrag kan inte genomföras i tid.	All data raderas i de system som vanligtvis används i arbetet. Mer än hälften kan återställas. Några uppdrag kan inte genomföras i tid.	All data raderas i de system som vanligtvis används i arbetet. Majoriteten data kan återställas. Enstaka uppdrag kan inte genomföras i tid.
Hinder har uppstått	**Skada orsakas, nytta förhindras**	Det installeras en wiper som gör att informationssystem som organisationen använder för att upprätthålla en molntjänst som organisationen tillhandahåller till sina kunder krypteras. Molntjänsten är helt nedstängd för alla användare.	Det installeras en wiper som gör att informationssystem som organisationen använder för att upprätthålla en molntjänst som organisationen tillhandahåller till sina kunder krypteras. Molntjänsten är helt nedstängd för mer än hälften, men inte alla, användare.	Det installeras en wiper som gör att informationssystem som organisationen använder för att upprätthålla en molntjänst som organisationen tillhandahåller till sina kunder krypteras. Molntjänsten är helt nedstängd för mindre än hälften, men fler än enstaka, användare.	Det installeras en wiper som gör att informationssystem som organisationen använder för att upprätthålla en molntjänst som organisationen tillhandahåller till sina kunder krypteras. Molntjänsten är helt nedstängd för enstaka användare.

Bedömning av påverkan på samhället

Tabell 6. Översikt som visar exempel på möjliga händelser och påverkan på samhället

Säkerhetshändelse	Faktisk incident	Kritisk	Allvarlig	Betydande	Måttlig
Hot uppstår	**Skada orsakas, nytta förhindras**	Det installeras skadlig kod i informationssystemen som upprätthåller en molntjänst där regionen lagrar alla tagna röntgenbilder. Inga tagna röntgenbilder lagras någon annanstans.	Det installeras skadlig kod i informationssystemen som upprätthåller en molntjänst där regionen lagrar alla tagna röntgenbilder. Enstaka tagna röntgenbilder lagras någon annanstans.	Det installeras skadlig kod i informationssystemen som upprätthåller en molntjänst där regionen lagrar alla tagna röntgenbilder. Mindre än hälften, men fler än enstaka, tagna röntgenbilder lagras någon annanstans.	Det installeras skadlig kod i informationssystemen som upprätthåller en molntjänst där regionen lagrar alla tagna röntgenbilder. Fler än hälften, men inte alla, tagna röntgenbilder lagras någon annanstans.
Skydd upphör	**Nytta förhindras, skada orsakas**	Alla reningssystem i dricksvattenverket på en viss plats har slutat att fungera.	Mer än hälften av alla reningssystem i dricksvattenverket på en viss plats har slutat att fungera.	Mindre än hälften av alla reningssystem i dricksvattenverket på en viss plats har slutat att fungera.	Enstaka reningssystem i dricksvattenverket på en viss plats har slutat att fungera.
Framgångsfaktor upphör	**Nytta förhindras**	Alla de tillgängliga telenäten på en viss plats förstörs.	Mer än hälften av de tillgängliga telenäten på en viss plats förstörs.	Mindre än hälften av de tillgängliga telenäten på en viss plats förstörs.	Enstaka tillgängliga telenät på en viss plats förstörs.
Hinder har uppstått	**Nytta förhindras**	Alla de tillgängliga telenäten på en viss plats blockeras.	Mer än hälften av de tillgängliga telenäten på en viss plats blockeras.	Mindre än hälften av de tillgängliga telenäten på en viss plats blockeras.	Enstaka tillgängliga telenät på en viss plats blockeras.

Exempel på samlad bedömning

Skadlig kod installeras och krypterar *alla* lagringsmedia i organisationens it-miljö. Den skadliga koden gör att informationssystem som används för att upprätthålla en molntjänst som organisationen tillhandahåller till sina kunder krypteras. Molntjänsten är helt nedstängd för *alla* användare. Regionen lagrar alla tagna röntgenbilder i molntjänsten. *Färre än hälften, men fler än enstaka* tagna röntgenbilder lagras också någon annanstans.

Bedömningsklasser för respektive nivå:

- *Kritisk* påverkan på it-miljöns lagringsmedia, *som värst kritisk påverkan* på hela it-miljön.
- *Kritisk* påverkan på molntjänsten som organisationen tillhandahåller till sina kunder, *som värst kritisk påverkan* på hela verksamheten.
- *Betydande* påverkan på möjligheten att inom regionens geografiska område bedriva vård med stöd av röntgenbilder, *som värst betydande påverkan* på all vårdverksamhet inom regionens geografiska område.

Om mer information sedan tillkommer kanske bedömningsklasserna justeras till följande:

- *Kritisk* påverkan på it-miljöns lagringsmedia, *som värst delvis kritisk påverkan* på hela it-miljön.
- *Kritisk* påverkan på molntjänsten som organisationen tillhandahåller till sina kunder, *som värst delvis kritisk påverkan* på hela verksamheten.
- *Allvarlig* påverkan på möjligheten att inom regionens geografiska område bedriva vård med stöd av röntgenbilder, *som värst delvis allvarlig påverkan* på all vårdverksamhet inom regionens geografiska område.

Information som skulle kunna tillkomma och ändra bedömningen enligt exemplet ovan är till exempel om det framkommer information om möjlighet till återställning såsom en säker kopia som kan återställas eller om vissa system i it-miljön fortfarande fungerar eller snabbt kan isoleras och skyddas. I de fallen kan den samlade påverkan mildras.

Fallstudier

Fallstudier

Genom ett antal kortare fallstudier testas ramverket i praktiken. Det ger insikter i hur det kan användas för att bedöma påverkan vid it-incidenter – och hur sådana bedömningar kan stärka samhällets motståndskraft.

Detta kapitel omfattar korta fallstudier där aktuella it-incidenter analyseras med hjälp av MSB:s ramverk för bedömning av it-incidenters påverkan på it-miljön, verksamheten och samhället. Fallstudierna har förkortats och förenklats i syfte att göra bedömning och resonemang lättare att följa. Samtliga redogörelser är baserade på uppgifter som kommunicerats öppet i media samt aktörernas egna publicerade analyser.

Varje fallstudie är indelad i följande delar:

- **Sammanfattning:** Innehåller en sammanfattande bedömning av incidenten och dess påverkan.
- **Incidentbeskrivning:** Innehåller en övergripande beskrivning, baserad på öppna källor, med avvägda detaljer för att kunna bedöma hur incidenten påverkar it-miljö, verksamheten respektive samhället.
- **Analys av it-miljöpåverkan:** Innehåller analys av incidentens påverkan på it-miljön utifrån MSB:s ramverk för bedömning av it-incidenter.
- **Analys av verksamhetspåverkan:** Innehåller analys av incidentens påverkan på en organisations verksamhet utifrån MSB:s ramverk för bedömning av it-incidenter.
- **Analys av samhällspåverkan:** Innehåller analys av incidentens påverkan på samhället utifrån MSB:s ramverk för bedömning av it-incidenter.
- **Lärdomar:** Här återges de lärdomar som kan dras utifrån fallstudien och analysen av påverkan på olika nivåer.

Ica och Apotek Hjärtat

- **Incidenten:** Ett datumfel i nya betalsystem gjorde att terminaler inte kunde hantera kortbetalningar på skottdagen.
- **Faktiska incidenter:** Faktiska incidenter uppstod i it-miljön (kortterminals-systemet), på verksamhetsnivå (försäljning och kundflöde), samt på samhällsnivå (tillgång till dagligvaror och läkemedel).
- **It-miljöpåverkan:** *Måttlig* fram till dagen innan den 29 februari och *kritisk* under delar av den 29 februari.
- **Verksamhetspåverkan:** *Måttlig* fram till dagen innan den 29 februari och *betydande* under delar av den 29 februari.
- **Samhällspåverkan:** *Måttlig* fram till dagen innan den 29 februari, och *måttlig* under delar av den 29 februari. *Betydande* i de delar av landet där Ica och Apotek Hjärtat var enda alternativ för att handla dagligvaror och läkemedel.

Incidentbeskrivning

Under förmiddagen den 29 februari 2024 uppstod problem med kortbetalningar i samtliga Ica-butiker och Apotek Hjärtats apotek runt om i landet. Problemen påverkade alla bankkort, oavsett kortutgivare. Alternativa betalningsmetoder såsom kontanter, Swish eller betalning via app fungerade som vanligt.[7]

Incidenten bestod i att datumet 29 februari (skottdagen) saknades i betalsystemet, vilket ledde till att terminalerna inte kunde hantera kortbetalningar.[8] Detta fel hade inte uppstått tidigare skottår, utan var kopplat till introduktion av nya terminaler. Vid 12.30 meddelade Ica-gruppen att kortbetalningar åter fungerar i de flesta butiker och apotek.[9]

Analys av it-miljöpåverkan

Analys av påverkan på it-miljö avgränsas till systemen som hanterar kortbetalningar. Ett systemfel i betalsystemet gjorde att datumet 29 februari saknades. Det resulterade i att terminalerna inte kunde hantera kortbetalningar. Avsaknaden av det aktuella datumet innebar en säkerhetshändelse i form av *framgångsfaktor upphör*. Säkerhetshändelsen hade pågått sedan de nya terminalerna introducerades. Innan den 29 februari var inte säkerhetshändelsen någon *faktisk incident*, men den 29 februari blev den det, av typen *nytta förhindras* när systemet försökte hantera betalningar på ett datum som systemet inte kunde känna igen. Det fanns inte heller någon alternativ funktionalitet att falla tillbaka på som kunde möjliggöra

Not 7. SVT, *Betalproblemet hos Ica löst: ”Skottdagsproblem”*. https://www.svt.se/nyheter/inrikes/betalproblem-pa-ica-kort-funkar-inte (Hämtad 04/2025).

Not 8. Dagligvarunytt!. *Betalhaveriet hos Ica löst.* https://www.dagligvarunytt.se/i-butik/sakerhet/betalhaveriet-hos-ica-lost/ (Hämtad 04/2025).

Not 9. SVT, *Betalproblemet hos Ica löst: ”Skottdagsproblem”*. https://www.svt.se/nyheter/inrikes/betalproblem-pa-ica-kort-funkar-inte (Hämtad 04/2025).

betalningarna ändå. Inget tyder på att Icas och Apotek Hjärtats it-system var påverkade på något annat sätt. Incidenten var avgränsad till endast den del av it-miljön som berör kortbetalningar. Bedömningen på it-miljö avser därför endast de delarna. Incidenten bedöms som *måttlig* fram till dagen innan den 29 februari och som *kritisk* under delar av den 29 februari.

Analys av verksamhetspåverkan

Analys av påverkan på verksamhetsnivå avser verksamheternas förmåga att ta betalt för dagligvaror, läkemedel och andra apoteksvaror. Eftersom möjligheten att ta emot kortbetalningar den 29 februari inte hade funnits sedan nya terminaler installerades hade en säkerhetshändelse av typen *framgångsfaktor upphör* på verksamhetsnivå pågått under en lång tid. När den 29 februari inföll innebar det att incidenten inte bara var en säkerhetshändelse eftersom det inte var möjligt att ta betalt via kort. Det var dock fortfarande möjligt att betala med andra betalmedel som swish, företagets appar eller kontanter i de flesta butiker. De uteblivna betalningarna hade viss påverkan på försäljningen den 29 februari och troligen måttlig påverkan på försäljningen på längre sikt. Uppgifter saknas om exakt hur många kortbetalningar som inte kunde genomföras den dagen, eller hur många betalningar som skedde med alternativa betalsätt. På verksamhetsnivå bedöms incidenten, av typen *nytta förhindras*, därför som *måttlig* fram till dagen innan den 29 februari och som *betydande* under delar av den 29 februari.

Analys av samhällspåverkan

Analys av påverkan på samhällsnivå avser möjligheten att handla dagligvaror, läkemedel och andra apoteksvaror. Där Ica och Apotek Hjärtat var enda alternativ hade en säkerhetshändelse på samhällsnivå pågått ända sedan de nya terminalerna installerades.

Säkerhetshändelsen var av typen *framgångsfaktor upphör.* Det pågick såvitt känt inte några incidenter hos Icas och Apotek Hjärtats konkurrenter den 29 februari. Det gick också att handla dagligvaror och apoteksvaror från de påverkade butikerna och apoteken genom att använda andra sorters betalmedel den dagen. I orter där både de aktuella verksamheterna och minst någon konkurrent till respektive organisation finns var samhällspåverkan därför *måttlig*, om det överhuvudtaget uppstod någon, under delar av den 29 februari. I områden där endast Ica respektive endast Apoteket Hjärtat finns var samhällspåverkan däremot *betydande*. På samhällsnivå (avseende möjligheten att handla dagligvaror, läkemedel och andra apoteksvaror) bedöms incidenten därför som *måttlig* fram till dagen innan den 29 februari, och som *måttlig* under delar av den 29 februari. Där Ica respektive Apotek Hjärtat var enda alternativ för inköp av dagligvaror, läkemedel och andra apoteksvaror var samhällspåverkan *betydande* under delar av den 29 februari. Incidenten är av typen *nytta förhindras* även på samhällsnivå.

Lärdomar

Fallstudien illustrerar att vissa säkerhetshändelser kan ligga dolda under lång tid – i detta fall ett datumfel som blev synligt först på skottdagen. Det betonar vikten av att testa system för sällsynta men förutsägbara scenarier. Analysen visar också att påverkan varierar geografiskt, och att förekomsten av alternativa betalsätt kan mildra samhällspåverkan. Analysen visar också ett exempel på att påverkan bedöms inom avgränsade delar. It-miljöpåverkan avgränsas till system för kortbetalningar och verksamhetspåverkan till förmåga att ta betalt. Ramverket hanterar avgränsningar per funktion och gradvis eskalering från måttlig påverkan till betydande under dagen när terminalerna slutade fungera.

Både Ica och Apoteket Hjärtat hade tillgång till alternativa betalningsmetoder vilket möjliggjorde försäljning trots störningen. Ramverket hjälper till att visa att tillgången till alternativa arbetssätt eller lösningar minskar påverkan. Slutligen visar fallstudien att ramverket möjliggör bedömning utifrån den allvarligast drabbade delen på respektive nivå.

Svenska kyrkan

- **Incidenten:** Utpressningsangrepp som innebar att Svenska kyrkans administrativa system fick stängas ned.
- **Faktiska incidenter:** Faktiska incidenter uppstod i it-miljön (administrativa system), verksamhetsnivå (hantering av administrativ verksamhet och begravningar) samt samhällsnivå (begravningsverksamhet).
- **It-miljöpåverkan:** *Allvarlig* påverkan.
- **Verksamhetspåverkan:** *Betydande* påverkan.
- **Samhällspåverkan:** *Måttlig* påverkan på begravningsverksamhet under tiden incidenten pågick, *betydande* på förlust av kontroll över personuppgifter på längre sikt.

Incidentbeskrivning

Den 23 november 2023 utsattes Svenska kyrkan för ett utpressningsangrepp. När Svenska kyrkan upptäckte incidenten vidtogs omedelbara åtgärder för att skydda it-system och information. Det innebar bland annat att Svenska kyrkan stängde ned all åtkomst till berörda system och bytte samtliga lösenord. Därefter pågick intensivt arbete med att återstarta alla system. Funktioner som har stor betydelse för församlingarnas arbete prioriterades.[10]

Den 15 november, åtta dagar före angreppet, skickade MSB/CERT-SE en varning via e-post om att angrepp av den aktuella typen kunde förekomma. Meddelandet skickades till en funktionsbrevlåda som främst används för användarfrågor. Varningen uppmärksammades dock inte som ett prioriterat säkerhetsmeddelande vid det tillfället. Enligt kyrkokansliet förekommer säkerhetsvarningar och larm om sårbarheter regelbundet – både från leverantörer som Microsoft, som rapporterar flera allvarliga sårbarheter varje vecka, och från myndigheter som MSB. Den stora mängden varningar kan bidra till att det är svårt att avgöra vilka som kräver omedelbara åtgärder.

Ansvaret för datorer och säkerhet hos Svenska kyrkan har till stor del legat på lokal nivå. Efter angreppet upptäcktes att flera datorer var felregistrerade och inte kunde hittas när de skulle installeras om. Det visade sig även att en del servrar uppkopplade mot kyrknätet inte hade uppdaterat säkerhetssystemen på flera år, samt att användare hade fel behörigheter i form av att för många hade rättigheter som administratörer.[11]

Not 10. TT. *Det fortsatta arbetet efter cyberangreppet.* https://via.tt.se/pressmeddelande/3393640/det-fortsatta-arbetet-efter-cyberangreppet?publisherId=1344892&lang=sv (Hämtad 04/2025).

Not 11. Kyrkans Tidning. *Darknet, lösensummor och telefonkedjor – läs om cyberattacken mot Svenska kyrkan.* https://www.kyrkanstidning.se/nyhet/darknet-losensummor-och-telefonkedjor-sa-gick-cyberattacken-mot-svenska-kyrkan-till (Hämtad 04/2025).

Angreppet påverkade bland annat system som hanterar ekonomi, fakturering, löner och begravningsverksamhet.[12] Det påverkade i sin tur arbetet i pastorat och församlingar i hela landet. Det gick exempelvis inte alls att boka vigslar eller dop. Kyrkoärenden fick skötas med papper och penna.[13]

Begravningsverksamheten uppges ha fungerat som vanligt utan större svårigheter i de flesta delar av landet, enligt Svenska kyrkan. De problem som fanns, och som uppmärksammades i medier, gällde främst gravsättning i familjegravar. Det var tillgången till den så kallade gravboken där det framgår hur tidigare gravsatta kistor och urnor är placerade som påverkades av angreppet. Utan tillgång till den kunde man inte gräva i familjegravar utan att riskera att skada de som tidigare gravsatts.[14]

Den 22 januari 2024 fungerade Svenska kyrkans webbplats igen efter att ha legat nere sedan november. Det dröjde ytterligare ett tag innan all information var uppdaterad och aktuell igen.

Den 21 maj 2024 konstaterades det att en stor mängd stulna data har publicerats på Darknet. De flesta filer som stulits kom från 3 100 datorer, vilket motsvarar ungefär 10 procent av Svenska kyrkans datoranvändare. Data hade även stulits från servrar.

Analys av it-miljöpåverkan

Analys av påverkan på it-miljö avgränsas till centrala administrativa system i Svenska kyrkans nationella och lokala nätverk. Enligt MSB:s ramverk för bedömning av it-incidenter innebär säkerhetshändelsen att ett *hot uppstår* när nya angreppsmetoder utvecklas och som utnyttjar funktioner i it-miljön som inte säkerhetsuppdaterats i tid.[15] Därefter inträffade ytterligare en säkerhetshändelse, ett angrepp, som innebar att en *framgångsfaktor upphör* när Svenska kyrkans it-system slås ut och en stor mängd data krypteras och exfiltreras. Den faktiska incidenten handlade om att system för ekonomi, fakturering, lön och bokningar påverkas och *nytta förhindras*. Påverkan bedöms som *allvarlig* för de centrala administrativa systemen och *som värst allvarlig* för hela Svenska kyrkans it-miljö eftersom den omfattar stora delar, men inte hela Svenska kyrkans it-miljö.

Not 12. TT. *Det fortsatta arbetet efter cyberangreppet.* https://via.tt.se/pressmeddelande/3393640/det-fortsatta-arbetet-efter-cyberangreppet (Hämtad 04/2025).

Not 13. SVT. *Stora problem efter cyberattack mot Svenska kyrkan*. https://www.svt.se/nyheter/lokalt/helsingborg/stora-problem-efter-cyberattack-mot-svenska-kyrkan--wv2vhq (Hämtad 04/2025).

Not 14. TT. *Det fortsatta arbetet efter cyberangreppet.* https://via.tt.se/pressmeddelande/3393640/det-fortsatta-arbetet-efter-cyberangreppet?publisherId=1344892&lang=sv (Hämtad 04/2025).

Not 15. Eftersom avsaknad av säkerhetsuppdatering inte är en förändring i sig är säkerhetshändelsen det förändrade hotet.

Analys av verksamhetspåverkan

Analys av påverkan på verksamhetsnivå avser administrativ verksamhet i Svenska kyrkans pastorat och församlingar i hela landet. Säkerhetshändelsen utgjordes av att verksamheten inte kunde använda de digitala systemen för viktiga administrativa funktioner, det vill säga att en *framgångsfaktor upphört*. *Nytta förhindras* när vigsel- och dopbokningar inte kunde hanteras digitalt. Det uppstod även förseningar och ökad belastning genom alternativa arbetssätt. Utifrån att flera väsentliga delar av verksamheten drabbats och behövde bedrivas genom alternativa arbetssätt över en längre tid bedöms verksamhetspåverkan som *betydande* för den administrativa verksamheten och *som värst betydande* för hela Svenska kyrkans verksamhet. Svenska kyrkan hade viss redundans i form av manuella arbetssätt.

Analys av samhällspåverkan

Analys av påverkan på samhällsnivå avser Svenska kyrkans roll som utförare av begravningsverksamhet samt följdverkningar som följd av ett dataintrång. Säkerhetshändelsen av typen *framgångsfaktor upphör* innebar en *faktisk incident* när Svenska Kyrkan utsattes för ett cyberangrepp som resulterade i störningar i system som hanterar ekonomi, fakturering, lön, bokning av vigslar och dop samt begravningsverksamhet. Den *faktiska incidenten* innebar att *nytta förhindrades* när störningen påverkade arbetet i pastorat och församlingar i hela landet. Kyrkoärenden stoppades inte helt utan många ärenden kunde ändå skötas genom manuella arbetssätt, exempelvis med hjälp av papper och penna.

På de allra flesta platser i landet fungerade den normala verksamheten för begravningar utan större svårigheter. Påverkan berörde specifikt begravningar i familjegravar vilket utgör en mindre andel av de begravningar som genomförs. Dessutom fanns viss redundans inom tjänsten då gravböcker även fanns tillgängliga fysiskt inom flera församlingar. Sammantaget gör detta att trots att incidenten pågick under en längre tid, innebar den bara *måttlig* påverkan på begravningsverksamhet och *som värst måttlig* påverkan på samhället.

Följdverkningar genom de läckta personuppgifterna innebar ytterligare en faktisk incident av typen *skada orsakas* i *betydande* omfattning för det långsiktiga förtroendet för samhällets institutioner och dess förmåga att säkerställa fri- och rättigheter såsom rätten till privatliv.

Lärdomar

Från analysen av Svenska Kyrkans it-incident framgår att en säkerhetshändelse kan pågå under lång tid innan den innebär påverkan och blir en faktisk incident. Nya angreppsmetoder som utvecklas kan utnyttja brister i konfiguration och uteblivna uppdateringar i system utan att säkerhetshändelsen upptäcks förrän angreppet genomförs. Det illustrerar vikten av detektionsförmåga och proaktiv sårbarhetshantering för att kunna hantera och åtgärda säkerhetshändelser i tid innan de innebär större påverkan.

Analysen visar även hur olika delar drabbas olika. Den värst drabbade delen styr den samlade bedömningen på varje nivå. Exempelvis var det centrala administrativa system som drabbades värst medan andra delar av it-miljön inte påverkades i samma utsträckning. Analysen visar sedan att samhällspåverkan kan vara begränsad trots att det handlar om en långvarig incident, eftersom det fanns redundans och alternativa arbetssätt. Ramverket hjälper till att identifiera att påverkan var lokal och begränsad till vissa typer av begravningar. Slutligen exemplifierar analysen hur ramverket möjliggör en separat klassificering av ny påverkan vid följdverkningar.

Tietoevry

- **Incidenten:** Ett utpressningsangrepp mot ett av Tietoevrys datacenter.
- **Faktiska incidenter:** Faktiska incidenter uppstod i it-miljön (datacenter), på verksamhetsnivå (leverans av molntjänst) och samhällsnivå (tillgång till stödsystem).
- **It-miljöpåverkan:** *Kritisk* påverkan.
- **Verksamhetspåverkan:** *Kritisk* påverkan.
- **Samhällspåverkan:** *Allvarlig* påverkan.

Incidentbeskrivning

Under natten mellan den 19 och den 20 januari 2024 drabbades ett av Tietoevrys datacenter i Sverige av ett utpressningsangrepp. När Tietoevrys övervakning upptäckte misstänkt och ovanlig aktivitet vidtogs åtgärder för att begränsa angreppets påverkan. Bland annat fattades ett beslut om att temporärt isolera plattformen som påverkades.[16]

Incidenten innebar påverkan för ett stort antal statliga myndigheter när hr-systemet Primula, som administreras av Statens Servicecenter, inte gick att nå. Primula nyttjas av 120 myndigheter med sammantaget omkring 60 000 anställda. Under tiden för störningen var det inte möjligt för organisationer som nyttjar tjänsten att exempelvis administrera löner eller medarbetares egenrapportering, såsom sjukfrånvaro eller semester.

Statens Servicecenter meddelade att de kunde implementera reservrutiner när incidenten inträffade och att händelsen inte påverkade januari månads löner vars hantering redan slutförts.[17]

Incidenten påverkade även ett stort antal aktörer inom hälso- och sjukvårdssektorn, inklusive flera regioner och kommuner. Detta primärt på grund av att plattformen Prator, som vårdinstanser nyttjar för kommunikation, var otillgänglig. Störningen innebar att flera hälso- och sjukvårdsinstanser behövde nyttja alternativa arbetssätt vid exempelvis utskrivning av patienter. Det medförde medarbete för vårdpersonal och i vissa fall även en fördröjning. Flera regioner bland andra Region Blekinge, Sörmland och Uppsala, gick upp i stabsläge för att hantera störningen. Den 2 februari var Prator i drift i Region Västerbotten och Region Blekinge, medan för Region Sörmland och Region Uppsala tog det ytterligare ett tag. Enligt Region Västerbotten har vården har anpassat sig bra

Not 16. Tietoevry. *Tietoevry: Slutsatser gällande ransomware-attacken*. https://www.tietoevry.com/se/nyhetsrum/alla-nyheter-och-pressmeddelanden/pressmeddelande/2024/04/tietoevry-slutsatser-gallande-ransomwarattacken/ (Hämtad 04/2025).

Not 17. Statens servicecenter. *Cyberattack påverkar Tietoevrys tjänster till ett antal kunder i Sverige*. https://www.statenssc.se/nyheter/nyhetsarkiv/2024-01-21-cyberattack-paverkar-tietoevrys-tjanster-till-ett-antal-kunder-i-sverige (Hämtad 04/2025).

trots störningarna, samtidigt har det inneburit extra belastning. Deras erfarenhet är att papper och penna fortfarande har stor betydelse när ett nödläge uppstår.[18]

I minst två fall kunde krypterad information tillhörande kundorganisationer inte återställas. I Vellinge kommun betraktades mycket av den information som påverkades, inklusive avslutade patientjournaler från äldreboenden och inom socialtjänsten, som förlorad.[19] Många av de informationssystem som driftades av Tietoevry behövde därutöver återställas från grunden, vilket orsakade omfattande merarbete för kommunen. Konsekvenserna av incidenten innebar ett omfattande administrativt pussel men det var aldrig någon risk för liv och hälsa. Enligt kommunen ska alla patienter fått vård enligt plan och det finns inga indikationer om att personuppgifter skulle ha spridits.[20]

Analys av it-miljöpåverkan

Analys av påverkan på it-miljö avgränsas till Tietoevrys påverkade datacenter. Säkerhetshändelsen handlade om att ett *hot uppstår* när datacentret utsätts för ett utpressningsangrepp. All information som lagrades i centrets molnlösningar krypterades, medan angriparna krävde en lösensumma för att dekryptera informationen. Den faktiska incidenten innebar att *nytta förhindras*. Eftersom händelsen hade en stark påverkan på datacentrets funktionalitet bedöms påverkan som *kritisk* för den avgränsade delen av Tietoevrys it-miljö, samt *som värst kritisk* för hela it-miljön. Ytterligare säkerhetshändelser och följdverkningar i form av faktiska incidenter omfattas inte av denna bedömning.

Analys av verksamhetspåverkan

Analys av påverkan på verksamhetsnivå avser leverans av Tietoevrys utbud av molntjänster. Säkerhetshändelser på verksamhetsnivå innebar att en *framgångsfaktor upphör* när kunddata som lagrades i datacentret krypterades. Den faktiska incidenten handlade om att *nytta förhindras* eftersom molntjänsterna inte kunde levereras som avsett. Notera att incidenten hos Tietoevry även innebär följdverkningar i form av incidenter hos de kunder som använder Tietoevry som leverantör av it. Dessa säkerhethändelser och följdverkningar i form av faktiska incidenter omfattas inte av denna bedömning. Bedömningen av verksamhetpåverkan är *kritisk* påverkan på Tietoevrys molntjänstutbud.

Verksamhetspåverkan sker även i de organisationer som påverkas av att molntjänsterna inte kunde levereras som avsett. I enlighet med metoden utgör detta separata följdincidenter som bedöms fristående från huvudincidenten och verksamhetspåverkan i Tietoevrys verksamhet. Exempel på verksamhetspåverkan är störningar hos de myndigheter som använder hr-systemet Primula för administration. När systemet inte var tillgängligt innebar det en säkerhetshändelse av

Not 18. Dagens Medicin. *Regionchefer drar lärdomar efter hackerattacken*. https://www.dagensmedicin.se/vardens-styrning/digitalisering/regionchefer-drar-lardomar-efter-hackarattacken/ (Hämtad 04/2025).

Not 19. Vellinge kommun. *IT-attacken som drabbat Vellinge kommun får stora följder.* https://vellinge.se/nyhetsarkiv/2024/01/it-attacken-som-drabbat-vellinge-kommun-far-mycket-stora-foljder/ (Hämtad 04/2025).

Not 20. SVT. *Efter hackerattacken i Vellinge: Journaler spårlöst borta.* https://www.svt.se/nyheter/lokalt/skane/efter-hackerattacken-journaler-sparlost-borta-i-vellinge (Hämtad 04/2025).

typen *framgångsfaktor upphör* i den del av verksamheten som hanterar personalfrågor. *Nytta förhindras* där det saknades alternativa arbetssätt. Bedömningen är *som värst betydande* verksamhetspåverkan för den del av verksamheten som hanterar personalfrågor på de myndigheter som använder Primula till det att alternativa arbetssätt implementerades och påverkan minskade.

Analys av samhällspåverkan

Samhällspåverkan i samband med Tietoevrys incident utgjordes av avbrott i tillgång till information och informationssystem som flera av Tietoevrys kunder nyttjade inom sin dagliga verksamhet. Säkerhetshändelsen på samhällsnivå innebar att en *framgångsfaktor upphör.* Den faktiska incidenten handlade om att *nytta förhindras* för ett större antal statliga myndigheter men även kommuner, företag och aktörer inom hälso- och sjukvårdssektorn. Tietoevry kunde återställa stora delar av de drabbade informationssystemen under de första dagarna efter angreppet, men i ett mindre antal fall förblev tjänsterna och informationen inom dem otillgängliga till och med mitten av mars. I ett begränsat antal fall kunde den krypterade informationen inte återställas.[21] Sammantaget bedöms påverkan på samhällsnivå att *nytta förhindras* i *allvarlig* omfattning för de samhällsfunktioner som har påverkats.

Händelsen innebar även följdincidenter på samhällsnivå. Precis som med exemplet ovan med verksamhetspåverkan för de myndigheter som använder Primula analyseras följdincidenter som innebär samhällspåverkan separat. Exempel på följdincident som innebar samhällspåverkan är påverkan på hälso- och sjukvårdssektorn när kommunikationsplattformen Prator inte var tillgänglig. Säkerhetshändelsen innebar att en *framgångsfaktor upphörde*. Där alternativa arbetssätt saknades innebar det påverkan i form av att *nytta förhindras* avseende möjligheten att bedriva hälso- och sjukvårdsverksamhet. Påverkan bedöms till *betydande* och innebar förutom merarbete även förseningar.

Lärdomar

Fallstudien visar att ramverket skiljer på huvudincident och följdincidenter vilket är avgörande för en strukturerad analys. Störningen i Tietoevrys datacenter fick spridning i flera andra organisationer. Ramverket ger analytiskt stöd genom att klargöra att verksamhetspåverkan och samhällspåverkan hos kundorganisationer är följdincidenter och ska analyseras separat från leverantörens incident. Det möjliggör en mer nyanserad bedömning per aktör. Angreppet mot datacentret utlöste både tekniska och verksamhetsrelaterade säkerhetshändelser. Ramverket gör det möjligt att klassificera och förstå dessa händelser i sin egen rätt, även om de inträffar samtidigt. Säkerhetshändelsen i it-miljön innebar att *hot uppstod*, medan säkerhetshändelsen i verksamheten innebar att *framgångsfaktor upphörde.* Fallstudien ger slutligen exempel på hur bedömning av avgränsade delar görs som grund för den samlade bedömningen.

Not 21. Tietoevry. *Tietoevry: Slutsatser gällande ransomware-attacken.* https://www.tietoevry.com/se/nyhetsrum/alla-nyheter-och-pressmeddelanden/pressmeddelande/2024/04/tietoevry-slutsatser-gallande-ransomwarattacken/ (Hämtad 04/2025)

Crowdstrike

- **Incidenten:** Felaktig uppdatering distribueras automatiskt.
- **Faktisk incident:** Faktisk incident uppstod på verksamhetsnivå (distribution av programvara) och på samhällsnivå (tillgång till flera samhällsviktiga verksamheter).
- **It-miljöpåverkan:** *Ingen påverkan.*
- **Verksamhetspåverkan:** *Allvarlig* för den felaktiga leveransen och *som värst betydande* för förtroendeskadan.
- **Samhällspåverkan:** *Som värst allvarlig.*

Incidentbeskrivning

Under morgonen den 19 juli 2024 uppmärksammades omfattande globala störningar i säkerhetsplattformen Crowdstrike. Företaget bekräftade att störningarna orsakats av en felaktig uppdatering som automatiskt skickats ut till kunder. På förmiddagen samma dag drog Crowdstrike tillbaka uppdateringen och skickade ut en ny version för att åtgärda felet.[22] Enligt Microsoft slogs omkring 8,5 miljoner enheter ut globalt.[23] Många kunder kunde inte installera rättelsen eftersom systemen redan låg nere.

Incidenten hos Crowdstrike orsakade omfattande störningar globalt och drabbade flera sektorer. I Australien sammankallades ett krismöte på regeringsnivå.[24] Mediebranschen påverkades, bland annat tvingades nyhetskanalen Sky News i Storbritannien stänga sin verksamhet tillfälligt.[25] Flygtrafiken störtes i både USA och Europa, med problem i biljett- och incheckningssystem, förseningar och tillfälliga flygplatsstängningar – däribland sju amerikanska och Berlins flygplats.[26] [27] Hälso- och sjukvården i Storbritannien, USA och Tyskland drabbades, med störningar i journalsystem, inställda operationer och påverkan på det amerikanska nödnumret 911. Även bank- och finanssektorn globalt påverkades, med svårigheter att nå handelsplattformar och betalningssystem.[28]

Not 22. Crowdstrike. *Remediation and guidance hub: Channel file 291 incident.* https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/ (Hämtad 04/2025).

Not 23. SVT. *Experten: Det kan vi lära oss av it-haveriet.* https://www.svt.se/nyheter/inrikes/experten-det-kan-vi-lara-oss-av-it-haveriet (Hämtad 04/2025).

Not 24. Dagens PS. *Global krasch: ”Värre än en cyberattack”.* https://www.dagensps.se/varlden/global-krasch-varre-an-en-cyberangrepp/ (Hämtad 04/2025).

Not 25. Dagens PS. *Global krasch: ”Värre än en cyberattack”.* https://www.dagensps.se/varlden/global-krasch-varre-an-en-cyberangrepp/ (Hämtad 04/2025).

Not 26. Dagens Nyheter. *Problemen kan dröja kvar i dagar efter globala it-haveriet.* https://www.dn.se/varlden/flyg-stoppas-over-hela-varlden-efter-globalt-it-haveri/ (Hämtad 04/2025).

Not 27. Svenska Dagbladet. *Globalt it-kaos – flera flygplatser har stängt.* *https://www.svd.se/a/OooP1l/it-problem-varlden-over-flyg-stalls-in* (Hämtad 04/2025).

Not 28. Dagens Nyheter. *Problemen kan dröja kvar i dagar efter globala it-haveriet.* https://www.dn.se/varlden/flyg-stoppas-over-hela-varlden-efter-globalt-it-haveri/ (Hämtad 04/2025).

I Sverige noterades störningar framför allt inom transportsektorn. Ett flertal regioner rapporterade problem med webbplatser och biljettsystem i kollektivtrafiken under förmiddagen den 19 juli, men trafikpåverkan uteblev och problemen åtgärdades snabbt. Flygplatser upplevde förseningar till följd av internationella störningar, och både SAS och Ryanair rapporterade påverkan.[29] LKAB:s gruva i Malmberget utrymdes som en säkerhetsåtgärd men produktionen återupptogs samma dag.[30] Karlstads kommun rapporterade om störningar i tre system, dock utan större konsekvenser.[31]

Analys av it-miljöpåverkan

Incidenten utgjorde inte en säkerhetshändelse hos Crowdstrike. Den felaktiga uppdateringen orsakade däremot sekundära effekter hos Crowdstrikes kunder. Servrar och klienter som körde Microsoft Windows och Falcon Sensor blev obrukbara efter att ha mottagit uppdateringen. I miljöer där redundans saknades utgjorde detta sannolikt en säkerhetshändelse av typen *hinder uppstår*, och faktiska incidenter där *nytta förhindrades*. De följdverkningar som den felaktiga uppdateringen ledde till i de påverkande kundmiljöerna omfattas inte i bedömningen ”ingen påverkan” på it-miljö utan avser endast Crowdstrikes egna it-miljö.

Analys av verksamhetspåverkan

Analys av påverkan på verksamhetsnivå avser leverans av programvara. Säkerhetshändelsen innebar att *framgångsfaktor upphör* för Crowdstrikes leverans när den avtalade uppdateringen skickades ut automatiskt och innehöll fel. *Nytta förhindras* när förtroendet från kunder och andra intressenter påverkades negativt. Det kan dock antas påverka företaget först om kunder väljer andra leverantörer. De faktiska incidenterna handlade om att *nytta förhindras* när verksamheten inte kunde leverera som planerat till sina kunder. Påverkan bedöms som *allvarlig* för den felaktiga leveransen samt *som värst allvarlig* för hela verksamheten.

Den misslyckade uppdateringen får även följdverkningar för förtroendet, vilket utgör ytterligare en incident som en reaktion på den ursprungliga händelsen. Påverkan bedöms som *som värst betydande* för förtroendeskadan.

Not 29. RTE. *Ryanair cancels flights, NCTs disrupted over IT outage.* https://www.rte.ie/news/ireland/2024/0719/1460766-ryanair-cyber-outage/ (Hämtad 04/2025).

Not 30. SVT. *Efter utrymningen – gruvan I Malmberget öppen igen.* https://www.svt.se/nyheter/lokalt/norrbotten/gruvan-i-malmberget-utrymt-pa-grund-av-it-problem (Hämtad 04/2025).

Not 31. Arvika Nyheter. *Regionen höjer beredskapen efter IT-haveriet – så påverkas kommun och räddningstjänst.* https://www.arvikanyheter.se/2024/07/19/regionen-hojer-beredskapen-efter-it-haveriet-sa-paverkas-kommun-och-raddningstjanst-fbe50/ (Hämtad 04/2025).

Analys av samhällspåverkan

Analys av påverkan på samhällsnivå avser flera sektorer, såsom flygtrafik, hälso- och sjukvård, media, bank och finans samt transporter. Säkerhetshändelsen på samhällsnivå handlade om att en *framgångsfaktor upphör* i samband med den felaktiga uppdateringen. Det innebar påverkan på möjligheten att bedriva en rad samhällsviktiga verksamheter som en följd av att *nytta förhindrades*. Bedömningen motiveras med att flera sektorer i samhället påverkades *allvarligt* av incidenten när deras ordinarie verksamhet störtdes, exempelvis behövde operationer ställas in och planerade flygningar stoppas. Påverkan på samhället är *som värst allvarlig*.

Lärdomar

Crowdstrikes incident orsakade störningar i miljontals kundsystem. Ramverket gör det tydligt att följdincidenter i kundmiljöer ska analyseras separat. Det skapar struktur i analysen, särskilt vid händelser som slår brett, och säkerställer att bedömningar görs på rätt nivå och inom rätt avgränsning. I fallstudien framgår exempel på att säkerhetshändelser kan övergå till faktiska incidenter extremt snabbt. Ramverkets klassificering hjälper till att tydliggöra utveckling och konsekvenser från att *framgångsfaktor upphör* till att *nytta förhindras*. Det visar samtidigt på behovet av kvalitetskontroller innan distribution.

Fallstudien visar att samhällspåverkan kan uppstå indirekt via teknikleverantörer. Även om Crowdstrike inte själva tillhandahåller samhällsviktiga tjänster visar ramverket att ett tekniskt fel i deras miljö ändå kan leda till påverkan på samhällsnivå. Slutligen visar analysen att ramverket stödjer aggregering av påverkan från många sektorer utan att överdriva effekten. Samhällspåverkan bedöms som ”*som värst allvarlig*” tack vare ramverkets princip om att bedömningen ska utgå från det mest påverkade området. Händelser med spridd och ojämn påverkan kan därmed ändå få en tydlig samlad bedömning.

Karolinska Institutet

- **Incidenten:** Misslyckad automatisk påfyllning av flytande kväve till kryofrysarna.
- **Faktisk incident:** Faktisk incident uppstod i verksamheten (förstört forskningsmaterial) och på samhällsnivå (tillgång till forskningsresultat).
- **It-miljöpåverkan:** *Allvarlig* påverkan.
- **Verksamhetspåverkan:** *Kritisk* påverkan till det att materialet kan ersättas.
- **Samhällspåverkan:** *Allvarlig* till det att materialet kan ersättas.

Incidentbeskrivning

På kvällen den 22 december 2023 aktiverades ett larm i fryshotellet i byggnaden Neo på Karolinska Institutet. Larmet aktiverades då den rutinmässiga automatiska påfyllningen av flytande kväve till kryofrysarna, nödvändigt för temperaturhållningen i frysarna, hade misslyckats. I kryofrysarna förvarades stora mängder världsunikt forskningsmaterial och patientprover som samlats in från ett flertal institutioner under 30 års tid.[32] När temperaturen i kryofrysarna steg till följd av avbrottet i kvävetillförseln förstördes stora delar av detta forskningsmaterial. Karolinska Institutet uppskattar att notan för incidenten omfattar omkring en halv miljard kronor.[33]

På förmiddagen samma dag, den 22 december 2023, utfördes ett planerat servicearbete i anslutning till fryshotellet. Servicearbetet utlöste ett larm, vilket orsakade att en ventil stängdes vid den yttre lagringstanken där flytande kväve lagras och varifrån den automatiska påfyllningen till kryofrysarna inleds. När servicearbetet slutförts skulle larmet ha kvitterats och återställts, men detta skedde inte och ventilen förblev stängd.[34] Detta ledde till att kryofrysarna stod utan påfyllning av kväve vilket i sin tur gjorde att temperaturen i frysarna gradvis steg.

Under julhelgen upptäckte medarbetare på Karolinska Institutet vid flera tillfällen att kryofrysarna i fryshotellet larmade och rapporterade detta till sina överordnade. Trots detta genomfördes inga kontroller av kryofrysarna förrän på eftermiddagen den 27 december, nästan 5 dygn efter den misslyckade påfyllningen av flytande kväve.[35] Vid en mer grundlig kontroll av frysarna den 28 december konstateras det att 16 av de 19 kryofrysarna i fryshotellet har en förhöjd temperatur och att en betydande del av frysarnas innehåll förstörts.

Not 32. DN. *KI kände till brister i larmsystemet – världsunikt material förstört.* https://www.dn.se/sverige/ki-kande-till-brister-i-larmsystemet-varldsunikt-material-forstort/ (Hämtat 04/2025).

Not 33. Aftonbladet. *Kostnaden för fryshaveriet: En halv miljard.* https://www.aftonbladet.se/nyheter/a/0Q5pg0/karolinska-institutet-polisanmaler-fryshaveriet-kostnad-pa-en-halv-miljard (Hämtad 04/2025).

Not 34. Karolinska Institutet. *Utredning fryshaveri Neo.* https://nyheter.ki.se/media/144225/download (Hämtad 04/2025).

Not 35. Ibid.

Karolinska Institutets haveriutredning pekar på organisatoriska brister som orsak till incidenten. Händelsen inträffade inte på grund av en enskild händelse eller felkälla utan en kombination av otydligheter i uppdrag, mandat, kommunikation och informationsdelning. Brister fanns även i kunskap och kompetens för att garantera funktionen hos verksamhetskritiska system.[36]

Analys av it-miljöpåverkan

Analys av påverkan på it-miljö avgränsas till de tekniska system som övervakar frysarna. Systemet fallerade på grund av ett misstag när nödvändiga åtgärder i samband med underhållsarbete inte vidtogs. Brister i underhållsarbetet orsakade en säkerhetshändelse av typen *hinder uppstår* när ventilen inte längre öppnades som förväntat. Utifrån MSB:s ramverk innebar händelsen att en faktisk incident av typen *nytta förhindras* inträffade med *allvarlig påverkan* på ventilens funktion, och *som värst delvis allvarlig påverkan* på hela it-miljön.

Analys av verksamhetspåverkan

Analys av påverkan på verksamhetsnivå avser tillgång till det forskningsmaterial som förvaras i frysarna. Säkerhetshändelsen innebar att *skydd upphör* när den automatiska påfyllningen inte fungerade. Det resulterade i att materialet i frysarna förstördes. När forskningsmaterialet förstördes fanns inga alternativa underlag att använda och möjligheten för institutionen att bedriva forskning påverkas negativt under lång tid framöver. Verksamheten ställs inför omfattande kostnader för att reparera skadan. Den faktiska incidenten utgörs av att *nytta förhindras* i *kritisk* omfattning för de påverkade frysarna och den verksamhet som bygger sin forskning på materialet som förvaras där. Bedömningen avser den tidsperiod till materialet kan ersättas.

Analys av samhällspåverkan

Analys av påverkan på samhällsnivå avser tillgång till forskningsresultat. Säkerhetshändelsen handlade om att *framgångsfaktor upphör* när världsunikt forskningsmaterial och patientprover som samlats in under 30 års tid gått förlorat. Materialet är unikt och kan inte ersättas och den faktiska incidenten innebar att *nytta förhindras*. Samhället kommer inte att kunna ta del av eventuella framsteg som forskningsmaterialet skulle kunna ha gett upphov till. Samhällspåverkan bedöms *som värst allvarlig* utifrån förlorad förmåga att upprätthålla forskning och experimentell utveckling tills det att materialet är ersatt.

Not 36. Karolinska Institutet. *Utredning fryshaveri Neo*. https://nyheter.ki.se/media/144225/download (Hämtad 04/2025).

Lärdomar

Fallstudien visar att ramverket hjälper till att identifiera när en säkerhetshändelse som att *skydd upphör* övergår till en *faktisk incident* och att analysen innefattar både mänskliga, tekniska och organisatoriska faktorer. I fallstudien visas exempel på verksamhetspåverkan med långsiktig betydelse. Ramverket stödjer samtidigt klassificering av påverkan när effekterna är fördröjda, diffusa eller icke-ekonomiska till sin karaktär.

Slutord

Slutord

It-incidenter kan resultera i påverkan på viktiga samhällsvärden. Rapporten har presenterat ett ramverk för bedömning av it-incidenters samhällpåverkan i syfte att ge branschen ett gemensamt förhållningssätt till sakområdet. Samhället är dock dynamiskt och i ständig förändring vilket innebär att bedömningskriterierna även bör anpassas i takt med samhällets utveckling.

Att mäta samhällspåverkan av en it-incident är en komplex uppgift där påverkan kan innefatta allt från större ekonomiska påföljder för samhällsbärande institutioner till sociala och hälsorelaterade konsekvenser med bäring på, exempelvis, befolkningens mående eller produktivitet. Det kan innefatta kortsiktiga och omvälvande förändringar, men även konsekvenser vars omfattning först blir möjligt att observera på längre sikt.

Fallstudierna visar att MSB:s ramverk för att bedöma it-incidenters påverkan är ett användbart verktyg för att förstå tekniska, organisatoriska och samhälleliga konsekvenser. Svenska Kyrkans incident illustrerar hur nya angreppsmetoder kan utnyttja ouppdaterade system. Fallet med Ica och Apotek Hjärtat visar hur en latent brist i it-miljön kan få genomslag först senare, och hur alternativa arbetssätt spelar roll i att minska verksamhets- och samhällspåverkan. Tietoevrys och Crowdstrikes incident visar hur en störning hos en leverantör kan innebära separata följdincidenter i kundorganisationer och hur ramverket bidrar till att förstå dem var för sig. Händelsen hos Karolinska Institutet visar att verksamheter kan drabbas av påverkan även på lång sikt och att samhällspåverkan kan vara allvarlig även när den inte är omedelbar.

För att stärka förmågan att tolka och förstå konsekvenserna av it-incidenter kommer MSB att tillämpa det presenterade ramverket i sin egen analysverksamhet. Ramverket kommer användas både för operativa analyser av enskilda incidenter och för att följa långsiktiga trender i hotbilden. Syftet är att säkerställa att konsekvenser bedöms systematiskt, strukturerat och med hänsyn till både tekniska, organisatoriska och samhälleliga dimensioner. Myndigheten uppmanar också andra aktörer – såväl offentliga som privata – att använda ramverket aktivt i sitt eget arbete. Ramverket utgör ett verktyg för att skapa enhetliga, transparenta och nyanserade analyser av it-incidenter.

Ramverket är inte statiskt. Precis som samhället utvecklas, behöver också vår förståelse för incidenters påverkan kontinuerligt förfinas. Erfarenheter från verkliga incidenter, nya forskningsrön och samhällsutvecklingen kommer att vara avgörande för hur ramverket vidareutvecklas framöver. Denna rapport markerar därför inte ett slut, utan ett första steg i en levande modell för bedömning.

Genom att använda en gemensam bedömningsmodell och en enhetlig terminologi – en gemensam taxonomi – för olika typer av påverkan, ges bättre förutsättningar att tolka, beskriva och jämföra konsekvenser av it-incidenter. Det förbättrar vår kollektiva förmåga att kommunicera risker, planera åtgärder och fördela resurser – både inom enskilda organisationer och på samhällsnivå.

Bilaga 1

Bilaga 1: Ramverk för klassifikation och bedömning av incidenters påverkan

Att bedöma konsekvenserna av en it-incident är avgörande för att förstå dess påverkan på samhället. Genom att öka förståelsen för hur it-incidenter påverkar enskilda verksamheter såväl som samhället i stort är det möjligt att skapa en grund för evidensbaserat beslutsfattande. Detta möjliggör bättre prioriteringar och förebyggande åtgärder.

I denna rapport presenteras fallstudier av verkliga it-incidenter och deras klassificerade och bedömda påverkan på it-miljö, organisation och samhälle. Syftet med metoden är att den utifrån en större mängd bedömningar kommer fördjupa kunskapsläget om hur många och vilka it-incidenter som faktiskt får påverkan på it-miljön, organisationen eller samhället trots att det i enskilda fall kan innefatta svårbedömda avvägningar när bedömningsgrundande information är bristfällig eller saknas.

Grundläggande begrepp

Följande grundläggande begrepp utgör en utgångspunkt för de analyser som utförs inom den strategiska analysen på informations- och cybersäkerhetsområdet på MSB.

Tabell 7. Grundläggande begrepp

Begrepp	Förklaring
Incident	En inträffad oönskad händelse.[37]
Framgång	En inträffad önskad händelse.[38]
Hot	Något som orsakar, eller bidrar till att orsaka, en incident.
Hinder	Något som förhindrar, eller bidrar till att förhindra, en framgång.
Framgångsfaktor	Något som orsakar, eller bidrar till att orsaka, en framgång.
Skydd	Något som förhindrar, eller bidrar till att förhindra, en incident.
Risk	En möjlig oönskad händelse.
Chans	En möjlig önskad händelse.
Sårbarhet	Avsaknad av något som förhindrar, eller bidrar till att förhindra, en incident.
Brist	Avsaknad av något som orsakar, eller bidrar till att orsaka, en framgång.
Frihet	Avsaknad av något som orsakar, eller bidrar till att orsaka, en incident.

Not 37. Det är viktigt att notera att händelsen här ska förstås som oönskad *utifrån vad den leder till*, d.v.s. att en oönskad effekt infinner sig, snarare än att det är en händelse som inträffar istället för en önskad händelse. Att en e-postfiltreringstjänst felaktigt markerar ett legitimt affärsmejl som skräppost är en händelse som kan anses vara oönskad eftersom den förväntade händelsen var att mejlet skulle levereras korrekt till mottagaren. En sådan händelse räknas dock inte som en incident i detta ramverk.

Not 38. I enlighet med den föregående fotnoten är det viktigt att notera att händelsen här ska förstås som önskad *utifrån vad den leder till,* d.v.s. att en önskad effekt infinner sig, snarare än att det är en händelse som inträffar istället för en oönskad händelse. Att ett mejl skickas till och mottas av den tilltänkta mottagaren när avsändaren trycker på ”Skicka” är en önskad händelse i den relevanta bemärkelsen. Att det visade sig att skadlig kod inte installerades när en användare klickade på en okänd länk, d.v.s. att oönskad händelse uteblev, är inte en framgång i detta ramverk.

Typer av incidenter

I detta analytiska ramverk görs en distinktion mellan två typer av händelser: *säkerhetshändelser* och *faktiska incidenter*.

Säkerhetshändelse

En **säkerhetshändelse** definieras som en händelse som påverkar säkerheten i it-miljön, organisationens verksamhet eller samhället negativt. Det är viktigt att notera att en säkerhetshändelse inte nödvändigtvis innebär att en faktisk skada har uppstått. Organisationer med redundanta system och effektiva skyddsmekanismer kan hantera säkerhetshändelser utan att de leder till några konkreta problem.

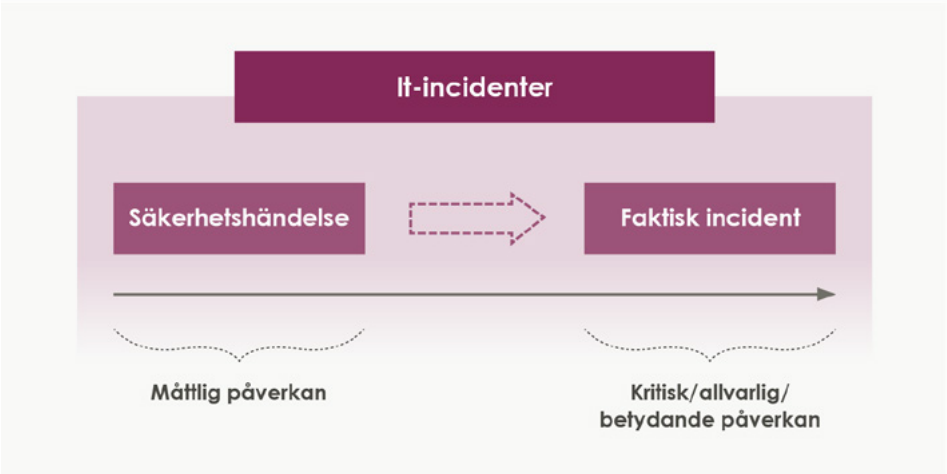
Faktisk incident

En **faktisk incident** uppstår när en säkerhetshändelse orsakar direkt eller indirekt negativ påverkan på it-miljön, organisationens verksamhet eller samhället. Detta inträffar när kompensatoriska mekanismer, som redundans eller skydd, inte är tillräckliga. En faktisk incident innebär att skada har uppstått, eller att organisationen har förlorat nyttan av en viss funktion.

En faktisk incident orsakas alltid av (minst) en säkerhetshändelse, men det är inte alltid säkerhetshändelser vare sig orsakar eller leder till faktiska incidenter.

Begreppen *it-påverkan, verksamhetspåverkan* och *samhällspåverkan* åsyftar i ramverket sådana säkerhetshändelser respektive faktiska incidenter som inträffade oönskade händelser orsakar eller resulterar i it-miljön, verksamheten respektive i samhället.

Figur 2. Illustration av hur it-incidenter, säkerhetshändelser och faktiska incidenter förhåller sig till varandra



Säkerhetshändelser

Det finns fyra typer av säkerhetshändelser: *Hot uppstår, skydd upphör, framgångsfaktor upphör* och *hinder uppstår.*

Hot uppstår

Definition: Något som kan orsaka eller bidra till att orsaka att en incident inträffar (ett hot) uppstår.

Exempel på ett hot som uppstår i it-miljön

Utpressningsprogramvara som kan kryptera data och göra den otillgänglig för organisationen installeras. Ett annat exempel är att en filyta som innehåller känslig information görs fritt tillgänglig på internet.

Exempel på ett hot som uppstår i organisationens verksamhet

Utpressningsprogramvara som krypterar informationssystem som används för att upprätthålla en molntjänst som organisationen levererar till sina kunder.

Exempel på ett hot som uppstår på samhällsnivå

Det installeras utpressningsprogramvara i informationssystemen som upprätthåller molntjänsten där regionen lagrar alla tagna röntgenbilder.

Skydd upphör

Definition: Något som kan förhindra eller bidra till att förhindra att en incident inträffar (ett skydd) upphör.

Exempel på ett skydd som upphör i it-miljön

En brandvägg som skyddar från obehörig åtkomst avaktiveras vid en konfigurationsändring.

Exempel på ett skydd som upphör i organisationens verksamhet

Ett angrepp riktas mot ett centralt system för åtkomsthantering och av-aktiverar multifaktorautentisering. Organisationens skydd mot intrång har därmed upphört.

Exempel på ett skydd som upphör på samhällsnivå

Alla reningssystem i dricksvattenverket på en viss plats har slutat att fungera.

Framgångsfaktor upphör

Definition: Något som orsakar eller bidrar till att orsaka att en framgång inträffar upphör.

Exempel på en framgångsfaktor som upphör i it-miljön

En router tappar förmågan att kanalisera trafik på ett korrekt sätt. Ett annat exempel är att en hårddisk går sönder, och att data som fanns i den därför blir otillgänglig.

Exempel på en framgångsfaktor som upphör i organisationens verksamhet

All data raderas i systemen där man normalt arbetar.

Exempel på en framgångsfaktor som upphör på samhällsnivå

Alla de tillgängliga telenäten på en viss plats förstörs.

Hinder uppstår

Definition: Något inträffar som förhindrar eller bidrar till att förhindra att en framgång inträffar uppstår.

Exempel på ett hinder som uppstår i it-miljön

En ny brandväggsregel läggs till, vilket resulterar i att legitim nätverkstrafik blockeras. Ett ytterligare exempel är att ett antivirusprogram felaktigt stoppar åtkomst till filer.

Exempel på ett hinder som uppstår i organisationens verksamhet

En tjänst för realtidskoordinering slutar fungera.

Exempel på ett hinder som uppstår på samhällsnivå

Alla tillgängliga telenät på en viss plats blockeras.

Faktiska incidenter

När en säkerhetshändelse inträffar kan den antingen hanteras utan påverkan eller leda till en faktisk incident. Det avgörs av huruvida verksamheten har tillräcklig redundans eller alternativa lösningar. Det finns fyra typer av faktiska incidenter: *Skada orsakas, skada förhindras, nytta förhindras* och *nytta orsakas.*

Tabell 8. Illustration av vilka säkerhetshändelser som utgör faktiska incidenter

Typ av säkerhetshändelse	Beskrivning	Exempel	Möjlig incidenttyp
Hinder uppstår	Något blockerar en funktion från att fungera som avsett.	En felaktig nätverkskonfiguration gör att en molntjänst inte kan kommunicera med andra system.	Nytta förhindras/ Skada förhindras
Framgångsfaktor upphör	En viktig faktor som krävs för att upprätthålla en funktion slutar fungera.	Ett kritiskt back-up-system går offline, vilket gör att dataförlust inte kan återställas.	Nytta förhindras/ Skada förhindras
Hot uppstår	En säkerhetshändelse innebär en ökad risk för negativ påverkan.	Ett cyberspionage avslöjar känsliga företagsdata för en konkurrent.	Skada orsakas/ Nytta orsakas
Skydd upphör	Ett skyddssystem som tidigare förhindrade oönskade händelser slutar fungera.	En brandväggsregel tas bort, vilket möjliggör ett externt cyberangrepp.	Skada orsakas/ Nytta orsakas

Skada orsakas

Definition: Skada orsakas för entiteten, eller för andra, på ett sätt som inte ligger i entitetens intresse. I ramverket är entiteten antingen organisationen eller samhället.

Exempel på att skada orsakas i it-miljön

Skadlig kod gör att hårddiskarna den installeras i krypteras (säkerhetshändelsen). Den skadliga koden infekterar alla organisationens hårddiskar.

Exempel på att skada orsakas i organisationens verksamhet

Skadlig kod infekterar organisationens informationssystem och krypterar de system som används för att upprätthålla en molntjänst som organisationen tillhandahåller till sina kunder. Detta utgör själva säkerhetshändelsen eftersom det påverkar verksamhetens tillgänglighet. Eftersom samtliga informationssystem som är nödvändiga för att molntjänsten ska fungera blir obrukbara, upphör organisationens möjlighet att leverera tjänsten till sina kunder. Denna påverkan på verksamheten innebär att säkerhetshändelsen blir en faktisk incident, eftersom den direkt hindrar organisationen från att bedriva sin kärnverksamhet.

Exempel på att skada orsakas på samhällsnivå

Genom att den skadliga koden krypterar molntjänsten krypteras även röntgenbilder och de verktyg för att analysera och bearbeta röntgenbilder som regionens hälso- och sjukvårdsorganisationer har lagrat där. Detta utgör en säkerhetshändelse, eftersom det påverkar tillgängligheten till kritisk medicinsk information och arbetsverktyg. Eftersom samtliga röntgenbilder och analysverktyg enbart lagras inom den drabbade molntjänsten, saknas alternativa sätt att analysera nya röntgenbilder. Detta gör att säkerhetshändelsen utgör en faktisk incident på samhällsnivå, då den direkt påverkar regionens hälso- och sjukvård och kan få konsekvenser för patienters diagnoser och behandlingar.

Det är viktigt att notera att skada kan orsakas på en nivå utan att det nödvändigtvis leder till skada på andra nivåer. Exempelvis kan skada uppstå i it-miljön genom att programvara med skadlig kod krypterar viss lagringsmedia, men om organisationen har alternativa system eller backuper kan dess verksamhet ändå fortsätta relativt obehindrat. På samma sätt kan skada orsakas i organisationens verksamhet utan att detta nödvändigtvis leder till skada på samhällsnivå. Om vissa röntgenbilder lagras i regionens och kommunernas egna system, eller om en annan molntjänst kan användas för att analysera och bearbeta bilderna, kan konsekvenserna för samhället mildras.

Det som gör incidenten till en faktisk incident av typen *skada orsakas* (det är också en faktisk incident av andra typer) på de olika nivåerna är att:

1. En beståndsdel i organisationens it-miljö förstörs och det saknas redundanta beståndsdelar som möjliggör att it-miljön fortsätter att fungera som avsett.
2. En beståndsdel i organisationens verksamhet förstörs och det saknas redundanta beståndsdelar som möjliggör att verksamheten fortsätter att fungera som avsett.
3. En beståndsdel i samhällsviktig verksamhet förstörs och det saknas redundanta beståndsdelar som möjliggör att samhällsservicen kan fortsätta att fungera som avsett.

Skada förhindras

Definition: Skada förhindras för entitetens konkurrenter, eller för andra, på ett sätt som inte ligger i entitetens intresse.[39]

Exempel på att skada förhindras i it-miljön

Ett cyberangrepp slår ut informationssystem som används för att styra ett försvarssystem. Angriparna har installerat skadlig kod i det nätverk som hanterar kommunikation mellan ledningscentralen och de operativa luftvärnssystemen. Detta gör att systemet inte kan ta emot eller skicka order. Eftersom hela styrfunktionen är beroende av denna digitala kommunikation och alternativ saknas, innebär denna säkerhetshändelse en incident som påverkar it-miljön inom försvarsorganisationen.

Exempel på att skada förhindras i organisationens verksamhet

På verksamhetsnivå innebär säkerhetshändelsen med styrsystemet att försvarsorganisationen inte kan utföra sitt uppdrag, vilket är att skydda landets luftrum och avvärja fientliga angrepp. Försvarspersonalen är beroende av fungerande digitala system för att styra luftvärnet, och utan dessa kan hot inte bemötas i tid. Detta innebär en incident med påverkan på verksamheten, eftersom organisationens försvarsförmåga tillfälligt neutraliseras.

Exempel på att skada förhindras på samhällsnivå

Angreppet påverkar landets säkerhet eftersom fienden kan genomföra angrepp utan att möta motstånd från luftförsvaret. Eftersom missilförsvaret inte kan användas, och det saknas andra omedelbara försvarsåtgärder, innebär detta en faktisk incident på samhällsnivå.

Not 39. Detta ramverk är framtaget enbart i analytiskt syfte för att möjliggöra en systematisk bedömning av it-incidenters påverkan på olika nivåer. Syftet är att ge ett heltäckande och strukturerat stöd för analys, inte att på något sätt uppmana, uppmuntra eller legitimera handlingar som syftar till att orsaka skada eller påverka system, organisationer eller samhällsfunktioner på ett negativt sätt. Ramverket är neutralt och avsett för incidentanalys och riskbedömning i syfte att stärka motståndskraft och säkerhet, inte för att stödja eller inspirera till skadliga aktiviteter.

Det är dock även i detta exempel viktigt att notera att skada kan förhindras på en nivå utan att det nödvändigtvis innebär att skada förhindras på andra nivåer. Exempelvis kan försvarssystemet på it-miljönivå blockeras av ett cyberangrepp, men om det finns ett parallellt system eller alternativa kommunikationskanaler kan försvarsorganisationen fortfarande ha möjlighet att styra och avfyra vapen via andra vägar. På samma sätt kan försvarsorganisationens verksamhet förhindras på grund av att missilförsvaret är otillgängligt. Om andra försvarsåtgärder, såsom bemannade flygföretag eller andra vapensystem, kan aktiveras, behöver dock inte konsekvensen på samhällsnivå bli kritisk.

Om nationen dessutom har andra försvarssystem i drift, exempelvis andra luftvärnssystem eller stöd från allierade, kan skadan på samhällsnivå mildras, även om skada har förhindrats på it-miljö- och verksamhetsnivå.

Det som gör incidenten till en faktisk incident av typen skada förhindras (även om den kan vara en faktisk incident av andra typer) på de olika nivåerna är att:

1. En beståndsdel i organisationens it-miljö sätts ur funktion och det saknas alternativa tekniska lösningar som möjliggör att it-miljön fortsätter att fungera enligt plan.
2. En beståndsdel i organisationens verksamhet sätts ur funktion och det saknas alternativa lösningar inom organisationen som skulle kunna ersätta funktionen på samma sätt.
3. En beståndsdel i samhällets försvarsförmåga sätts ur funktion. Det saknas redundanta försvarssystem som skulle kunna fylla samma funktion.

Nytta förhindras

Definition: Nytta förhindras för entiteten, eller för andra, på ett sätt som inte ligger i entitetens intresse.

Exempel på att nytta förhindras i it-miljön

Ett angrepp krypterar databasen där en grossist i läkemedelsbranschen hanterar orderinformation och automatiserad transportkoordinering. Detta utgör säkerhetshändelsen. Systemet kan inte behandla beställningar och funktionaliteten är helt blockerad. Detta innebär en incident av typen *nytta förhindras* i it-miljön eftersom funktionalitet för distribution inte är tillgänglig på något sätt.

Exempel på att nytta förhindras i organisationens verksamhet

Grossisten av läkemedel kan inte ta emot nya beställningar från sjukhus och apotek. Viss lagerhantering fungerar fortfarande manuellt, men distributionskedjan är påverkad och inga nya läkemedel kan skickas ut. Detta innebär att säkerhetshändelsen även utgör en faktisk incident som *förhindrar nytta* för verksamheten.

Exempel på att nytta förhindras på samhällsnivå

Störningarna i distributionstjänsten innebär att sjukhus och vårdcentraler inte får några nya leveranser av mediciner. Det resulterar i att vissa behandlingar måste skjutas upp eller begränsas. Detta gör att säkerhetshändelsen utgör en faktisk incident på samhällsnivå, då den direkt påverkar möjligheten att bedriva hälso- och sjukvård och kan få konsekvenser för patienters behandlingar.

På samma sätt som i tidigare exempel kan nytta kan förhindras på en nivå utan att det nödvändigtvis leder till att nytta förhindras på andra nivåer. Exempelvis kan nytta förhindras i it-miljön genom att ett cyberangrepp krypterar logistiksystemets databaser, men om läkemedelsgrossisten har en redundant infrastruktur eller manuella alternativ kan verksamheten ändå fortsätta, även om det blir mindre effektivt. På samma sätt kan nytta förhindras i verksamheten genom att läkemedelsgrossisten inte kan hantera orderflödet, men om det finns andra leverantörer av läkemedel kan den totala påverkan på samhället mildras. Om vården dessutom har lokala läkemedelslager eller kan omfördela medicin mellan sjukhus och apotek, kan samhällets beroende av just denna grossist minska, och konsekvenserna blir mindre allvarliga.

Det som gör incidenten till en faktisk incident av typen nytta förhindras (även om den kan vara en faktisk incident av andra typer) på de olika nivåerna är att:

1. En beståndsdel i organisationens it-miljö sätts ur funktion. Eftersom det saknas alternativa tekniska lösningar, kan it-miljön inte fortsätta att fungera som avsett.
2. En beståndsdel i organisationens verksamhet sätts ur funktion, eftersom läkemedelsgrossisten inte kan leverera beställningar till sjukhus och apotek. Det saknas redundanta lösningar inom verksamheten, vilket innebär att distributionen av läkemedel avstannar.
3. En beståndsdel i samhällsviktig verksamhet sätts ur funktion, eftersom sjukhus och vårdcentraler inte får sina mediciner i tid. Eftersom det saknas alternativa distributionsvägar i tillräcklig omfattning, kan samhällets förmåga att säkerställa tillgång till läkemedel inte upprätthållas fullt ut.

Nytta orsakas

Definition: Nytta orsakas för entitetens konkurrenter, eller för andra, på ett sätt som inte ligger i entitetens intresse.

Exempel på att nytta orsakas i it-miljön

Säkerhetshändelsen utgörs av att angripare exploaterar en sårbarhet i sjukhusets lagringsinfrastruktur, vilket leder till en faktisk incident när de även utnyttjar lagrings- och beräkningskapacitet för att bryta kryptovaluta. Lagringsutrymmet fylls upp av mining-relaterade beräkningar, vilket förhindrar sjukhusets egna system från att fungera optimalt.

Exempel på att nytta orsakas i organisationens verksamhet

Eftersom sjukhusets it-system är belastade av kryptomining, fungerar inte de digitala patientjournalerna i realtid. Detta utgör säkerhetshändelsen. Vårdpersonal har svårt att snabbt få fram provsvar, röntgenbilder och annan viktig patientdata, vilket skapar fördröjningar i vårdbeslut och utgör en faktisk incident i verksamheten.

Exempel på att nytta orsakas på samhällsnivå

Säkerhetshändelsen med störningar i patientjournalerna för att kapaciteten nyttjas av andra utgör en faktisk incident på samhällsnivå, då den påverkar möjligheten att bedriva hälso- och sjukvård och kan få konsekvenser för patienters behandlingar.

Precis som i tidigare exempel är det även här viktigt att uppmärksamma att nytta kan orsakas på en nivå utan att det nödvändigtvis leder till att nytta orsakas på andra nivåer. Exempelvis kan nytta orsakas i it-miljön genom att angripare får åtkomst till sjukhusets system och utnyttjar dess resurser för egen vinning genom kryptomining, utan att det omedelbart medför någon direkt effekt på verksamhetsnivån. Om sjukhuset har tillräcklig it-resiliens, lastbalansering och alternativa beräkningsresurser, kan den medicinska verksamheten fortsätta relativt obehindrat, trots att angriparna utnyttjar it-miljön.

På samma sätt kan nytta orsakas i verksamheten utan att det direkt leder till betydande konsekvenser på samhällsnivå. Om exempelvis sjukhusets interna administrativa processer påverkas men den akuta sjukvården kan fortsätta tack vare alternativa system eller manuella reservrutiner, kan konsekvenserna på samhällsnivå begränsas. Om patientdata även lagras i en alternativ hälsoportal som är oberoende av sjukhusets interna system, kan vårdpersonal fortfarande få fram viktig medicinsk information, vilket mildrar effekterna av incidenten.

Det som gör incidenten till en faktisk incident av typen *nytta orsakas* (även om den också kan vara en faktisk incident av andra typer) på de olika nivåerna är att:

1. En beståndsdel i organisationens it-miljö används för någon annans nytta, och det saknas skyddsåtgärder som hindrar att it-miljön fortsätter att exploateras av obehöriga.
2. En beståndsdel i organisationens verksamhet används på ett sätt som missgynnar organisationen, och det saknas alternativ som gör att verksamheten kan fungera ostört.
3. En beståndsdel i samhällsviktig verksamhet exploateras på ett sätt som leder till negativa konsekvenser för samhället, och det saknas redundanta system eller processer som säkerställer att sjukvården kan fortsätta fullt ut utan påverkan.

Alla incidenter är säkerhetshändelser men alla incidenter är inte faktiska incidenter

Här presenteras några exempel som illustrerar att alla incidenter är säkerhetshändelser, men att inte alla incidenter är faktiska incidenter. Däremot är alla faktiska incidenter också säkerhetshändelser.

Nytta behöver inte förhindras bara för att ett hinder uppstår eller en framgångsfaktor upphör. En organisation kan undvika att nytta förhindras genom att ha redundans i sina informationssystem. Om en komponent, exempelvis en hårddisk, går sönder eller blockeras, innebär det inte nödvändigtvis att funktionen hårddisken bidrar med upphör helt, så länge det finns andra hårddiskar med ledigt utrymme tillgängliga. Redundanta system kan säkerställa att information fortfarande kan sparas och tjänster fortsätter att fungera. Däremot, om information inte längre kan sparas förhindras nytta antingen för att alla lagringsmedier är fulla eller trasiga (framgångsfaktor upphör) eller att de är blockerade (hinder uppstår).

Skada behöver inte orsakas bara för att ett hot uppstår eller ett skydd upphör. Ett hot som introduceras i en organisations informationssystem orsakar inte nödvändigtvis skada, särskilt om det finns effektiva skydd, exempelvis säkerhetsprogramvara som identifierar och neutraliserar skadlig kod, eller en brandvägg, som blockerar hotet från att sprida sig. På samma sätt behöver ett skydd som upphör att fungera inte innebära att skada orsakas, om det inte samtidigt finns ett hot som faktiskt kan utnyttja den sårbarhet som skyddet tidigare förhindrade. Om en skada däremot uppstår, exempelvis att en komponent förstörs och måste ersättas, beror det på att komponenten bidrog till funktionalitet (framgångsfaktor upphör) alternativt utgjorde en del av organisationens skydd (skydd upphör).

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publikationsnummer MSB2600 – juni 2025 ISBN-nummer 978-91-7927-635-5