Myndigheten för samhällsskydd och beredskap

Medfinansierat av Europeiska unionens fond för ett sammanlänkat Europa

Cyberangrepp mot samhälls-viktiga informationssystem

25 rekommendationer för stärkt skydd mot cyberangrepp

Cyberangrepp mot samhällsviktiga informationssystem
– 25 rekommendationer för stärkt skydd mot cyberangrepp

Foto omslag: Adobe Stock
Tryck: By Wind
Produktion: Advant

Publikationsnummer: MSB2287 – januari 2024
ISBN: 978-91-7927-459-7

Förord

Under inledningen av 2023 ökade antalet cyberangreppsförsök mot statliga myndigheter och leverantörer av samhällsviktiga tjänster kraftigt. Den stora majoriteten av dessa var överbelastningsangrepp som enligt uttalanden i sociala medier förment genomfördes som en motreaktion på ”koranbränningarna”. Kombinerat med det försämrade säkerhetspolitiska läget, så har betydelsen av motståndskraft mot cyberangrepp aldrig varit viktigare.

Den här rapporten ger en övergripande bild av cyberangreppsförsök mot statliga myndigheter och NIS-leverantörer och dess konsekvenser. Jag vill passa på att framföra min uppskattning till de organisationer som rapporterar it-incidenter till MSB. Ert engagemang ökar vår förståelse av era utmaningar, samtidigt som det ger MSB förutsättningar att ta fram relevant stöd utefter behoven.

Rapporten visar att många cyberangrepp är relativt osofistikerade men att de trots detta ofta ”lyckas” påverka organisationer negativt. Det indikerar brister och att säkerhetsarbetet måste stärkas. Leveranskedjeincidenter, där ett cyberangrepp påverkar eller sprids till många organisationer samtidigt, kan leda till stora konsekvenser för samhället. Det är därför av särskild vikt att alla organisationer ser över säkerheten i sina leveranskedjor. En grundläggande förutsättning för förbättringsarbetet är att organisationers ledningsgrupper engagerar sig och vid behov tillför resurser.

Ändamålsenliga skydd minskar sannolikheten att bli utsatt för cyberangrepp, men tyvärr finns det tillfällen då skyddet inte räcker. Det är därför avgörande att en organisation övar incidenthantering regelbundet. God kommunikation och incidenthantering är särskilt viktigt när tjänsten eller informationssystemet är utkontrakterat och organisationen därför själv saknar rådighet.

Slutligen vill jag med emfas påpeka att det enda sättet att förekomma en angripare är att arbeta systematiskt och riskbaserat med helheten utifrån allriskperspektivet. Min förhoppning är att rapporten inspirerar till ökade studier så att din organisation arbetar proaktivt med skydd för att kunna motstå cyberangreppsförsök och därigenom bidrar till samhällets motståndskraft.

Stockholm, 2024-01-17

Åke Holmgren

Avdelningschef, Avdelningen för cybersäkerhet
och säkra 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 till följd av antagonistisk aktivitet.

Allriskperspektivet: Ett förhållningssätt där man strävar efter att bedöma alla risker för något man önskar skydda och att analysera alla möjliga orsaker till att en risk realiseras.

Artificiell Intelligens (AI): AI kan beskrivas som en uppsättning tekniker som med stöd av stora mängder datorkraft och data, med varierande grad av självständighet, kan identifiera mönster och samband samt beräkna sannolikhet. Till skillnad från vanliga program så kan AI algoritmer användas för att lösa problem som det inte finns någon tydlig lösning på. Exempel på AI-tekniker inkluderar bland annat maskininlärning och djupinlärning. Maskinlärning använder sig av algoritmer som baserat på träningsdata ”lär” sig föra statistiska resonemang och därmed lösa uppgifter. Djupinlärning kan beskrivas som en mer avancerad form av maskininlärning som använder sig av artificiella neuronnätverk för lära sig lösa mer komplexa uppgifter över tid med mindre mänsklig intervention. En teknik som har utvecklats snabbt under de senaste åren är generativ AI. Generativ AI inkluderar modeller som baserat på träningsdata lär sig producera nytt innehåll, inkluderande text, bilder och ljud.

Behörighetshantering: Behörighetshantering innebär att organisationer arbetar för att säkerställa att endast behöriga användare och informationssystem har åtkomst till it-miljön. Organisationen ska utforma sin hantering av behörigheter på ett sådant sätt att varje digital identitet inte har mer åtkomst till information och informationssystem än vad den behöver.

Brist: Avsaknad av något som orsakar, eller bidrar till att orsaka, en framgång.

Cyberangrepp: En antagonistisk handling som uppfyller legalitets-, praktik-, konsekvens- och uppsåtsvillkoret som förklaras på sida 23.

Cyberangreppsförsök: Ett angreppsförsök som uppfyller legalitets- och praktikvillkoret men som inte uppfyller konsekvensvillkoret, det vill säga inte resulterat i en händelse som negativt påverkat den angripna it-miljöns konfidentialitet, riktighet eller tillgänglighet. Villkoren förklaras på sida 23.

Digital leveranskedja: Tjänster och infrastruktur som levererar eller möjliggör leverans av digitala produkter som används för att upprätta, upprätthålla, utveckla eller återställa en organisations informationshantering och informationssystem.

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

Felkälla: Samlingsterm för hot, hinder, sårbarheter och brister.

Framgång: En inträffad önskad händelse.

Framgångsfaktor: Något som orsakar, eller bidrar till att orsaka, en framgång.

Hinder: Något som förhindrar, eller bidrar till att förhindra, en framgång.

Hot: Något som orsakar, eller bidrar till att orsaka, en incident.

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 (såsom väderfenomen, jordbävningar, solstormar, etc.)

Incidenthantering: En systematisk och strukturerad metod och process för att identifiera, dokumentera, analysera och lösa incidenter.

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. It-miljö omfattar både informationssystem som hanteras internt och de som är utkontrakterade.

Komponent: De ingående inslagen i en mekanism.

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

Kontinuitetshantering: En systematisk och strukturerad metod och process för att dokumentera och planera verksamheten i organisationen för att upprätthålla en tolerabel nivå oavsett vilken störning den utsätts för.

Mekanism: En kombination av komponenter som i samverkan och tillsammans med en trigger kan orsaka att en viss händelse inträffar.

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.

Möjlighet: Avsaknad av något som förhindrar, eller bidrar till att förhindra, en framgång.

NIS-leverantör: Leverantörer av samhällsviktiga och digitala tjänster som omfattas av NIS-regleringen.

NIS-regleringen: Samlingsnamn på den lag (SFS 2018:1174), förordning (SFS 2018:1175) och de myndighetsföreskrifter som antagits i Sverige för att implementera NIS-direktivet (EU) 2016/1148.

Riktighet: En aspekt av informationssäkerhet som i korthet innebär att det går att lita på att information är korrekt och inte manipulerad eller förstörd.

Risk: En möjlig oönskad händelse.

Skydd: Något som förhindrar, eller bidrar till att förhindra, en incident.

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

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

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).

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

Trigger: Något som kan tillföras en mekanism så att en viss händelse orsakas.

Ändringshantering: En systematisk och strukturerad metod och process som syftar till att möjliggöra ändringar i en organisations målsättningar, processer eller teknologier. Ändringshantering bygger på effektivitet, kontroll och riskminimering.[1]

1. Begreppet har mer specifika definitioner inom vissa it-relaterade ramverk för förvaltning respektive utveckling av it-system.

Sammanfattning

Sammanfattning

2023 inleddes med ett omfattande antal överbelastningsangrepp. Samtidigt brukar cyberangreppsförsök utgöra mindre än en femtedel av den totala mängden it-incidenter som rapporteras in till MSB. Utifrån identifierade utmaningar har rekommendationer tagits fram för hur en organisation kan stärka sitt skydd mot cyberangreppsförsök, samt minimera skador om en incident ändå inträffar. De organisationer som arbetar systematiskt och riskbaserat utifrån ett allriskperspektiv står bäst rustade.

Den här rapporten redogör för angreppsbilden mot statliga myndigheter och leverantörer av samhällsviktiga tjänster baserat på it-incidentrapporter som MSB mottagit från april 2019 till september 2023. Utifrån allriskperspektivet är det viktigt att påtala att antalet cyberangreppsförsök utgör mindre än en femtedel av den totala mängden it-incidenter som rapporterats in till MSB fram till 2022. Andra orsaker till it-incidenter är misstag, systemfel eller naturhot. Av de totalt 1 542 incidenter som rapporterats under tidsperioden utgör 16 procent cyberangreppsförsök. Statliga myndigheter står för merparten av de rapporterade it-incidenterna, även om andelen är minskande över tid.

Antalet inrapporterade cyberangreppsförsök har minskat över tid, men ökade under 2023. Ökningen består av ett onormalt stort antal överbelastningsangrepp under inledningen av 2023. De aktuella överbelastningsangreppen uppgavs i media och på olika chattgrupper vara motreaktioner på ”koranbränningarna”. Även om antalet cyberangreppsförsök således ökade bör det, av allt att döma, förstås som en tillfällig topp snarare än en del av en trend med ett konstant ökande antal cyberangreppsförsök mot statliga myndigheter och NIS-leverantörer.

Analysen av cyberangreppsförsöken visar att 53 procent av it-incidenterna beskriver en säkerhetshändelse som resulterat i faktisk påverkan på en organisations verksamhet. Resterande cyberangreppsförsök bedöms ha misslyckats eller haft så begränsade konsekvenser att de inte uppnått organisationspåverkan.

Många av de cyberangrepp som har resulterat i påverkan har utförts med hjälp av mindre sofistikerade metoder. Detta tyder på att det finns brister i skydd och rutiner och att säkerhetsarbetet hos organisationer behöver stärkas, men också att med relativt begränsade förbättringar kan bättre säkerhet uppnås.

Cyberangrepp kan innebära allvarliga konsekvenser för de som drabbas. Återhämtningsperioden kan bli både lång och dyr. Om det informationssystem som drabbas upprätthåller samhällsviktiga tjänster kan det i värsta fall innebära risk för liv och hälsa. Om andra är beroende av ett drabbat informationssystem kan dessutom många organisationer och medborgare påverkas. Många organisationer verkar dessutom i komplexa ekosystem av digitala leveranskedjor och har sällan full rådighet över sin egen it-miljö. Monoberoenden i de digitala leveranskedjorna kan leda till särskilt svåra utmaningar. MSB:s analys visar på vikten av att en organisation kartlägger leveranskedjorna och planerar alternativa arbetssätt om något skulle inträffa i en tjänst hos en leverantör som organisationen är beroende av för att kunna fortsätta sin verksamhet.

I en säkerhetspolitiskt mer osäker tid är det centralt att organisationer avsätter resurser för att se över vilka skyddsåtgärder som är relevanta för att implementera och öva. Detta för att stärka sitt skydd mot cyberangreppsförsök, men också för att minimera skador om organisationen trots allt drabbas. Baserat på analysen av angreppsbilden och slutsatser från tidigare rapporter har MSB identifierat sex specifika problemområden där organisationer har stora utmaningar, nämligen:

- systematiken i säkerhetsarbetet,
- incident- och kontinuitetshantering,
- medarbetarnas kunskaper,
- behörighetshantering,
- ändringshantering,
- digitala leveranskedjor.

Utifrån dessa problemområden har 25 rekommendationer formulerats. Rekommendationerna riktar sig till beslutsfattare, verksamhetsutvecklare och strateger inom it-avdelningar, men också säkerhetsfunktioner och verksamhetsstöd, samt CISO och andra ansvariga för informations- och cybersäkerhetsarbetet.

Slutsatser och rekommendationer

Slutsatser och rekommendationer

Det säkerhetspolitiska läget är allvarligt. Ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete med planering, införande, uppföljning och övning av förebyggande säkerhetsåtgärder är viktigt för att skydda sig mot cyberangreppsförsök. MSB har tagit fram rekommendationer för hur en organisation kan stärka sitt skydd mot cyberangrepp, samt minimera skador om ett angrepp trots allt inträffar.

MSB har utifrån it-incidentrapporteringen och tidigare rapporter identifierat sex problemområden som medför särskilda utmaningar hos organisationer gällande arbetet med att stärka skyddet mot cyberangreppsförsök. Utifrån identifierade utmaningarna har de rekommendationer som presenteras tagist fram.

Det kan finnas andra relevanta problemområden som borde lyftas fram. MSB har emellertid fokuserat på de områden som framträder av utförliga beskrivningar av händelseförlopp i it-incidentrapporteringen eller som har beskrivits som utmaningar hos organisationer i tidigare rapporter och undersökningar MSB har genomfört.

De problemområden som många organisationer behöver hantera bättre är:

- **Systematiken i säkerhetsarbetet:** Ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete utifrån allriskperspektivet är centralt för att förebygga och hantera it-incidenter. För att kunna förbättra sitt motstånd mot cyberangreppsförsök är det avgörande att organisationer har de grundförutsättningar som krävs. MSB ser att många organisationer i offentlig förvaltning saknar en ledning som engagerar sig i säkerhetsfrågor, systematiska arbetssätt och resurser för att utföra det förebyggande arbetet. MSB har i tidigare rapporter återkommande framfört denna grundläggande problematik.
- **Incident- och kontinuitetshantering:** Det som utgör en särskild utmaning för organisationer är att hantera it-incidenten som orsakats av ett cyberangrepp innan den får konsekvenser som påverkar organisationen. Under ett pågående angrepp saknas ofta rätt beredskap, kompetenser och förmåga att åtgärda situationen effektivt. Organisationer kan även sakna tydliga gemensamma riktlinjer, regler och arbetssätt, samt fungerande kommunikationsstrukturer för att hantera it-incidenter till följd av ett cyberangrepp. Även inövade arbetssätt för att bevara viktiga tillgångar saknas, likväl kontinuitetsplaner för alternativa arbetssätt om exempelvis informationssystem som i vanliga fall används är otillgängliga.

- **Medarbetarnas kunskaper:** I it-incidentrapporteringen nämns ofta nätfiske och svaga lösenord som orsak till att en angripare får initial åtkomst till en organisations informationssystem. Dagens angripare kan ha avancerade verktyg till sin hjälp för att producera övertygande och komplexa lösenords- och nätfiskeangrepp, som är svåra för medarbetarna att identifiera, vilket innebär en utmaning för organisationer. Medarbetare som saknar kunskap om hot och sårbarheter tenderar även i större utsträckning att välja svaga lösenord eller återanvända samma lösenord, något som angripare aktivt kan utnyttja. Det finns många databaser med läckta autentiseringsuppgifter som en angripare kan använda för att se om medarbetaren återanvänder sina lösenord eller använder sig av ett enkelt system. Organisationer kan även sakna tillgång till tekniska verktyg för att upptäcka svaga lösenord eller för att tvinga medarbetare att välja starkare lösenord.
- **Behörighetshantering**: Sårbarheter inom organisationen kan uppstå i samband med bristfällig behörighetshantering. En förklaring till en del av de här utmaningarna skulle kunna vara att många organisationer har relativt hög personalomsättning, och fortlöpande förändringar i verksamheten, vilket i sin tur skulle kunna försvåra för organisationer att lyckas förebygga behörighetsrelaterade it-incidenter. Detta kan leda till att sårbarheter uppstår när exempelvis medarbetare som borde förblivit obehöriga ges tillgång till känsliga informationssystem eller filytor. Bristfälliga rutiner för att avaktivera äldre användarkonton kan även gynna angriparen.
- **Ändringshantering:** Det är vanligt att organisationer har byggt sina informationssystem och sin it-miljö så att det finns utmaningar och osäkerhetsfaktorer med att genomföra uppdateringar. Organisationer kan sakna tydliga rutiner för ändringshantering och det kan ta lång tid innan kända sårbarheter hanteras. Det kan även behövas specialistkompetens för att genomföra ändringen på ett säkert sätt. Inte sällan finns även risk att ändringen orsakar kompatibilitetsproblem med andra informationssystem. Organisationer kan även sakna en testmiljö som liknar produktionsmiljön, vilket medför utmaningar med att kontrollera att ny mjukvara och andra uppdateringar inte orsakar problem innan de installeras i produktionsmiljön. Sammantaget innebär detta att många organisationer lämnar sårbarheter utan åtgärd under alltför lång tid. Organisationer som regelbundet skannar efter sårbarheter hittar ofta gamla och allvarliga sårbarheter. Några av de mer uppmärksammade cyberangreppen de senaste åren såsom WannaCry[2] har varit möjliga tack vare oåtgärdade sårbarheter.
- **Digitala leveranskedjor:** I det moderna digitala ekosystemet är digitala leveranskedjor en naturlig del. Det är kostnadseffektivt att använda specialiserade lösningar, men användandet är inte riskfritt. Att bibehålla säkerheten i den egna it-miljön kan vara en utmaning när organisationen saknar insyn i sina bakomliggande leveranskedjor och deras säkerhet. En utmaning för många organisationer ligger i att få information från leverantörer om pågående eller inträffade cyberangreppsförsök. En annan utmaning organisationer möter är om det bara finns en eller ett fåtal leverantörer av en viss tjänst som motsvarar ens kvalitetskrav eller är kompatibel med ens arbetssätt. Detta i sin tur

2. WannaCry är ett utpressningsprogram som riktar sig mot datorer med operativsystemet Microsoft Windows. I maj 2017 infekterade WannaCry uppskattningsvis över 200 000 datorer i 150 länder.

leder till monoberoenden som innebär att en organisation är beroende av en tjänst och att det saknas alternativa tjänster att använda om den tjänst som används upphör.

Rekommendationerna är framtagna för att stödja organisationer i arbetet med att prioritera säkerhetsåtgärder, för att stärka skyddet mot cyberangrepp och för att minimera skador om organisationen trots allt blir drabbad. I kapitlet *Angreppsbilden* redovisas de it-incidentrapporter som rapporterats med cyberangreppsförsök som bakomliggande orsak och i kapitlet *Utmaningar i säkerhetsarbetet* redogörs för de utmaningar som ligger till grund för de specifika rekommendationerna.

Det enda sättet att ligga steget före en angripare är att fortlöpande arbeta systematiskt och riskbaserat med helheten. Som stöd i det arbetet kan MSB:s vägledningar med fördel konsulteras:

- Vägledning säkerhetsåtgärder i informationssystem[3],
- Grundläggande säkerhet i cyberfysiska system[4], och
- Ökad säkerhet i industriella informations- och styrsystem[5].

3. MSB. *Vägledning säkerhetsåtgärder i informationssystem*, https://www.informationssakerhet.se/stod--vagledning/saker-hantering-av-information2/Vagledning_sakerhetsatgarder_i_informationssystem/ (hämtad 11/2023).

4. MSB. *Grundläggande säkerhet i cyberfysiska system*, https://rib.msb.se/filer/pdf/29983.pdf (Hämtad 11/2023).

5. MSB. *Ökad säkerhet i industriella informations- och styrsystem*, https://rib.msb.se/filer/pdf/29984.pdf (Hämtad 11/2023).

Rekommendationer till ledningen:

1. Förbättra organisationens säkerhetskultur genom att sätta tydliga mål och förväntningar för säkerhet, regelbundet kommunicera vikten av säkerhet, uppmuntra medarbetare att rapportera säkerhetshändelser och förbättringsförslag, och föregå med gott exempel.
2. Arbeta systematiskt och riskbaserat och tilldela nödvändiga resurser utifrån riskanalysen.
3. Investera i utbildningar för en kompetenshöjning och ökad medvetenhet hos medarbetarna.
4. Investera och delta i cyberkrisövningar.
5. Inventera regelbundet vilka potentiella utmaningar som bromsar säkerhetsarbetet och använd Infosäkkollen och It-säkkollen för att identifiera brister.

Rekommendationer till personal med ansvar för informations- och cybersäkerhet:

Incident- och kontinuitets-hantering	Medarbetarnas kunskaper	Behörighets-hantering	Ändrings-hantering	Digitala leveranskedjor
6. Leta aktivt efter tecken på skadlig aktivitet och använd tjänster eller tekniska verktyg för att tidigt upptäcka cyber-angrepp.	10. Utbilda medarbetare regelbundet för att kunna motstå social manipulation, använda starka lösenord och säker hantering av dem.	14. Inventera och identifiera alla behörig-heter från olika informations-system.	18. Säkerställ att personal med rätt kompetens utför ändringar.	22. Inför tydliga klausuler vid upp-handling om infor-mationsplikt från leverantörer om it-incidenter.
7. Inför arbets-sätt för att enkelt kunna anmäla och följa upp säkerhets-händelser.	11. Använd flerfaktors-autentisering.	15. Säkerställ att endast behö-riga användare och informa-tionssystem har åtkomst.	19. Kartlägg informationssystem regelbundet och upprätta en test-miljö som så långt det är möjligt efter-liknar produktions-miljön och testa ändringar innan de införs.	23. Granska och dokumentera beroenden i orga-nisationens infor-mationssystem, särskilt gällande externa leveran-törer.
8. Planera och öva för cyberangrepp.	12. Markera extern e-post och använd tekniska verktyg för att filtrera bort e-post med skadliga länkar eller bilagor.	16. Inför arbets-sätt för att regel-bundet granska behörigheter.	20. Uppdatera organisationens kritiska informa-tionssystem som exponeras mot internet när nya sårbarheter upp-täcks.	24. Planera och inför egna arbets-sätt för hantering av it-incidenter hos en leverantör.
9. Inför och öva kontinuitets-planer för exempelvis kommunikation under en cyberkris.	13. Använd tekniska verktyg för att regel-bundet se över användning av svaga, läckta eller stulna lösenord.	17. Använd automatiserad behörighets-hantering för planering och verifiering av föränderliga organisations-behov.	21. Basera sår-barhetsanalysen på information om nya sårbarheter, säkerhetsuppda-teringar, generella råd och rekommen-dationer för att öka motståndskraften genom omvärlds-bevakning.[6]	25. Inför alterna-tiva arbetssätt om något skulle inträffa en tjänst hos en leverantör, som organisatio-nen är beroende av för att kunna fortsätta sin verk-samhet.

6. Exempelvis genom att regelbundet besöka MSB:s webbplatser.

Om rapporten

Om rapporten

Rapporten ger en övergripande bild av cyberangreppsförsök mot statliga myndigheter och NIS-leverantörer och dess konsekvenser. Rekommendationer har tagits fram baserat på de utmaningar som identifierats vid analys av angreppsbilden och slutsatser från tidigare MSB rapporter. Rapporten är den tredje delen i en serie av tematiska rapporter.[7]

Kapitlet om *Angreppsbilden* baseras på de it-incidentrapporter som MSB mottar. Ju mer information som MSB får om it-incidenter, desto bättre bild får myndigheten av behovsbilden och därmed hur det förebyggande arbetet kan utvecklas och struktureras. Vissa organisationer har rapporteringsplikt eftersom den verksamhet som bedrivs anses särskilt kritisk för vårt samhälle. Rapporteringskraven varierar beroende på vilken reglering som en organisation berörs av. De organisationer som har krav på sig att rapportera it-incidenter till MSB är statliga myndigheter[8] och leverantörer av samhällsviktiga[9] och digitala tjänster[10] (NIS-leverantörer). Rapporteringsplikten kommer vidgas till fler organisationer och sektorer när NIS 2-direktivet träder i kraft.[11]

Rapporten har sin grund i de it-incidentrapporter som mottagits av MSB mellan april 2019 till september 2023. Tyvärr saknar många av de mottagna incidentrapporterna utförliga beskrivningar av händelseförloppet. Sammantaget kan det medföra att vissa problem eller behov som borde inkluderats i rapporten saknas. Utöver it-incidenterna har även publikt kända it-incidenter analyserats för att exemplifiera de utmaningar och konsekvenser som angrepp kan medföra.

---

7. Den första var: *Hoten mot de digitala leveranskedjorna: 50 rekommendationer för att stärka samhällssäkerheten*, https://rib.msb.se/filer/pdf/29829.pdf.
Den andra var: *Ändringar som både hotar och skyddar: 20 rekommendationer för säkrare ändringar i våra informationssystem*, https://rib.msb.se/filer/pdf/30193.pdf.

8. MSB. *Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av it-incidenter för statliga myndigheter* (MSBFS 2020:8) https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs-2020-8-foreskrifter-om-rapportering-av-it-incidenter-for-statliga-myndigheter.pdf.

9. MSB. *Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster* (MSBFS 2018:9) https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs2018_9.pdf.

10. MSB. *Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av incidenter för leverantörer av digitala tjänster* (MSBFS 2018:10) https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs2018_10.pdf.

11. EU. *NIS2-direktivet* (EU 2022/2555) https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX-:32022L2555&qid=1701943333306.

Nedan redogörelse för det cyberangrepp som Kalix kommun utsattes för ger en uppfattning om vad ett cyberangrepp riktat mot en samhällsviktig aktörs informationssystem kan åstadkomma.

Natten mot torsdag den 16 december 2021 drabbades Kalix kommun av en allvarlig driftstörning. Det stod snart klart att kommunen blivit utsatt för ett utpressningsangrepp där en angripare krypterat och låst kommunens informationssystem. För att återställa informationen krävde angriparen en lösensumma. Cyberangreppet kom att påverka stora delar av kommunens verksamhet, däribland hemsjukvård, hemtjänst, skolor och bibliotek.[12, 13]

Angreppet innebar att kommunen inte kunde använda datorer, telefoner eller e-post och istället tvingades att arbeta med papper och penna. Det tvingade fram en helomställning i arbetssätten för exempelvis hemtjänst och hemsjukvård. Dessa verksamheter kom inte längre åt de scheman, journaler och medicinlistor som låg i informationssystemen. Arbetet blev tidsödande och krävde bland annat att medarbetare använde sig av whiteboardtavlor för schemaplanering. De fick även bläddra i fysiska pärmar med beslut om beviljade insatser för att säkerställa att samtliga brukare fick rätt stöd. För att kommunens 1 900 anställda inte skulle bli utan sin jullön betalades novemberlönen ut i stället för decemberlönen. Det var inte bara Kalix kommun som påverkades utan även aktörer såsom leverantörer, samarbetspartners och invånare, som inte kunde kommunicera med kommunen via de normala kontaktvägarna.

Det skulle dröja till mitten av januari 2022 innan de flesta informationssystem fungerande igen, och ännu längre innan allt återgått till ett normalläge för kommunen. Kostnaden för att återställa systemen och samtidigt uppgradera it-säkerheten beräknades uppgå till 2,5 miljoner kronor.[14] Det är oklart vad incidentens totala kostnad blev, men troligen blev det betydligt högre. Kalix kommun betalade aldrig någon lösensumma, utan har istället förordat efterlevnad av MSB:s rekommendationer att inte betala[15] och hantering av it-incidenter.[16, 17]

12. Stahle, Nils. *It-attacken mot Kalix kommun – detta har hänt*. SVT. 2021-12-17. https://www.svt.se/nyheter/lokalt/norrbotten/it-attacken-mot-kalix-kommun-detta-har-hant (hämtad 08/2023).

13. Warne, Karin. *Så ledde Kalix IT-chef arbetet under hackerattacken*. Vision. 2022-05-06. https://vision.se/chefenifokus/arkiv/2022/nr2/sa-ledde-kalix-it-chef-arbetet-under-hackerattacken/ (hämtad 08/2023).

14. Svenska dagbladet. *It-attacken mot Kalix har kostat 2,5 miljoner*. 2022-01-14. https://www.svd.se/a/JxG1k4/notan-for-attacken-i-kalix-2-5-miljoner-kronor (hämtad 05/2023).

15. MSB. *Metoder som används vid cyberangrepp – Betalning till angriparna*, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/cyberhot/metoder-som-anvands-vid-cyberangrepp/ (Hämtad 10/2023).

16. MSB. *Råd och stöd*, https://www.cert.se/rad-och-stod/ (Hämtad 10/2023).

17. Hannu, Filip. *Lärdomen efter it-attacken i Kalix: Följ checklistan och lägg pengar på det*. SVT. 2022-05-22. https://www.svt.se/nyheter/lokalt/norrbotten/kommundirektorens-lardom-efter-attacken-folj-checklistan-och-lagg-pengar-pa-det (hämtad 08/2023).

De störningar som uppstod till följd av cyberangreppet mot Kalix kommun fick konsekvenser för brukare, medborgare och andra organisationer. Risken för att fler än den egna organisationen och dess informationssystemen drabbas växer i takt med att organisationer förflyttar allt mer av sin verksamhet till en digital miljö.

Den här rapporten har producerats för att öka förståelsen för angreppsbilden mot statliga myndigheter och leverantörer av samhällsviktiga tjänster, samt belysa de utmaningar organisationer har i sitt säkerhetsarbete och vilka förebyggande åtgärder som bör prioriteras.

I likhet med tidigare tematiska rapporter inkluderas delar av MSB:s analymodell för den som själv systematiskt vill analysera it-incidenter relaterade till cyberangrepp.

Rapporten är framtagen med stöd av medel från EU:s Connecting Europe Facility-fond och riktar sig främst till beslutsfattare, verksamhetsutvecklare och strateger inom it-avdelningar, men också säkerhetsfunktioner och verksamhetsstöd, samt CISO och andra ansvariga för informations- och cybersäkerhetsarbetet.

Antagonistisk cyberaktivitet

Antagonistisk cyberaktivitet

Digitaliseringen har gett stora fördelar för samhället, men innebär också att angripare kan använda sig av cyberangrepp som ett verktyg för att uppnå både kort- och långsiktiga mål. Förståelse för hur cyberangrepp kan yttra sig, och de bakomliggande syftena, kan bidra till organisationers förmåga att möta cyberhoten.

Cyberangrepp har genom åren kommit att definieras på olika sätt. De olika definitionerna har uppkommit i samband med att hot som uppstår inom cyberrymden har blivit en aktualitet för flera olika typer av aktörer, med olika syn på vad som utgör ett hot och vad som är skyddsvärd information. I denna rapport förstås ett cyberangrepp som ett cyberangreppsförsök som har påverkat it-miljön. Cyberangrepp genomförs som en, eller en serie av, interaktion(er) mellan *angriparen* och *målet*. Målet för cyberangreppet kan utgöra en individ eller en organisation. För att utgöra ett cyberangrepp måste interaktionen mellan angriparen och målet uppfylla fyra villkor. Interaktionen måste vara något som:

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

Legalitetsvillkoret uppfylls när angriparen saknar en legal rätt att utföra en handling inom ramen för interaktionen. Obehöriga ska begränsas att ta del av eller göra ändringar i informationssystem med hjälp av tekniska säkerhetslösningar för åtkomstkontroll och autentisering. Om informationssystemets komponenter saknar adekvat skydd kan det dock finnas flera sätt för en angripare att ta del av,

ändra eller blockera tillgången till information utan en legal rätt att vidta sådana åtgärder. I vissa fall kan angripare dessutom upptäcka sätt att ta sig förbi de skydd som finns. De fall där hotet kommer inifrån den egna organisationen eller där angriparen lyckats tillskansa sig giltiga inloggningsuppgifter på annat sätt, och därmed har teknisk tillgång, är exempel på scenarion där angriparen har teknisk behörighet, men saknar legal rätt. Legalitetsvillkoret möjliggör en åtskillnad mellan cyberangrepp och exempelvis ett penetrationstest.

Praktikvillkoret uppfylls när interaktionen mellan angriparen och målet utgör en eller flera händelser. En händelse inom sammanhanget innebär att angriparens handlande måste, inom ramen för interaktionen, ha resulterat i att något upphört, uppstått eller ändrats inom målets it-miljö. Händelsen kan till exempel bestå i att skadlig kod installerats, att digitala informationstillgångar har raderats, att information har kopierats eller att it-komponenter har konfigurerats om. En avgränsning av begreppet *cyberangrepp* skulle kunna innebära att det endast inkluderar interaktioner som sker *i* cyberrymden. På så vis räknas inte fysiskt sabotage av informationssystem och nätverksinfrastruktur som cyberangrepp. MSB avgränsar begreppet cyberangrepp så att händelser i den fysiska miljön, såsom elavbrott och bränder (även om de skulle vara avsiktligt anlagda), inte räknas i statistiken över cyberangrepp.

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

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

Skillnaden mellan cyberangreppsförsök och it-incidenter

MSB skiljer på cyberangreppsförsök och it-incidenter. En incident definieras i denna rapport som en inträffad oönskad händelse. Vid en it-incident består det oönskade av de effekter som har uppstått i termer av konfidentialitet, riktighet eller tillgänglighet (incidentvillkoret).

Cyberangreppsförsök, likt misstag, systemfel och naturhändelser, utgör möjliga orsaker till it-incidenter.

Det är otillgängligheten hos en webbtjänst som är incidenten. Det är ett överbelastningsangrepp, en felkonfiguration vid ändringsarbete, ett elavbrott, eller något annat, som är orsaken till att webbtjänsten inte är tillgänglig.

Genom tillämpa en sådan distinktion blir det möjligt att jämföra antalet gånger exempelvis en webbtjänst blir otillgänglig, och hur länge, på grund av cyberangrepp med antalet gånger samma webbtjänst blir otillgänglig på grund av andra orsaker. Genom att göra den jämförelsen kan de mest frekventa respektive mest allvarliga felkällorna identifieras och hanteras.

Angriparens syfte

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

Målet för cyberangreppet behöver inte vara den angriparen huvudsakligen vill påverka. Det finns även situationer då en aktör kan bli ett mål för ett angrepp på grund av att angriparen vill påverka användare av målets tjänster. I denna rapport förstås detta som att angriparen ämnar påverka andra *via* målet. När angriparens syfte är att påverka allmänheten så kan samhällsviktig verksamhet utgöra potentiella mål.

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

Att *förhindra nytta* för målet eller hos andra via målet. Att nytta förhindras innebär att viss aktivitet eller produktion avstannar eller fördröjs. En angripare som önskar att nytta förhindras verkar efter målsättningen att organisationen som utgör målet inte ska kunna nyttja informationssystem och andra it-komponenter som möjliggör viss aktivitet eller produktion. Det kan handla om göra det svårt eller omöjligt för organisationen att nyttja centrala informationssystem, och därav påverka hela organisationen, eller enstaka tjänster. En angripares syfte kan också tänkas vara att förhindra nytta för andra individer, organisationer eller stater

via målet för angreppet. Om syftet är att förhindra kommunikation för allmänheten så skulle målet för angreppet exempelvis kunna vara en telekomoperatör. Exempel på metoder som angriparen skulle kunna använda sig av i syfte att förhindra nytta inkluderar överbelastningsangrepp som försvårar eller omöjliggör transmissionen av legitim datatrafik till och från angripna nätverkskomponenter.

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

Att *orsaka nytta* för angriparen eller hos andra som angriparen stödjer. En angripare som ämnar gynna sig själv kommer att genomföra cyberangrepp för att amplifiera sin egen förmåga eller sitt välstånd. Det kan handla om att extrahera känsliga informationstillgångar från målet eller att tjäna pengar. Det kan också handla om cyberangrepp som utförs i syfte att införliva delar av den angripna it-miljön inom den egna produktionen. En angripare som ämnar orsaka nytta åt någon som angriparen stödjer på bekostnad av målet kan tänkas utföra underrättelseaktivitet som kan gynna denne. Exempel på angreppsmetoder som angriparen kan använda vändas i syfte att orsaka nytta åt sig själv eller någon den stödjer är att installera spionprogram eller ett program för kryptomining[18] inom målets it-miljö som kan användas för att extrahera känslig information respektive utvinna kryptovaluta. Även utpressningsprogram används i detta syfte. Angriparen kräver då målet på en lösensumma i utbyte mot krypteringsnycklar som kan dekryptera informationstillgångar som angriparen krypterat.

Att *förhindra skada* för angriparen eller andra som angriparen stödjer. En angripare som vill förhindra motparten från att orsaka angriparen, eller andra som angriparen stödjer, skada kommer verka efter målsättningen att negativt påverka informationssystem eller informationstillgångar som skulle kunna användas till detta syfte. Aktörer som blir mål för dessa typer av angrepp har en förmåga att agera på ett sådant sätt som kan orsaka skada. Det kan exempelvis röra sig om

18. Både spionprogram och kryptominers är exempel på skadlig programvara. Spionprogram kan används för att överföra information om exempelvis användaraktivitet från målet till angriparen. Kryptominers kan installeras på offrets dator i syfte att använda processorkraften till att utvinna kryptovaluta.

institutioner som arbetar med brottsbekämpning eller nyhetspublicering. Om angriparen stödjer en statlig aktör eller beväpnad gruppering skulle det även kunna handla om att slå ut eller störa offensiv militär förmåga. Angreppsmetoder som angriparen kan tänkas nyttja i syfte att förhindra skada korrelerar ofta med metoder som skulle kunna användas för att förhindra nytta eller orsaka skada för ett mål. En angripare som vill förhindra publiceringen av viss information skulle exempelvis kunna installera en wiper inom målets informationssystem för att i förebyggande syfte radera information som identifierats som skadlig.

Typer av angripare

När olika typer av aktörer som utför cyberangrepp omtalas brukar det oftast refereras till de mer organiserade sammanslutningarna. Dessa inkluderar allt från ”hacktivister” och cyberkriminella till statsaktörer och statsunderstödda grupper. Gemensamt för dem alla är att de genom internets globala räckvidd har en förmåga att utföra cyberangrepp långt ifrån deras egen geografiska hemvist.

Det övergripande syftet med angreppet kan vara allt från ekonomiskt, ideologiskt, politiskt till geostrategiskt motiverat och underbygger den antagonistiska relation som angriparen utvecklat gentemot målet.

Antagonistiska cyberhot

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

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

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

Ibland talas det om avancerade eller kvalificerade cyberhot. Ett sätt att förstå avancerade cyberhot är som en delmängd av sådana företeelser som ryms inom den föreslagna definitionen av cyberhot ovan. Ett första sätt att avgränsa sådana cyberhot är att ställa ett ytterligare villkor om att sådana cyberhot, såvida inte åtgärder vidtas för att stoppa dem, orsakar *faktiska incidenter* [19]. En faktisk incident definieras i denna rapport som en inträffad oönskad händelse där:

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

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

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

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

Utförandet av cyberangrepp

Det finns många olika angreppsmetoder[20] och deras sofistikation varierar kraftigt beroende på vilka tekniker och resurser som används för det specifika angreppsförsöket. Massutskick av skräppost innehållande skadliga länkar och överbelastningsangrepp kan exempelvis sägas utgöra relativt osofistikerade metoder, men samtidigt varierar dessa i utformning och skala, och därmed potentiell verkansgrad.

19. Typ av incident. En händelse där nytta förhindras eller skada orakas för den den drabbade organisationen eller nytta orsakas eller skada förhindras för en av organisationens konkurrenter (se bilaga 1 för en mer djupgående redogörelse).

20. MSB, *Metoder som används vid cyberangrepp*, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/cyberhot/metoder-som-anvands-vid-cyberangrepp/ (Hämtad 11/2023).

Vid vissa cyberangrepp fokuserar angriparen främst på att övervaka och komma över information utan att nödvändigtvis förstöra eller ändra den. Dessa angrepp kan ske i det dolda och utan att den som angrips märker av angreppet. Alternativt kan det ta tid innan angreppet uppmärksammas. Andra cyberangrepp är mer direkt påtagliga och upptäcks därför ofta i ett tidigare skede. Det inkluderar angrepp vars övergripande syfte är att generera uppmärksamhet.

Syftet med angreppet avgör huruvida angriparen försöker få och eskalera åtkomst till it-miljön eller använder sig av andra metoder för att påverka it-miljöns funktionalitet. Mer sofistikerade cyberangrepp påbörjas ofta med ett intrång i målets it-miljö. Intrångsförsöket kan bestå av ett antal komponenter[21] eller steg, där exempelvis ett intrångsförsök (förenklat) ofta innefattar följande:

1. Inledande åtkomst,
2. Befästande av position,
3. Lateral rörelse,
4. Måluppfyllelse.

Inledande åtkomst används av angriparen för att försöka komma in i en organisations nätverk och informationssystem. Angriparen kan nyttja olika intrångsmetoder såsom nätfiske, användande av komprometterade autentiseringsuppgifter eller leveranskedjeangrepp.[22] Den här fasen kan också inkludera rekognoscering och andra förberedande aktiviteter som syftar till att avslöja *hur* ett intrång kan genomföras mot målet.

När angriparen har åtkomst försöker denne *befästa sin position* för att behålla åtkomsten vid omstarter, ändrade autentiseringsuppgifter eller andra avbrott som kan häva åtkomsten. Detta kan exempelvis göras genom åtkomst-, åtgärds- eller konfigurationsändringar eller genom att ersätta legitim kod såsom startkod.[23] Det kan också göras genom att ta över flera användarkonton.

Lateral rörelse, det vill säga när angriparen rör sig djupare in i informationssystem eller it-miljö, kan genomföras genom att dra nytta av systemsvagheter, felkonfigurationer eller sårbarheter. Angriparen kan också installera egna fjärråtkomstverktyg eller använda legitima referenser med inbyggda nätverks- och operativsystemverktyg vilket kan vara svårupptäckt för målet.[24, 25] Vid exekvering av skadlig kod används ofta flera metoder tillsammans för att uppnå ett bredare mål. Fjärråtkomstverktyg kan exempelvis användas för att köra ett ”PowerShell”-skript[26] för att utforska ett nätverk och stjäla data. Angriparen kan också försöka

21. Komponenter kan beskrivas med olika grader av detaljering. MITRE är ett exempel på ramverk för att beskriva cyberangrepp, https://attack.mitre.org/.

22. Mitre. *Initial Access*. 2018-10-17 (uppdaterad 2019-07-19). https://attack.mitre.org/tactics/TA0001/ (hämtad 06/2023).

23. Mitre. *Persistence*. 2018-10-17 (uppdaterad 2019-07-19). https://attack.mitre.org/tactics/TA0003/ (hämtad 06/2023).

24. Mitre. *Privilege Escalation*. 2018-10-17 (uppdaterad 2021-01-06). https://attack.mitre.org/tactics/TA0004/ (hämtad 06/2023).

25. Mitre. *Lateral Movement*. 2018-10-17 (uppdaterad 2019-07-19). https://attack.mitre.org/tactics/TA0008/ (hämtad 06/2023).

26. Ett PowerShell-skript är en oformaterad textfil som innehåller ett eller flera PowerShell-kommandon dvs PowerShell är ett kommandoradsgränssnitt och ett skriptspråk som används för automatisering.

utöka rättigheterna hos de konton som angriparen har kontroll över, eller genom att ta kontroll över exempelvis administratörskonton.

För *måluppfyllelse* krävs nästan alltid att angriparen först utforskar nätverket och informationssystemen för att hitta sitt mål. Med oprivilegierad åtkomst kan angriparen komma in, men oftast krävs högre behörighet för att kunna fortsätta. Som en del i att nå måluppfyllelse kan angriparen nyttja olika metoder för att försöka påverka information och informationssystemens konfidentialitet, riktighet och tillgänglighet. Se nedan exempel på ett angrepp där angriparen befäst sin position, rört sig lateralt och krypterat filer samt låst ute anställda från deras datorer. Det övergripande syftet, givet ett antagande om att det utfördes av vinstdrivande kriminella, var att orsaka nytta för angriparen. Då angriparen inte fick betalt har syftet med angreppet inte uppfyllts och därmed har inte måluppfyllelse uppnåtts, även om angreppets påverkan blev omfattande.

Angreppet mot Norsk Hydro – en dyr historia som drabbade 350 000 anställda

- **Typ**: Utpressningsangrepp
- **Faktisk incident:** Nytta förhindras, skada orsakas.

Morgonen den 19 mars 2019 möttes tusentals anställda på Norsk Hydro, en av världens största aluminiumtillverkare, av en skärmnotis som meddelade att informationssystemen krypterats och kunde återställas i utbyte mot en avsevärd lösensumma. Vissa anställda kunde överhuvudtaget inte logga in på sina datorer.[27] För att förhindra spridning av viruset tvingades det multinationella bolaget stoppa vissa verksamheter, medan andra fick hanteras genom manuella arbetsprocesser.[28] Utredare kunde snart slå fast att det utpressningsvirus som infiltrerat informationssystemen var en skadlig programvara som gick under namnet *LockerGoga*.[27]

Hur angriparna initialt fick tillgång till Norsk Hydros informationssystem är okänt. Klart står dock att angriparna inledningsvis har riktat sig mot enskilda kontoanvändare med lägre behörigheter för att, väl inne i systemet, ha berett sig tillgång till användare på högre administratörsnivå. När angriparna hade röjt tillgång till domänadministratörer planterades den skadliga kod som krypterade filer och låste ut anställda från sina datorer.[29]

27. Cohen, Gary. *Throwback Attack: Norsk Hydro gets hit by LockerGoga ransomware*. Industrial Cybersecurity Pulse. 2021-05-21. https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-norsk-hydro-gets-hit-by-lockergoga-ransomware/ (hämtad 9/2023).

28. Austin, Patrick Lucas. *This Company Was Hit With a Devastating Ransomware Attack –But Instead of Giving In, It Rebuilt Everything*. Time. 2021-06-14. https://time.com/6080293/norsk-hydro-ransomware-attack/ (hämtad 9/2023).

29. Greenberg, Andy. *A Guide to LockerGoga, the Ransomware Crippling Industrial Firms*. Wired. 2019-03-25. https://www.wired.com/story/lockergoga-ransomware-crippling-industrial-firms/ (hämtad 9/2023).

Trots tidiga krishanteringsinsatser orsakade LockerGoga betydande skada. Angreppet påverkade samtliga av Norsk Hydros 350 000 anställda och företaget tvingades övergå till att arbeta med papper och penna under tre veckors tid. Kunskapsbrist kring manuella produktionsprocesser gjorde att företaget fick ta in tidigare anställda pensionärer med erfarenhet av pappersbaserat arbete. Parallellt fick Norsk Hydro, som aldrig betalade den lösensumma som angriparna avkrävde, granska och återställa tiotusentals skadade datorer och servrar. I vissa fall tog det tre månader att återupprätta informationssystemen.[30] Den sammantagna kostnaden för förlorade intäkter och skadeåtgärdande insatser bedöms ha landat på mellan 300 och 350 miljoner norska kronor.[31] Norsk Hydros öppenhet kring angreppet, exempelvis i form av dagliga presskonferenser, tros ha bidragit till att förhindra att bolaget föll kraftigt på aktiemarknaden.[32]

Det ”lyckade” cyberangreppet

Ett cyberangrepp kan ses som ”lyckat” utifrån angriparens synvinkel om syftet med angreppet uppfylls. *Tabell 1* beskriver hur måluppfyllelsen nås utifrån angriparens syfte att *orsaka skada* eller att *förhindra nytta* hos målet eller hos andra via målet, alternativt genom att *orsaka nytta* eller *förhindra skada* för sig själv, eller för andra för vilkas räkning angriparen genomför angreppet.

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

30. Cohen, Gary. *Throwback Attack: Norsk Hydro gets hit by LockerGoga ransomware*. Industrial Cybersecurity Pulse. 2021-05-21. https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-norsk-hydro-gets-hit-by-lockergoga-ransomware/ (hämtad 9/2023).

31. Affärsvärlden. *Så slog cyberangreppet mot Norsk Hydros resultat.* 2019-06-05. https://www.affarsvarlden.se/artikel/sa-slog-cyberangreppet-mot-norsk-hydros-resultat-6961055 (hämtad 9/2023).

32. Austin, Patrick Lucas. *This Company Was Hit With a Devastating Ransomware Attack–But Instead of Giving In, It Rebuilt Everything*. Time. 2021-06-14. https://time.com/6080293/norsk-hydro-ransomware-attack/ (hämtad 9/2023).

Tabell 1. Angriparens måluppfyllelse utifrån syftet och effekten att orsaka skada eller förhindra nytta hos den som angrips, eller att orsaka nytta eller förhindra skada för sig själv.

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

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

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

Se nedan exempel på ett angrepp som skulle kunna kategoriseras som ett *lyckat vårdslöst cyberangrepp*.

Rysslands angrepp mot Viasats satellitbaserade KA-SAT-nätverk

- **Typ:** Överbelastningsangrepp, skadlig programvara
- **Faktisk incident:** Nytta förhindras för den angripne, skada förhindras för angriparen

I det initiala skedet av den fullskaliga ryska invasionen av Ukraina lanserade Ryssland en rad cyberangrepp som tros ha syftat till att överväldiga den ukrainska försvarsförmågan. Angreppen, riktade mot myndigheter och kritisk infrastruktur, genomfördes genom att bland annat exekvera skadlig kod i form av wiper-programvara. Rysslands angrepp mot telekomföretaget Viasat, vars satellitbaserade KA-SAT-nätverk försörjer tiotusentals människor och organisationer i Ukraina och övriga Europa med internetåtkomst, har benämnts som den mest framgångsrika.[33]

Den 24 februari 2022, timmarna innan Ryssland inledde den fullskaliga invasionen av Ukraina, riktade ryska hackare överbelastningsangrepp mot det nätverk dit Viasats satellitutrustning var uppkopplad. Genom att exploatera en felkonfigurerad VPN i nätverket installerade angriparna därefter wiperprogramvara (idag känd som *AcidRain*). Den skadliga koden innebar att många av de modem som kommunicerar med Viasats *KA-SAT*-satellit inaktiverades, med omfattande avbrott som följd.[34]

Angreppet mot Viasat tros ha hämmat det ukrainska försvarets möjlighet att leda och samverka under krigets inledande fas.[35] Därutöver lämnades tusentals ukrainare utan internet. Konsekvenserna nådde också Centraleuropa, där över 500 000 bredbandskunder förlorade internetåtkomst – i vissa fall upp till två veckor.[36] Det tyska energibolaget Enercon förlorade även möjlighet att styra och kontrollera 5 800 vindkraftverk.[37]

33. Lewis, James Andrew. *Cyber War and Ukraine. Center for Strategic and International Studies*. 2022-06-16. https://www.csis.org/analysis/cyber-war-and-ukraine (hämtad 2023/08).

34. Poireault, Kevin. *Five Takeaways From the Russian Cyber-Attack on Viasat's Satellites*. Infosecurity Magazine. 2023-05-09. https://www.infosecurity-magazine.com/news/takeaways-russian-cyberattack/ (hämtad 2023/08).

35. Svenska dagbladet. *EU: Ryssland bakom cyberattack mot satellit*. 2022-05-10. https://www.svd.se/a/V9J77J/eu-ryssland-bakom-cyberattack-mot-satellit (hämtad 2023/08).

36. CyberPeace Institute. *Case Study: Viasat*. 2022-06. https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat (hämtad 2023/08).

37. Greig, Jonathan. *Viasat confirms report of wiper malware used in Ukraine cyberattack*. The Record. 2022-04-01. https://therecord.media/viasat-confirms-report-of-wiper-malware-used-in-ukraine-cyberattack (hämtad 2023/09).

Om cyberkrigföring

Cyberangrepp kan och har använts som en metod för att uppnå taktiska och operationella mål inom både hybridkrigföring och fullskaligt krig. Dessa angrepp kan, men måste inte, innefatta orsakande av förstörelse. Ett cyberangrepp i väpnad konflikt, oavsett om den är offensiv eller defensiv, kan orsaka personskada eller dödsfall alternativt förhindra nytta, skada eller förstörelse av föremål. Cybermedel kan också användas för att lokalisera mål som sedan angrips med andra medel. Utöver cyberangrepp kan traditionella vapen och stridsmetoder användas för att fysiskt förstöra datorer, störa eller förstöra nätverk, alternativt för att påverka, lura eller till och med döda användarna.

Cyberangrepp inom krigföring har bland annat används av Ryssland inom ramen för den fullskaliga invasionen av Ukraina. I rapporten *När kriget kom nära*[38] har MSB kartlagt vilka typer av cyberangreppsförsök som utförts och dess syften. Figuren nedan illustrerar till vilket syfte cyberangrepp och fysiska attacker mot nätverk, informationssystem och annan it-infrastruktur har använts för att uppnå kort- och långsiktiga mål.

Kategorisering av cyberangreppsförsök som riktats mot Ukraina	
Att förhindra nytta i det ukrainska samhället	**Att orsaka skada i det ukrainska samhället**
• Störa eller slå ut samhällsviktig verksamhet. • Störa eller slå ut industri eller annan verksamhet av vikt för landets ekonomi. • Störa integrering mot EU och andra länder i ”Väst”.	• Korrumpera funktioner inom staten och näringslivet. • Skapa misstro, rädsla och konflikter. • Förstöra dyr teknisk utrustning eller viktiga informationstillgångar.
Att förhindra skada för angriparen eller angriparens uppdragsgivare.	**Att orsaka nytta för angriparen eller angriparens uppdragsgivare.**
• Påverka ukrainska staten så att den inte gör val som går emot Rysslands intresse. • Begränsa landets möjligheter att försvara sig självt militärt. • Förhindra oönskade avslöjanden i media eller på sociala medier.	• Spionage. • Skapa sympatier för Ryssland eller ryska ståndpunkter.

38. MSB, *När kriget kom nära: årsrapport it-incidentrapportering 2022*, https://www.msb.se/sv/publikationer/nar-kriget-kom-nara--arsrapport-it-incidentrapportering-2022/ (hämtad 10/2023).

Cyberangreppens konsekvenser

Cyberangreppens konsekvenser

Ett cyberangrepp kan innebära allvarliga konsekvenser för den organisation som drabbas. Om informationssystemet dessutom upprätthåller samhällsviktig verksamhet kan det även innebära allvarliga konsekvenser för samhället.

En incident är en inträffad oönskad händelse. Orsaken till en it-incident kan delas in i fyra övergripande kategorier[39]:

- *angrepp* (antagonistiska hot),
- *misstag* (icke-antagonistiska hot),
- *systemfel* (tekniska hot) och
- *naturhändelser* (väderfenomen, jordbävningar, solstormar etc.).

Allriskperspektivet

Allriskperspektivet är ett förhållningssätt där man strävar efter att bedöma alla risker för det som ska skyddas och att analysera alla möjliga orsaker till att en risk realiseras. Normalbilden är att de vanligaste orsakerna till inrapporterade it-incidenter är misstag (ofta i samband med ändringar i it-miljön) och systemfel (som ofta hade kunnat undvikas genom ändringar i it-miljön). Att utgå ifrån allriskperspektivet för att upprätthålla samhällsviktiga informationssystem är därmed centralt.

Hot är något som orsakar, eller bidrar till att orsaka, att en oönskad händelse inträffar. Det är när en oönskad händelse inträffar som en incident uppstår. Incidenter orsakade av cyberangrepp får ofta större uppmärksamhet i media i jämförelse med andra it-incidenter. I termer av konsekvenser spelar det dock ingen roll om det är ett angrepp, misstag eller systemfel som gör att exempelvis ett livsuppehållande informationssystem slutar att fungera. Om systemet inte repareras eller ersätts kan patienter avlida. Konsekvenserna här är de effekter som inträffar om inget aktivt görs för att stoppa dem. Det är viktigt att komma

39. Kategorisering som MSB använder för inrapporterade it-incidenter.

ihåg att den vanligaste orsaken till rapporterade it-incidenter till MSB under 2022 var systemfel, följt av misstag och därefter cyberangreppsförsök.[40]

En it-incident som orsakas av ett cyberangrepp mot informationssystem som upprätthåller samhällsviktig verksamhet kan få allvarliga konsekvenser för den enskilda organisationen som drabbas, men även individer och för samhället i stort. Detta skildras exempelvis i cyberangreppet mot Kalix kommun[41] och i exemplet nedan.

Cyberangrepp bidrog till att ett dödsfall inte kunde förhindras

- **Typ:** Utpressningsangrepp.
- **Faktisk incident:** Nytta förhindras.

Den 10 september 2020 utsattes universitetssjukhuset i Düsseldorf, Tyskland, för ett cyberangrepp som låste de informationssystem som användes för bland annat kommunikation och samordning av patienter. Det hårt ansatta sjukhuset tvingades ställa in operationer och halvera sin patientkapacitet.[42] När sjukhuset samma natt mottog ett larm om en svårt sjuk kvinna hänvisades ambulansen till ett sjukhus beläget en timma bort, varvid kvinnan avled under färden.[43] Den tragiska händelsen har beskrivits som det första dödsfall som föranletts av ett cyberangrepp.[42]

Angriparna introducerade den skadliga programvaran genom att exploatera en sårbarhet hos sjukhusets nätverksleverantör. När sårbarheten väl åtgärdades fanns viruset redan planterat i informationssystemen. Utpressningsangreppet tros egentligen varit riktat mot det universitet som sjukhuset hörde samman med och angriparna kom, efter uppmaning från polisen, att överlämna över dekrypteringsnycklarna utan att någon lösensumma utbetalats.[42] Skadan var emellertid redan skedd och det skulle ta två veckor innan sjukhuset kunde återöppna sin akutmottagning, och ytterligare tid innan det kom upp i full kapacitetsnivå.[44] Angriparna, som inte kunnat identifieras, står misstänkta av tysk polis för dråp.[45]

40. MSB, *När kriget kom nära: årsrapport it-incidentrapportering 2022*, https://www.msb.se/sv/publikationer/nar-kriget-kom-nara--arsrapport-it-incidentrapportering-2022/ (Hämtad 11/2023).

41. Se kapitlet *Om Rapporten*.

42. Eddy, Melissa; Perlroth, Nicole. *Cyber Attack Suspected in German Woman´s death*. The New York Times. 2020-09-18. https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html (hämtad 9/2023).

43. Dobos, Lars. *Patient avled efter ransomware-attack mot sjukhus*. Tech World. 2020-09-18. https://techworld.idg.se/2.2524/1.739684/avliden-ransomware-sjukhus (hämtad 9/2023).

44. Silomon, Jantje. *The Düsseldorf Cyber Incident*. Institute for Peace Research and Security Policy. 2020-09-30. https://ifsh.de/en/news-detail/the-duesseldorf-cyber-incident (hämtad 9/2023).

45. Tidy, Joe. *Police launch homicide inquiry after German hospital hack*. BBC. 2020-09-18. https://www.bbc.com/news/technology-54204356 (hämtad 9/2023).

Organisationspåverkan

En it-incident som påverkar riktigheten, tillgängligheten eller konfidentialiteten i en it-miljö kan oberoende av orsak få konsekvenser utanför den. It-incidenten kan störa den dagliga verksamheten hos organisationer med konsekvenser som exempelvis minskad produktivitet, nedsatt kommunikation, försämrad webbplatsprestanda eller avbrott i tjänster.

It-incidenten kan också innebära kostnader i form av reparation och återhämtning av den skada som har orsakats organisationen. Organisationer kan dessutom få juridiska påföljder om de inte följer lagar eller regler om exempelvis dataskydd. Om it-incidenten blir offentliggjord eller exempelvis leder till någon form av dataläckage kan det skada kundförtroende och varumärkets värde, eller till och med innebära att organisationen går i konkurs som i exemplet om dataintrång hos det finska bolaget Vastaamo.[46] De olika konsekvenserna av en it-incident kan i sin tur leda till olika former av merarbete, stress och oro bland medarbetare inom organisationen och deras kunder.

För att snabbare kunna hantera pågående och förebygga framtida incidenter är det avgörande att it-incidenter rapporteras[47, 48] och att information delas.

Kategorier av påverkan

Olika taxonomier kan användas för att kategorisera påverkan av it-incidenter där exempelvis forskning föreslår att påverkan eller skadan av ett cyberangrepp kan delas in i fem huvudkategorier bestående av fysisk/digital skada, ekonomisk skada, psykologisk skada, skada på anseende eller social och samhällelig skada[49]. ENISA använder en liknande taxonomi med fem huvudkategorier.[50]

Det svenska krisberedskapssystemet är strukturerat kring värnandet av ett antal samhälleliga skyddsvärden. I NIS-sammanhang är det i synnerhet tre utpekade skyddsvärden som är av särskild vikt. Vid en it-incident som berör en samhällsviktig tjänst ska en bedömning göras om störningen negativt påverkar människors hälsa, användarnas ekonomi och/eller användarnas förtroende för den samhällsviktiga tjänsten. Påverkan på dessa skyddsvärden är viktigt för att kunna avgöra allvarlighetsgraden av störning i en samhällsviktig tjänst. Det kan vara enklare att ha en uppfattning om påverkan på vissa skyddsvärden än andra. Exempelvis kan leverantörer av samhällsviktiga tjänster inom hälso- och sjukvård enklare bedöma om människors hälsa påverkas negativt av störningen, men ha svårare att avgöra påverkan på användarnas ekonomi.

46. Dataintrång hos Vastaamo ledde till internationell skandal.

47. Statliga myndigheter ska rapportera it-incidenter som inträffar i myndighetens informationssystem eller i tjänster som myndigheten tillhandahåller åt en annan organisation. Läs mer om it-incidentrapportering för statliga myndigheter på MSB:s hemsida, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/it-incidentrapportering-for-statliga-myndigheter/.

48. Både leverantörer av samhällsviktiga och digitala tjänster ska rapportera incidenter till MSB. Läs mer om incidentrapportering för NIS-leverantörer på MSB:s hemsida, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/incidentrapportering-for-nis-leverantorer/.

49. Agrafiotis, Ioannis; Nurse, Jason R C; Goldsmith, Michael; Creese, Sadie; Upton, David. *A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate*. 2018. https://doi.org/10.1093/cybsec/tyy006 (hämtad 09/2023).

50. ENISA. *ENISA Threat Landscape 2022*. 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (hämtad 06/2023).

Angreppets psykologiska dimension

En sak som skiljer cyberangrepp från it-incidenter som har orsakats av andra faktorer, såsom exempelvis misstag eller systemfel, är hur olika aktörer reagerar på incidenten. En reaktion är inte en konsekvens per se och sker inte nödvändigtvis automatiskt.

Ett cyberangrepp kan sägas ha tre kategorier av aktörer vars reaktioner är viktiga. Dessa aktörer är *angriparen*, *målet* och *tredje part* (exempelvis en organisation som använder en tjänst som tillhandahålls av målet). I allmänhet blir tredje part mer orolig och benägen att agera på ibland mindre genomtänkta sätt när det konstateras att en it-incident har orsakats av ett cyberangrepp. En anledning till reaktionen är att information om incidenten och hur den påverkar eller kommer att påverka tredje part ofta är bristfällig. Detta i sin tur leder till att organisationer inte vet hur de ska agera eller vilka säkerhetsåtgärder som skulle behöva vidtas om exempelvis känslig information om kunder eller informationssystem har röjts.

En inträffad it-incident som orsakats av ett angrepp betyder att angreppsförsöket åtminstone har lett till en påverkan eller haft effekt (se tabell 1), och i värsta fall till att angreppet har lyckats. Detta skulle kunna innebära att angriparen försöker göra ett angrepp igen, antingen mot samma mål, eller mot någon annan. Det kan även innebära att angriparen genom målet, har lyckats angripa även andra och att de inte har upptäckt det. Oro hos tredje part, som grundar sig på otillräcklig information om vad som har hänt eller misstro mot den som förmedlar informationen eller informationen i sig, skapar osäkerhet kring angreppets påverkan. Rykten och felaktiga spekulationer kan då uppstå som leder till ickeönskvärda reaktioner.

När det gäller målet kan reaktionen bli mer uppjagad och oroad om det handlar om ett cyberangrepp, samtidigt som det då finns möjlighet att beskylla en annan part för it-incidenten. Om det istället handlar om en it-incident som målet av misstag själv har orsakat, blir det svårare att rikta skulden åt annat håll.

Se nedan exempel på den psykologiska påverkan ett cyberangrepp kan få både för patienter och organisationen när känslig och konfidentiell information har hamnat i felaktiga händer och kunnat användas för utpressning.

Dataintrång hos Vastaamo ledde till internationell skandal

- **Typ:** Dataintrång.
- **Faktisk incident:** Nytta orsakas, skada orsakas.

Den 21 oktober 2020 meddelade det finska psykoterapicentret Vastaamo att de blivit utsatta för dataintrång och utpressning.[51] Omkring 36 000 patienters konfidentiella information hade stulits.[52] Informationen som stals från vuxna och ungdomar utgjorde personligt och känsligt material såsom journaler, terapianteckningar, diagnoser och klientuppgifter.[53] Ett flertal av filerna publicerades på ”dark web”[54]. Många av patienterna mottog också utpressningsmejl där de blev ombedda att betala 200 euro för att förhindra att deras uppgifter skulle offentliggöras.[55]

I efterhand har det framkommit att Vastaamo blivit angripet två gånger, såväl 2018 som 2019. Vastaamos VD, Ville Tapio, ska även ha varit medveten om säkerhetsbristerna som funnits i informationssystemen vilket resulterade i att styrelsen begärde dennes avgång.[53] Fallet ses som exceptionellt och juridiskt sett komplicerat – framförallt på grund av den stora mängden offer. Även från offrens synvinkel har fallet varit komplicerat med osäkerheter kring vad som händer och vad de ska göra för att få sina rättigheter hörda.[56]

Vastaamo gick i konkurs 2021, endast månader efter att dataintrånget hade offentliggjorts.[57] Totalt har mer än 25 000 patienters anmälningar om utpressning rapporterats in till den finska polisen, vilket gör fallet till det största kriminalfallet i finsk historia. Dess omfattning, men också hänsynslöshet i form av utpressningsförsök riktade mot privatpersoner och minderåriga, har gjort händelsen till en internationell skandal.[55]

Samhällspåverkan

Många informationssystem utgör idag mer än ett stöd för organisationer, de är en direkt förutsättning för verksamhetens funktionalitet. Utvecklingen innebär såväl stora möjligheter som risker. Riskerna för informationssystem som upprätthåller samhällsviktig verksamhet och annan kritisk infrastruktur ökar på grund av den utbredda användningen av system som exempelvis styr och övervakar industriella

51. Svenska Yle. *Dataintrånget mot Vastaamo: Det här har hänt och det här vet vi nu*. 2022-10-28. https://svenska.yle.fi/a/7-1496439 (hämtad 07/2023).

52. Helsinki Times. *The Cyber attack that rocked the nation*. 2020-12-22. https://www.helsinkitimes.fi/columns/columns/331-david-kirp/18450-the-cyber-attack-that-rocked-the-nation.html (hämtad 07/2023).

53. Yle. *Vastaamo board fires CEO says he kept data breach secret for year and a half*. 2020-10-26. https://yle.fi/a/3-11614603 (hämtad 07/2023).

54. Dark web syftar på de delar av internet som inte är avsedda eller synliga för allmänheten. De används bland annat för olagliga affärer och annan kriminell verksamhet, men allt är nödvändigtvis inte olagligt på dark web.

55. The Guardian. *'Shocking' hack of psychotherapy records in Finland affects thousands*. 2020-10-26. https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland (hämtad 07/2023).

56. Yle. *Åklagaren har väckt åtal i Vastaamofallet. Aleksanteri Kivimäki åtalas för bland annat grovt dataintrång och försök till grov utpressning. Åklagaren vill se ett sju år långt fängelsestraff*, https://svenska.yle.fi/a/7-10043734 (Hämtad 11/2023).

57. *Helsinki Times. Young Finnish man detained in absentia over data breach at Vastaamo*. 2022-10-31. https://www.helsinkitimes.fi/finland/finland-news/domestic/22438-young-finnish-man-detained-in-absentia-over-data-breach-at-vastaamo.html (hämtad 07/2023).

processer. Många av dagens informationssystem har dessutom beroenden som sträcker sig både inom och mellan organisationer. I och med digitaliseringen och de komplexa beroendekedjor som växt fram har it-incidenter som påverkar flera organisationer blivit vanligare. Samhället har därmed en ny sorts sårbarhet.

En incident hos en organisation som ingår i en digital leveranskedja kan få betydligt större samhällspåverkan än en incident hos en organisation som inte fyller en viktig roll för andra. Därför är sårbarheter hos organisationer och informationssystem som ingår i digitala leveranskedjor attraktiva för en angripare. En angripare kan exempelvis skriva programvara som skannar internet efter sårbar mjukvara hos olika organisationer och som därefter interagerar med mjukvaran på ett sätt som möjliggör ett intrång, spridning av skadlig kod eller annan antagonistisk verksamhet. När många organisationer både använder samma internetanslutna mjukvara, och saknar skydd som kan blockera angrepp via den mjukvaran, kan många organisationer drabbas samtidigt. Det kan i sin tur leda till stor samhällspåverkan. Se nedan exempel på hur ett cyberangrepp kan ge samhällspåverkan.

Utpressningsangrepp slog ut hundratals mil av oljeledningar i USA

- **Typ:** Utpressningsangrepp.
- **Faktisk incident:** Nytta förhindras.

Den 7 maj 2021 upptäckte Colonial Pipeline, som står för nästan hälften av bränsletillförseln i östra USA, intrång i sin administrativa it-miljö som visade sig vara ett utpressningsangrepp.[58] Colonial pipeline valde att stänga ned hundratals mil av sina oljeledningar. Oljeledningarnas funktion bygger på digitala lösningar, exempelvis i form av pumpar och sensorer som övervakar och styr flödena, vilka alla är anslutna till ett centralt system som är känsligt för cyberangrepp.[59] Utöver att låsa datorer och servrar i den administrativa it-miljön, stal angriparna också en stor mängd känslig data som de hotade med att läcka om en lösensumma inte betalades.[60] Angreppet har kallats det största cyberangrepp som någonsin drabbat den amerikanska energisektorn.[61]

De avstängda oljeledningarna orsakade stora problem i sydöstra USA där bränslet tog slut helt på vissa platser. Bensinpriserna rusade och många bunkrade också bensin.[58] Till följd av bränslebristen utlystes nödläge i sammanlagt 17 delstater, en åtgärd som bland annat syftade till att öka de alternativa transportvägarna för olja och gas.[62] De avstängda oljeledningarna försörjde också flera flygplatser med bränsle, vilket tvingade flera flygbolag att ändra och i

58. Cohen, Zachary; Sands, Geneva; Egan, Matt. *What we know about the pipeline ransomware attack: How it happened, who is responsible and more*. CNN. 2021-05-10. https://edition.cnn.com/2021/05/10/politics/colonial-ransomware-attack-explainer/index.html (hämtad 9/2023).

59. BBC. *Colonial Pipeline: US fuel firm resumes service after cyber-attack*. 2021-05-12. https://www.bbc.com/news/business-57090428 (hämtad 9/2023).

60. Robertson, Jordan; Turton, William. *Colonial Hackers Stole Data Thursday Ahead of Shutdown.* Bloomberg. 2021-05-09. https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown (hämtad 9/2023).

61. Höök, Peter. *Amerikanska Colonial Pipeline stänger oljeledningar efter ransomattack*. Infrastrukturnyheter.se. 2021-05-12. https://www.infrastrukturnyheter.se/20210512/24691/amerikanska-colonial-pipeline-stanger-oljeledningar-efter-ransomattack (hämtad 9/2023).

62. Collier, Kevin. *Colonial pipeline hack claimed by Russian group DarkSide spurs emergency order from White House*. NBC News. 2022-05-10. https://www.nbcnews.com/tech/security/colonial-pipeline-hack-claimed-russian-group-darkside-spurs-emergency-rcna878 (hämtad 9/2023).

vissa fall att ställa in planerade flygrutter.[63] Cyberangreppet uppskattas ha kostat Colonial Pipeline 4,4 miljoner dollar. Med hänvisning till den stora påverkan på det amerikanska samhället valde bolaget, redan samma dag som angreppet inträffade, att betala ut lösensumman till angriparna.[64] Det var dock först efter sex dagar som de avstängda oljeledningarna åter kunde tas i bruk.[65]

Notera: Betalning till angriparna är ett sätt att finansiera (och därmed motivera fortsatt) grovt kriminell verksamhet och MSB avråder starkt från att göra det.[66]

Vissa typer av samhällsviktiga tjänster tillhandahålls av ett flertal organisationer, ofta i konkurrens med varandra. Det innebär att om det blir ett avbrott hos exempelvis en bank kan betalningar skötas med stöd av andra banker. Det finns alltså redundans i samhället när det är möjligt för fler än en organisation att tillhandahålla samma slags tjänst. För att betalningar ska omöjliggöras krävs alltså att ett antal organisationer blir oförmögna att tillhandahålla sina tjänster samtidigt. Det är framförallt i sådana lägen som det kan sägas att ett cyberangrepp får allvarliga samhällskonsekvenser.

Följande tre risker i digitala leveranskedjor som kan leda till allvarliga samhällskonsekvenser har identifierats:

1. När sådant som inte ska levereras i en digital leveranskedja ändå levereras till många organisationer samtidigt varpå hot eller hinder uppstår hos dem,
2. När sådant som ska levereras i en digital leveranskedja inte levereras till många organisationer samtidigt varpå brister uppstår hos dem,
3. När många organisationer har samma eller liknande internetexponerade och sårbara mekanismer.

63. Josephs, Leslie. *Pipeline outage forces American Airlines to add stops to some long-haul flights, Southwest flies in fuel*. CNBC. 2021-05-10. https://www.cnbc.com/2021/05/10/colonial-pipeline-shutdown-forces-airlines-to-consider-other-ways-to-get-fuel.html (hämtad 9/2023).

64. BBC. Colonial Pipeline boss confirms $4.4m ransom payment. 2021-05-19. https://www.bbc.com/news/business-57178503 (hämtad 9/2023).

65. Lyons, Kim. *Colonial Pipeline says operations back to normal following ransomware attack*. The Verge. 2021-05-15. https://www.theverge.com/2021/5/15/22437730/colonial-pipeline-normal-ransomware-attack-fuel (hämtad 9/2023).

66. MSB. *Metoder som används vid cyberangrepp, Ransomware, Betalning till angriparna*, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/cyberhot/metoder-som-anvands-vid-cyberangrepp/ (hämtad 9/2023).

Exempel på en it-incident i en leveranskedja till följd av ett cyberangrepp kan vara att skadlig kod tar sig in i leverantörens eller andra organisationers informationssystem. Särskilt allvarliga konsekvenser kan uppstå vid så kallade monoberoenden, det vill säga när organisationer är beroende av en tjänst och det saknas alternativa tjänster om tjänsten upphör. Se nedan exempel på konsekvenser av en it-incident hos en leverantör av trygghetslarm när deras tjänst slutade fungera och annan tjänst saknades för avnämarna.

Angrepp mot NIS-leverantör orsakade störningar hos trygghetslarm som användes av 100 000 personer

- **Typ:** Driftstörning pga. intrång
- **Faktisk incident:** Nytta förhindras.

Strax efter midnatt den 23 mars 2023 uppstod störningar i trygghetslarm som användes av hemtjänster i kommuner i hela Sverige.[67] Störningarna innebar att vårdpersonal inte mottog någon signal vid inkommande larm från äldre eller sjuka.[68] Samtliga drabbade kommuner använde sig av samma trygghetslarmsleverantör, Careium, som också tillhandahöll den it-miljö i vilken larm vidarebefordrades från vårdtagare till vårdgivare.[69]

På kvällen den 23 mars konstaterade Careium att avbrottet i trygghetslarmen orsakats av ett angrepp.[70] Störningarna varade i över ett halvt dygn och drabbade 100 000 personer, i sammanlagt 150 kommuner.[71] Avsaknad av tjänster som kunde ersätta trygghetslarmens funktion förvärrade angreppets påverkan, med konsekvenser för människors liv och hälsa. Under den tid då trygghetslarmen var otillgängliga fick flera hemtjänster gå upp i stabsläge för att säkerställa att vårdtagare var oskadda. Verksamheterna tvingades kalla in extra personal och arbeta enligt strikta prioriteringslistor.[72]

Careiums utredning av händelsen visade att det inte kan uteslutas att en obehörig fått tillgång till personuppgifter i samband med angreppet. Företagets slutbedömning är att det under sådana omständigheter rör sig om åtkomst till en ”mycket begränsad mängd information”.[73]

67. Hannes, Forssell. SVT. *Trygghetslarmen fungerar igen efter cyberattack*. https://www.svt.se/nyheter/lokalt/dalarna/trygghetslarm-i-falun-ur-funktion (hämtad 8/2023).

68. Cision. *Careiums larmsystem i Sverige är återigen i drift*. https://news.cision.com/se/careium/r/careiums-larmsystem-i-sverige-ar-aterigen-i-drift,c3739863 (hämtad 8/2023).

69. Careium. *Careiums larmsystem i Sverige är återigen i drift*. https://www.careium.com/sv-se/tjanster/alla-tjanster/larmmottagning/ (hämtad 8/2023).

70. Cision. *Careiums larmsystem i Sverige är återigen i drift*. https://news.cision.com/se/careium/r/careiums-larmsystem-i-sverige-ar-aterigen-i-drift,c3739863 (hämtad 8/2023).

71. Dagens samhälle. *It-attack slog ut 100 000 trygghetslarm*. https://www.dagenssamhalle.se/samhalle-och-valfard/digitalisering/it-attack-slog-ut-100-000-trygghetslarm/ (hämtad 8/2023).

72. Mjölby kommun. *Nu fungerar trygghetslarmen som vanligt igen*. https://www.mjolby.se/nyheter/nyheter/2023-03-23-uppdatering-nu-fungerar-larmen-igen---detta-efter-en-tillfallig-driftstorning-med-vara-trygghetslarm (hämtad 12/2023).

73. Careium. *Careium bistår fortsatt sina kunder med anledning av personuppgiftsincident enligt GDPR*. https://www.careium.com/sv-se/om-careium/future-of-care/uppdaterad-information-med-anledning-av-personuppgiftsincidenten/ (hämtad 8/2023).

Enligt MSB:s analys av inrapporterade it-incidenter finns indikationer på att organisationer ofta saknar digitala alternativ om exempelvis deras it-tjänsteleverantör skulle drabbas av ett längre avbrott. Sådana indikationer kan exempelvis ses bland NIS-leverantörer både inom hälso- och sjukvård när det gäller trygghetslarm, men också inom dricksvattenförsörjning där övervakningssystemen på anläggningar skickar sensordata över en teleoperatörs nät.

Motståndskraft i samhällsviktiga informationssystem

För att samhällsviktiga informationssystem ska vara motståndskraftiga krävs att de är robusta, resilienta och har redundans.

- **Robusthet** uppnås genom att organisationen bedriver ett systematiskt riskförebyggande och riskhanterande arbete.
- **Resiliens** uppnås genom att organisationen planerar och övar på såväl incidenthantering som kontinuitetshantering. Resiliens kan förstärkas genom samarbete. Att ha tillgång till reservdelar och komponenter är centralt för god resiliens.
- **Redundans** uppnås genom att ha en fungerande marknad där organisationer kan konkurrera och där det finns möjlighet för fler än en organisation att tillhandahålla samma slags tjänst.

Angreppsbilden

Angreppsbilden

MSB får årligen in över 300 it-incidentrapporter från statliga myndigheter och NIS-leverantörer. Ungefär 30–50 av dessa beskriver cyberangreppsförsök. De flesta inrapporterade cyberangrepp har begränsad påverkan och har primärt utförts med hjälp av mindre sofistikerade metoder. It-incidentrapporteringen är en viktig informationskälla i MSB:s arbete med att ta fram behovsbaserat stöd. Incidentdata bidrar såväl till MSB:s nulägesbild som till den långsiktiga strategiska analysen.

Det här kapitlet redogör för angreppsbilden mot statliga myndigheter och leverantörer av samhällsviktiga tjänster utifrån de it-incidenter som orsakats till följd av cyberangreppsförsök. I kapitlet redovisas de it-incidentrapporter som inkommit till MSB från 1 april 2019 till och med den 30 september 2023 och som rapporterat ett cyberangreppsförsök som bakomliggande orsak.[74] Rapporten är avgränsad till nämnd tidsperiod då rapporteringskrav för NIS-leverantörer trädde i kraft under våren 2019.

Mörkertalet

Det finns rapporteringspliktiga aktörer som inte rapporterar in it-incidenter, inklusive cyberangreppsförsök, till MSB. Mörkertalet består av minst två olika fenomen, nämligen att:

- organisationer inte inrapporterar alls,
- organisationer inte inrapporterar allt de ska inrapportera.

Mörkertalet framkommer bland annat genom att:

- vissa rapporteringspliktiga organisationer aldrig har rapporterat in en it-incident till MSB,
- det vid leveranskedjeincidenter inkommer rapporter från vissa, men inte alla, drabbade rapporteringspliktiga organisationer.

74. Det är angreppsbilden som framträder utifrån it-incidentrapporteringen som MSB redogör för. De problemområden som tydligt framkommit av it-incidentrapporteringen har inkluderats, och särskilda problemområden synliggjorts. Att somliga rapporteringspliktiga organisationer inte rapporterar it-incidenter, kombinerat med att många av de mottagna incidentrapporterna saknar utförliga beskrivningar av händelseförloppet är olyckligt. Sammantaget riskerar detta att begränsa förståelsen för det operationella nuläget, såväl som trender över tid, och därför medföra att vissa problem eller behov som borde bemötas och hanteras missas.

Även om ett mörkertal förekommer ser MSB att it-incidentrapporteringen ger en bra överblick av angreppsbilden mot statliga myndigheter och, delvis, NIS-leverantörer sett till fördelningen av rapporterade orsaker och konsekvenser. MSB bedömer därmed att underlaget är fullgott för extrapolering. En bekymrande aspekt är om it-incidentrapporteringen är representativ för hela populationen eftersom vissa NIS-sektorer rapporterar in få it-incidenter. MSB tar hänsyn till detta inom ramen för de analyser som är baserade på it-incidentrapporteringen.

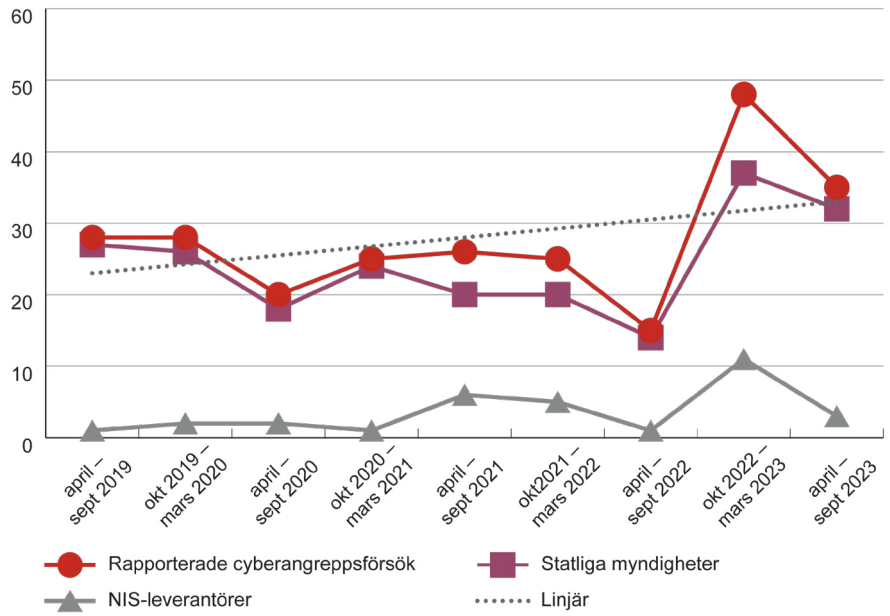
Mellan april 2019 till september 2023 har MSB mottagit totalt 1 542 it-incidentrapporter. Av det totala antalet inkomna rapporter anges cyberangreppsförsök som orsaken i 250 fall. Detta motsvarar 16 procent av det totala antalet inkomma rapporter. Därtill tillkommer 41 rapporter som beskriver antagonistiska handlingar, men som inte uppfyller villkoren för att klassas som ett cyberangrepp.[75]

Av de 250 cyberangreppsförsök som rapporterats till MSB från april 2019 till september 2023 har 87 procent inkommit från statliga myndigheter och 13 procent från NIS-leverantörer. Den noterbart stora differensen beror delvis på att kriterierna för NIS-leverantörers it-incidentrapporteringsplikt är högre än för statliga myndigheter.[76] Detta begränsar förvisso jämförelser om angreppsbilden något, men det är samtidigt så att de cyberangreppsförsök som förorsakar större påverkan är rapporteringspliktiga för alla och därmed jämförbara. Som redogörs för mer detaljerat längre ner så är det 53 procent av rapporterade cyberangreppsförsök som bedöms ha resulterat i någon form av organisationspåverkan.

75. I kapitlet Om antagonistisk cyberaktivitet i denna rapport så definieras fyra villkor som interaktionen mellan angriparen och målet måste uppfylla för att klassificeras som ett cyberangrepp. I enlighet med dessa har 41 incidentrapporter som beskriver antagonistisk aktivitet inte bedömts falla under definitionen. De flesta av dem utgör bedrägerier som utförts via mejl, men det finns även fall av fysiskt sabotage av it-komponenter.

76. När NIS 2 träder i kraft kommer samma krav ställas på alla rapporteringspliktiga organisationer.

Figur 1. Antal cyberangreppsförsök och utveckling från april 2019 till september 2023



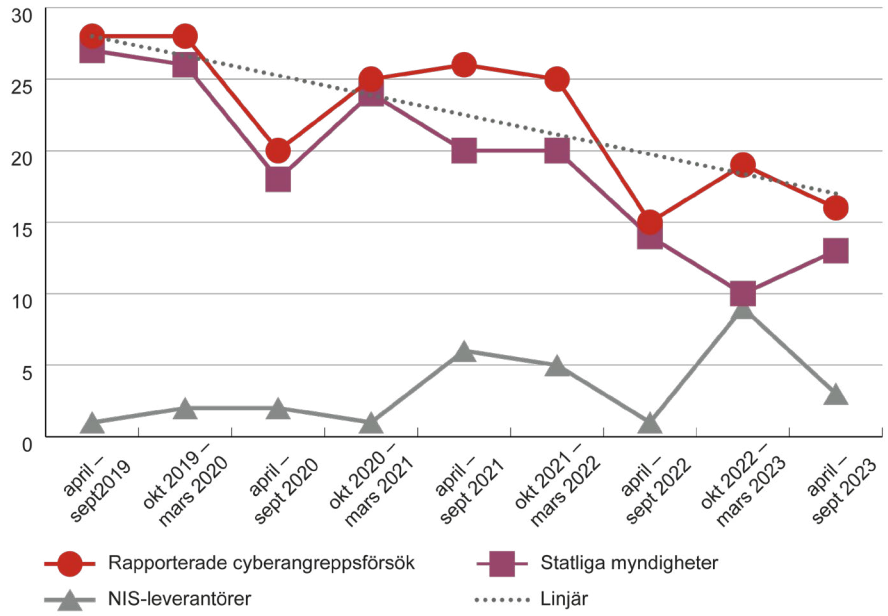
Linjediagram som redogör för det totala antalet cyberangreppsförsök som rapporterats av statliga myndigheter och NIS-leverantörer från 1 april 2019 till 30 september 2023. Diagrammet inkluderar en trendlinje som redogör för utvecklingen över tid.

Frekvensen av inrapporterade cyberangreppsförsök från både myndigheter och NIS-leverantörer mellan april 2019 och september 2023 har varit relativt stabil. *Figur 1* visar att det under de flesta halvårsperioder rapporterats 20 till 30 cyberangrepps-försök. Frekvensen har dock fluktuerat mer sedan 2021. Det lägsta antalet cyber-angreppsförsök, 15 fall, rapporterades under perioden april till och med september 2022. Det högsta antalet, 48 fall, rapporterades från oktober 2022 till mars 2023.

Det inkom ett relativt stort antal rapporter om cyberangreppsförsök under inled-ningen av 2023. Angreppen förannonserades på sociala medier som motreak-tioner på de ”koranbränningar” som i omgångar genomfördes under perioden. Överbelastningsangreppen bör därmed inte nödvändigtvis ses som representativa för en långsiktig trend av ökat antal cyberangreppsförsök mot statliga myndigheter och NIS-leverantörer. Däremot får det ses som sannolikt att liknande episoder med hög aktivitet kommer uppstå även i framtiden.

Det går vidare att se att det under perioden oktober 2022 till och med mars 2023 rapporterades in fler cyberangreppsförsök från såväl statliga myndigheter som NIS-leverantörer. Särskilt överbelastningsangreppen fick mycket uppmärksamhet i media och MSB har noterat att fler incidenter, såväl gällande ”lyckade” som ”misslyckade” överbelastningsangrepp, rapporterades in när frågan belystes och aktualiserades på samhällsnivå.

Figur 2. Utvecklingen mellan april 2019 till september 2023 exkluderande externt triggade cyberangreppsförsök



Linjediagram som redogör för antalet cyberangreppsförsök som rapporterats in av statliga myndigheter och NIS-leverantörer undantaget angreppsförsök som bedömts vara kopplade till ett externt ”trigger-fenomen”. Med extern trigger åsyftas en specifik händelse eller fenomen i den fysiska världen där något har hänt som i sin tur kan påvisas ha fungerat som en motivator för att agera antagonistiskt mot Sverige eller svenska intressen. För att en händelse ska räknas som en trigger ska en tydlig ökning i antalet inrapporterade incidenter som har orsakats av angrepp kunna observeras i statistiken, och det ska också finnas oberoende evidens som indikerar att ökningen kan kopplas till triggerfenomenet.

MSB har analyserat alla de inkomna incidentrapporter som beskriver cyberangreppsförsök under tidsperioden och kan endast identifiera ett fenomen, de s.k. ”koranbränningarna”, som motsvarar ovan villkor. I figuren har överbelastningsangrepp från perioden 21 januari till 4 maj 2023 exkluderats. Under den nyss angivna tidsperioden rapporterades det in fyra gånger så många överbelastnings-angrepp som för hela 2022, det vill säga långt över normalbilden.

Figur 2 redogör för alla de inrapporterade cyberangreppsförsöken under perioden, undantaget de överbelastningsangrepp som har kunnat kopplas till motreaktioner på ”koranbränningarna”. Det som kvarstår är en representation av den normal-bild som incidentrapporteringen ger.

I jämförelse mellan *Figur 1* och *2* ges en annorlunda bild av frekvensen av inrap-porterade cyberangreppsförsök. Normalbilden i *Figur 2* visar på ett minskat antal inrapporterade cyberangreppsförsök sett över hela mätperioden. Det kan till del förklaras av att antalet inrapporterade it-incidenter totalt sett minskat under samma period. NIS-leverantörerna har förvisso rapporterat in fler cyberangrepps-försök, men statliga myndigheter som också står för majoriteten av de inrappor-terade incidenterna har bidragit med ett successivt minskande antal rapporter om cyberangreppsförsök under mätperioden. Att statliga myndigheter rapporterar in färre cyberangreppsförsök kan bero på en kombination av (i) generellt avta-gande rapporteringsvilja, (ii) minskad benägenhet att rapportera in ”misslyckade” angreppsförsök (särskilt gällande nätfiske), (iii) bättre skydd som föranlett färre it-incidenter och (iv) att angripare över tid alltmer betraktat statliga myndigheter som lågprioriterade mål.

Typer av cyberangreppsförsök

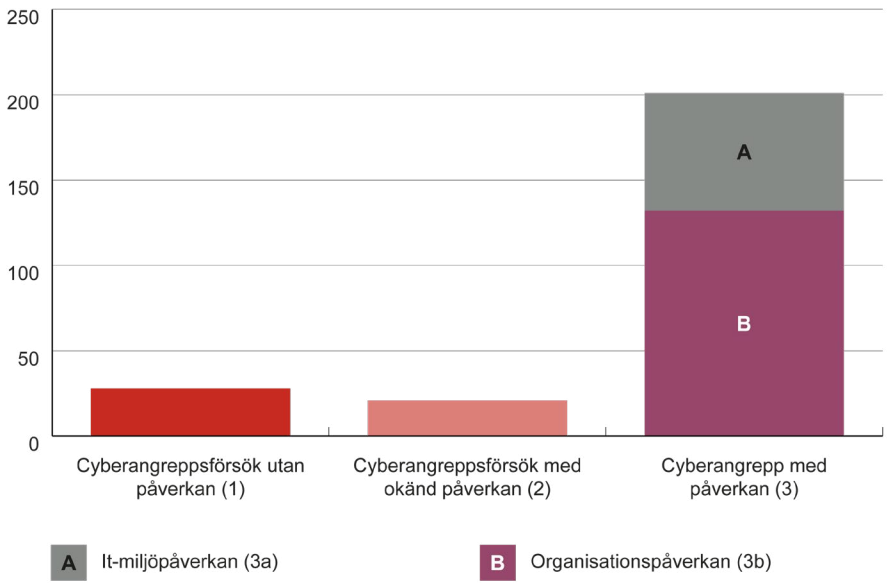
Cyberangreppsförsöken som rapporterats från rapporteringspliktiga organisationer har varierat både gällande utförandemetod och verkansgrad. Vissa utgör fullföljda cyberangrepp som har haft stor påverkan på organisationens it-miljö, och i sin tur organisationen i stort, medan andra, misslyckade försök, inte har haft någon påverkan alls. Cyberangreppsförsöken som analyserats inom ramen för denna rapport kan delas in i tre övergripande kategorier:

1. Cyberangreppsförsök *utan påverkan*
   Cyberangreppsförsök utan påverkan inkluderar de cyberangreppsförsök som inte resulterat i någon påverkan på den angripna it-miljön eller information som lagras eller behandlas däri. Att cyberangreppsförsöket inte påverkat it-miljön eller information däri innebär att det inte påverkat konfidentialiteten, riktigheten eller tillgängligheten inom it-miljön. Totalt faller cirka elva procent, sammanlagt 28 fall, av de 250 rapporterade cyberangreppsförsöken under denna kategori.
2. Cyberangreppsförsök *med okänd påverkan*
   Cyberangreppsförsök med okänd påverkan inkluderar de rapporterade cyberangreppsförsök där det inte gått att avläsa, baserat på den inskickade it-incidentrapporten, huruvida det har haft någon påverkan på it-miljön eller information som lagras eller behandlas däri. Totalt faller cirka åtta procent, sammanlagt 21 fall, av de 250 rapporterade cyberangreppsförsöken under denna kategori.
3. Cyberangrepp *med påverkan*
   Cyberangrepp med påverkan inkluderar de cyberangreppsförsök som påverkat den angripna it-miljön, eller information som lagras och eller behandlas däri, och därav kan beskrivas som ett fullföljt cyberangrepp. Att cyberangreppet påverkat it-miljön eller information däri innebär att it-miljöns eller informationens konfidentialitet, riktighet eller tillgänglighet har påverkats. Dessa incidenter utgör 80 procent, sammanlagt 201 fall, av de rapporterade cyberangreppsförsöken. Cyberangrepp med påverkan kan vidare delas in i två relaterade underkategorier:
   a. Cyberangrepp med *it-miljöpåverkan*
   b. Cyberangrepp med *organisationspåverkan*

Kategori I inkluderar de 34 procent av fall som *endast* resulterat i it-miljöpåverkan. Med it-miljöpåverkan åsyftas att cyberangreppet har resulterat i oönskade konsekvenser för it-miljön eller information som lagras eller behandlas däri. Kategori II inkluderar de incidenter som av MSB bedöms ha resulterat i it-miljöpåverkan samt ett faktiskt negativt utfall för den drabbade organisationen. Inom denna kategori räknas även tjänster som organisationen levererar och som primärt används av externa användare. Kategori II står för 66 procent av de 201 cyberangrepp som har haft it-miljöpåverkan. Sett till den totala mängden inkomna cyberangreppsförsök har med andra ord 53 procent av fallen resulterat i en störning eller annan händelse som påverkat organisationen på ett oönskvärt sätt.

Figur 3 illustrerar fördelningen av rapporterade cyberangreppsförsök enligt kategoriseringen.

Figur 3. Kategorier av cyberangreppsförsök



Stapeldiagram som redogör för hur många cyberangreppsförsök som (1) inte har någon påverkan, (2) har okänd påverkan, respektive (3) har resulterat i påverkan. Cyberangrepp med påverkan kan delas in i de som *enbart* har resulterat i it-miljöpåverkan respektive de som har resulterat i it-miljöpåverkan *och* organisationspåverkan.

Cyberangreppsförsök utan påverkan

MSB har mottagit 28 it-incidentrapporter där den rapporterande organisationen beskriver en inträffad säkerhetshändelse[77] utan någon påverkan på organisationens it-miljö. En säkerhetshändelse kan bestå av att ett hot uppstår, en framgångsfaktor upphör, ett hinder uppstår eller ett skydd upphör. Säkerhetshändelser som inte resulterat i en incident inom it-miljön utgör oftast misslyckade intrångsförsök där angriparen använt sig av metoder såsom nätfiske eller systematisk prövning av olika inloggningsuppgifter för att få tillgång till användarkonton. Rapportören beskriver ofta att nätfiskemejl skickats till användarkonton, men att ingen interaktion skett, alternativt att det hanterats av etablerade skyddsmekanismer. Att just angreppsförsök mot konton rapporteras in i större utsträckning än andra effektlösa cyberangreppsförsök kan antas bero på att de är enklare att upptäcka. It-incidentrapporter som beskriver nätfiskeförsök utan påverkan var mer vanligt förekommande tidigare under den analyserade mätperioden. Det bedöms bero på att statliga myndigheters benägenhet att rapportera dessa händelser har minskat.

77. En säkerhetshändelse är en inträffad oönskad händelse. Det kan handla om att 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). Det är endast om säkerhetshändelsen har påverkat konfidentialiteten, riktigheten eller tillgängligheten hos it-miljön eller information som behandlas eller lagras däri som säkerhetshändelsen utgör en it-incident.

Cyberangreppsförsök med okänd påverkan

21 inrapporterade fall saknar en tydlig specifikation på om cyberangreppsförsöket har resulterat i påverkan. Liksom i kategorin cyberangreppsförsök utan påverkan beskrivs oftast ett intrångsförsök, varav många består av ett inledande nätfiskeförsök. Till skillnad från it-incidentrapporterna inom föregående kategori beskrivs dock inte utfallet, vilket gör det svårt att avläsa huruvida cyberangreppsförsöket har avvärjts eller ej. Förutom nätfiskeförsök återfinns även andra metoder för dataintrång inom denna kategori. Bland annat förekommer det fall då rapportören beskriver försök till att utnyttja sårbarheter i exempelvis kod.

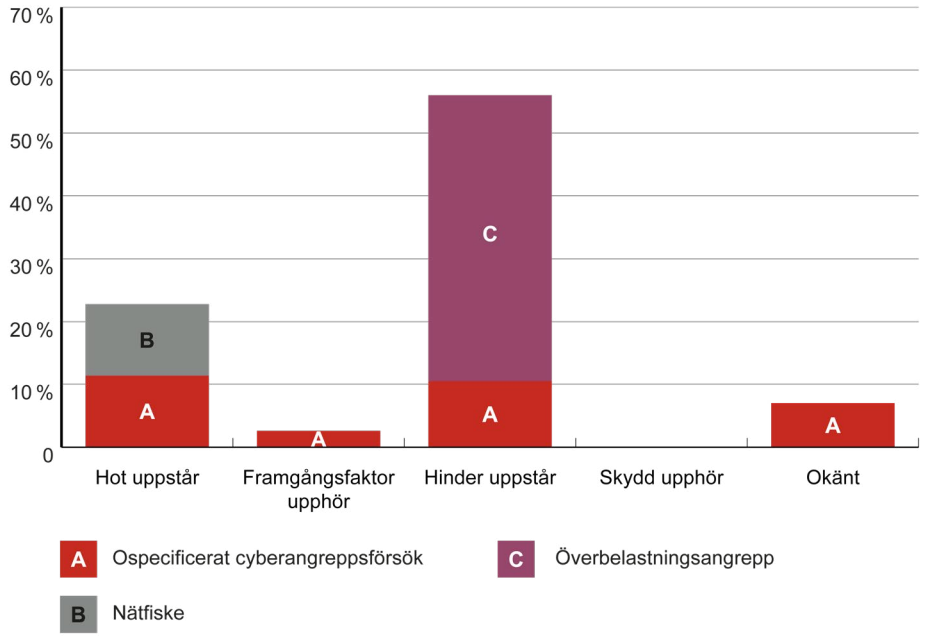
Cyberangrepp med påverkan

Totalt 201 cyberangrepp bedöms ha påverkat konfidentialiteten, riktigheten eller tillgängligheten inom den rapporterande organisationens it-miljö eller information som lagras eller behandlas däri. Av dessa 201 har 132 fall även resulterat i reell organisationspåverkan. Nedan redovisas vilka typer av it-miljöpåverkan respektive organisationspåverkan som beskrivs.

It-miljöpåverkan

Påverkan på it-miljön eller information däri redogörs i den här rapporten som typer av säkerhetshändelser inom it-miljön. I *Figur 4* redogörs för förekomsten av olika typer av säkerhetshändelser som uppstått i samband med cyberangreppet.

Figur 4. Säkerhetshändelser som påverkat it-miljön



Stapeldiagram som redogör för vilka typer av säkerhetshändelser som uppstått i samband med ett cyberangrepp. Diagrammen inkluderar hur stor andel av dessa som beskriver angreppsmetoderna överbelastningsangrepp och nätfiske.

Att angriparen genom cyberangreppet påverkat tillgängligheten inom målets it-miljö eller till information däri är den vanligaste formen av inrapporterad påverkan. Totalt består 129 fall, sammantaget 64 procent, av de cyberangrepp som

påverkat it-miljön eller information däri av att något tillkommit it-miljön i samband med angreppet, vilket bidragit till att ett *hinder uppstått*. Dessa incidenter inkluderar händelser då något tillförts, eller en ändring har gjorts, som har blockerat funktionalitet eller tillgången till information inom ett eller flera informationssystem. De flesta av dessa fall har inte tillkommit som en konsekvens av ett intrång i it-miljön och angreppen har sällan påverkat den interna miljöns funktionalitet. Istället är det den externa åtkomsten till den drabbade organisationens it-miljö eller information däri som har påverkats. Överbelastningsangrepp, då stora mängder datatrafik tillförs och därmed blockerar tillgången till servrar och andra nätverkskomponenter, utgör majoriteten av de cyberangrepp som resulterar i att ett hinder uppstått. Ett annat förekommande, men jämförelsevis ovanligt fall, är när angriparen har installerat skadlig kod. Genom att nyttja exempelvis utpressningsprogram har angriparen då aktivt förhindrat tillgången till informationstillgångar genom att lägga ett lager av kryptering ”ovanpå” dem.

Den näst vanligaste typen av fall är att incidenten har medfört att ett *hot uppstått*, vilket rapporterats vid 26 procent (52 fall) utav de 201 fall då cyberangreppet påverkat it-miljön eller information däri. Denna kategori inkluderar incidenter som framförallt påverkat informationssystemens konfidentialitet, riktighet eller en kombination av båda. Till skillnad från när ett hinder uppstått beror dessa incidenter oftast på ett intrång i it-miljön. Det handlar framförallt om incidenter då exempelvis ett av organisationens användarkonton blir kapade och börjar skicka ut spammeddelanden eller att skadligt innehåll läggs till hemsidor som tillhör eller nyttjas av organisationen. Endast ett fåtal beskriver att skadlig kod som i sig utgör ett hot har installerats. Dessa inkluderar skadlig kod såsom bakdörrar och spionprogram. Flera av fallen då konton blivit kapade har resulterat i att ett hinder uppstått i nästa led, då spamutskick gör att organisationens domän svartlistas. I 19 procent av fallen då ett hot uppstår har organisationen valt att genomföra akuta nedstängningar av drabbade servar och informationssystem som en del av incidenthanteringsprocessen.

Endast 3 procent beskriver förekomsten av en säkerhetshändelse där en *framgångsfaktor upphört*. I ytterligare 6 procent har den inträffade säkerhetshändelsen bedömts vara *okänd* då händelseförloppet inte redogjorts för mer ingående i mottagen it-incidentrapport. Det inkluderar fall då organisationen har redogjort för organisationspåverkan men inte mer ingående beskrivit it-incidentens karaktär. Att en framgångsfaktor upphört innebär att information, inkluderande funktioner, tagits bort eller på annat sätt slutat att fungera. Inom sammanhanget innebär dessa händelser att angripare har tagit bort information eller avaktiverat funktioner som används av användare eller informationssystemen. De flesta fall som bedöms höra till denna kategori beskriver att information på hemsidor manipulerats eller raderats. Att ytterst få it-incidenter platsar inom denna kategori visar på att det är ovanligt att angripare vidtar åtgärder för att radera information. Det är istället betydligt vanligare, med hänsyn till resonemanget ovan, att angripare antingen väljer att blockera tillgången till information alternativt använder den egna upprättade tillgången till information för sina egna syften.

Ingen av rapporterna beskriver antagonistiska handlingar som resulterat i att *skydd upphört* i samband med att angriparen tagit bort eller manipulerat etablerade skyddsmekanismer inom it-miljön. Däremot informerar 14 rapportörer (7 procent) om att ett skydd upphört *innan* cyberangreppsförsöket utfördes i samband med ändringar

som medarbetare eller en leverantör vidtagit. Alltså har sju procent av de cyberangrepp som påverkat it-miljön eller information däri föregåtts av att ändringar utförts. Det har antingen möjliggjort händelseförloppet eller bidragit till att konsekvenserna blivit mer omfattande. Exempel på ändringar som gjorts inkluderar att brandväggar och överbelastningsskydd konfigurerats om eller att känsliga it-komponenter av misstag anslutits till internet i samband med större ändringar.

De it-incidentrapporter i vilka rapportören beskriver att ändringar kan ha medfört att cyberangreppet påverkade it-miljön eller information däri inkluderar ofta mer utförliga beskrivningar av händelseförloppet än genomsnittet. MSB gör bedömningen att misstag vid ändringar i realiteten sannolikt utnyttjas av angripare i en större utsträckning än vad som framgår inom it-incidentrapporteringen. Säker ändringshantering är en viktig komponent inom arbetet med att förebygga och hantera cyberangrepp.

Vem upptäckte cyberangreppsförsöket?

I 58 procent av it-incidentrapporter där frågan har kunnat besvaras uppges att cyberangreppsförsöket först upptäckts av den egna personalen. Därefter har 25 procent upptäckts av eget tekniskt detekteringssystem. Att det är vanligare att it-incidenten upptäcks av medarbetare indikerar att många organisationer inte har förutsättningar att upptäcka angrepp förrän angreppsförsöket kunnat noteras av medarbetare.[78]

Det är endast tre fall som baserat på analysen bedöms ha orsakat mer än en typ av säkerhetshändelse. I dessa fall rör det sig både om att ett hot uppstått såväl som att ett hinder har uppstått inom it-miljön. Detta är ett resultat av installerad skadlig kod exekverats och spridits.

När ett hinder har uppstått som påverkat it-miljön eller information däri brukar den genomsnittliga incidenten pågå i cirka 47 timmar. Standardavvikelsen är dock hög och mediantiden är istället cirka 11 timmar. Under tidsperioden incidenten pågår är tillgången till vissa it-komponenter eller informationstillgångar helt eller delvis blockerad. Den genomsnittliga upptäcktstiden, alltså tiden mellan det att it-incidenten uppstod till att den upptäcktes, har pågått i cirka 3 timmar (mediantid cirka 2 minuter) och den genomsnittliga hanteringstiden, alltså tiden mellan det att hantering påbörjats till det att it-incidenten upphörde, har pågått i 43 timmar (mediantid 9 timmar).[79]

78. Procentsatserna är baserade på de frågor om it-incidentens upptäckt som inkluderas i det nuvarande rapportformuläret för statliga myndigheter (introducerat oktober 2020) och rapportformuläret för NIS-leverantörer. Frågan har besvarats i 154 utav de totalt 168 it-incidentrapporter i vilka rapportören har använt sig av nuvarande rapportformulär (92 procent).

79. Tidsangivelser är baserade på besvarade delfrågor om tid som inkluderas i det nuvarande rapportformuläret för statliga myndigheter (introducerat oktober 2020) och rapportformuläret för NIS-leverantörer. Totalt 168 cyberangreppsförsök har rapporterats med hjälp av dessa formulär. Tidsangivelserna bygger på de incidentrapporter i vilka rapportören har svarat på alla delfrågor om tid i rapportformulären. Detta inkluderar tid för incident, upptäckt, störning, påbörjad hantering, incidentens upphörande och störningens upphörande. Rapporter i vilka svaret varit ofullständigt har exkluderats. Då en hög standardavvikelse förekommer har även it-incidenter som pågått i över 1 000 timmar exkluderats. Tidsangivelse för genomsnitt och median för kategorin hinder uppstår bygger på underlag från totalt 59 av 103 it-incidentrapporter som härrör från kategorin och i vilka rapportören har använt sig av nuvarande rapporteringsformulär (57 procent).

I jämförelse har den genomsnittliga inrapporterade incidenten till följd av ett cyberangrepp som orsakats av att ett hot uppstått inom it-miljön i snitt pågått i över 218 timmar, alltså mer än fem gånger så länge som en it-incident till följd av att ett hinder uppkommit. Det bör noteras att medianen ligger på 169 timmar och att ett fåtal fall drar upp genomsnittet lite. Den genomsnittliga upptäcktstiden har pågått i 131 timmar (mediantid 64 timmar) och genomsnittliga hanteringstiden har pågått i 87 timmar (mediantid 15 timmar).[80]

Den stora tidsskillnaden mellan incidenter då ett hinder respektive ett hot uppstår beror delvis på att det kan ta längre tid att identifiera hotet, exempelvis skadlig kod, om det inte resulterat i någon synlig påverkan. Speciellt om angriparen aktivt försöker undgå upptäckt. I jämförelse är ofta syftet med att blockera tillgången till information för användare och informationssystem att angreppet ska upptäckas. Tidsskillnaden beror sannolikt även på att olika angreppsmetoder används. När ett hot introduceras inom it-miljön krävs det att organisationen hanterar det för att hotet ska upphöra. Medan så generellt också är fallet när ett hinder uppstår så består majoriteten av dem fallen av överbelastningsangrepp vars effekt upphör i samband med angreppet.

Att genomsnittstiden för it-incidenter där ett hot eller ett hinder uppstår överstiger flera dagar är allvarligt. Det kan tyda på bristande beredskap och förmåga att på kort tid hantera situationen. Ju längre hanteringstid desto högre risk att den egna organisationen eller tredje part påverkas av incidenten.

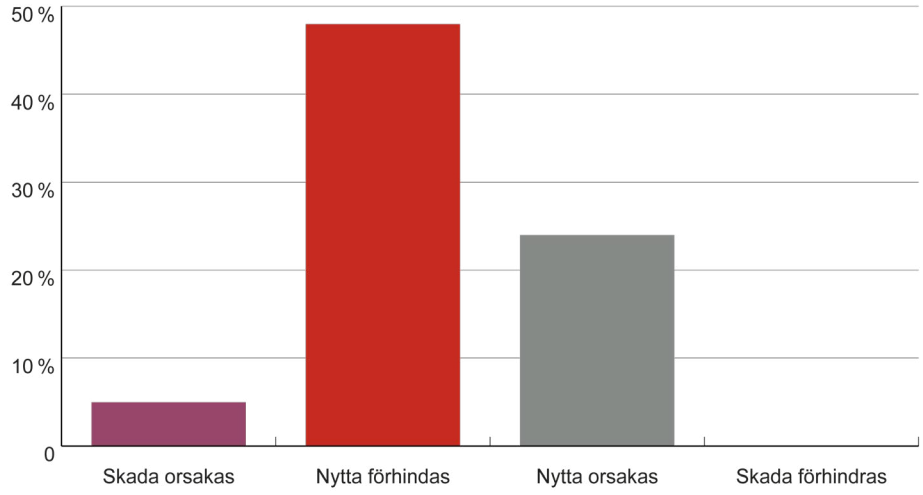
Organisationspåverkan

De säkerhetshändelser som har påverkat den drabbade organisationens it-miljö bedöms i 66 procent av fallen (132 fall) ha resulterat i organisationspåverkan. I de fall it-incidenten har resulterat i organisationspåverkan har förutom en säkerhetshändelse en *faktisk incident* inträffat.[81] En faktisk incident kan bestå i att nytta förhindrats eller att skada orsakats organisationen eller via den drabbade organisationen, alternativt att nytta orsakats eller skada förhindrats för angriparen. I *Figur 5* nedan redovisas andelen av respektive typ av faktisk incident bland rapporterade cyberangrepp med organisationspåverkan.

80. Tidsangivelse för genomsnitt och median för kategorin hot uppstår bygger på underlag från totalt tio stycken av de 26 it-incidentrapporter som härrör från kategorin och i vilka rapportören har använt sig av nuvarande rapporteringsformulär (38 procent). Det höga bortfallet beror bland annat på att många rapportörer inte känner till när hotet introducerades inom it-miljön och därmed ej kan besvara frågan vid den tidpunkt som rapporten skickades till MSB.

81. En händelse där den drabbade organisationen orsakas skada eller förhindras nytta, alternativt där en annan organisation olovligen orsakas nytta eller förhindras skada (se bilaga 1 för en mer djupgående redogörelse).

Figur 5. Faktiska incidenter med organisationspåverkan



Liggande stapeldiagram som beskriver fördelningen av typer av faktiska incidenter. Diagrammet visar att *nytta förhindras* är den vanligaste faktiska incidenten som uppstår till följd av ett cyberangrepp.

Den vanligaste typen av faktisk incident är att organisationen eller tredje part har *förhindrats nytta*. 48 procent av rapporterade cyberangrepp med påverkan har resulterat i att nytta förhindrats (96 fall). Att nytta förhindrats för en organisation är ofta en konsekvens av att det har uppstått ett hinder (en säkerhetshändelse) som påverkat it-miljön eller information däri. I dessa fall har därmed blockerad funktionalitet lett till att organisationen eller andra intressenter inte kunnat utnyttja tjänster i syfte att bedriva verksamhet (det vill säga att producera någon form av nytta). Det vanligaste scenariot är att nytta förhindrats i samband med att organisationens förmåga att kommunicera externt påverkats negativt. Detta inkluderar fall då hemsidor och relaterade e-tjänster såväl som mejl och VPN-lösningar blivit otillgängliga för användare under en längre period. I fall då hindret har påverkat en tjänst eller funktion som är tidskritisk har avbrott som pågått under en mycket kort tid resulterat i att nytta förhindras. I flera av dessa fall har nytta förhindrats andra organisationer eller allmänheten som en konsekvens av störningen.

Den genomsnittliga störningen som inträffat då nytta förhindras varar i cirka 49 timmar. Standardavvikelsen är dock hög och medianfallet motsvarar cirka 19 timmar. Under perioden störningen pågår är den påverkade tjänsten eller informationssystemet periodvis eller konstant helt eller delvis obrukbart. Den genomsnittliga upptäcktstiden har pågått i 6 timmar (mediantid 7 minuter) och genomsnittliga hanteringstiden har pågått i cirka 45 timmar (mediantid 9 timmar).[82] Att nytta ofta förhindras i samband med många cyberangrepp visar på att organisationerna saknar redundans och visar på ett uppenbart behov av att stärka den egna incident- och kontinuitetshanteringen.

Den näst vanligaste kategorin, *nytta orsakas*, beskriver istället hur angreppet direkt resulterat i positivt utfall för angriparen, på bekostnad av målet eller tredje part.

82. Tidsangivelser för genomsnitt och median för kategorin nytta förhindrats bygger på underlag from totalt 41 av de 77 it-incidentrapporter som härrör från kategorin och i vilka rapportören har använt sig av nuvarande rapporteringsformulär (53 procent).

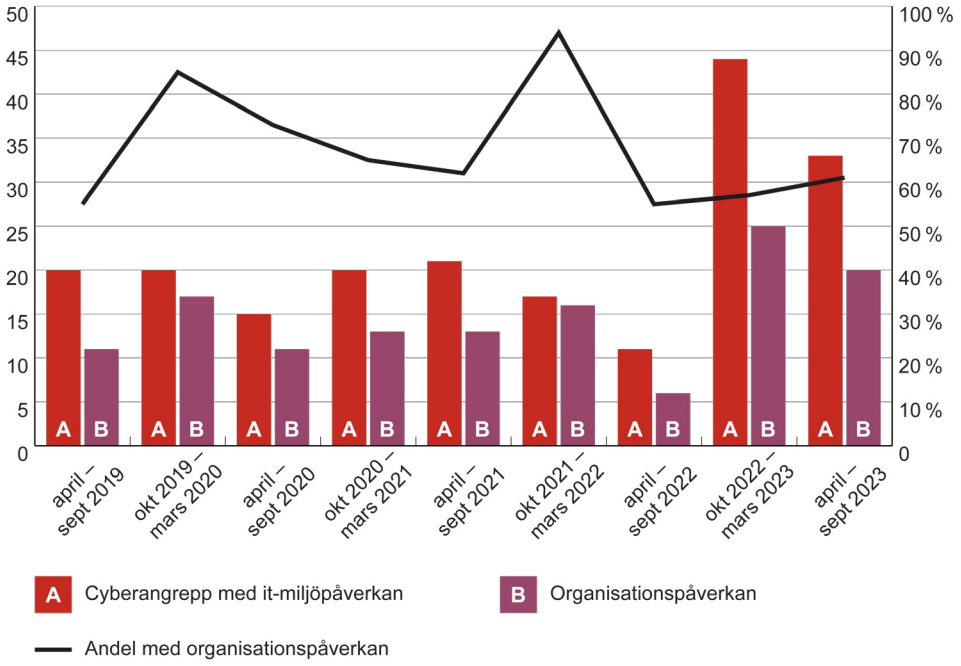
Att incidenten resulterat i att nytta orsakats angriparen har inträffat i 24 procent av de rapporterade cyberangreppen med påverkan (48 fall). Kategorin beskriver framförallt incidenter där en angripare har lyckats extrahera känslig information från organisationen eller lyckats utnyttja organisationens resurser för sina egna syften, exempelvis genom att tillskansa sig och använda sig av kapade användarkonton för att sprida spam eller stjäla pengar. En händelse beskriver exempelvis att angriparen, efter att ha kapat ett användarkonto, ändrat vilket bankkonto som medarbetarens lön ska betalas ut till. Att nytta ofta orsakas i samband med att användaruppgifter och konton kapas av angripare visar på vikten av att organisationer arbetar effektivt med behörighetshantering i syfte att hantera dessa risker.

Att *skada orsakats* målet eller tredje part har inträffat i fem procent av de rapporterade cyberangreppen med påverkan (tio fall). Att skada orsakats innefattar oftast att angreppet har fått (påtagliga) ekonomiska konsekvenser. Rapportörer beskriver att en framgångsfaktor upphört i samband med att angriparen har raderat information och att organisationen inte har kunnat återställa den information som har förlorats. Till skillnad från när nytta förhindras är det ovanligt att skada orsakas för allmänheten eller andra organisationer via målet för angreppet.

I totalt 22 fall bedöms cyberangreppet ha orsakat påverkan som sträcker sig över mer än en kategori. Det vanligaste är då att en angripare orsakat både nytta för sig själv, samt orsakat att nytta förhindrats för organisationen. Det har rapporterats i 86 procent av dessa fall. Det kan exempelvis handla om fall då angripares spamutskick från kapade konton resulterar i att organisationens domän svartlistas eller att trafik till och från organisationen på annat sätt blockeras. Även om syftet med angreppet i första hand inte var att förhindra nytta så blev det ändå en konsekvens av angreppet.

Som redogörs för i *Figur 6* har andelen cyberangrepp som orsakat organisationspåverkan varit relativt stabilt över tid trots att antalet inkomna rapporter har ökat under det senaste året. Ungefär 60 procent av de rapporterade cyberangreppsförsöken bedöms ha resulterat i någon form av organisationspåverkan under perioderna mellan april till september 2022 och april till september 2023.

Figur 6. Cyberangrepp som bedömts orsaka organisationspåverkan under perioden



Stapeldiagram som redogör antalet inrapporterade cyberangrepp med it-miljöpåverkan respektive de it-incidenter som bedöms resulterat i organisationspåverkan. Den procentuella andelen av it-incidenter som resulterat i organisationspåverkan redovisas separat.

Cyberangrepp inom digitala leveranskedjor

I MSB:s rapport *Hoten mot de digitala leveranskedjorna*[83] från 2021 beskriver myndigheten det tilltagande beroendet av komplexa digitala leveranskedjor som ett fenomen som ökar risken för omfattande störningar bland organisationer och samhället i stort. Det är förvisso systemfel och misstag som ligger bakom de flesta rapporterade leveranskedjeincidenterna, men även ett icke-försumbart antal har tillkommit till följd av cyberangrepp.

Digitala leveranskedjor

En digital leveranskedja kan förstås som de tjänster och infrastrukturer som levererar eller möjliggör leverans av digitala produkter vilka används för att upprätta, upprätthålla, utveckla eller återställa en organisations informationshantering och informationssystem.

83. MSB, *Hoten mot de digitala leveranskedjorna – 50 rekommendationer för att stärka samhällssäkerheten* https://www.msb.se/sv/publikationer/hoten-mot-de-digitala-leveranskedjorna--50-rekommendationer-for-att-starka-samhallssakerheten/ (Hämtad 11/2023).

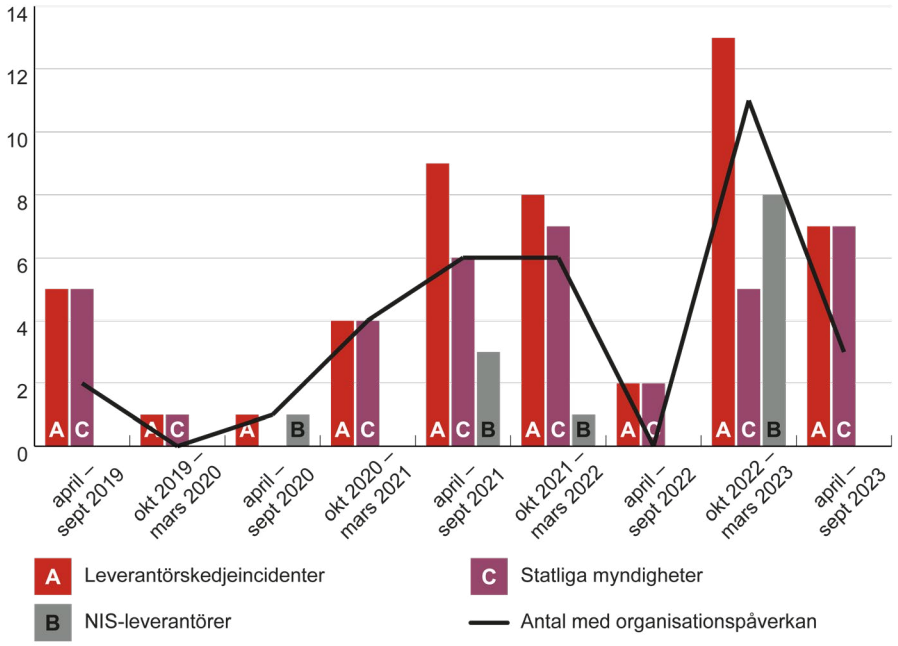
I 50 av de 250 cyberangreppsförsöken som rapporterats till MSB uppges en leverantör åt rapporterande organisation ha blivit angripen. Det kan röra sig om båda leverantörer av specifika tjänster och organisationens it-drift. Det gör att leverantörskedjeincidenter utgör 20 procent av det totala antalet inrapporterade cyberangreppsförsöken. Leveranskedjeincidenter förekommer i mer än 40 procent av rapporterna från NIS-leverantörer. Motsvarande siffra för myndigheter är 17 procent. Skillnaden skulle kunna bero på att NIS-leverantörer i större utsträckning är beroende av underleverantörer, samt att de i större utsträckning använder sig av samma leverantörer. Fördelningen kan dock även vara en konsekvens av att NIS-leverantörer primärt rapporterar in it-incidenter som orsakat större störningar. Skillnaden skulle då kunna bero på att leverantörsincidenter generellt leder till mer omfattande störningar. Ett mindre antal av dessa rapporter refererar till samma bakomliggande leverantör och händelse.

44 av leverantörsincidenterna bedöms ha påverkat rapporterande organisations it-miljö eller information däri och 33 bedöms även ha orsakat organisationspåverkan. Det allra vanligaste är att nytta förhindrats den egna organisationen i samband med att leverantörens tjänster upplever störningar alternativt blir helt otillgänglig. Leverantören beskrivs oftast som utsatt för ett överbelastningsangrepp, men det finns även flera fall då tjänsten blir otillgänglig i samband med ett intrång i leverantörens it-miljö.

De organisationer vars verksamhet är beroende av tjänster från en leverantör som drabbas av ett cyberangrepp riskerar att råka ut för långtgående konsekvenser. I genomsnitt pågår en störning som konsekvens av ett cyberangrepp mot en leverantör i 18 timmar. Medianfallet pågår i cirka 8 timmar och även här är det ett fåtal incidenter som driver upp genomsnittet. Ovan tidsangivelser baseras på ett begränsat urval och därmed är tidsangivelserna relativt osäkra.[84] Att dessa incidenter resulterar i störningar som får organisationspåverkan och kan pågå under en längre tid visar på vikten av att organisationer granskar deras leverantörsrelationer och säkerställer att redundans och alternativa arbetsmetoder finns tillgängliga vid bortfall av viktiga tjänster och annan funktionalitet.

84. Tidsangivelser för genomsnitt och median för kategorin leverantörskedjeincidenter bygger på underlag från totalt 13 av 44 it-incidentrapporter som härrör från kategorin och i vilka rapportören har använt sig av nuvarande rapporteringsformulär (30 procent). Det höga bortfallet bedöms delvis bero på att fler rapportörer inte fått information om it-incidentens omfång från den drabbade leverantören vid den tidpunkt som rapporten skickats till MSB.

Figur 7. Cyberangrepp som orsak till leverantörskedjeincidenter



Stapeldiagram som beskriver hur många leverantörsincidenter som rapporterats av statliga myndigheter respektive NIS-leverantörer mellan april 2019 till september 2023. Antalet leverantörsincidenter med organisationspåverkan per halvår redogörs i en separat linje.

Angreppsmetod: Överbelastningsangrepp

Överbelastningsangrepp är en angreppsmetod som används för att förhindra åtkomst till en tjänst genom att exempelvis belasta tjänsten eller den infrastruktur som tjänsten är beroende av. Sådana angrepp kan utföras på flera olika sätt, men de flesta som inrapporteras till MSB utgör så kallade DDoS-angrepp.[85] DDoS-angrepp utnyttjar exempelvis botnät[86] för att distribuera och samtidigt exponentiellt öka mängden datatrafik som aktivt skickas mot drabbade it-komponenter, vilket blockerar legitim trafiks åtkomst. Överbelastningsangreppen som rapporteras av statliga myndigheter och NIS-leverantörer rapporteras ofta i en relativt stor mängd under en begränsad tid.

Till följd av att antalet överbelastningsangrepp ökat kraftigt sedan inledningen av 2023 så utgör överbelastningsangrepp den vanligast förekommande angreppsmetoden mellan april 2019 och september 2023. Överbelastningsangrepp utförs ofta som en reaktion på handlingar och händelser som angriparen, eller angriparens uppdragsgivare, misstycker till eller ser en chans att utnyttja för egna syften.

85. Ett DDoS-angrepp, eller Distributed denial of service-angrepp, är ett överbelastningsangrepp där angriparen använder sig av flertalet olika, ofta kapade, enheter för att skicka stora mängder datatrafik till en server eller annan it-komponent i syfte att begränsa dennes förmåga att bearbeta legitim inkommande datatrafik. Enheterna som bidrar till angreppet brukar sägas ingå i ett botnät.

86. Ordet botnät består av orden ”robot” och ”nätverk”. Angripare använder särskilda trojanska virus för att bryta säkerheten hos ett flertal användares datorer, ta kontroll över varje dator och organisera alla de smittade datorerna i ett nätverk av ”bot-program” som angriparen kan hantera på distans.

Ett talande exempel är det 50-tal överbelastningsangrepp som rapporterades i koppling till ”koranbränningarna” i Sverige under början av 2023.

Överbelastningsangrepp under 2023

Under inledningen av 2023 ökade antalet överbelastningsangrepp kraftigt. Dessa angrepp förannonserades på sociala medier som en reaktion på en serie koranbränningar, där den första genomfördes 21 januari 2023.

Exempelvis skrev gruppen ”Anonymous Sudan” att Sverige och svenska organisationer skulle drabbas av vedergällning för att dessa inte förhindrat händelserna. Angreppen riktades mot såväl offentlig som privat sektor. Som brukligt vid överbelastningsangrepp fick de flesta mycket begränsad påverkan. Händelserna blev uppmärksammade på grund av anledningen till angreppen och mängden aktörer som blev angripna.[87]

Under hela tidsperioden rapporterades totalt 105 it-incidenter som beskriver överbelastningsangrepp som bakomliggande orsak. Angreppen uppvisar stor variation i fråga om utförandeteknik, volym och tidsomfång. Även om överbelastningsangrepp kan göra viktiga tjänster otillgängliga så pågår störningen oftast under begränsad tid. Även i fall där angreppet pågår under längre tid brukar det inte vara fråga om ett konstant bortfall, utan istället av perioder med längre svarstider varierat med perioder av ett fullkomligt bortfall. När angreppet har resulterat i någon form av störning bedöms den i genomsnitt pågå, till och från, i cirka 43 timmar. Även här bör det dock noteras att medianen ligger på närmare 11 timmar och att ett fåtal fall drar upp genomsnittet.[88] Att störningen består under en längre period tros bero på att fler organisationer begränsar extern tillgång till it-miljön under en period i syfte att avvärja angreppet. Överbelastningsangreppen utgör i vissa fall flera korta och återkommande angrepp, snarare än ett angrepp som aktivt pågår under hela den period som rapporten beskriver.

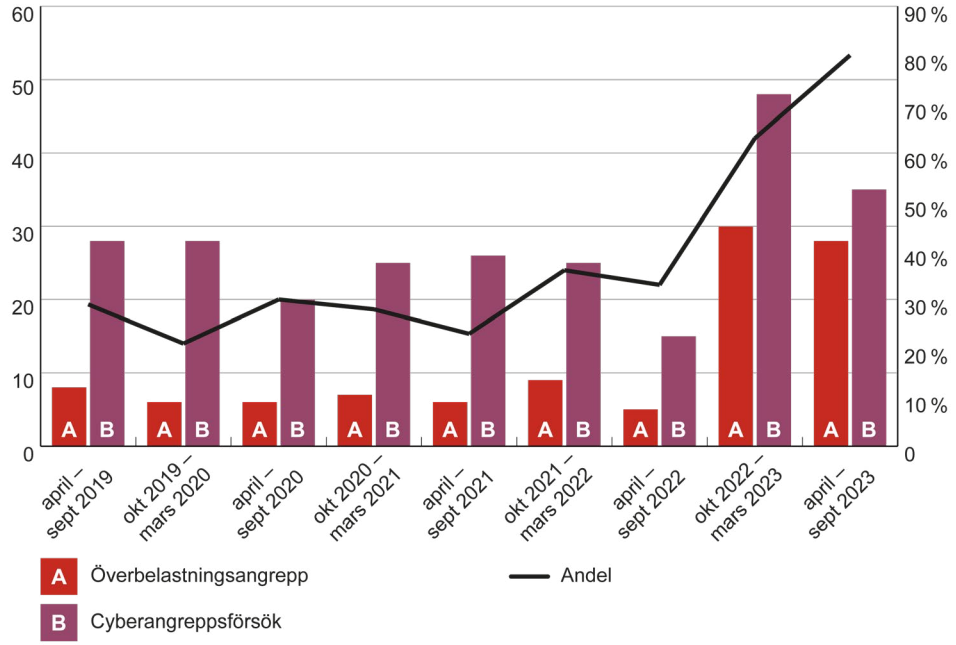
I den här rapporten bedöms 56 procent (59 fall) av alla rapporterade överbelastningsangrepp ha orsakat att nytta förhindras på något sätt. I de flesta fall har webbsidor och tillhörande e-tjänster blivit otillgängliga, alternativt fått långa svarstider under en tidsperiod. I 16 procent av de aktuella incidentrapporterna har den rapporterande organisationen angett en bedömning som betyder att en faktisk incident inte har inträffat, och organisationen har därmed förblivit opåverkad av angreppet. I resterande 27 procent går det inte att bedöma om it-incidenten resulterat i organisationspåverkan. När blockerad funktionalitet inte orsakat någon organisationspåverkan beror det oftast på att organisationen inom kort tid lyckats kompensera för bortfallet. Det kan också handla om att bortfallet inte resulterat i att nytta förhindrats organisationen, eftersom det skedde då användare saknade behov av tjänsten, exempelvis på helger eller under natten.

87. Karin Lindström, *Fortsatta attacker mot svenska mål*, 2023-02-20 https://computersweden.idg.se/2.2683/1.776492/overbelastningsattackerna-fortsatter--expert-pekar-ut-ryska-killnet (Hämtad: 2023-10-28).

88. Tidsangivelser för genomsnitt och median för kategorin överbelastningsangrepp bygger på underlag from totalt 58 av de 88 it-incidentrapporter som härrör från kategorin och i vilka rapportören har använt sig av nuvarande rapporteringsformulär (66 procent).

De flest överbelastningsangrepp går att hantera innan de påverkat målets it-miljö om organisationen har rätt förutsättningar för att göra det. Att en majoritet av överbelastningsangreppen trots allt bedöms resultera i störningar som får organisationspåverkan visar på att många organisationer saknar tillräcklig redundans inom deras nätverksinfrastruktur och tekniska lösningar för att både detektera och avvärja överbelastningsangrepp.

Figur 8. Rapporterade överbelastningsangrepp



Stapeldiagram som redogör för antalet överbelastningsangrepp respektive det totala antalet cyberangreppsförsök som rapporterats in mellan 1 april 2019 till 30 september 2023. Andelen överbelastningsangrepp av det totala antalet rapporterade cyberangreppsförsök under perioden redogörs i linjen.

Angreppsmetod: Nätfiske

Nätfiske är den näst vanligaste förekommande metoden bakom inrapporterade cyberangrepp. Angreppsmetoden är en form av social manipulation där offret luras till att klicka på skadliga länkar eller annan media, alternativt luras till att uppge inloggningsuppgifter. Nätfiske kan handla om både massutskick och riktade angrepp som utformats för att lura en viss målgrupp. Under perioden april 2019 till september 2023 har totalt 45 fall av nätfiske rapporterats.[89]

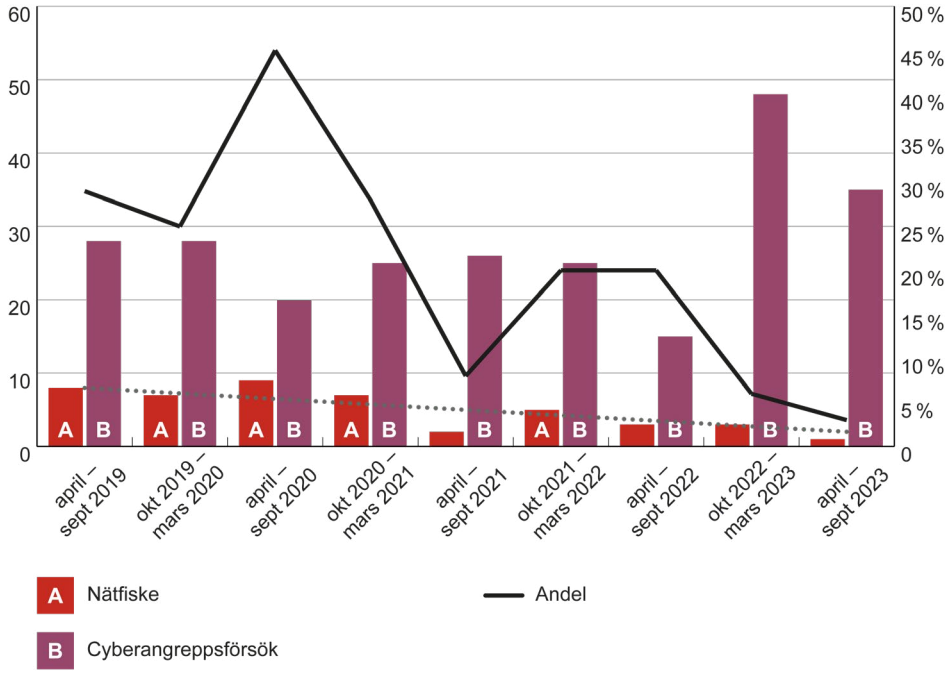
Nätfiskeförsök som rapporterats till MSB har ofta antingen relativt begränsade konsekvenser för it-miljön eller så har de helt misslyckats. Det är endast 44 procent av rapporterade fall som i denna analys bedömts orsaka någon form av organisationspåverkan. Konsekvensen av dessa cyberangrepp är oftast att en angripare får

89. Nätfiske är även en vanligt förekommande komponent i många av de angrepp som exkluderats från datamängden i denna rapport på grund av att de inte uppfyller praktikvillkoret som redogörs i första kapitlet i denna rapport. Det inkluderar bland annat mejlbedrägerier där man genom att spoofa mejladresser exempelvis försöker lura användare att betala ut en summa pengar.

tillgång till användarkonton och information av varierande känslighetsgrad. I ett begränsat antal fall har dock angreppen lett till tillgänglighetsstörningar i samband med att skadlig kod har installerats och spridits inom organisationens it-miljö. Som tidigare nämnts finns det även fall där spamutskick från kapade användarkonton orsakat att kommunikation från den rapporterande organisationen har blockerats.

Frekvensen av rapporterade fall av nätfiske har minskat över tid. Den negativa trenden kan bero på ökad kunskap och tilltagande försiktighet bland medarbetare, men också på att etablerade skyddsmekanismer har blivit bättre på att filtrera bort och isolera skadligt innehåll. En annan förklaring skulle kunna vara en minskande benägenhet av statliga myndigheter, som står för majoriteten av rapporterade nätfiskeförsök, att rapportera in dessa händelser.

Figur 9. Rapporterade nätfiskeförsök



Stapeldiagram som redogör för förekomsten av nätfiske respektive det totala antelet rapporterade cyberangreppsförsök mellan 1 april 2019 till 30 september 2023. Andelen nätfiskeförsök av det totala antalet rapporterade cyberangreppsförsök under perioden redogörs i en linje.

Även om nätfiskeförsök är överrepresenterade bland angreppsförsök som misslyckas så visar faktumet att det förblir den näst vanligaste observerade angreppsmetoden på vikten av att organisationer vidtar åtgärder både för att förebygga och hantera konsekvenserna av användares interaktioner med nätfiskemeddelanden. Det inkluderar både att arbeta för att öka medarbetares kunskaper om dessa metoder samt att utveckla incidenthanteringsprocesser som syftar till att begränsa konsekvenserna vid ett lyckat nätfiskeförsök.

Utmaningar i säkerhetsarbetet

Utmaningar i säkerhetsarbetet

Ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete med planering, införande, uppföljning och övning av förebyggande säkerhetsåtgärder är viktigt för att skydda sig mot cyberangreppsförsök. Dessa säkerhetsåtgärder bidrar till att både öka skyddet mot it-incidenter till följd av cyberangrepp och att minimera skador om angreppet trots allt inträffar. I det här kapitlet redogörs för några av de identifierade problemområden där organisationer har utmaningar i sitt dagliga säkerhetsarbete.

För att vara lyckosam i säkerhetsarbetet krävs arbetssätt för att fortlöpande identifiera organisationens skydds- och förbättringsbehov. Utmaningarna är många och ofta går säkerhetsarbetet långsamt. För de organisationer där arbetet går trögt är det särskilt viktigt att stanna upp och se över vad som kan göras bättre.

I arbetet med denna rapport har sex specifika problemområden identifierats som medför särskilda utmaningar hos organisationer gällande arbetet med att stärka skyddet mot cyberangreppsförsök. Dessa områden är (I) systematiken i säkerhetsarbetet, (II) incident- och kontinuitetshantering, (III) behörighetshantering, (IV) medarbetarnas kunskaper, (V) ändringshantering samt (VI) digitala leveranskedjor. Det kan finnas andra relevanta problemområden som borde lyftas fram. MSB har emellertid fokuserat på de områden som framträder av utförliga beskrivningar av händelseförlopp i it-incidentrapporteringen eller som har beskrivits som utmaningar hos organisationer i tidigare rapporter och undersökningar MSB har genomfört.

Systematiken i säkerhetsarbetet

För att kunna förbättra sitt motstånd mot cyberangreppsförsök är det avgörande att organisationer har de grundförutsättningar som krävs för att arbeta systematiskt och riskbaserat med sin informations- och cybersäkerhet.

Utmaningar

- Ledningens engagemang
- Resursbrist

En generell utmaning, där det finns stor förbättringspotential, gäller upprätthållandet av engagemanget för och den grundläggande systematiken i säkerhetsarbetet. Detta kräver en strategisk och långsiktig planering. Det ska finnas en säkerhetskultur som avspeglas i organisationens idéer och sociala beteenden där säkerhetstänket finns i varje medarbetares DNA. MSB ser att många organisationer i offentlig förvaltning saknar en ledning som engagerar sig i säkerhetsfrågor.[90] När ledningen och chefer i en organisation är engagerade i säkerhetsarbetet reflekteras det i medarbetarnas engagemang.[91] Motsatsen gäller tyvärr också, det vill säga att om ledningen är mindre engagerad i säkerhetspraxis, kommer medarbetarna imitera detta riskfyllda beteende.[92]

Resursbrist är en annan utmaning i det förebyggande arbetet för många organisationer.[93] Resurser behövs dels för att ta reda på vilka utmaningar organisationen har, för att implementera systematiska och riskbaserade arbetssätt, utbilda och öva medarbetare samt att leda och samordna arbetet. I detta ingår även att drifta och förvalta organisationens it-miljö på ett säkert sätt.

Ledningen kan främja en god säkerhetskultur genom att sätta tydliga mål och förväntningar för säkerhetsarbetet. Vidare ska ledningen kommunicera vikten av säkerhet regelbundet, erbjuda utbildning och övningsmöjligheter, uppmuntra medarbetare att rapportera säkerhetshändelser och förbättringsförslag, samt själv föregå med gott exempel genom att följa organisationens säkerhetsrutiner.

Incident- och kontinuitetshantering

För att kunna hantera it-incidenter till följd av av cyberangrepp så att påverkan på organisationen och dess it-miljö minimeras behövs arbetssätt för både incident- och kontinuitetshantering.

Utmaningar

- Hantera cyberangrepp tidigt
- God beredskap
  - Rätt kompetens
  - Gemensamma riktlinjer
  - Kommunikation

Sett till den totala mängden inrapporterade cyberangreppsförsök har 53 procent av fallen resulterat i en störning eller annan händelse som påverkat organisationen. Den genomsnittliga störningen i samband med att nytta förhindras pågår i cirka 49 timmar. Tidsangivelser för när hinder och hot uppstår visar att organisationer har svårt att hantera den uppkomna it-incidenten snabbt och att det i vissa fall (speciellt när ett hot uppstår) dessutom tar lång tid innan it-incidenten upptäcks.[94]

90. MSB. *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen*, Resultatredovisning Infosäkkollen 2021. 2022. https://rib.msb.se/filer/pdf/30002.pdf (hämtad 09/2023).

91. Se MSB:s övningsmaterial för *Övning – Informationssäkerhet för ledningen*, https://www.msb.se/sv/publikationer/ovning--informationssakerhet-for-ledningen/.

92. Dhillon, Gurpreet. *Information Security: Text & Cases* (andra upplagan). Burlington: Prospect Press, 2018.

93. MSB. *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen*, Resultatredovisning Infosäkkollen 2021. 2022. https://rib.msb.se/filer/pdf/30002.pdf (hämtad 09/2023).

94. Upptäcktstiden definieras som tiden mellan det att incidenten uppstod och att den upptäcktes. Hanteringstiden definieras som tiden mellan det att hanteringen av incidenten inleds och det att incidenten upphör.

Detta tyder på att det finns behov av att stärka arbetet med incident- och kontinuitetshantering hos organisationer.

Incident- och kontinuitetshantering

När ett cyberangrepp upptäcks behöver organisationen hantera det i enlighet med dess rutiner för incidenthantering. I arbetet ingår att dokumentera incidenten, prioritera och tilldela uppgifter till lämpliga medarbetare, samt att snabbt hitta lösningar för att minimera konsekvenserna.

Kontinuitetshantering handlar om att säkerställa att en organisation kan fortsätta sin verksamhet även vid oplanerade händelser. I arbetet ingår att på förhand identifiera och hantera risker, dokumentera och planera för att upprätthålla sin verksamhet på en tolerabel nivå oavsett vilken störning den utsätts för.

De utmaningar många organisationer kan möta i arbetet med incident- och kontinuitetshantering inbegriper att hantera cyberangrepp tidigt och att ha god beredskap. För att ha god beredskap krävs rätt kompetens, gemensamma riktlinjer, samt välfungerande kommunikationsrutiner såväl internt som externt.

Idag upptäcks och rapporteras de flesta cyberangreppsförsök som beskrivs i it-incidentrapporterna av medarbetare[95]. Ofta upptäcks det i samband med en störning, exempelvis när informationssystemen har långa svarstider eller ett informationssystem helt slutar att fungera. Detta tyder på att ett cyberangrepp inte har hanterats innan konsekvenser har uppstått. En förklaring till detta kan vara att organisationer saknar tekniska lösningar för att upptäcka exempelvis skadlig kod eller intrång tidigt. Det kan även vara så att angreppet upptäcktes i ett tidigare skede men att de som arbetar med hanteringen av angreppet inte har rätt mandat eller behörigheter för att arbetet ska gå tillräckligt snabbt. Sådana mandat kan exempelvis handla om att ha rätt att genomföra nödåtgärder såsom en akutnedstängning för att begränsa påverkan och undvika följdeffekter. En annan förklaring kan vara att det saknas effektiva arbetssätt för att rapportera händelser utöver det vanliga om medarbetare misstänker att något är fel, men inte är helt säkra.

Avsaknaden av god beredskap leder till att det tar längre tid att hantera it-incidenter till följd av ett cyberangrepp och återgå till ett normalläge. Förberedelser hjälper till att förutse och hantera stressen som en kris kan orsaka, oavsett om det är cyberrelaterat eller inte. Med stress och trötthet ökar dessutom risken för missförstånd under en pågående incident. Under de första timmarna är det ofta svårt att veta exakt vad som händer, att avgöra orsaker till incidenter, att identifiera källan eller källorna och att förutse hur händelseförloppet kommer att utvecklas. Medarbetarnas förmåga att hålla huvudet kallt, samarbeta och snabbt fatta rätt beslut grundas i att de har övat. Medarbetare som har övat kan agera snabbare för att begränsa negativ påverkan om ett angrepp inträffar.

95. Se faktaruta *Vem upptäckte cyberangreppsförsöket?* s. 55.

För god beredskap behöver organisationer även ha inövade arbetssätt för att bevara viktiga tillgångar, exempelvis genom att ta säkerhetskopior och öva på att återläsa dem, samt se till att det finns kontinuitetsplaner för alternativa arbetssätt om exempelvis informationssystem som i vanliga fall används är otillgängliga.

God beredskap kräver även att rätt kompetens finns hos organisationer. En av utmaningarna är att medarbetare med den tekniska kunskap och erfarenhet som krävs för att utföra det arbete som behövs vid ett cyberangrepp saknas.[96] Detta arbete kan exempelvis inkludera att analysera angreppet, avvärja påföljande angrepp eller vidta andra åtgärder för att minimera ytterligare skada. Organisationer som saknar dessa resurser själva bör överväga att avtala med extern part som är specialiserade för uppgiften, alternativt se till att ha cyberförsäkring[97] som ger tillgång till rätt kompetens och hjälp vid en incident.

Ett cyberangrepp påverkar ofta flera delar av organisationen och kan därför behöva hanteras av medarbetare som är ovana att arbeta tillsammans. Vid en incident med stor påverkan på organisationen kan it-avdelningen exempelvis behöva arbeta nära ledningen, kommunikations-, rätts- och personalavdelningar och andra berörda. Om grupperna övar tillsammans kan en gemensam terminologi och arbetssätt tas fram inte minst för hur organisationen kommunicerar kring incidenten internt och externt så att ryktesspridning kan undvikas. Vid ett cyberangrepp (eller som en följd av de åtgärder organisationen vidtar för att bemöta ett pågående cyberangrepp) kan även de vanliga kommunikationskanalerna som e-post, internchatt och andra verktyg sluta fungera eller på annat sätt vara påverkade, vilket försvårar både intern och extern informationsspridning.

Det vanligaste scenariot vid ett angrepp är att nytta förhindrats i samband med att organisationens förmåga att kommunicera externt påverkats negativt. Detta inkluderar fall då webbsidor och relaterade e-tjänster såväl som mejl och VPN-lösningar blivit otillgängliga för användare under en längre tid, eller under en tidskänslig period då organisationen behövt tjänsten. Organisationer behöver ha inövade planer för kommunikation och informationsspridning som kan användas under en pågående incident. Dessa är viktiga för att medarbetare i en organisation ska veta hur de ska agera och att de får information om hur organisationen ska kommunicera externt.

96. Li, Yuchong; Liu, Qinghui. *A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments*. 2021. https://www.sciencedirect.com/science/article/pii/S2352484721007289 (hämtad 07/2023).

97. MSB avråder från att använda cyberförsäkringar istället för att bedriva ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete utan det kan vara ett komplement till arbetet.

Medarbetarnas kunskaper

För att stärka sitt motstånd mot cyberangreppsförsök är det viktigt att regelbundet förbättra medarbetarnas kunskaper om de olika angreppssätt som används av antagonister.

Utmaningar

- Social manipulation
- Användning av svaga, samma och standardlösenord
- Läckta lösenord

Den mänskliga faktorn är en utmaning för varje organisations säkerhetsarbete. I it-incidentrapporteringen till MSB nämns ofta nätfiske och svaga lösenord som anledningen till hur en angripare får initial åtkomst till en organisations informationssystem. Liknande observationer har gjorts av den amerikanska cybersäkerhetsmyndigheten CISA.[98] Att hantera social manipulation, användning av svaga lösenord, standardlösenord, samt läckta lösenord utgör en särskild utmaning för organisationer.

Genom olika sociala manipulationsmetoder[99] kan medarbetare luras till att utföra handlingar som medför att ett hot uppstår. Medarbetare kan exempelvis luras till att klicka på en länk i sin e-post som leder till att skadlig programvara installeras i organisationens informationssystem. Den skadliga programvaran kan vara en wiper- eller utpressningsprogramvara som i sin tur kan leda till att skada orsakas genom att organisationens filer raderas eller att ett hinder uppstår om filer eller informationssystemet blockeras. Angripare kan idag med hjälp av olika verktyg skapa alltmer övertygande och komplexa varianter av social manipulering och det är svårt för medarbetare att identifiera dessa hot.[100]

Både tekniska verktyg och utbildning behövs för att minska riskerna. Tekniska verktyg kan till viss del användas mot nätfiske via e-post för att filtrera bort meddelanden som innehåller skadliga länkar eller bilagor. Utbildning av medarbetare kan i sin tur bidra till en förbättrad förmåga att identifiera social manipulation eller andra tekniker som används.

Förutom nätfiske påtalas svaga lösenord[101] i it-incidentrapporteringen som en orsak till hur en angripare får initial åtkomst till en organisations informationssystem. Svaga lösenord gör det också enklare för angriparen att befästa sin position och med lateral rörelse komma djupare in i organisationens it-miljö[102]. Vidare är det ett problem om medarbetare använder samma lösenord till flera olika tjänster, om standardlösenordet för ett informationssystem inte har ändrats eller om

98. CISA (Cybersecurity and Infrastructure Security Agency, som är en del av Department of Homeland Security). *CISA Analysis: Fiscal Year 2022 Risk and Vulnerability Assessments*. 2023-06. https://www.cisa.gov/sites/default/files/2023-07/FY22-RVA-Analysis%20-%20Final_508c.pdf (hämtad 09/2023).

99. Social manipulation (”social engineering”) är inom it-säkerhet metoder som används av angripare för att manipulera personer till att utföra handlingar som exempelvis att klicka på länkar, avslöja lösenord eller annan konfidentiell information.

100. CERT-SE vill belysa detta problem och har sammanställt förslag på åtgärder samt generella tips för alla som hanterar e-post, https://www.cert.se/2023/09/oka-motstandskraften-mot-bedraglig-e-post.

101. Svaga lösenord innebär att en stor del av lösenorden går att gissa sig till utifrån modifierade ordlistor eller genom att prova ett litet antal mycket vanligt förekommande lösenord mot ett stort antal kontonamn.

102. Läs mer om detta i stycket *Utförandet av cyberangrepp* under kapitlet *Antagonistisk cyberaktivitet*.

samma lösenord som används på arbetet också används i olika tjänster som medarbetare nyttjar privat. Organisationer har inte alltid tillgång till tekniska verktyg för att upptäcka användningen av svaga lösenord eller kunskap saknas om hur teknik kan användas för att tvinga medarbetare till att välja starkare lösenord.

Stulna eller läckta lösenord kan läggas ut av angriparna på nätet så att de antingen finns relativt fritt tillgängliga eller kan köpas av andra kriminella aktörer. Organisationer behöver då ha tillgång till webbtjänster för att identifiera om användaruppgifter finns åtkomliga på nätet och ändra lösenord för de användare vars uppgifter kan vara komprometterade. Tvåfaktorautentisering med någon form av kodgenerator kan med fördel användas vid inloggning som ett komplement till namn och lösenord. Tyvärr har även dessa lösningar brister eftersom telefoner kan komprometteras, SIM-kort kopieras och signaler avlyssnas. Även här spelar den mänskliga faktorn roll då användare kan luras att lämna ifrån sig namn, lösenord och engångskoder. Med hjälp av en fysisk säkerhetsnyckel som ersätter SMS-koder och mobilappar för tvåfaktorautentisering kan en större säkerhet uppnås.

Behörighetshantering

För att säkerställa att endast behöriga användare får tillgång till organisationens informationssystem behövs arbetssätt för behörighetshantering.

Utmaningar

- Hög aktivitet medför att säkerhetsarbetet inte hänger med

It-incidentrapporteringen visar att det är vanligt att användarkonton blir kapade och därefter används för att exempelvis skicka ut spammeddelanden eller skadligt innehåll. Ett exempel beskriver att angriparen, efter att ha kapat ett användarkonto, ändrat det bankkonto som medarbetarens lön ska betalas ut till. I it-incidentrapporteringen redovisas även cyberangreppsförsök där en angripare systematiskt prövar olika inloggningsuppgifter mot olika tjänster. Även om dessa oftast utgör misslyckade intrångsförsök händer det att angripare lyckas ta sig in. Dessutom påvisar rapporteringen att säkerhetshändelser sker hos organisationer som leder till att sårbarheter uppstår när exempelvis obehöriga ges tillgång till informationssystem eller filytor, eller genom att gamla användarkonton inte avaktiveras och sedan används i antagonistiskt syfte.[103]

Behörighetshantering

Behörighetshantering innebär att organisationer arbetar för att säkerställa att endast behöriga användare och informationssystem har åtkomst till it-miljön och utforma sin behörighetshantering på ett sådant sätt att varje digital identitet inte har mer åtkomst till information och informationssystem än vad den behöver.

103. Se stycket *Cyberangrepp med påverkan*, under kapitel *Angreppsbilden*.

En potentiell förklaring till en del av de här utmaningarna skulle kunna vara att många organisationer har relativt hög personalomsättning, och fortlöpande förändringar i verksamheten, vilket i sin tur skulle kunna försvåra för organisationer att lyckas förebygga behörighetsrelaterade it-incidenter. Det finns många inslag i den vardagliga verksamheten som direkt eller indirekt påverkar identitets- och behörighetshantering. Det kan vara svårt att i praktiken säkerställa att endast de som ska ha rättigheter har det, och att de endast har de rättigheter som de ska ha, när de ska ha dem. Exempel på aspekter som utmanar behörighetshanteringen är introduktion av nya informationssystem, ändringar i och utfasning av informationssystem, nya anställningar, personalflyttar inom organisationen och avslut av anställning, samt hantering av inhyrd personal.

En indikation på att organisationen arbetar med behörighetshantering på ett otillfredsställande sätt kan exempelvis vara att organisationen saknar fastslagen styrning av och dokumenterade arbetssätt för hantering av behörigheter. Brister kan exempelvis ses vid avsaknad av loggning och spårbarhet, eller att behörigheter finns kvar långt efter att en medarbetare har slutat.

Övergripande viktiga steg i arbetet med behörigheter är översyn och insamling av alla behörigheter från olika informationssystem, vilket i sig kan utgöra en utmaning då behörigheter och verksamhetsprocesser kan ändras under arbetets gång. Nästa steg är att skapa användargrupper utifrån roller, som har olika uppgifter, i informationssystemen. Till sist beslutas vilka behörigheter som ska ges till medarbetare, konsulter och om dessa behörigheter byggas på utifrån avdelnings- eller enhetstillhörighet, samt om eventuella specifika roller behövs. Sedan behövs dokumenterade arbetssätt för att regelbundet granska alla behörigheter.

En automatiserad behörighetshantering kan underlätta planering och verifiering av användarnas behörigheter och även göra det möjligt att justera behörigheten i förhållande till de föränderliga behov som organisationen har. Med automatiserad behörighetsanalys kan även avvikelser flaggas samt göra det enklare för olika delar av organisationen att godkänna eller avslå behörighetsförändringar.

Ändringshantering

För att kunna genomföra ändringar i informationssystem utan att nya sårbarheter introduceras krävs arbetssätt för ändringshantering.

Utmaningar

- Kompetensbrist
- Kompabilitetsproblem
- Tiden för återstart
- Kompromitterad uppdatering
- Funktionell testmiljö

It-incidentrapporteringen har över tid visat att säker ändringshantering i informationssystem är ett återkommande problemområde för många organisationer.[104] I it-incidentrapporteringen noteras att sju procent

104. MSB, *Ändringar som både hotar och skyddar*, https://www.msb.se/sv/publikationer/andringar-som-bade-hotar-och-skyddar-20-rekommendationer-for-sakrare-andringar-i-vara-informationssystem/ (hämtad 07/2023).

av angreppsförsöken som påverkat organisationens it-miljö har ägt rum i samband med eller efter att en ändring har genomförts i ett informationssystem[105]. Ett exempel på att ändringshanteringen har brister kan vara att en brandvägg avaktiveras vid en uppdatering varvid en sårbarhet uppstår som utnyttjas av en angripare.

Ändringshantering

Ändringshantering är en systematisk och strukturerad metod och process som syftar till att på ett effektivt, kontrollerat och riskminimerat sätt möjliggöra ändringar i en organisations målsättningar, processer eller teknologier. Ändringshantering involverar förberedelser inför ändringar, genomförande av ändringar och stöd till anpassning efter att ändringar har genomförts. Ändringar kan genomföras som ett resultat av nya behov, krav eller målsättningar.

En ändring i ett informationssystem kan även leda till att ett hot[106] uppstår. Det kan exempelvis ske om en medarbetare kopplar en hårddisk mot internet under ett arbete med en uppdatering eller genom att en filyta som innehåller känslig information råkas göras tillgänglig via internet.

Att förebygga ändringsrelaterade it-incidenter kan försvåras av exempelvis kompetensbrist, kompatibilitetsproblem, att tiden för återstart överskrider vad organisationen kan acceptera, eventuellt komprometterade uppdateringar och avsaknad av en tillräckligt produktionslik funktionell testmiljö.

Flera av de senaste årens mest uppmärksammade angrepp har baserats på att kända sårbarheter har utnyttjats. Det har ofta funnits tillgängliga uppdateringar eller andra ändringsmöjligheter att tillgå för att ge det skydd som behövs, men ändringarna har inte gjorts i tid eller på ett korrekt sätt.[107]

Verksamhetskritiska informationssystem som exponeras mot internet ska alltid säkerhetsuppdateras när nya sårbarheter upptäcks. Det är dock vanligt att organisationer har byggt och ordnat sina informationssystem så att det finns stora utmaningar och osäkerhetsfaktorer med att göra ändringar. Det kan exempelvis behövas specialistkompetens för att genomföra en ändring på ett säkert sätt, vilket kan saknas. Det kan också finnas en risk att ändringen orsakar kompatibilitetsproblem gentemot andra informationssystem. Rädslan för att ändringen ska ta för lång tid eller att informationssystemet inte ska kunna återstartas efter ändringen kan också vara orsaker till att många avvaktar med ändringar, även de som ger direkt skydd mot en sårbarhet. Det kan även finnas en upplevd risk för att en uppdatering ska medföra nya sårbarheter om den exempelvis blivit komprometterad.

105. Stycket *Cyberangrepp med påverkan*, under kapitel *Angreppsbilden*. Andelen kan verka liten, men förklaras delvis av att bara ett begränsat antal av rapporterna har utförliga beskrivningar av vad som har hänt. Om man exkluderar de rapporter som har ofullständiga eller otydliga beskrivningar ökar andelen där detta är ett problem betydligt.

106. Med andra ord en sårbarhet uppstår. Se *bilaga 1* för mer detaljer kring hur grundbegrepp kan förstås.

107. MSB, *Ändringar som både hotar och skyddar*, https://www.msb.se/sv/publikationer/andringar-som-bade-hotar-och-skyddar-20-rekommendationer-for-sakrare-andringar-i-vara-informationssystem/ (hämtad 07/2023).

Organisationer kan också sakna arbetssätt för att säkerställa att programuppdateringar kommer från en tillförlitlig leverantör. Sådana arbetssätt kan exempelvis inkludera att uppdateringar tas emot på en särskild server och att leverantören skyddar sina filer mot manipulation med hjälp av signering. Tillgång till en testmiljö, som så långt det är möjligt liknar produktionsmiljön, där uppdateringar kan prövas innan de införs i produktionsmiljön är ett sätt att upptäcka och kringgå några av utmaningarna vid ändringshantering. Det kan dock vara en utmaning i sig att lyckas med att upprätta en funktionell testmiljö eftersom organisationernas it-miljö ofta är komplex och föränderlig.

Att lämna kända sårbarheter ohanterade kan öka sannolikheten för att ett angreppsförsök resulterar i en it-incident. Detta gäller särskilt om informationssystemet är uppkopplat mot internet. Om organisationen dessutom är del av en digital leveranskedja ökar risken för att fler organisationer eller samhället blir drabbat när en incident inträffar. Regelbundna analyser av risker i organisationens it-miljö som även innefattar leverantörer och deras underleverantörer är därför viktigt. Detsamma gäller omvärldsbevakning för att ta del av information om nya sårbarheter, nyutvecklade skydd, säkerhetsuppdateringar, generella råd och rekommendationer för att öka motståndskraften genom att exempelvis läsa veckobrev från CERT-SE[108]. I MSB:s rapport *Ändringar som både hotar och skyddar*[109] redogörs för vikten av att ha fungerande arbetssätt för ändringshantering och rekommendationer för säkrare ändringar i informationssystem.

Digitala leveranskedjor

Säkerheten i digitala leveranskedjor är viktig eftersom it-incidenter till följd av cyberangrepp kan få påverkan inte bara på organisationen som drabbas, utan även andra organisationer som ingår i samma leveranskedja.

Utmaningar

- Information om it-incidenter
- Komplexa leveranskedjor
- Monoberoenden

20 procent av det totala antalet inrapporterade cyberangreppsförsök utgörs av leverantörskedjeincidenter. Organisationer vars verksamhet är beroende av tjänster från en leverantör som drabbas av ett cyberangrepp riskerar att råka ut för långtgående konsekvenser. It-incidentrapporteringen visar att i genomsnitt pågår en störning som konsekvens av ett cyberangrepp mot en leverantör i 18 timmar. Medianfallet pågår i cirka åtta timmar och även här är det ett fåtal incidenter som driver upp genomsnittet. Ovan tidsangivelser baseras dock på ett begränsat urval. Att dessa incidenter resulterar i störningar som får organisationspåverkan och kan pågå under en längre tid tyder på att organisationer har utmaningar i arbetet med digitala leverankedjor.[110]

108. CERT-SE står för Computer Emergency Response Team – Sweden. Det är Sveriges nationella CSIRT (Computer Security Incident Response Team) som har till uppgift att stödja det svenska samhället i arbetet med att hantera och förebygga it-säkerhetsincidenter, https://www.cert.se/.

109. MSB. *Ändringar som både hotar och skyddar: 20 rekommendationer för säkrare ändringar i våra informationssystem*. 2022. https://www.msb.se/sv/publikationer/andringar-som-bade-hotar-och-skyddar-20-rekommendationer-for-sakrare-andringar-i-vara-informationssystem/ (hämtad 06/2023).

110. För mer information se stycke *Cyberangrepp inom digitala levernskedjor* under kapitel *Angreppsbilden*.

Det som kan vara en utmaning och som hindrar organisationer att lyckas med att kontrollera säkerheten i sina digitala leveranskedjor innefattar avsaknad av information om inträffade it-incidenter från leverantörer, komplexa leveranskedjor och monoberoenden.

Att organisationer inte får information om it-incidenter som pågår eller har skett hos en leverantör gör det svårt för dem att veta hur de ska agera eller vilka säkerhetsåtgärder som behöver vidtas. Det gör det även svårt eller omöjligt för dem att vidare förmedla information om det inträffade till sina kunder. Ofullständig information kan i sin tur leda till spekulation och ryktesspridning med påverkan och andra konsekvenser som kunde ha stoppats.[111] För att undvika detta bör tydliga klausuler om informationsplikt från leverantörer om it-incidenter som på något sätt påverkat eller påverkar deras organisation införas i avtal. Organisationerna ska kunna kräva att bli informerade under den tid leverantören är utsatt för att kunna fatta välgrundade beslut.[112] Förutom tidpunkt när tjänsten beräknas fungera igen är det viktigt att få vetskap om misstanken finns att organisationens information är åtkomlig för obehöriga eller i övrigt kompromitterad.

En särskilt svår utmaning uppstår när många organisationer har starka behov av att använda en tjänst som tillhandahålls via en digital leveranskedja, och det endast finns en, eller några få, tillhandahållare av en sådan tjänst – d.v.s. när det råder ett *monoberoende*. Ett monoberoende riskerar innebära att en organisation är avhängig en leverantörs tjänst och om det saknas alternativa tjänster blir organisationen sårbar om tjänsten upphör eller blir otillgänglig. I det förebyggande arbetet är planer för alternativa lösningar viktiga, liksom planer och arbetssätt för hur organisationen ska agera och samordna sig med leverantören om en it-incident inträffar.

Cloud Hopper – ett sofistikerat leveranskedjeangrepp

- **Typ:** Nätfiske och skadlig kod.
- **Faktisk incident:** Nytta orsakas.

Onsdagen den 5 april 2017 avslöjade företagen PwC och BAE, samt det brittiska nationella cybersäkerhetscentret (NCSC-UK) ett världsomspännande cyberangrepp som tros ha pågått i månader, kanske till och med år.[113] Angreppet har påstått vara en del av ett omfattande statsfinansierat cyberspionage där Sverige var ett av de femton drabbade länderna.[114] Det uppmärksammade angreppet var riktat mot bolag som sköter it-tjänster, i detta fall molntjänster i form av datalagringsutrymme och serverkapacitet, åt andra företag, organisationer och myndigheter. Angreppet kom därför att kallas för Cloud Hopper.

111. Att organisationer inte får information från sina leverantörer innebär även att incidentrapporterna till MSB saknar viktig information. Denna information är central för att kunna informera andra organisationer som skulle kunna vidta åtgärder i förebyggande syfte, för framtida analyser samt för planering av organisationers och hela Sveriges cybersäkerhetarbete.

112. Informationsplikten ska gälla även om det inte är leverantören själv har har incidenten, d.v.s. om leverantören själv har drabbats av en leveranskedjeincident.

113. Sallinen, Jani. *Så angrep Kina ”naiva” Sverige i det fördolda*. Svenska Dagbladet. 2018-04-21. https://www.svd.se/a/xRbQdQ/sa-angrep-kina-naiva-sverige-i-det-fordolda (hämtad 9/2023).

114. SVT. *Stor internationell cyberattack avslöjad – Sverige drabbat*. 2017-04-05. https://www.svt.se/nyheter/inrikes/stor-internationell-cyberattack-avslojad-sverige-drabbat (hämtad 9/2023).

Genom att ge sig på den svagaste länken i leveranskedjan kunde angriparna effektivt komma åt känslig information som lagrades av aktörer inom bland annat offentlig sektor, it, kommunikation, energi och forskning.[115] Flera svenska företag och organisationer påverkades av angreppet. Exakt hur många aktörer som fick sina känsliga uppgifter stulna är inte klarlagt.

Angriparna bakom Cloud Hopper tog sig in hos måltavlornas underleverantörer genom nätfiske. Genom att noga kartlägga it-tjänsteleverantörer och deras personal, exempelvis via sociala medier, kunde angriparna skräddarsy mejl som riktades mot anställda. När en anställd öppnade mejlet installerades skadlig kod som gjorde det möjligt för en angripare att nå de servrar där data tillhörande it-tjänsteleverantörens kunder fanns lagrad. Väl inne i informationssystemet kunde angriparen röra sig diskret, vilket är anledningen till att intrånget kunde pågå i det fördolda så pass länge. Hur stora mängder information angriparna lyckades samla in är oklart, även om det troligtvis rör sig om mycket stora kvantiteter.[116]

115. Sentor. *Cloud Hopper – en supply chain-attack som gav eko*. 2021-03-29. https://www.sentor.se/artikel/cloud-hopper-en-supply-chain-attack-som-gav-eko/#Vilka%20utsattes%20för%20Cloud%20Hopper? (hämtad 9/2023).

116. SVT. *Stor internationell cyberattack avslöjad – Sverige drabbat*. 2017-04-05. https://www.svt.se/nyheter/inrikes/stor-internationell-cyberattack-avslojad-sverige-drabbat (hämtad 9/2023).

Framåtblick

Framåtblick

Det försämrade säkerhetsläget kombinerat med en allt snabbare teknisk utveckling kan komma att förändra angreppsbilden mot svenska organisationer. I framåtblicken avhandlas några av de faktorer som kan komma att påverka förekomsten, såväl som effekten, av framtida cyberangreppsförsök. Kapitlet avslutas med en kortare redogörelse om hur kommande EU-regleringar och initiativ på cyberområdet inverkar på organisationers arbete med antagonistiska cyberhot framöver.

Flera myndigheter bedömer att säkerhetsläget har försämrats under de senaste åren.[117] Det innebär förvisso inte per automatik att fler cyberangreppsförsök utförs på kort sikt, men däremot kan det påverka angriparens incitament att utföra olika former av angrepp i en ogynnsam riktning. Osäkerhet, misstro och konflikter, såväl inrikes som i omvärlden, kan bidra till ett ökat intresse bland antagonistiskt sinnade aktörer att använda sig av cyberangrepp. När cyberangrepp bedöms vara ett effektivt verktyg för att uppnå strategiska mål kan aktiviteten öka och metoderna bli allt mer sofistikerade.

En faktor som skulle kunna bidra till att angreppsbilden på sikt förvärras är den ökande spridningen av desinformation och en negativ bild av Sverige på allt mer fragmenterade sociala medieplattformar. Myndigheten för psykologiskt försvar påvisar hur mängden desinformation som riktats mot Sverige och svenska organisationer har ökat under det gångna året.[118] Med ökad desinformation eller en förändrad Sverigebild skulle incitamenten för att utföra angrepp mot svenska organisationer och samhällsviktiga tjänster kunna öka. Överbelastningsangreppen som utfördes i efterdyningarna av ”koranbränningarna” under första halvåret av 2023 exemplifierar konsekvenser till följd av att uppfattningen om Sverige utomlands påverkats.[119] Att organisationer omvärldsbevakar och är extra uppmärksamma på ökad desinformation eller en förändrad Sverigebild är därmed befogat.

I en orolig omvärld ökar sannolikheten för att störningar inom digitala leveranskedjor inträffar och blir långvariga. Således kan även cyberangrepp mot

117. Säkerhetspolisen. *Cyberangrepp ständigt pågående hot mot Sverige*. 2022-03-11. https://www.sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2022-03-11-cyberangrepp-standigt-pagaende-hot-mot-sverige.html (hämtad 06/2023).

118. Myndigheten för psykologiskt försvar (MPF). *Ökad spridning av desinformation riktas mot Sverige* https://www.mpf.se/2023/08/18/okad-spridning-av-desinformation-riktas-mot-sverige/ (hämtad 12/2023).

119. Svenska Institutet (SI). *Koranbränningen 2023*, https://si.se/koranbranningen-2023/ (hämtad 12/2023).

aktörer utanför Sverige få allvarliga konsekvenser för svenska organisationer. Organisationer bör bedöma risken att de digitala leveranskedjor de är beroende av drabbas av långvariga störningar eller annan problematik.

Den tekniska utvecklingen

Artificiell intelligens (AI), Internet of Things (IoT) och kvantberäkning (”quantum computing”[120]) är några teknikområden där det skett stora framsteg under de senaste åren och där utvecklingen sannolikt kommer att accelerera ytterligare. Hur innovationer inom dessa områden kommer att påverka angreppsbilden mot svenska organisationer beror dels på hur och i vilken utsträckning de kommer att integreras inom organisationers verksamhet. Om organisationer för hastigt gör sig beroende av exempelvis nya IoT- eller AI-lösningar som i ett senare skede visar sig besitta kritiska sårbarheter kan det utnyttjas av angripare. Därtill skulle angreppsbilden kunna påverkas av i vilken utsträckning angriparen kommer kunna använda sig av dessa teknologier för att utföra angrepp, särskilt mot äldre informationssystem. I samband med större teknikskiften kan det uppstå problem om äldre lösningar som fortfarande används av många organisationer inte längre uppfyller önskvärd säkerhet.

Under det gångna året har det spekulerats mycket kring framförallt AI:s positiva framtida roll inom samhället såväl som de säkerhetsrisker AI kan medföra. AI kan användas för att effektivisera och vidareutveckla cyberangreppsmetoder, exempelvis kan ”generativ AI” användas för att konstruera mer sofistikerade nätfiskemeddelanden. Angripare kan även använda AI för att lista ut användarlösenord, utföra automatiserad sårbarhetsskanning och anpassningsbar utveckling av skadlig kod.[121] Omvänt kan organisationer använda AI för att öka sitt skydd mot angrepp eller skademinimera. Med hjälp av AI blir det lättare att identifiera mönster för cyberangrepp mot kritisk infrastruktur och nätverksaktivitet, samt att upptäcka skadlig kod i realtid. Denna information kommer göra det enklare att identifiera och förstå risker.

EU-regleringar

I november 2022 antog EU-kommissionen förslaget om en revidering av NIS-direktivet, det så kallade NIS 2-direktivet. Direktivet avser i korthet att öka harmoniseringen mellan medlemsländer för att öka informations- och cybersäkerheten inom hela unionen, men även att minska bördan på organisationer som har verksamhet i flera länder.[122] Direktivet föreskriver bland annat minimikrav för säkerhetsåtgärder, ökade och mer specificerade rapporteringsskyldigheter och inrättandet av ett europeiskt sårbarhetsregister.

120. Quantum computing är ett datavetenskapligt område baserat på principen om kvantfysik (studiet av hur atomära partiklar existerar och interagerar med varandra). Den förklarar materias och energis beteende på atomära och subatomära nivåer.

121. Islam, Rabiul. *AI And Cybercrime Unleash A New Era Of Menacing Threats*. Forbes. 2023-06-23. https://www.forbes.com/sites/forbestechcouncil/2023/06/23/ai-and-cybercrime-unleash-a-new-era-of-menacing-threats/ (hämtad 06/2023).

122. Europeiska kommissionen. *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (hämtad 06/2023).

Parallellt med NIS 2-direktivet införs även CER-direktivet (Critical Entities Resilience)[123] som ställer krav på åtgärder för att stärka motståndskraften i viss samhällsviktig verksamhet. Detta direktiv samspelar och kompletterar NIS 2-direktivet (som inriktar sig på nätverk och informationssystem) på så vis att det adresserar entiteternas förmåga att förebygga, skydda mot, reagera på, hantera och återhämta sig från hybridattacker, naturkatastrofer, terrorhot och folkhälsosituationer.[124] Båda direktiven avser höja kraven på organisationer och därmed göra samhället mer motståndskraftigt mot it-incidenter.

Ett förlag som kan komma att få stor påverkan inom EU är AI-förordningen. EU:s AI-förordning syftar till att försäkra att AI-system som används i EU är säkra, transparenta, spårbara, icke-diskriminerande och miljövänliga. För att förhindra skadliga effekter bör AI-system även övervakas av människor för att hjälpa till att säkerställa att systemen används på ett etiskt ansvarsfullt sätt. Utformningen av själva lagen förhandlas i skrivande stund mellan EU-länderna med målet att nå en överenskommelse i slutet av 2023.[125] Det återstår att se hur den slutgiltiga lagen lyder.

EU:s Cybersolidaritetsinitiativ är ett ytterligare förslag till nya regelverk som syftar till att stärka cybersäkerheten inom EU. Initiativet består av tre delar: Etablerandet av en cybersäkerhetskompetensakademi, ändringar i EU:s cybersäkerhetsakt och ett förslag till en cybersolidaritetsakt. Cybersolidaritetsakten består i sin tur av tre delar; den europeiska cyberskölden (ett nätverk av SOC- eller CERT-liknande organisationer som arbetar med att bevaka cybermiljön och upptäcka antagonistiska cyberhot), den europeiska cybernödmekanismen (en struktur med ”cyberinsatsstyrkor” som kan sättas in för att hantera storskaliga cyberincidenter) och en utvärderingsmekanism (en slags it-haverikommission som ska utvärdera storskaliga cyberincidenter efter de har inträffat, i syfte att säkerställa lärdomar och ett förstärkt förebyggande arbete).

Som tidigare nämnts kan det försämrade säkerhetsläget och den snabba tekniska utvecklingen komma att påverka angreppsbilden mot svenska organisationer. Genom att konstruktivt implementera de kommande regleringarna och att fortsätta att arbeta systematiskt och riskbaserat med informations- och cybersäkerhet, utifrån allriskperspektivet, står vi dock bättre rustade.

123. Europeiska unionens officiella tidning. *Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG*. 2022-12-27 https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32022L2557&from=SV (hämtad 06/2023).

124. Europeiska unionens råd. *EU resilience: Council adopts a directive to strengthen the resilience of critical entities*. 2022-12-08. https://www.consilium.europa.eu/en/press/press-releases/2022/12/08/eu-resilience-council-adopts-a-directive-to-strengthen-the-resilience-of-critical-entities/ (hämtad 06/2023).

125. Europaparlamentet. *EU:s AI-förordning: första förordningen om artificiell intelligens*. 2023-06-14. https://www.europarl.europa.eu/news/sv/headlines/society/20230601STO93804/eu-s-ai-akt-forsta-forordningen-om-artificiell-intelligens (hämtad 06/2023).

Bilaga 1

Bilaga 1: Ramverk för analys av it-incidenter

För att läsaren ska kunna följa hur MSB i arbetet med denna rapport övergripande har analyserat hot, sårbarheter, risker och it-incidenter som möjliggjort eller uppstått i samband med antagonistisk aktivitet presenteras i det här kapitlet det ramverk som myndigheten har använt. Ramverket kan också användas av organisationer som själva önskar systematisera sin analys av incidenter.

Bilagan är indelad i fyra delar:

- **Grundbegrepp**: De tolv begreppen nedan utgör en utgångspunkt för merparten av de analyser som utförs inom den strategiska analysen på informations- och cybersäkerhetsområdet vid MSB.
- **Säkerhetshändelser och faktiska incidenter**: Med utgångspunkt i grundbegreppen och några ytterligare koncept definieras en taxonomi för incidenter indelad i två typer: säkerhetshändelser och faktiska incidenter. Den här taxonomin, tillsammans med den som presenteras i det nästföljande avsnittet, har legat till grund för att klassificera de händelseförlopp som har beskrivits i de it-incidentrapporter som har analyserats i arbetet med denna fördjupande rapport.
- **Kausala förlopp i komplexa informationssystem:** Flera händelser kan sammantaget ha skapat förutsättningarna för att en incident uppstår. Likaså kommer kontextuella faktorer påverka incidentens konsekvenser. Begreppen *mekanism*, *komponent* och *trigger* utgör en taxonomi för att klassificera incidentens beståndsdelar och underlättar därigenom förståelsen för incidentens kausala förlopp. Den här taxonomin utgör tillsammans med taxonomin i det föregående avsnittet grunden för klassificeringen av inrapporterade incidenter som har skett inom ramen för arbetet med den här rapporten.
- **Tillämpningar av begreppen på it-incidenter som orsakats av cyberangrepp**: Här visas hur grundbegreppen, taxonomin för klassificering av incidenter i säkerhetshändelser respektive faktiska incidenter samt taxonomin för att klassificera händelser utifrån kausala förlopp kan användas för analys av incidenter som har orsakats av cyberangrepp.

Grundbegrepp

Analysen tar sin utgångspunkt i en stringent tillämpning av följande begrepp:

Tabell 2. Grundbegrepp

Begrepp	Förklaring
Incident	En inträffad oönskad händelse.
Framgång	En inträffad önskad händelse.
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.[126]
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.
Möjlighet	Avsaknad av något som förhindrar, eller bidrar till att förhindra, en framgång.
Frihet	Avsaknad av något som orsakar, eller bidrar till att orsaka, en incident.

Säkerhetshändelser och faktiska incidenter

I syfte att bättre redogöra för it-incidenters påverkan görs i den här rapporten en distinktion mellan incidenter som kan beskrivas som *säkerhetshändelser* och incidenter som kan beskrivas som *faktiska incidenter*. En säkerhetshändelse kan förstås som en händelse där något upphör eller uppstår som potentiellt påverkar organisationens it-miljö negativt. En säkerhetshändelse behöver inte resultera i att någon skada faktiskt uppstår, eller att någon nytta faktiskt uteblir. Organisationer som har redundanta system och fungerande skydd kan drabbas av säkerhetshändelser utan att faktiska incidenter inträffar.

En faktisk incident kan i sin tur förstås som en incident där en säkerhetshändelse har inträffat utan att kompenserande redundans eller lämpliga skydd finns på plats, varför skada uppstår eller nytta uteblir för organisationen. Medan begreppet säkerhetshändelse alltså avser händelser som påverkar säkerheten inom ett informationssystem, beskriver en faktisk incident en händelse som direkt eller indirekt missgynnat den egna organisationen. I denna rapport har begreppet *organisationspåverkan* också använts för att beskriva denna företeelse. Både säkerhetshändelser

126. Det är vanligt att risk definieras, eller uttrycks, i termer av konsekvens och sannolikhet. I den här nomenklaturen kan en risk (det vill säga en möjlig oönskad händelse) *bedömas* i termer av de konsekvenser den skulle medföra om den inträffade, samt sannolikheten för att den ska inträffa.

och faktiska incidenter är exempel på incidenter, men en faktisk incident kan inte uppstå om en säkerhetshändelse inte har inträffat.

Det finns fyra typer av säkerhetshändelser (som definieras med stöd av grundbegreppen som presenteras i det föregående avsnittet) och fyra typer av faktiska incidenter. De är:

- **Hot uppstår:** något introduceras i it-miljön som orsakar eller bidrar till att orsaka att en incident uppstår. Exempel på detta skulle kunna vara att utpressningsprogramvara installeras i informationssystemet, eller att en filyta som innehåller känslig information upprättas och görs fritt tillgänglig från internet.
- **Skydd upphör/sårbarhet(er) uppstår**: något tas bort från i it-miljön som tidigare förhindrade eller bidrog till att förhindra att en incident uppstår (speciellt om inget annat skydd introduceras som kan blockera de hot som annars inte längre är blockerade). Exempel på detta skulle kunna vara att en brandvägg avaktiveras eller att man missar att lägga till krav på inloggning när man tillgängliggör en filyta med känslig information mot internet.
- **Framgångsfaktor(er) upphör/brist(er) uppstår**: något i it-miljön upphör som tidigare orsakade eller bidrog till att orsaka att en framgång uppstår (speciellt om ingen annan framgångsfaktor introduceras som orsakar de framgångar som annars inte längre orsakas). Exempel kan vara att en router tappar förmågan att kanalisera trafik, eller att en hårddisk går sönder och data som finns på den inte längre går att nå.
- **Hinder uppstår**: Något introduceras i it-miljön som förhindrar eller bidrar till att förhindra att en framgång uppstår. Exempel kan vara att en brandväggsregel läggs till som gör att legitim trafik blockeras, eller att en antivirusprogramvara felaktigt stoppar försök att öppna filer som inte är skadliga.

Faktiska incidenter inkluderar i sin tur händelser då:

- **Skada orsakas**: Skada orsakas för organisationen, eller för andra, på ett sätt som inte ligger i organisationens intresse. Exempel på sådan skada kan vara att komponenter i en it-miljö skadas, eller att det uppstår kostnader.
- **Skada förhindras**: Skada förhindras för andra organisationer eller aktörer på bekostnad av organisationen. Exempel på sådan skada kan vara att försvarssystem (i militära sammanhang) inte kan avfyras, eller att information som kan vara skadlig för någon inte kan publiceras (exempelvis att en medierapport om missförhållanden inte kan publiceras).
- **Nytta förhindras**: Nytta förhindras för organisationen, eller för andra, på ett sätt som inte ligger i organisationens intresse. Exempel på sådan nytta kan vara att tjänster som organisationen tillhandahåller blir otillgängliga, varpå organisationen inte kan få betalt och organisationens kunder inte kan få del av nyttan som tjänsten ska ge, eller att ett flöde (såsom data, el eller kyla) som organisationen ska leverera till andra organisationer avbryts.
- **Nytta orsakas**: Nytta orsakas för andra organisationer eller aktörer på bekostnad av organisationen. Exempel på sådan nytta kan vara att affärshemligheter skickas ut eller tillhandahålls till konkurrenter, eller att organisationens el och informationssystemens processorkraft och minneskapacitet används för kryptokapning och därmed för att olovligen generera vinst för någon annan.

Av central betydelse i modellen är att alla incidenter är säkerhetshändelser, men att inte alla incidenter är faktiska incidenter. Däremot är alla faktiska incidenter också säkerhetshändelser. Här är några exempel som illustrerar detta:

- **Nytta behöver inte förhindras bara för att ett hinder uppstår eller för att en framgångsfaktor upphör**: Om en organisation har redundans för komponenterna i sina informationssystem så måste inte en blockerad eller trasig komponent i ett informationssystem innebära att det inte längre finns några komponenter som fyller den funktionen i informationssystemet överhuvudtaget. Om exempelvis en hårddisk går sönder eller blockeras så kan information fortfarande sparas om det finns andra hårddiskar med outnyttjat utrymme tillgängliga. Om det däremot skulle bli så att information inte längre kan sparas (nytta förhindras) så kommer det att vara för att organisationens lagringsmedier är fulla eller sönder (framgångsfaktor upphör) eller blockerade (hinder uppstår).
- **Skada behöver inte orsakas bara för att ett hot uppstår eller för att ett skydd upphör**: Om en organisation har skydd i sina informationssystem så måste inte introduktionen av ett hot i informationssystemet innebära att hotet orsakar en incident – skyddet kanske blockerar hotet. Om en organisation har ett skydd i ett informationssystem (en brandvägg exempelvis) och det skyddet upphör så måste det inte nödvändigtvis innebära att det finns ett hot i informationssystemet som orsakar en incident. Om det däremot skulle bli så att en komponent förstörs och måste ersättas (skada orsakas) så kommer det samtidigt att vara så att den komponenten fyllde någon slags önskvärd funktion (varför en framgångsfaktor upphör) eller utgjorde ett skydd (varför ett skydd upphör).

Kausala förlopp i komplexa informationssystem

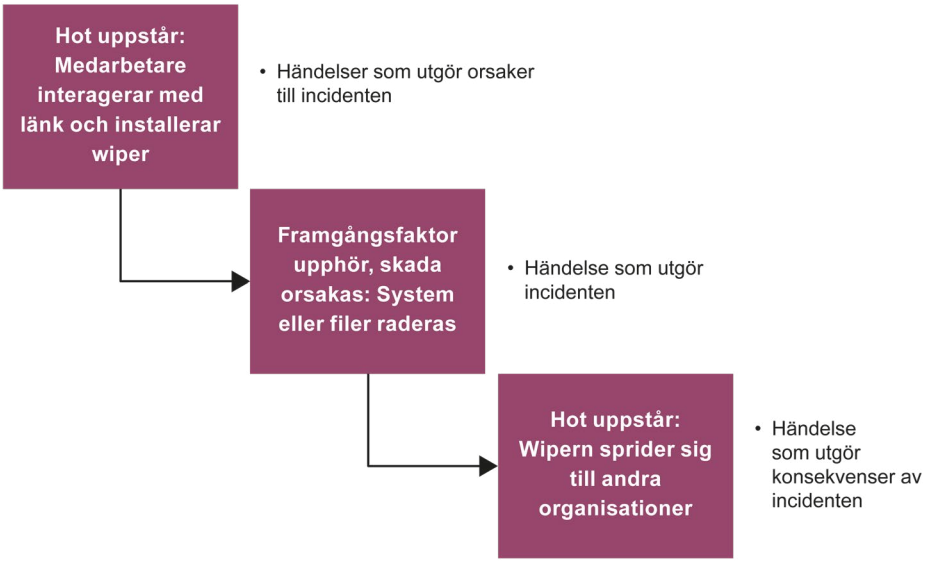
Inom komplexa informationssystem är händelser som inträffar resultat av att flera faktorer samverkar och interagerar på olika, ibland oförutsägbara, sätt. En utmatning ifrån ett informationssystem uppstår inte bara genom att en inmatning tillförs till systemet. Innan inmatningen kan göras behöver informationssystemet vara ordnat på vissa sätt, och ha vissa inbyggda inslag. Exempelvis behöver informationssystemet ha ett minne, en processor, ett operativsystem och en algoritm som kan ta inmatningen och utifrån den utföra ett antal instruktioner som resulterar i någonting nytt, som därpå blir till utmatningen. Informationssystemets respektive delar, elen det drivs av och algoritmen det innehåller utgör alla *komponenter* i en *mekanism*. Tillförseln av en specifik inmatning till mekanismen är *triggern* som tillsammans med komponenterna i mekanismen gör att en specifik utmatning orsakas. Om ett syfte med informationssystemet är att kunna generera en viss typ av utmatningar och det inte finns ett minne i informationssystemet, eller om algoritmen som behövs för att generera den eftersökta utmatningen saknas i informationssystemet, då är mekanismen *inkomplett* i förhållande till det syftet.

Hot, hinder, framgångsfaktorer och skydd kan alla utgöra mekanismer eller vara komponenter i mekanismer. Att en it-incident uppstår eller upphör kan bidra till förändringar inom it-miljön som i sin tur kan bidra till instabilitet och ökad risk under olika skeden inom ett kausalt förlopp. Händelsen att en mekanism eller

komponent uppstår kan utgöra (1) en orsak, en trigger, till att en incident inom ett informationssystem uppstår, men det kan också utgöra (2) incidenten i sig som en följd av en utlöst trigger eller (3) en konsekvens av incidenten. Vid närmare analys av händelseförloppet kopplat till en it-incident är det viktigt att kunna urskilja säkerhetshändelser från varandra i syfte att identifiera hur komponenter och mekanismer samverkat och således varför det resulterade i ett sammantaget negativt utfall.

Tillämpningar av begreppen på it-incidenter som orsakats av cyberangrepp

I den här rapporten är it-incidenten som uppstått till följd av ett cyberangrepp i fokus och därav den/de säkerhetshändelse/er och faktiska incidenter som angreppen resulterat i. För att förstå hur incidenten har uppstått och vilka följdeffekter den får är det dock viktigt att också undersöka hela händelseförloppet. När en angripare exempelvis skickar stora mängder datatrafik mot en organisations it-miljö kan detta i sig beskrivas som att ett hot uppstår. Det är i sin tur en orsak till att ett hinder i nästa skede blockerar tillgången till drabbade it-komponenter. Hindret som uppstått utgör den säkerhetshändelse som påverkar it-miljön och kan beskrivas som den huvudsakliga incidenten.



Vilken eller vilka säkerhetshändelser som utgör själva incidenten kan förenklat beskrivas som den eller de händelser som kompromitterat tillgängligheten, konfidentialiteten och/eller riktigheten inom organisationens it-miljö. I de fall den rapporterande organisationen beskriver en säkerhetshändelse som inte utmynnat i en incident redogörs beskrivna säkerhetshändelser endast som potentiella *orsaker* till att en incident kunnat uppstå. I de fall en incident även kan klassificeras som en faktisk incident har detta kategoriserats separat.

Nedan följer ett antal exempelscenarion för att demonstrera hur klassificeringen av it-incidentrapporter genomförts.

Exempelincident 1: Installation av skadlig kod

Händelser som kopplar till orsaken:

1. Egen personal avaktiverar brandväggen (skydd upphör/sårbarhet uppstår)
2. Medarbetare mottar nätfiskemejl som skulle ha blockerats om brandväggen inte var avaktiverad (hot uppstår)
3. Medarbetare klickar på länken i mejlet (trigger: hot uppstår)
4. Wiper installeras automatiskt (hot uppstår)

Händelsen som är incidenten:

5. Informationssystem och filer förstörs och raderas (framgångsfaktor upphör, Faktisk incident: skada orsakas, nytta förhindras)

Händelser som kopplar till konsekvenserna:

6. Wipern sprider sig till andra organisationer via den drabbade organisationen (hot uppstår)

Exempelincident 2: Överbelastningsangrepp

Händelser som kopplar till orsaken:

1. En tekniker ändrar av misstag en konfiguration i existerande överbelastningsskydd på ett sätt som gör att skyddets duglighet minskar (skydd upphör/sårbarhet uppstår)
2. En angripare skickar stora mängder datatrafik, exempelvis initierande TCP-sessionsförfrågningar, till en organisations webbserver (trigger: hot uppstår)

Händelsen som är incidenten:

3. Webbservern blir överbelastad och användare kommer under tiden för angreppet inte åt innehåll på organisationens hemsida eller relaterade e-tjänster (hinder uppstår, Faktisk incident: nytta förhindras).

Händelser som kopplar till konsekvenserna:

4. Mängden datatrafik minskar och serverns svarsförmåga återetableras (hinder upphör, ingen konsekvens)

Exempelincident 3: Misslyckat cyberangreppsförsök

Händelser som kopplar till orsaken:

1. Ett mejl innehållande skadlig kod skickas till medarbetare vid en organisation (trigger: hot uppstår)

Händelsen som är incidenten:

2. Antivirusprogram flaggar för skadligt innehåll. Den skadliga koden isoleras och tas bort (hot upphör, ingen incident)

Ett samarbete mellan:

Myndigheten för samhällsskydd och beredskap

Medfinansierat av Europeiska unionens fond för ett sammanlänkat Europa

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB2287 – januari 2024 ISBN 978-91-7927-459-7