Myndigheten för samhällsskydd och beredskap

En inblick i Sveriges cybersäkerhet

Årsrapport it-incidentrapportering 2021

En inblick i Sveriges cybersäkerhet
– Årsrapport it-incidentrapportering 2021

Foto omslag: Melker Dahlstrand
Produktion: Advant

Publ nr: MSB1913 – februari 2022
ISBN: 978-91-7927-234-0

Förord

Året som gått och händelserna i vår omvärld har på många sätt förstärkt den utveckling som redan var på gång och samtidigt visat vad konsekvenserna kan bli när utvecklingen sker i en högre hastighet än säkerhetsarbetet. Händelser under det senaste året som angreppet som drabbade Coop i somras eller nu senast sårbarheterna i Log4j och angreppet mot Kalix kommun är i sig inte nya företeelser, men de har bidragit till att aktualisera säkerhetsfrågorna. Även den rådande halvledarbristen har belyst säkerhetsfrågan, fast ur ett annat perspektiv. De incidentrapporter MSB mottar och som redogörs för i den här rapporten visar dock på att säkerhetsfrågorna behöver vara bredare än att bara handla om enskilda händelser.

Vi bör ta tillvara på det ökade fokuset på säkerhetsfrågor och vi måste lära oss av de incidenter som skett. Vi har en möjlighet att agera nu och minska gapet mellan digitaliseringen och säkerhetsarbetet. Vissa organisationer har precis påbörjat sin resa mot ett systematiskt och riskbaserat informationssäkerhetsarbete, medan andra kommit betydligt längre. Jag är dock övertygad om att samtliga, oavsett nuvarande nivå, kan stärka sin förmåga ytterligare på det här området. Jag är också övertygad om att vi kommer att behöva hjälpas åt för att stärka samhällets förmåga och motståndskraft, inte minst i ljuset av det pågående totalförsvarsarbetet. Min förhoppning är att svenska organisationer genom den här och andra publikationer på området får den kunskap som behövs för att kunna agera och stärka sitt informations- och cybersäkerhetsarbete. Genom detta kommer vi alla att kunna bidra till ett säkert digitaliserat Sverige.

Stockholm, 2022-01-15

Åke Holmgren
Avdelningschef, Avdelningen för cybersäkerhet och säkra kommunikationer
Myndigheten för samhällsskydd och beredskap

Innehåll

Begreppsförteckning

Detta kapitel innehåller de begrepp som är centrala för rapporten. I denna rapport avses med

Allriskperspektiv: 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.

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

Halvledare: Halvledare utgörs av material vars elektriska ledningsförmåga är mellan ledares och isolatorers. På grund av detta kan de användas som små strömbrytare i datorchip – och är därför fundamentala för modern elektronik.

Incident: En inträffad oönskad händelse. Vid incidentrapportering delas orsak 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, etc.)

Konfidentialitet: En aspekt av informationssäkerhet som kort innebär att endast behöriga kan ta del av informationen.

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

Riktighet: En aspekt av informationssäkerhet som kort innebär att vi kan lita på att informationen är korrekt och inte manipulerad eller förstörd.

Utpressningsvirus/-program: (eng. Ransomware) virus som krypterar hela eller delar av en verksamhets information som lagras på drabbade informationssystem och gör informationen otillgänglig. Oftast ställs krav på lösensumma för att (påstått) få tillbaka informationen och/eller undvika att informationen blir offentliggjord.

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

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

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

Sammanfattning

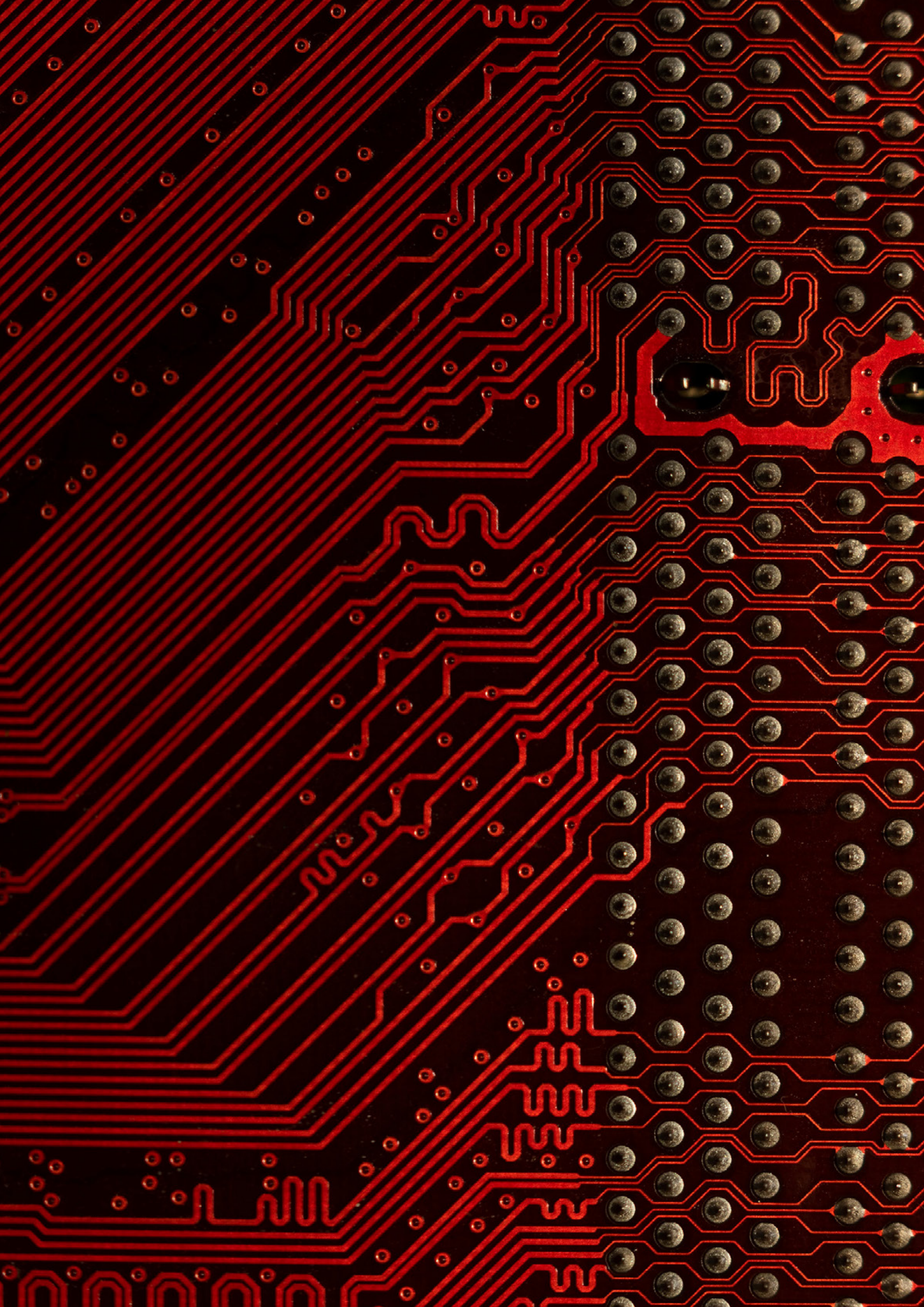
Digitaliseringen och sammankopplingen av allt fler informationssystem och infrastrukturer är på många sätt positiv men bidrar även till nya eller förändrade sårbarheter och hot som riskerar att få konsekvenser på både organisations- och samhällsnivå. Under 2021 har detta blivit extra tydligt genom bland annat en fortsatt förflyttning av arbetsplatsen till hemmet, ett ökat beroende av digitala produkter samt flera angrepp och misstag som orsakat märkbara konsekvenser. Alla dessa händelser har bidragit till att rikta blicken mot gapet mellan den takt i vilken digitaliseringen respektive säkerhetsarbetet sker vilket har lett till både ett ökat fokus och stora satsningar på området.

Denna årsrapport har sin grund i den it-incidentrapportering MSB mottar från både statliga myndigheter och från leverantörer av samhällsviktiga och digitala tjänster. Rapporten riktar sig främst till beslutsfattare, informations- och säkerhetsansvariga samt omvärldsbevakande och analyserande roller hos både statliga myndigheter och NIS-leverantörer. Innehållet kan även vara värdefullt för motsvarande roller hos andra organisationer. Årsrapporten, tillsammans med en sammanställning av inrapporterade it-incidenter, överlämnas även till regeringen i enlighet med myndighetens instruktion.

Rapporten innehåller förutom sammanställning av de incidenter som inkommit till MSB även lärande exempel, information om incidentrapporteringen och rekommendationer till rapportens målgrupper. Sammanställningen av incidentrapporteringen under 2021 visar att rapporteringen har minskat och att systemfel och misstag återigen är de mest frekventa orsakerna till incidenterna. Incidenterna inträffar ofta vid misslyckad förändringshantering och påverkar oftast tillgängligheten.

För att motverka de bakomliggande problemen till de incidenter som rapporterats rekommenderas att se över:

- Rutiner för förändringshantering.
- Kontinuitetsplaner.
- Informationstillgångar och deras beroenden.
- Hur utvecklingsarbete ger säkra system.
- Information om digitala leveranskedjor.
- Arbetet med incidenter.



Ett år av förändring

Världen är sedan länge sammankopplad på ett sätt som fördjupas för varje år som går. Det senaste året har inte varit något undantag. Även om digitaliseringen och sammankopplingen av allt fler informationssystem och infrastrukturer på många sätt är positiv bidrar den även till nya eller förändrade sårbarheter och hot som riskerar att få konsekvenser, inte bara för enskilda organisationer, utan också för hela samhällets säkerhet. Under 2021 har samhällets beroende av digitala produkter och deras leveranskedjor aktualiserats. Ju mer samhället digitaliseras, desto större beroenden till underleverantörer av produkter och tjänster. Under pandemin har det också blivit extra tydligt hur beroende organisationer är av att deras underleverantörer skyddar sin information tillräckligt så att deras produkter och tjänster levereras på avtalat sätt. Pandemin har även förstärkt en utveckling som var på gång redan innan där många arbetsplatser, genom att öka distansarbetet, förlagt hela eller delar av arbetet utanför organisationens lokaler.

Två typer av hot som har fått stor uppmärksamhet under det gångna året är utpressningsvirus och angrepp mot digitala leveranskedjor.[1] Angreppen mot Colonial Pipelines i USA den 7 maj, mot Kaseya den 2 juli och mot Kalix kommun den 16 december är exempel på uppmärksammade utpressningsvirusangrepp. Angreppet mot Kaseya, är även ett exempel på ett angrepp mot en digital leveranskedja precis som angreppet mot företaget SolarWinds, vars efterverkningar fick stor påverkan under årets början.

Angreppet mot Kaseya

Den 2 juli 2021 uppstod störningar i kassasystemet hos bland annat dagligvarukedjan Coop, Apotek Hjärtat, SJ och ST-1. Störningarna hindrade butikerna från att kunna ta betalt av sina kunder. Snart hade runt 800 Coop-butiker fått stänga ned i stora delar av landet medan systemen uppdaterades manuellt på plats i butik. Dagen efter störningarna upptäcktes och bekräftades det att de orsakats av ett angrepp. Angreppet hade inte riktats direkt mot de drabbade svenska företagen. Angreppet hade inte heller riktats direkt mot leverantören av tjänsten för betalningarna, Visma Esscom. Angreppet hade i stället riktats mot det amerikanska mjukvaruföretaget Kaseya.

MSB:s hantering inleddes i ett tidigt skede och inkluderade bedömning av tillgänglig teknisk data för att kunna vidta nödvändiga åtgärder. Därefter togs kontakter med drabbade verksamheter för att erbjuda tekniskt stöd i deras respektive hantering av händelsen. MSB hade löpande samverkan med motsvarande funktioner i andra länder samt svenska cybersäkerhetsmyndigheter för att sprida och ta emot information och kontakter. Den tekniska hanteringen, förstärkt av ett antal mediekontakter och rekommendationer kring lämpliga skyddsåtgärder, bidrog till att den del av angriparnas infrastruktur som stod i Sverige togs ner.

1. För mer information om hot mot digitala leveranskedjor se rapporten Hoten mot de digitala leveranskedjorna – 50 rekommendationer för att stärka samhällssäkerheten (länk: https://rib.msb.se/filer/pdf/29829.pdf)

Det är dock inte bara angrepp som orsakat uppmärksammade incidenter under det gångna året. Misstag hos företaget Fastly orsakade att många hemsidor världen över blev otillgängliga under delar av dagen den 8 juni och misstag under ett uppdateringsarbete hos Facebook ledde till att tjänster så som Facebook, Instagram och Whatsapp inte kunde användas under flera timmar den 4 oktober.

Även naturhändelser har lett till omfattande konsekvenser. Exempel på detta är när jordbävningar i Japan, snöoväder i Texas och uteblivet monsunregn i Taiwan utgjorde några av många orsaker som bidrog till en omfattande brist på halvledare. En brist som i sin tur ledde till förhöjda priser på elektronik och produktionsstopp i bland annat fordonsindustrin.

Alla dessa händelser har bidragit till att rikta blicken mot gapet mellan den takt i vilken digitaliseringen respektive säkerhetsarbetet sker. Detta gäller inte minst i vilken utsträckning informationssystem är beroende av andra informationssystem och infrastruktur för att fungera, det vill säga sammankopplingen och sårbarheten hos de digitala leveranskedjorna. Ett ökat fokus mot och förståelse för sårbarheter i digitala leveranskedjor har bidragit till stora satsningar på området. USA har lagt fram förslag på stora satsningar på inhemsk infrastruktur och halvledarproduktion och i maj lades en presidentorder fram för att öka cybersäkerheten i nationen. I EU lades det i september fram ett motsvarande förslag för att minska Europas beroende till omvärlden gällande halvledarproduktion.

Den nya långtidsbudgeten inom EU innehåller stora satsningar på bland annat säker digitalisering och cybersäkerhet. De två ramprogrammen DIGITAL och Horizon Europe kommer under kommande år utlysa medel för satsningar inom stärkt cybersäkerhet, stärkt försvar för samhällsviktig verksamhet, men också till uppbyggnad av säker kommunikation. En effekt man vill uppnå är ökad innovation och en stor del av stöden kommer gå till små och medelstora företag.

Förutom ekonomiska satsningar för att stärka informations- och cybersäkerheten har flera länder och mellanstatliga samarbeten publikt pekat ut ansvariga för flera av den senaste tidens uppmärksammade angrepp, i en utsträckning som inte skett tidigare. Angreppet mot Microsoft Exchange under början på året där sårbarheter utnyttjades för att få behörighet till och stjäla information från eller orsaka skada i mejlservrar pekades initialt ut av Microsoft att ha kopplingar till Kina. Senare pekade talespersoner från USA, Storbritannien, NATO och EU officiellt ut, att det var grupperingar med kopplingar till kinesiska staten som genomförde angreppet. Även i fallet med angreppet mot SolarWinds pekade USA och Storbritannien under våren ut en ansvarig nation, i detta fall Ryssland, mot vilka man även införde sanktioner. I båda fallen har de utpekade ansvariga nationerna nekat till anklagelserna. Att peka ut ansvariga för angrepp inom cyberområdet[2] på detta sätt kan ses som ett tecken på den ökade konkurrensen och spänningen som utvecklats inom cyberområdet. Det har även förts dialoger om att etablera gemensamma normer inom cyberområdet, något som länge saknats.

2. Vem som attribuerar, och under vilka former, är eventuellt också under förändring. Med anledning av den senaste tidens våg av ransomware, och statsunderstödda aktörers cyberangrepp, har Lloyds, en världsledande försäkringsmarknadsplats, meddelat att cyberförsäkringar inte längre bör täcka kostnader för vare sig staters vedergällnings-cyberangrepp, eller för cyberangrepp som resulterar i storskaliga negativa effekter för stater. För att kunna avgöra när försäkringsbolag ska vara undantagna från att behöva betala kostnaderna för incidenter med hänvisning till ovanstående föreslår man att försäkringsbolag själva ska kunna attribuera, om inte statsaktörer gör det själva inom en viss tid. Se exempelvis: Lloyd's of London suggests insurers should not cover 'retaliatory cyber operations' between nation states, Gareth Corfield, the Register, 2021-11-30. Länk: https://www.theregister.com/2021/11/30/lloyds_london_cyber_insurance_clauses/ (hämtad 2021-12-01)

Sårbarheterna i Microsoft Exchange-mejlservrar

Under början av 2021 upptäcktes ett antal sen tidigare okända sårbarheter i lokalt installerade mejl-servrar från Microsoft. Sårbarheterna innebar att obehöriga aktörer kunde ta kontroll över mejlservern och få höga behörigheter. Sårbarheterna och de följande angreppen som utnyttjade dem påverkade användare över hela världen, i såväl privata som offentliga verksamheter.

Allt eftersom mer information framkom och angreppsmetoderna ändrades publicerade MSB regelbundna uppdateringar kring sårbarheterna och rekommendationer kring lämpliga åtgärder för att förhindra att svenska organisationer skulle drabbas av skadlig inverkan på deras it-miljöer. Information delades i ett antal webbartiklar och genom blixtmeddelanden till it-personal runtom i Sverige när rapporter inom att sårbarheterna utnyttjades aktivt av angripare. MSB har även under året varit i kontakt med svenska organisationer som drabbats av omfattande driftstörningar, och i vissa fall även utpressningsvirus, som en följd av sårbarheterna och erbjudit tekniskt stöd till dessa. Sårbarheterna är fortsatt aktuella i MSB:s hantering. Operativ samverkan har skett såväl nationellt som internationellt. Sunet, det svenska universitetsdatanätverket har bistått med regelbundna skanningar av den svenska ip-miljön efter sårbara installationer och delat resultaten med MSB för vidare hantering och analys.

För att ytterligare bemöta cyberrelaterade incidenter har man inom EU arbetat vidare med både ett koncept för en sammanslutning av europeiska Security Operations Center (SOC) och en Joint Cyber Unit (JCU). I december 2020 presenterade kommissionen ett förslag till nytt direktiv, NIS2, som ska ersätta nuvarande NIS-direktiv. NIS-förslaget innehåller bland annat skärpta krav på informationssäkerhetsarbete och incidentrapportering. Förslaget innebär också att fler verksamheter och sektorer kommer att omfattas av NIS-regleringen. För närvarande pågår trilogförhandlingar om NIS2-förslaget mellan Europeiska unionens råd, Europaparlamentet och Europeiska kommissionen. Ännu är det för tidigt att säga hur dessa förslag kommer att påverka cybersäkerheten i europeiska unionen. Frågor om cybersäkerhet är både aktuella och viktiga för EU som union och för Sverige som medlemsland, inte minst inför Sveriges stundande ordförandeskap under det första halvåret 2023.

För att ytterligare stärka europeisk forskning och innovation inom området har det europeiska kompetenscentrumet för cybersäkerhet (ECCC) inrättats i Bukarest. Kompetenscentrumet kommer att leda ett europeiskt nätverk av nationella samordningscenter som inrättas i varje medlemsstat. I det gemensamma uppdraget ingår att bygga upp en europeisk kompetensgemenskap av behovsägare och utförare av cybersäkerhetsforskning och innovationer samt främja och genomföra cybersäkerhetsutlysningar inom ramen för Horizon Europe och DIGITAL Europe. Den andra september fick MSB regeringens uppdrag att förbereda inrättandet av Sveriges del i nätverket i form av det nationella samordningscentret för forskning och innovation inom cybersäkerhet. Målsättningen är att det nationella samordningscentret ska invigas under andra kvartalet 2022.

Under året har även det nationella cybersäkerhetscentrets verksamhet tagit form efter det formella beslutet i slutet på 2020 om att det ska inrättas. Bland annat har en rapport om erfarenheterna från pandemin släppts, en konferens har hållits och den första personalen har rekryterats.

Inom ramen för totalförsvarsarbetet, publicerade Försvarsmakten och MSB under hösten den gemensamma rapporten Handlingskraft[3] som är en samlad plan för ett starkare totalförsvar. I denna uppmärksammas vikten av informations- och cybersäkerhet genom att ”stärkt informations- och cybersäkerhet” utpekades som ett av sex fokusområden[4] för arbetet perioden 2021 till 2025. Arbetet med fokusområdet bedrivs av Försvarsmakten och MSB tillsammans med beredskapsansvariga myndigheter.

I samhället i stort och i media har också vikten av stärkt informations- och cybersäkerhet uppmärksammats, inte minst genom angreppet mot Kalix kommun och det tidigare nämnda angreppet som bland annat drabbade butikskedjan Coop. Händelserna lyfte upp informations- och cybersäkerhet på agendan och påverkade människors vardag på ett påtagligt sätt. Vikten av att digitalisera säkert och ha alternativ om ordinarie informationssystem inte fungerar är något som berör alla, från samhällsnivå till enskilda medborgare i deras vardag.

3. https://www.msb.se/contentassets/323649d6eb8440f7abbd421fc0874094/handlingskraft.pdf
4. Fokusområdena är ett antal områden som initialt bör prioriteras i planeringen för att öka förmågan och bidra till att uppnå det övergripande målet för totalförsvaret. Dessa områden är Beredskapsplaner och krigsorganisation, Ledning och samverkan, Försörjningsberedskap, Ge och ta emot stöd, Försvarsvilja, och Stärkt informations- och cybersäkerhet.

Exempel på misstag

En portal som tillhandahålls av en myndighet hade inte uppdaterats under en månads tid, trots att datumet för senaste uppdatering hade ändrats. Portalen används för datauttag och används av tredje part. Under den aktuella perioden kunde myndigheten inte tillhandahålla aktuell information till användare, det vill säga att det inte var den senast uppdaterade informationen som visades i systemet. Informationen i portalen används i bland annat beslutsunderlag hos olika offentliga aktörer.

Rekommendation

Man bör se till att alla förändringar i it-miljön speglas i interna verifieringsrutiner, så att det kan säkerställas att alla förändringar genomförts på ett tillfredsställande sätt och enligt de förväntningar som ställts upp. På så sätt kan eventuella avvikelser uppdagas i ett tidigt skede, så att informationen återställs och återges på ett korrekt sätt. Detta bör även kombineras med eventuella utbildningsåtgärder för att förhindra att liknande problem uppstår framgent. Se även till att det finns en ansvarig för att förändringar i it-miljön sker korrekt och fullständigt och av behörig personal, antingen inom den egna organisationen eller specificerat hos leverantören.

Om rapporten och incidentrapportering

Årsrapporten grundar sig i den it-incidentrapportering MSB mottar från både statliga myndigheter och från leverantörer av samhällsviktiga och digitala tjänster (NIS-leverantörer).[5] För att sätta incidentrapporteringen i en kontext bygger årsrapporten även på information från övriga informationskällor så som löpande omvärldsbevakning, dialoger med offentlig och privat sektor och de svar som mottagits inom ramen för Infosäkkollen.[6] Genom att analysera informationen utifrån ett allriskperspektiv ger detta en övergripande bild över samhällets informations- och cybersäkerhet. På samhällsnivå är kännedomen om allvarliga incidenter avgörande för att skapa förståelse, mildra konsekvenserna och öka skyddet. I kombination med andra rapporter och vägledningar som publiceras av både MSB och andra myndigheter[7] bidrar årsrapporten till att svenska organisationer har tillgång till information och stöd för att kunna bedriva sina verksamheter med tillräckligt god informations- och cybersäkerhet.

Årsrapporten riktar sig främst till beslutsfattare, informations- och säkerhetsansvariga samt omvärldsbevakande och analyserande roller hos både statliga myndigheter[8] och NIS-leverantörer. Beskrivningarna av de incidenter som inträffat, hot, sårbarheter, konsekvenser och rekommendationer kan även vara värdefulla för motsvarande roller hos de flesta organisationer. Årsrapporten, tillsammans med en sammanställning av inrapporterade it-incidenter, överlämnas även till regeringen i enlighet med myndighetens instruktion.

För att kunna sammanställa en övergripande bild, är incidentrapporteringen som görs till MSB mycket viktig. När information om it-incidenter hos både statliga myndigheter och NIS-leverantörer sammanställs på ett jämförbart sätt ger det möjlighet att identifiera trender och dra slutsatser om samhällets informations- och cybersäkerhet. Informationen i rapporterna ingår därför som en del i det strategiska analysarbete MSB bedriver och som ett underlag till att inrikta myndighetens eget och andras arbete på området.

Utöver krav på att rapportera it-incidenter ska statliga myndigheter och NIS-leverantörer tillse att incidentrapporteringen är en del i arbetet med att identifiera, bedöma, åtgärda och utreda orsaken till inträffade incidenter i organisationens

5. MSB har sedan 2018 publicerat en årsrapport för statliga myndigheters it-incidentrapportering och sedan 2021 en årsrapport för den it-incidentrapportering MSB mottar från leverantörer av samhällsviktiga och digitala tjänster. För att ta ett bredare grepp på samhällets samlade informations- och cybersäkerhet görs detta nu som en rapport baserad på båda typerna av it-incidentrapportering. En separat fördjupningsrapport som enbart fokuserar på incidentrapporteringen från samhällsviktiga och digitala tjänster kommer fortfarande att göras.
6. Infosäkkollen är ett verktyg som stödjer uppföljning och förbättring av systematiskt informationssäkerhetsarbete i kommuner, regioner och statliga myndigheter. Läs mer på https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/infosakkollen/.
7. Exempelvis de årsrapporter och hotbeskrivningar som publiceras av Försvarets radioanstalt (FRA), Militära underrättelse- och säkerhetstjänsten (MUST) och Säkerhetspolisen.
8. Inklusive de sex sektoriella tillsynsmyndigheter som har i uppdrag att bedriva tillsyn av de identifierade leverantörerna av samhällsviktiga och digitala tjänster i de respektive sektorerna. Dessa är Energimyndigheten, Finansinspektionen, Inspektionen för vård och omsorg, Livsmedelsverket, Post- och telestyrelsen samt Transportstyrelsen.

informationssäkerhetsarbete. Genom att rapportera it-incidenter till MSB kan organisationer få stöd i arbetet med att återställa verksamheten.

Incidentrapporteringen ger MSB möjlighet att se vilket behov av olika stöd som finns och att kunna ta fram detta. Därmed hjälper de som rapporterar incidenter också andra och är med och skapar ett mer robust samhälle där man själv kan få bättre hjälp. För att få ett så ändamålsenligt underlag som möjligt, är det inte bara viktigt att samtliga incidenter som omfattas av rapporteringsplikten rapporteras in men även att incidentrapporterna håller god kvalitet. Ett mer robust samhälle är av stor vikt för totalförsvaret och innebär även att vi står bättre rustade och stärker det civila försvaret.

MSB:s uppgift inom Sveriges informations- och cybersäkerhet

MSB arbetar för att minska sårbarheterna och stärka motståndskraften mot hot, på alla nivåer i samhället. Den roll MSB har inom området är att:

- samordna arbetet med samhällets informations- och cybersäkerhet
- stödja det systematiska arbetet
- förebygga och hantera it-incidenter
- tillhandahålla säkra elektroniska kommunikationer med tillhörande tjänster
- utveckla och förvalta ledningsplatser.

I detta ingår bland annat att rapportera till regeringen om förhållanden i samhällets informations- och cybersäkerhet som kan innebära att åtgärder behöver vidtas.

Vem ska rapportera, och vad ska rapporteras

Förutom fördelarna för både samhället och den egna organisationen med att rapportera it-incidenter så har vissa organisationer krav på sig att rapportera. Rapporteringskraven varierar beroende på vilken reglering som organisationen berörs av. De organisationer som har krav på sig att rapportera it-incidenter till MSB är statliga myndigheter och leverantörer av samhällsviktiga och digitala tjänster. Ibland kan en och samma it-incident behöva rapporteras till flera olika myndigheter och ibland ska det bara rapporteras till en. Det är exempelvis viktigt att anmäla en incident till Polismyndigheten om det rör sig om en brottslig gärning och får incidenten sådan påverkan på personuppgifter att den är rapporteringspliktig enligt dataskyddsförordningen (GDPR) ska den rapporteras till Integritetsskyddsmyndigheten. Incidenten ska rapporteras till Säkerhetspolisen, och i vissa fall även till Försvarsmakten, om det rör sig om en incident som faller under rapporteringsskyldigheten enligt säkerhetsskyddsförordningen. MSB uppmanar alla organisationer att se över vilka rapporteringskrav en it-incident kan påverkas av så det är tydligt för organisationen när en rapporteringspliktig it-incident har inträffat och hur den ska hanteras.

För statliga myndigheter

Vilka it-incidenter som ska rapporteras och vilka statliga myndigheter som ska rapportera regleras i krisberedskapsförordningen.[9] MSB har genom förordningen mandat att utfärda föreskrifter som ytterligare förtydligar vilka it-incidenter som ska rapporteras och hur rapporteringen ska gå till. Detta görs i MSB:s föreskrifter om statliga myndigheters rapportering av it-incidenter.[10]

9. Förordningen om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (2015:1052).
10. MSBFS 2020:8.

Exempel på angrepp

En kommun har med hjälp av en it-leverantör utrett följderna av ett eventuellt intrång i Microsoft Exchange till följd av sårbarheterna i lösningen som publicerades i mars 2021. Programvaran var säkerhetsuppdaterad till den senaste versionen men attackförsök hade gjorts mot webappen som ger tillgång till olika Microsoft-program på mobila enheter. Inga webshells eller bevis på aktivitet efter attackförsöken hittades. En forensisk utredning inleddes och it-avdelningen genomförde en rad åtgärder, bland annat lösenordsbyten hos alla användare med administrationsbehörighet, utökad loggning av inkommande trafik samt översyn av hårdvara i systemet. Verksamheten påverkades inte nämnvärt under incidenten, endast en mindre störning inträffade i samband med att sårbarheten lagades.

Rekommendation

Den aktuella kommunen vidtog ett antal korrekta åtgärder för att säkra sin it-miljö till följd av händelsen, samt för att mildra konsekvenserna om liknande störningar uppstår igen. Såväl tekniska insatser som informationsinsatser sattes in för att säkra system och parallellt utbilda anställda om vikten av cyberhygien som att skydda lösenord, hur känslig information bör delas, och så vidare. Vidare är rekommendationen att se över de skyddslösningar och kontrollsystem som används i it-miljön för att säkerställa att tillräckligt skydd är installerat i alla led.

För att en incident ska vara rapporteringspliktig krävs förutom att myndigheten omfattas av rapporteringsplikten att incidenten:

- påverkat riktigheten, tillgängligheten eller konfidentialiteten hos den information som bedömts ha behov av utökat skydd,[11]
- inneburit att informationssystem som behandlar information som bedömts ha behov av utökat skydd inte kunnat upprätthålla avsedd funktionalitet,
- påverkat myndighetens förmåga att utföra sitt uppdrag, eller
- övrigt allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller i tjänster som myndigheten tillhandahåller åt en annan organisation.

Samtliga statliga myndigheter under regeringen omfattas av kravet på rapportering förutom Regeringskansliet, kommittéväsendet, Säkerhetspolisen, Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt och Totalförsvarets forskningsinstitut. För utlandsmyndigheterna tillämpas bestämmelserna endast i den utsträckning som bestäms i föreskrifter som meddelas av Regeringskansliet genom utrikesdepartementet.

Rapporteringen till MSB sker vid två tillfällen.

- Inom sex timmar från att myndigheten identifierat att en incident är rapporteringspliktig ska myndigheten underrätta CERT-SE vid MSB om incidenten via telefon 010-240 40 40.
- Inom fyra veckor från det första rapporteringstillfället ska en slutgiltig incidentrapport lämnas utifrån incidentrapporteringsformuläret.[12]

För leverantörer av samhällsviktiga och digitala tjänster

NIS-direktivet som antogs av EU år 2016 syftar till att höja nivån av säkerhet i nätverk och informationssystem som anses vara centrala för medlemsstaternas och den inre marknadens funktion. I Sverige har direktivet implementerats genom lagen respektive förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster.[13] MSB har genom dessa mandat att utfärda föreskrifter gällande identifiering och anmälan av leverantörer av samhällsviktiga tjänster, informationssäkerhet och incidentrapportering.[14]

För att en incident ska vara rapporteringspliktig krävs att:[15]

- störningen haft sitt ursprung i ett nätverk eller informationssystem
- leverantören är rapporteringspliktig
- incidenten orsakat en störning med betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten.

11. Bedömningen av om informationen är i behov av utökat skydd ska ske genom informationsklassning enligt 6 § p.1 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).
12. Tillgänglig på msb.se.
13. SFS 2018:1174 & 2018:1175.
14. MSBFS 2018:7, 2018:8, 2018:9, 2018:10 & 2018:11.
15. För ytterligare detaljer kring vilka incidenter som ska rapporteras se MSBFS 2018:9, 2018:10 & 2018:11 samt Vägledning för ifyllande av incidentrapporteringsformulären för samhällsviktiga respektive digitala tjänster som finns tillgängliga på msb.se.

De organisationer som omfattas av rapporteringskraven är de som är leverantörer av samhällsviktiga tjänster och digitala tjänster. Leverantörer av samhällsviktiga tjänster finns inom följande sektorer:

- bankverksamhet
- finansmarknadsinfrastruktur
- transport
- leverans och distribution av dricksvatten
- digital infrastruktur
- hälso- och sjukvård
- energi.

Begreppet leverantörer av digitala tjänster omfattar:

- Internetbaserade marknadsplatser.
- Internetbaserade sökmotorer.
- Molntjänster.

Incidentrapporteringen genomförs vid tre tidpunkter:[16]

- Inom sex timmar från att leverantören har identifierat att en incident är rapporteringspliktig ska leverantören underrätta CERT-SE vid MSB om incidenten via telefon 010-240 40 40.
- Inom 24 timmar från det att leverantören har identifierat att en incident är rapporteringspliktig ska skriftlig rapportering lämnas utifrån det första och andra skedet i incidentrapporteringsformuläret.
- Inom fyra veckor från det första rapporteringstillfället ska skriftlig rapportering lämnas utifrån det tredje skedet i incidentrapporteringsformuläret.

En incident har inträffat!

Om en it-incident konstateras är det viktigt att organisationen vidtar åtgärder för att minska konsekvenserna av incidenten i enlighet med det arbetssätt organisationen har valt. Om incidenten dessutom konstateras vara rapporteringsskyldig till MSB ska CERT-SE kontaktas på anvisat sätt. I vissa fall kan det vara lämpligt att även vända sig till CERT-SE för att få stöd i att bedöma om en incident är rapporteringspliktig eller inte. Alla organisationer som bedömer att de behöver stöd med att vidta lämpliga åtgärder vid en it-incident vända sig till CERT-SE för stöd, oavsett om det handlar om en rapporteringspliktig incident eller inte. All känslig information som rapporteras till CERT-SE omfattas av sekretess.[17]

Vid en inledande kontakt med CERT-SE kommer ett antal frågor att ställas så som:

- Vad har hänt?
- Hur och när upptäcktes problemet?
- Vilka parter är inblandade i incidentarbetet?
- Finns det en brottsmisstanke och har en polisanmälan upprättats?
- Finns det behov av stöd från CERT-SE och kontaktvägar för detta?

16. Varje skede har ett tillhörande frågeformulär tillgängligt på msb.se/NIS.
17. Med stöd av 18 kap 8 § 3 p. i offentlighets och sekretesslagen (2009:400). Tillämpningen har prövats flera gånger i Kammarrätten, där domsluten stöder MSB:s ställningstagande till sekretessbedömningen. Se bland annat dom från Kammarrätten i Göteborg, mål nr 5032-16.

CERT-SE

Den operativa incidenthanteringen vid MSB bedrivs av CERT-SE, Sveriges nationella CSIRT (Computer Security Incident Response Team). Uppgiften är att stödja samhället i arbetet med att hantera och förebygga it-incidenter. Detta görs bland annat genom att sprida information, samordna åtgärder och genom att avhjälpa eller lindra effekter av incidenter. CERT-SE samverkar även med andra myndigheter och är kontaktpunkt gentemot motsvarande funktioner i andra länder. Vid extra akuta eller allvarliga sårbarheter, hot eller incidenter kan information också skickas direkt till berörda parter.

Under 2021 publicerade CERT-SE 141 webbartiklar med information gällande sårbarheter, hot och risker med tillhörande rekommendationer. Utöver dessa publiceringar har blixtmeddelanden om brådskande incidenter och/eller sårbarheter skickats ut vid totalt 4 tillfällen. Under året har CERT-SE även kunnat stödja samhället vid flera större uppkomna incidenter. Exempel på dessa inkluderar angreppet mot mjukvaruleverantören Kaseya, som innebar stor påverkan för främst COOP men även Apotek Hjärtat, SJ och ST-1. Vidare hantering och stöd har också erbjudits vid andra större incidenter, bland annat kopplat till sårbarheter i e-posttjänsten Microsoft Exchange och Folkhälsomyndighetens smittskyddsdatabas SmiNet samt även vid angreppet mot den norska it-leverantören Volue som påverkade energisektorn.

Information om sårbarheter och hot samt förslag på åtgärder publiceras löpande på www.cert.se.

Hur känner man igen en incident?

I metodstödet[18] för informationssäkerhet får du hjälp med hur du kan utforma och förbättra din organisations arbete med incidenter. Bland annat beskrivs hur du kan utforma arbetssätt för hur:

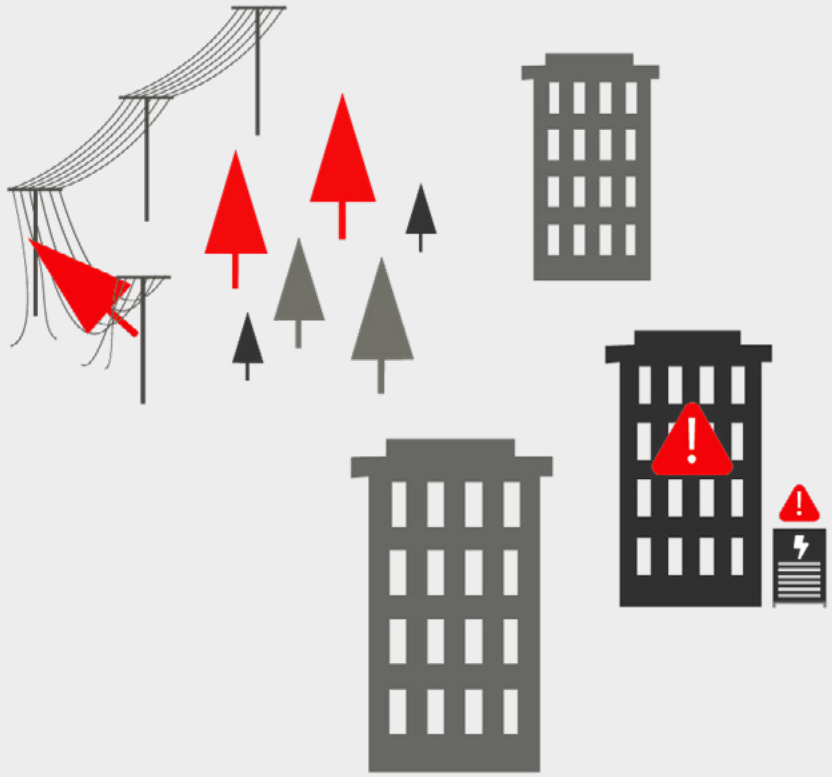
- Misstänkta incidenter anmäls.
- Incidenter bedöms utifrån allvarlighetsgrad och behov av åtgärder.
- Åtgärder för att motverka incidentens negativa påverkan på verksamheten genomförs.
- Utreda orsaken till incidenten och lära av detta.

Hur incidenter ska anmälas och bedömas varierar beroende på organisation. Slutanvändarna behöver kunna bedöma om en onormal händelse uppstår och förstå att det ska anmälas. Sådana bedömningar kan exempelvis grunda sig på om:

- Obehörig misstänks ha eller har fått åtkomst till information.
- Information är felaktigt förändrad.
- Information är inte tillgänglig på det sätt verksamheten kräver.

Därefter tar medarbetare med särskild uppgift att bedöma händelser över för att göra bedömning om händelsen är en incident eller inte. I vissa organisationer görs den första bedömningen av supportorganisationen som dagligen hanterar slutanvändarnas problem. Bedömer supportorganisationen att anmält problem inte är ett vanligt supportärende lämnas det över till incidentorganisationen som bedömer allvarligheten i incidenten och om incidenten behöver åtgärdas för att återfå normal verksamhet. Incidentorganisationen brukar också hålla samman den utredning som görs när verksamheten fungerar normalt igen. Utredningen syftar till att förstå vad som hänt, grundorsaken till incidenten och definiera åtgärder som förhindrar att incidenten återkommer vid senare tillfälle.

18. https://www.informationssakerhet.se/metodstodet/utforma/#incidenthantering-anchor.



Exempel på naturhändelse och systemfel

Ett strömavbrott påverkade tillgången på information och infrastruktur hos en leverantör som levererar it-drift och support till sex kommuner. Kommunernas förvaltningar och bolag drabbades och flera samhällsviktiga verksamheter påverkades i olika grad. Hos en av kommunerna var flera hälso- och sjukvårdssystem otillgängliga under avbrottet, vilket påverkade funktionaliteten för exempelvis trygghetslarm på särskilda boenden, journalåtkomst och signering. Till följd av strömavbrottet ska reservkraft gå igång automatiskt men i detta fall startades inte reservkraften på grund av ett nödstopp som placerats på motorn utlöstes vid start.

Rekommendation

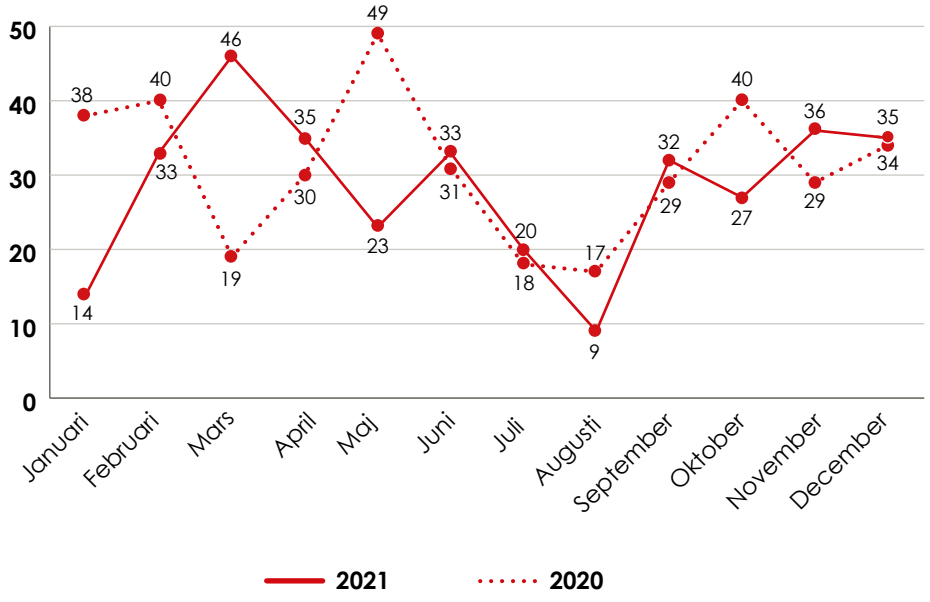
Säkerställ att interna rutiner finns på plats så att all samhällsviktig verksamhet kan erbjudas även vid tillbud som strömavbrott, väderstörningar och så vidare. När det gäller samhällskritisk verksamhet inom exempelvis hälso- och sjukvård är det av yttersta vikt att ha redundanta system tillgängliga som snabbt kan rullas ut vid behov. Se därför till att upphandla redundanta leverantörer, så att man snabbt kan ställa om till en annan aktör om problem med tjänsteleverans eller liknande uppstår, för att minimera samhällsstörningen. Se även över rutiner och dokumentation så att liknande händelser inte inträffar i ett kritiskt läge.

När det gäller externa leverantörer så är det viktigt att upphandla stränga serviceavtal om vilka krav som ställs på tjänsten. Dessa bör inkludera mätbara krav på kostnader, driftsäkerhet, antal fel, hastighet samt incidenthantering.

Rapporterade incidenter under 2021

343 rapporter om it-incidenter inkom till MSB under 2021. Av dessa var 261 rapporter från statliga myndigheter och 82 rapporter från leverantörer av samhällsviktiga och digitala tjänster. Detta kan jämföras med 374 inrapporterade incidenter under 2020 där 286 kom från statliga myndigheter och 88 från NIS-leverantörer.

Diagram 1. Linjediagram med antal inkomna it-incidentrapporter per månad 2020-2021



Vi kan därmed konstatera att antalet rapporterade it-incidenter från både statliga myndigheter och NIS-leverantörer minskat jämfört med tidigare år.

MSB har tidigare konstaterat att det sannolikt sker en underrapportering jämfört med den totala mängd it-incidenter som inträffar och som är rapporteringspliktiga hos berörda organisationer, det vill säga att det är för få it-incidenter som rapporteras.[19] MSB redogjorde redan föregående år för att en orsak till den förhållandevis låga rapporteringsgraden kan ha att göra med restriktionerna på grund av covid-19-pandemin och särskilt rekommendationerna kring hemarbete. Under större delen av 2021 har den offentliga sektorn

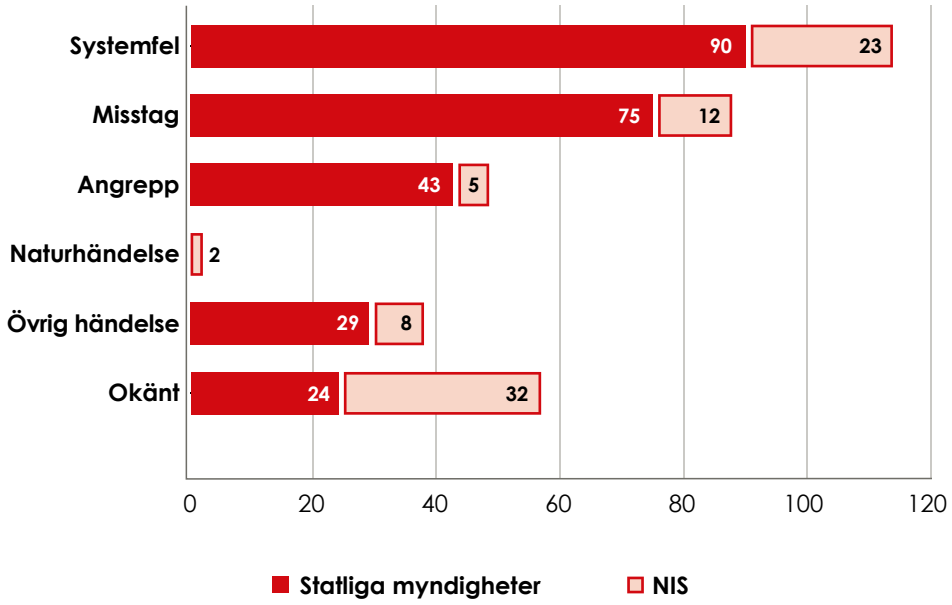
19. Gällande underrapportering hos statliga myndigheter har Försvarets forskningsinstitut tidigare genomfört en undersökning som visar att det är många faktorer som samspelar och bidrar till att rapportering uteblir. För mer information se IT-incidenter på statliga myndigheter. Orsaker till utebliven rapportering, Rapportnummer: FOI-R--4815--SE.

rekommenderats att arbeta hemifrån i så stor utsträckning som verksamheten tillåter. Situationen med utbrett distansarbete har även förekommit inom många delar av det privata näringslivet. En följd av att många arbetar hemifrån kan vara att personal som normalt varit en del i att uppmärksamma och hantera it-incidenter fått förändrade eller utökade arbetsuppgifter, så som att upphandla och drifta it-stöd eller hantera förändrade riktlinjer och arbetsmetoder, kopplat till utökning av användningen av it-stöd för distansarbete. Det kan också vara så att förflyttningen av en del av personalen från den fysiska arbetsplatsen lett till att det funnits färre på plats för att uppmärksamma vissa typer av it-incidenter, särskilt om stödsystem och arbetsrutiner för att hantera sådant på distans inte har utvecklats i samma takt.

Systemfel och misstag orsakade de flesta incidenterna

Den vanligaste rapporterade orsaken till incidenterna har varit systemfel följt av misstag och sedan angrepp. Fördelningen stämmer väl överens med hur det har sett ut de senaste åren där det har varit systemfel och misstag som orsakat de flesta incidenterna. En orsak till att det är just dessa kategorier som orsakar de flesta incidenterna är att system och infrastrukturer blivit både stora och komplexa på ett sätt som gör att det lätt uppstår fel i systemdelar eller vid sammankoppling av systemdelar och misstag vid drift och förvaltning. Detta yttrar sig i rapporteringen genom att rapportören ofta beskriver att det är vid förändringshantering som incidenterna uppstår. Detta vittnar också om att förebyggande informationssäkerhetsarbete så som kartläggning av informationstillgångar, framtagande av processer, metoder och policyer behöver bli mer i linje med den omfattande och komplexa miljö de ska stödja, så att dessa incidenter inte uppstår lika ofta.

Diagram 2. Antal incidenter 2021 fördelade på orsak.

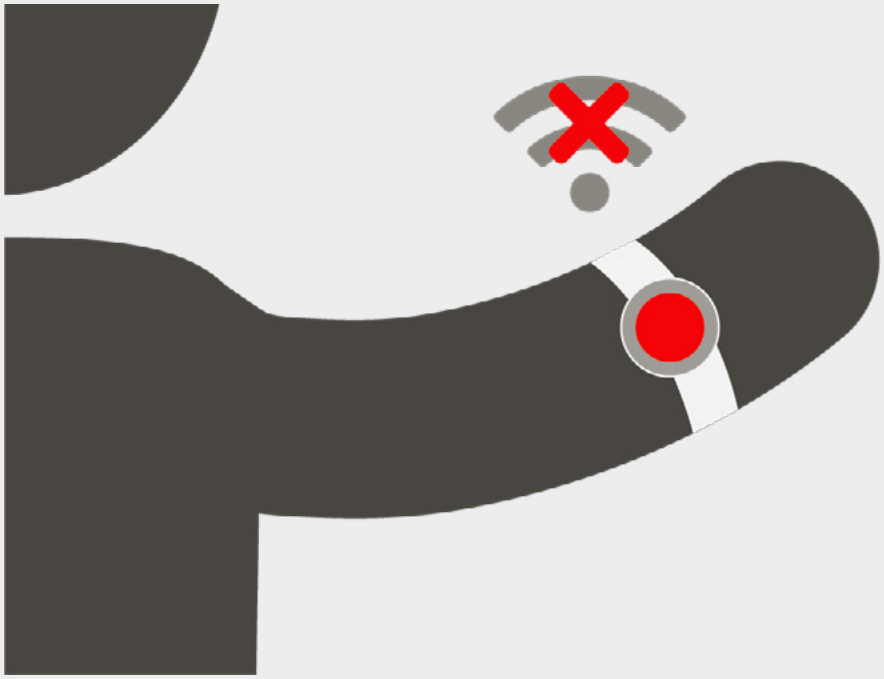


Angrepp är en kategori av it-incidenter som ofta får stor uppmärksamhet i media, och som det rapporterats frekvent om internationellt under det gångna året. Den höga frekvensen av angrepp syns inte i rapporteringen till MSB utan i rapporteringen står istället angrepp för en mindre del av de rapporterade it-incidenterna. Detta är helt i linje med statistiken från tidigare år. En anledning till att det är lätt att tro att angreppens andel av inträffade it-incidenter är större, kan vara att nyhetsmedia fokuserar mer på avsiktliga hot som angrepp än oavsiktliga hot som systemfel och misstag.[20] Det är dock i sammanhanget viktigt att poängtera att frekvensen av angrepp inte säger någonting om hur allvarligt ett enskilt angrepp kan vara och att man bör ta det i beaktande när man genomför sina riskanalyser.

Av de inrapporterade incidenterna med möjligt antagonistiskt ursprung har 27 procent meddelat att de redan har eller ämnar anmäla incidenten till Polismyndigheten. Jämfört med tidigare år för statliga myndigheter visar det att graden av polisanmälan ökat. Gällande incidentrapporter från NIS-leverantörer har rapporteringskravet endast funnits på plats under en begränsad tid så att data finns därför endast för två hela år av NIS-rapportering, med ett lågt antal bedömda angrepp. Således är det svårt att säga något om trenden av polisanmälningar inom kategorin mer än att andelen anmälda angrepp inte nämnvärt avviker från tidigare år.

Andelen incidenter där rapportören inte kunnat fastställa orsaken var 16 procent. Andelen incidentrapporter med okänd orsak är betydligt högre hos NIS-leverantörer. Anledningarna till den höga andelen rapporter där orsaken inte gått att fastställa kan vara flera. Dels kan det handla om att rapportören vid tillfället för rapporteringen enbart hunnit märka av konsekvenserna av incidenten och inte hunnit utreda orsaken, dels kan det handla om att rapportören inte har fått den information som krävs för att kunna avgöra orsaken. Särskilt om incidenten inträffar utanför den egna organisationen, hos en underleverantör vars produkter eller tjänster behövs för att den egna organisationens informa-tionssystem ska fungera, i en så kallad digital leveranskedja kan detta vara extra problematiskt. Av de inrapporterade incidenterna inträffade cirka 40 procent i just den digitala leveranskedjan. Denna fördelning är talande för det globalise-rade samhälle vi lever i där i många fall komplexa och långa kedjor av beroen-den växer fram.

20. För en mer detaljerad genomgång av den publika diskursen om informationssäkerhet se MSB:s rapport Is IT safe? En studie av den publika diskursen av informationssäkerhet i Sverige. MSB1802 – juli 2021 (2021), länk: https://rib.msb.se/filer/pdf/29705.pdf (hämtad 2021-09-21). För en vidare diskussion om hur diskursen och fokus på vissa, snarare än andra, problemområden successivt formas på informations- och cybersäkerhetsområdet, se MSB:s och SIPRI:s rapport Cyber-incident Management: Identifying and Dealing with the Risk of Escalation.SIPRI Policy Paper 55 – september 2020 (2020), länk: https://www.sipri.org/publications/2020/sipri-policy-papers/cyber-incident-management-identifying-and-dealing-risk-escalation (hämtad 2021-09-28).



Exempel på systemfel

Omkring 4 500 trygghetslarm inom äldrevården i en kommun var ur funktion på grund av en driftstörning mellan leverantören och en underleverantör. Larmet är en gsm-baserad lösning som används av kommunen samt privata aktörer inom äldrevården. Användaren aktiverar förbindelse med larmcentral med hjälp av en nödknapp när behov uppstår. Under störningen aktiverades manuella rutiner och extra tillsyn hos vårdtagare gjordes. Kommunen kunde inte se några konsekvenser hos vårdtagare under tiden att tjänsten var otillgänglig.

Rekommendation

I det specifika fallet verkar det som att kommunen hanterade störningen på ett tillfredställande sätt med hjälp av befintliga, manuella rutiner vilket medförde att inga vårdtagare påverkades nämnvärt av störningen med trygghetslarmen. Men generellt är det viktigt för alla verksamheter som levererar samhällskritiska tjänster att upphandla redundanta leverantörer, så att man snabbt kan ställa om till en annan aktör om problem med tjänsteleverans eller liknande uppstår. Det är även viktigt att det finns stränga serviceavtal på plats om vilka krav som ställs på tjänsten. Förutom krav på kostnader, driftsäkerhet, antal fel och hastighet bör incidenthantering vara ett krav. Kraven bör anges så att de blir mätbara.

Incidenterna gör att tjänster blir otillgängliga

I de incidentrapporter där rapportören har kunnat precisera vilken typ av system incidenterna inträffat i har system som används för administrativa uppgifter (kontorssystem) samt system för kommunikation varit de vanligast förekommande för både statliga myndigheter och NIS-leverantörer. Dessa, och de andra, incidenterna upptäcks oftast av egen personal, även om det i vissa fall är andras personal och både egna eller andras tekniska system som upptäcker incidenterna. Att medarbetare uppmärksammar ett problem först gäller för den majoritet av incidenterna som påverkat tillgängligheten. Medarbetare märker att de inte har tillgång till de tjänster, system eller den information de är behöriga till och på så sätt uppmärksammas organisationen om problemet. Medan incidenten pågår kommer organisationens förmåga att utföra sina uppgifter att vara nedsatt eller, i vissa fall, helt borta. Att en stor majoritet av incidenterna på något vis påverkat tillgängligheten är gemensamt för de rapporterade incidenterna från både statliga myndigheter och NIS-leverantörer. Samtidigt har endast en mindre del på något sätt påverkat riktigheten och konfidentialiteten. I rapporteringen från NIS-leverantörerna är dock andelen incidenter som påverkat tillgängligheten ännu större. Det är för att NIS-regleringens rapporteringsplikt endast uppstår om det har skett en störning i tjänsten (d.v.s. att tjänsten inte kan levereras som normalt), och de störningarna visar sig i de flesta fall genom att informationssystem, eller informationen i dem, blir otillgängliga snarare än genom att systemen på olika sätt börjar fungera på ett felaktigt sätt (riktighet) eller blir tillgängliga för obehöriga (konfidentialitet).

Rapporteringen från statliga myndigheter har dock under alla år som incidentrapporter mottagits till största delen också handlat om påverkan på informationssystems eller informations tillgänglighet, även om skillnaderna till framförallt påverkan på konfidentialitet är mindre än för NIS-leverantörer. Det är också viktigt att poängtera att påverkan med avseende på en av de tre informationssäkerhetsaspekterna[21] ibland, i förlängningen, kan resultera i påverkan på en annan informationssäkerhetsaspekt. Ett angrepp eller angreppsförsök som i sig själv egentligen inte orsakar någon direkt påverkan på tillgängligheten, eller någon störning kan snabbt utvecklas till det om organisationen till exempel väljer att helt avaktivera en tjänst för att helt förhindra, eller undvika vidare påverkan på konfidentialiteten eller riktigheten.

Misslyckad förändringshantering är den bakomliggande orsaken till många incidenter

Baserat på den information MSB mottagit förefaller det vara flera hot och sårbarheter som ligger bakom, och i många fall samverkar, för att orsakade incidenter sker. En tydlig sådan bakomliggande orsak är hur förändringar av it-systemen genomförs. Det handlar både om förändringshantering som har genomförts i organisationens egna informationssystem och om förändringshantering som har utförts i informationssystem som upprätthåller tjänster man har utkontrakterat till någon annan organisation.

21. D.v.s. konfidentialitet, riktighet och tillgänglighet.

Effekterna av misslyckad förändringshantering varierar. I vissa fall handlar det om att förändringshanteringen har resulterat i att tjänsten som man försökte uppdatera eller omkonfigurera inte längre fungerar, eller inte fungerar på avsett sätt. I andra fall handlar det om att förändringshanteringen har resulterat i att informationssystemet eller tjänsten som man har justerat inte längre är kompatibel med andra informationssystem eller tjänster som man har. Detta kan då leda till oväntade följdeffekter om man inte har koll på vilka beroenden man har mellan informationssystem i sin it-miljö och informationsinfrastruktur. Brister i förändringshanteringen visar sig extra tydligt när många av dagens it-miljöer är både stora och komplexa med många beroenden både inom och utanför den egna organisationen.

Det finns många faktorer som gör att förändringshantering så pass ofta resulterar i incidenter. Eftersom förändringshantering ofta innebär att tjänsten måste vara nedstängd under arbetets gång försöker organisationer genomföra arbetet under så kort tid som möjligt. Det innebär ofta dels att själva förändringshanteringen sker under stressiga former, dels att utrymmet för att hantera situationen om något går fel är begränsat. Då tidsperioden för att genomföra förändringshanteringen ofta väljs för att påverka så få användare som möjligt sker förändringshantering ofta på natten, vilket i sin tur kan medföra en större trötthet och därigenom risk för misstag bland personalen som utför förändringarna.

En faktor som också kan spela in gällande incidenter vid förändringshantering är att det inte klargjorts och därför råder olika uppfattningar mellan den ansvariga chefen på it-avdelningen (systemägaren) och ansvariga chefen för den verksamhet där tjänsten används för informationsbehandling (informationsägaren) om hur tjänsten ska användas, och vad den får användas till. Det förekommer ändringar som inte förändrar informationssystem eller tjänster sett till hur de är tänkta att användas enligt it-avdelningen, men där följden ändå blir att organisationens förmåga att utföra sitt uppdrag påverkas eftersom tjänsten används på andra sätt än de som it-avdelningen har utgått från. Sådana skillnader mellan tänkta användningsområden och faktiska användningsområden kan uppstå av ett stort antal olika skäl. Det kan handla om att det finns otydlighet i ansvarsfördelning och rutiner hur informationssystem som införs eller förbättras godkänns utifrån att it-avdelningen och användarna redan från början är oense hur en tjänst ska användas. Det kan också handla om att tjänstens användningsområde i praktiken förändras över tid. Lagar och regler som inverkar på hur tjänsten får användas kan även tillkomma eller förändras. För att ett informationssystem ska fungera som tänkt behöver det anpassas till nya förutsättningar och behov.

Det kan också vara så att det saknas något som hade kunnat förbättra utfallet av förändringshanteringen så att en incident hade kunnat undvikas. Ibland saknas det exempelvis en överblick över hur olika informationssystem och tjänster samspelar med varandra i en komplex it-infrastruktur. Ännu svårare blir det om de egna informationssystemen och tjänsterna samspelar med informationssystem eller tjänster hos andra organisationer som man inte har insyn i. Det kan också vara så att förändringshanteringen som ska genomföras handlar om att installera en komponent eller en uppdatering som har levererats av en annan organisation. I dessa fall kan man inte alltid veta hur den nya komponenten eller uppdateringen kommer att fungera i ens egen miljö. Saknar organisationen en tillräckligt produktionslik testmiljö där förändringen kan testas kan konsekvenserna i produktionsmiljön bli stora. En ytterligare möjlig brist är att en del organisationer verkar sakna tillräckligt omfattande rutiner för att genomföra förändringshantering på ett strukturerat sätt som minimerar risken för att något går fel.

Exempel på misstag

Ett register för kommunikationstjänster hos en myndighet var otillgängligt till följd av ett planerat byte av hårdvara. När den nya hårdvaran skulle konfigureras hamnade den i ett icke aktivt läge. Efter knappt tre timmar kunde tekniker aktivera den nya hårdvaran. Den operativa driften hos myndigheten påverkades medan felsökning och felavhjälpning pågick. Systemet används för att hantera information om förbindelser och utrustning och som stöd vid bland annat felsökning, planering och projektering.

Rekommendation

Innan man gör förändringar i sin it-miljö bör se till att de genomförs i en testmiljö som inte påverkar den operativa verksamheten i sin organisation. Man bör även se över sina verifieringsrutiner, så att de genomförda ändringarna överensstämmer med de uppställda förväntningarna på den nya hård-, program- eller mjukvaran. Se även till att utse en person som är ytterst ansvarig för att förändringarna sker korrekt och fullständigt, samt att redundanta rutiner för den operativa verksamheten finns på plats.

Generella rekommendationer vid alla typer av uppdateringar är att skilja på produktionsdata som används löpande i verksamheten, och information som ska lagras för framtida bruk eller ska arkiveras. Backup av produktionsdata och arkiv bör inte finnas på samma ställe, och det är också lämpligt att ha en extra backup på annan fysisk plats om behov skulle uppstå.

Misstag i samband med förändringshanteringen kan bli särskilt problematiska om informationssystemet eller tjänsten som förändras är en tidig del i en längre digital leveranskedja eller påverkar många tjänster. Incidentrapporteringen visar tydligt att informationsdelningen om incidenter brister i sådana kedjor. Det gäller i synnerhet när informationen ska passera från organisationen som har incidenten och vidare genom ett antal andra organisationer innan den kommer till den egna organisationen. Incidentrapporteringen visar att organisationen som rapporterar incidenten där orsaken beror på incidenter som har inträffat flera steg bort i leveranskedjan dels är bristfällig i sitt omfång, dels kommer sent och dels kan ha tolkats och omtolkats ett antal gånger innan den kommer fram. Följderna för organisationer som har beroenden till denna kan bli att det blir svårare att ta beslut om lämpliga åtgärder, men det finns också en risk för att felaktiga beslut tas då informationen som man till slut tar emot är missvisande.

Problemen som uppstår vid förändringshantering blir också ett talande exempel för en större problematik med att säkerhetsarbetet inte sker i samma takt som utvecklingsarbetet. MSB har återkommande lyft gapet mellan digitaliseringen å ena sidan och säkerhetsarbetet å andra sidan. Det är dock inte enbart vid utvecklingsarbete som säkerhetsarbetet inte är tillräckligt utan den säkerhetsskuld som byggts upp är även den något som bidrar till incidenter och som behöver hanteras för att undvika de konsekvenser enskilda organisationer och samhället annars kan drabbas av.

Incidenterna får främst konsekvenser på organisationsnivå

Då tröskeln för när rapporteringsplikt uppstår är lite lägre satt för statliga myndigheter än för NIS-leverantörer finns det en del skillnader i hur det genomsnittligt ser ut i rapporteringen från de två grupperna.

Genomgående handlar det dock om att informationssystem som en följd av incidenter slutar vara tillgängliga för användarna. Från vissa organisationer kommer det återkommande rapporter om samma slags incident, i synnerhet när det handlar om incidenter i informationssystem som upprätthåller en tjänst som har utkontrakterats till någon annan organisation. Det verkar som att vissa organisationer accepterar att de återkommande drabbas av samma slags incident eller av andra orsaker inte kan åtgärda dem.

Incidenterna pågår sällan längre än ett dygn, och skadan som uppstår är oftast begränsad. Däremot förekommer det att organisationers förmåga att utföra sitt uppdrag på ett normalt sätt kan vara negativt påverkad i relativt stor omfattning under den tid som incidenten pågår. De flesta NIS-leverantörer uppger att den samhällsviktiga tjänst de tillhandahåller till största del gick att bedriva under störningarna som incidenten orsakat, även om det finns ett antal incidenter där tjänsten saknade flera funktioner. Det är dock ett antal som uppger att det inte alls gick att bedriva den samhällsviktiga tjänsten under tiden för störningen. Påverkan på den drabbade organisationen blir i dessa fall följaktligen en total eller delvis oförmåga att utföra sitt uppdrag. Något som även i förlängningen påverkar användarna av tjänsten. För statliga myndigheter målas en liknande bild upp av att de flesta incidenter enbart ledde till begränsad påverkan på organisationens verksamhet i stort, även om det i de flesta fall handlar om enskilda tjänster som slutar fungera under en begränsad tid.

Hur organisationer påverkas av incidenter i stort beror på vilken slags verksamhet de bedriver. Verksamheten kan ha mer eller mindre inslag av offentliga eller privata tjänster som berör olika aktörer internt och externt. Organisationen kan även vara beroende av, eller tillhandahålla system som andra organisationer har ett beroende till. Incidenter kan alltså utöver att skapa problem internt inom organisationen, påverka andra organisationer eller flertalet externa användare. Det är relativt vanligt att incidenterna som rapporteras till MSB medför konsekvenser för privatpersoner och, i viss mån, även andra organisationer. Däremot är det mycket ovanligt med gränsöverskridande konsekvenser.

I takt med att allt fler system kopplas samman och får beroenden till andra system eller tjänster kommer konsekvenserna av både incidenterna som sådana men också orsaken bakom incidenterna att kunna få allt större påverkan på samhället då flera viktiga verksamheter kan påverkas samtidigt. Ett exempel på detta är problemen i de globala digitala leveranskedjorna. Globala digitala leveranskedjor, beroenden till informationssystem i flera led där informationssystemen finns i flera olika länder, har bidragit till att förlänga tiden som konsekvenserna av en incident pågår i de fall komponenter, har behövt ersättas då väntetiderna på leveranser när det gäller specifika komponenter, såsom vissa halvledare, är avsevärt högre nu än före pandemin. Ett annat exempel kan vara när en incident inträffar i en organisations system varpå en annan organisations system slutar fungera för att den var beroende av den första organisationens system.

De inrapporterade incidenterna innebär dock endast i undantagsfall en allvarlig påverkan på samhällsnivå. Skälet till det är dock inte att incidenterna inte i sig är allvarliga, utan snarare för att samhället har etablerade sätt att kompensera för incidenter. Om en it-incident exempelvis leder till att viss vård inte kan bedrivas på ett sjukhus så går det ofta att, åtminstone under en tid, bedriva den vården på ett annat sjukhus. På motsvarande sätt kan drabbade individer och organisationer ofta vända sig till andra organisationer när deras förstahandsval har drabbats av en incident.[22] Det finns dock en växande risk i takt med sammankopplingen av olika system och tjänster att påverkan på samhällsnivå kan ske oftare. Särskilt om det inträffar en incident som gör att en tjänst eller produkt som det inte finns några, eller få, alternativ till slutar fungera.

22. Det är framförallt bristen på alternativ som gjorde sommarens angrepp mot Kaseya (som bl.a. drabbade COOP) särskilt allvarligt från ett samhällsperspektiv. På mindre orter finns sällan mer än en butik – och om det dessutom är långt till den närmaste orten där det finns en annan butik så kan det bli svårt för vissa att kompensera för att deras normala butik inte går att tillgå.

Exempel på misstag

En användare vid en myndighet hade felaktigt lagrat en fil med känsliga personuppgifter (bland annat ekonomisk information och bedömningar av ansökningar) på en samarbetsyta med många användare. Ett antal användare hade behörighet att läsa information som lagrades på den aktuella samarbetsytan, vilket innebär att informationen har kunnat nås av användare som inte hade behov av informationen.

Rekommendation

Det är olämpligt att känslig information lagras på en gemensam samarbetsyta som används av flera användare. Det försvårar eventuell spårning av vem som kan ha läst eller på annat sätt tagit del av informationen i den aktuella filen. Känslig information bör krypteras så att endast behöriga användare kan hantera och ta del av den. Rutiner kring vilka typer av filer och information som kan lagras på gemensamma arbetsytor bör sättas upp och en översyn av vilka som har tillgång till olika samarbetsytor bör också göras.

Slutsatser och rekommendationer

Systemfel och misstag är återigen det som orsakar de flesta incidenter som rapporteras till MSB. Incidenterna inträffar dessutom ofta under förändringshantering och resulterar i att de informationssystem, tjänster eller funktioner som påverkas blir otillgängliga under tiden som incidenten fortgår.

Omskrivna incidenter i vår omvärld har dessutom handlat om hur misstag, angrepp eller naturhändelse som drabbar en leverantör inom en digital leverantörskedja kan orsaka vidare incidenter och störningar hos tusentals organisationer. Detta belyser den komplexitet som vårt sammankopplade samhälle har, och som endast ser ut att öka. Liknande komplexitet och interna systemberoenden finns inom de flesta organisationer, där ett system kan vara helt avgörande för ett helt annat systems funktion. En incident, som exempelvis en felaktig uppdatering, eller till och med planerat avbrott kan innebära oväntade fel i helt andra delar av organisationens verksamhet. Det finns därmed ett behov av att öka säkerhetsarbetet och att förbättra arbetet med att kartlägga och hantera beroenden, vare sig de befinner sig helt internt eller någonstans i den digitala leveranskedjan.

Rekommendationerna grundar sig på det MSB kan observera i rapporteringen och även om rekommendationerna baseras på specifika organisationers inrapporterade brister kommer rekommendationerna, om de används, sannolikt minska risken för incidenter även inom andra organisationer.

För statliga myndigheter och leverantörer av samhällsviktiga tjänster finns föreskriftskrav på att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Övriga organisationer kan med fördel följa de föreskrifter och det stöd som MSB erbjuder för att få en säkrare it-miljö. Det är viktigt att arbeta både långsiktigt och förebyggande för att skapa förutsättningar för både färre incidenter och minskade konsekvenser när väl incidenter inträffar. För att kunna åstadkomma detta behöver man regelbundet analysera organisationens behov, krav och risker och vid behov förbättra sina arbetssätt och de säkerhetsåtgärder som behövs för att skydda organisationens information, informationssystem och nätverk.

Se över rutiner för förändringshantering

För att säkerställa att förändringshantering vid planerade förändringar i organisationens it-miljö sker med så liten risk för incidenter som möjligt är det viktigt att innan bedöma de risker som kan finnas och åtgärda dem. Tänk igenom och se till att de som har den kompetens som behövs för att genomföra förändringen finns tillgängliga. Överväg även val av tidpunkt för när förändringen ska

genomföras. Detta för att de som genomför förändringen ska ha så bra förutsättningar som möjligt men också för att ha resurser tillgängliga om någonting skulle gå fel. Inför arbetet är det också viktigt att man etablerar kanaler för hur information delas inom organisationen, och till externa leverantörer i de fall de berörs, så att rätt information når de som berörs i tillräckligt god tid för att deras verksamhet ska påverkas så lite som möjligt.

Se även till att de riktlinjer som finns för hur förändringshantering ska gå till och de rutiner som används vid förändringshantering är tydliga och att man på förhand har kartlagt vilka andra tillgångar som kan komma att påverkas av förändringen samt vad man ska göra om förändringen inte går som man hade tänkt.

Se över kontinuitetsplaner

Det är inte realistiskt att prata om en noll-vision gällande it-incidenter. Hur väl man än förbereder sig behöver man vara förberedd på att incidenter kan inträffa. Organisationer behöver därför ha ett utvecklat kontinuitetshanteringsarbete. Detta innebär i korthet att ha en kontinuitetsplan, en dokumenterad plan B, både för att återställa information, informationssystem och nätverk samt tydliggöra de alternativa arbetssätt som verksamheterna ska använda för att hantera de störningar incidenten medför.

Genom att utveckla kontinuitetsplaner kan man mildra konsekvenserna av inträffade risker. Det är viktigt att de kontinuitetsplaner man tar fram fungerar vid olika incidenter och för de som ska använda planerna. Se till att kontinuitetsplaner inkluderar beredskap för planerade avbrott till följd av exempelvis förändringshantering, elavbrott, internetbortfall, kommunikationsbortfall samt att även ha beredskap för att ens åtgärder kan gå fel.

Se över era planer efter en inträffad incident och förbättra dem utifrån de erfarenheter ni fick utifrån vad som fungerade bra och mindre bra med planerna under incidenten.

Ett sätt att undvika att behöva använda kontinuitetsplanerna är att införa redundans av de mest kritiska funktionerna.

Se över informationstillgångar och deras beroenden

För att minska risken för att incidenter inträffar eller att störningar som uppstår till följd av incidenter blir värre än vad de behöver bli, är det viktigt för organisationer att ha en god bild av sina informationstillgångar. Det vill säga den information de hanterar och de informationssystem som de använder och hur de förhåller sig till varandra. Med en växande komplexitet kan en enkel förändring i en del av informationssystemet leda till stora problem i ett annat system. Kunskap om hur olika informationssystem har beroenden till varandra är viktigt för en säker drift och förvaltning. Denna kunskap kan sedan användas för att undvika att onödiga följdincidenter inträffar och hjälpa organisationen att förutse var problem kan uppstå och att man kan planera för var organisationen troligen behöver fokusera sitt återställningsarbete, om en incident ändå skulle uppstå.

Exempel på angrepp

En myndighet misstänkte att en direktörs dator infekterats av någon form av spionprogram som hämtade information från datorn, bland annat Microsoft Outlook, och skickade e-post från ett annat konto i generaldirektörens namn till hens kontakter. En användare vid en annan myndighet mottog ett e-postmeddelande med en länk och en uppmaning att via länken granska viktiga uppgifter. E-postmeddelanden med liknande innehåll skickades även från myndighetens generella info@-adress. Det är oklart vilka konsekvenser incidenten medförde. Användarens inloggningsdetaljer byttes efter att incidenten upptäcktes.

Rekommendation

Till följd av den här typen av incident är det viktigt att vidta ett antal åtgärder för att förhindra att liknande sker igen. Dels är det viktigt att se över de skyddslösningar och kontrollsystem som används i it-miljön för att säkerställa att tillräckligt skydd är installerat i alla led. Det är även viktigt att fundera kring interna utbildningsinsatser för att utbilda personal om kända nätfiskemetoder och vikten av cyberhygien, men även eventuella behov av extern kommunikation kring händelsen (om det bedöms relevant för verksamheten och dess natur) för att hålla användare, aktörer och/eller medborgare informerade om status och eventuella konsekvenser och åtgärder till följd av händelsen.

Se över hur utvecklingsarbete ger säkra system

Även om digitalisering kan leda till stora effektivitetsvinster, och synergieffekter, måste organisationen för att utnyttja effektivitetsvinsterna arbeta för att minska de risker som samtidigt uppstår när information hanteras digitalt. Det är därför viktigt att säkerhetsarbetet är med från början i utvecklingsarbetet och sedan finns med under hela informationens och informationssystemens livscykel. Att inte ha med säkerhetsperspektivet från början kan leda till inte bara onödiga och potentiellt kostsamma incidenter utan också att det blir dyrare att åtgärda än vad det hade varit om man hade identifierat och omhändertagit riskerna från början.

Det handlar dock inte enbart om att säkra upp nya informationssystem och utan äldre system kan vara en risk. Riksrevisionen har tidigare uppmärksammat problematiken kring föråldrade it-system inom staten och den problematik det kan medföra gällande säkerhet och integrering med mer moderna system. Det är därför viktigt att ta ett helhetsgrepp gällande sina informationstillgångar och se till att all informationsbehandling, i både nya och äldre system har den säkerhet som krävs för att verksamheten ska kunna bedrivas på ett säkert sätt.

Se över information om digitala leveranskedjor

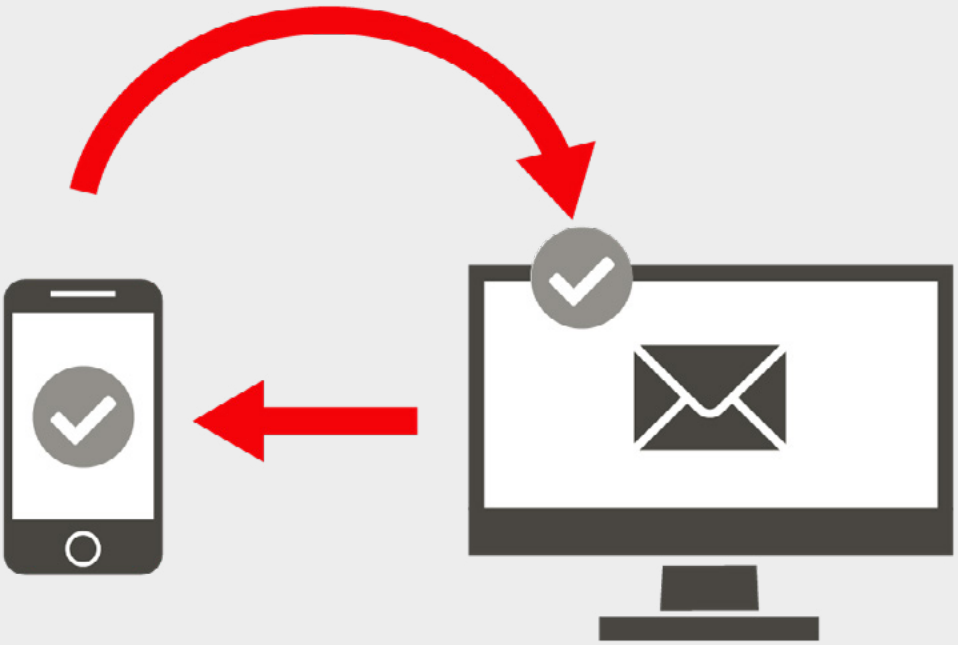
Problematiken kring digitala leveranskedjor är något som aktualiserats genom det senaste årets uppmärksammade incidenter. De digitala leveranskedjorna är problematiska på flera sätt. I incidentrapporteringen framträder detta på främst två sätt. Det handlar bland annat om att det är svårt att ha en överblick över sina digitala leveranskedjor det vill säga vilka beroenden man har till andras informationssystem, leveranser och tjänster, särskilt om man tittar bortom ens närmaste leverantörer. Det handlar också om svårigheten att få information, och att få denna tillräckligt snabbt och korrekt, när en incident inträffat någonstans i ens digitala leveranskedja. Det är därför viktigt att säkerställa i sina avtal och i dialoger med sina leverantörer att man får den information man behöver när en incident inträffar hos en underleverantör. I de flesta fall kan det även vara befogat att ställa krav på att ens leverantörer ska ha avtal med sina underleverantörer om att få sådan information i de fall incidenten inträffar flera led bort i den digitala leveranskedjan.

MSB har under hösten publicerat en rapport som tar ett helhetsgrepp på de problem som kan uppkomma i digitala leveranskedjor. Förutom beskrivningar av möjliga risker och dess konsekvenser ges även ger ett antal rekommendationer för att hantera riskerna. Rapporten erbjuder även ett strukturerat stöd för att analysera de risker organisationen kan behöva omhänderta. Rapporten finns tillgänglig på https://rib.msb.se/filer/pdf/29829.pdf

Se över arbetet med incidenter

När en incident inträffat behöver organisationens medarbetare veta vad de ska göra. Det behöver därför finnas regler och arbetssätt för hur incidenten anmäls, att den bedöms och att det finns personer som kan återställa verksamheten genom att åtgärda samt att orsaker till incidenten utreds. Utredningen utgör underlag till val av åtgärder så att incidenten inte inträffar igen. I arbetet med att åtgärda incidenten och återställa verksamheten till normalt läge behöver det finnas en incidentorganisation som kan engagera rätt kompetenser för att få en så heltäckande bild av incidenten och dess konsekvenser som möjligt. En del av arbetet för statliga myndigheter och leverantörer av samhällsviktiga och digitala tjänster är att kunna bedöma om incidenten är rapporteringspliktig. För detta behöver det finnas rutiner för att rapportera incidenten till MSB enligt ställda krav. Ett genomtänkt arbetssätt för alla arbetsuppgifter inom incidenthantering är en förutsättning för att kunna ta emot anmälningar om problem inifrån organisationen och från externa användare och underleverantörer men också att den egna organisationens efter avslutad incident kan utreda orsakerna till incidenten och lära från det som hänt.

MSB uppmanar även andra organisationer än de som har rapporteringsskyldighet att rapportera de incidenter som påverkar it-miljön till MSB. Formulär för rapportering av incidenter finns på msb.se. Fyll i de uppgifter som efterfrågas för att möjliggöra jämförelse mellan inkomna incidentrapporter.



Exempel på angrepp

En kommun upptäckte att ett användarkonto hade angripits och använts för att skicka bedrägliga e-postmeddelanden med försök till nätfiske till alla anställda inom kommunen. Händelsen orsakade stor påverkan då e-postkonton fick stängas ner tillfälligt medan e-postsystemet rensades. Datorer tillhörande användare som klickat på länken i e-postmeddelandet behövde samlas in och installeras om. Ett antal åtgärder infördes, bland annat utökat automatiskt skydd samt tvåfaktorsautentisering på alla e-postkonton.

Rekommendation

Tvåfaktorsautentisering bör införas på alla e-postkonton, och även för inloggning till sociala medieplattformar och andra forum där information från en organisation (vare sig inom den offentliga eller privata sektorn) delas med användare, kunder, medborgare eller motsvarande. Se över alla skyddslösningar och kontrollsystem som används i it-miljön så att säkerhetsnivån är tillfredsställande. Vid sidan om den tekniska översynen bör it-säkerhetsutbildningar hållas regelbundet med all personal inom verksamheten för att informera om nätfiske och andra bedrägliga metoder som används för att få tillgång till känslig information i utpressningssyfte.

Framåtblick

I takt med att pandemins påverkan på samhället avtar kommer troligtvis den extra drivkraft detta inneburit för digitaliseringen och teknikutvecklingen att minska. Däremot kommer sannolikt flera av de förändringar som gjorts med anledning av pandemin att kvarstå i någon form, exempelvis normaliseringen av hemmet som arbetsplats och de it-stöd och rutiner som behövs för detta.

Den problematik kring sårbarheterna i vår digitaliserade värld som uppmärksammats extra under året i form av ransomware, angrepp mot digitala leveranskedjor, naturhändelsers påverkan på försörjningen av grundläggande komponenter och misstag vid arbete i komplicerade infrastrukturer kommer sannolikt också att fortsätta. Det är även troligt att det vi sett under året snarare är början snarare än slutet på den typen av problem. I takt med ökade klimatförändringar kommer dess påverkan på världen vi lever i sannolikt bli större, så även inom informations- och cybersäkerheten. De angreppstrender som fått mycket uppmärksamhet i media under året kommer sannolikt också att fortsätta så länge världens länder inte gör gemensam sak för att påtagligt förändra incitamenten för att genomföra sådana handlingar eller att säkerhetsarbetet på ett markant sätt kommer ikapp med det arbete som görs med att digitalisera olika verksamheter. Så länge gapen mellan digitalisering och införda säkerhetsåtgärder inte minskar så kommer inte heller de misstag och systemfel som blivit både vanligare och mer svåröverskådliga i de komplexa system som växt fram att minska. MSB ser det som positivt att insikten att informationssystem vid incidenter kan skapa störningar i samhället lyfts upp i det allmänna medvetandet.

It-incidenter har under året påverkat människors vardag på ett mer märkbart vis än på länge. Samtidigt fokuserar toppmöten mellan stormakter på cyberangrepp, och en tydligare trend av att stater pekar ut varandra som skyldiga till olika angrepp syns. Informations- och cybersäkerhet går i och med detta mer från att vara ett separat ämne som främst hanteras av specifika yrkesgrupper med särskilda kunskaper inom området, till att beröra människor i allmänhet och tydligare synas på den politiska och diplomatiska agendan.

I likhet med klimatfrågan så kan en ökad exponering av frågorna, där negativa händelser ligger till grund, leda till att frågor lyfts på rätt nivå, att organisationer och nationer ökar ambitionen på sitt informations- och cybersäkerhetsarbete, och att nödvändiga investeringar sker. Liksom i klimatfrågorna så behöver utvecklingen vändas till det bättre, något vi bara kan åstadkomma om vi arbetar tillsammans med att skapa en säkrare digitalisering. I en uppkopplad värld är it-incidenter något som berör oss alla.

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ nr: MSB1913 – februari 2022 ISBN: 978-91-7927-234-0