Myndigheten för samhällsskydd och beredskap

Medfinansierat av Europeiska unionens fond för ett sammanlänkat Europa

ÅRSRAPPORT

NIS-leverantörers it-incidentrapportering 2020

En samlad bild över rapporterade it-incidenter i samhällsviktiga och digitala tjänster

Årsrapport över NIS-leverantörers it-incidentrapportering 2020 – En samlad bild över rapporterade it-incidenter i samhällsviktiga och digitala tjänster

MSB står ensamt ansvarig för denna publikation, vars innehåll inte nödvändigtvis återspeglar Europeiska unionens hållning.

Foto omslag: iStock
Tryck: DanagårdLiTHO
Produktion: Advant

Publikationsnummer: MSB1695 - februari 2021
ISBN: 978-91-7927-106-0

Förord

Denna rapport är den första sammanställningen som MSB genomför över inrapporterade NIS-incidenter från leverantörer av samhällsviktiga och digitala tjänster. Incidentrapporteringen som inkommit till MSB under 2020 visar att fler incidenter rapporteras jämfört med föregående år vilket stärker arbetet med att skapa en mer heltäckande bild av vilka incidenter som drabbar leverantörer av samhällsviktiga och digitala tjänster. 2020 har präglats av covid-19-pandemin vilket inneburit en hög påfrestning på hela samhället. Flertalet leverantörer av samhällsviktiga tjänster, framförallt inom hälso- och sjukvård, har haft en hög belastning på sina verksamheter. 2020 har för de flesta organisationer även inneburit stora förändringar i hur och var vi arbetar. Dagens samhälle är beroende av digitala lösningar för att upprätthålla funktionaliteten i våra samhällsviktiga tjänster. Då informations- och cybersäkerhetsarbetet sällan håller jämna steg med digitaliseringen skapas nya hot och sårbarheter för incidenter som kan orsaka störningar med inverkan på samhällets funktion. I arbetet med att öka informations- och cybersäkerheten i samhället är NIS-regleringen ett viktigt verktyg för att höja säkerhetsnivån, kartlägga vilka incidenter som sker och belysa de konsekvenser som incidenterna har på samhället. Incidentrapporteringen till MSB är avgörande för att minska konsekvenserna av it-relaterade störningar i samhällsviktiga och digitala tjänster och bidrar till att vi snabbt kan upprätta lägesbild och gå ut med varningar som större samhällsstörningar inträffar. NIS-leverantörernas incidentrapportering ger även en lägesbild som kan användas för att ta lärdom av incidenter, förebygga risker och stärka hanteringsförmågan.

MSB satsar på att höja kompetensen om NIS och kommer under kommande år genomföra ett antal aktiviteter där vi har ambitionen att höja kunskapsnivån om NIS och koppla samman aktörer som berörs av NIS-reglering. Däribland att genomföra en årlig konferens för leverantörer av samhällsviktiga tjänster, ge ut årsrapporter samt att skapa nya samarbetsforum för aktörerna att samverka inom.

Arbetet med tillämpningen av NIS är ett framgångsrikt samarbete mellan MSB, Energimyndigheten, Finansinspektionen, Inspektionen för vård och omsorg, Livsmedelsverket, Socialstyrelsen, Post- och telestyrelsen och Transportstyrelsen. Alla har en roll att spela i tillämpningen av NIS. Det är ett lagarbete och vi kommer inte att lyckas om inte alla bidrar.

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

Innehåll

Begreppslista

NIS-direktivet	(Eng. The Directive on Security of Networks and Information Systems) Namnet på EU-direktivet (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverk och informationssystem i hela unionen.
Samhällsviktig tjänst	Samhällsviktiga tjänster är tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. I rapporten används och avses NIS-regleringens definition som inbegriper tjänster inom bankverksamhet, finansmarknadsinfrastruktur, digital infrastruktur, leverans och distribution av dricksvatten, transporter, hälso- och sjukvård, energi.
Digital tjänst	En tjänst i den mening som avses i artikel 1.1 b i Europaparlamentets och rådets direktiv (2015/1535): en internetbaserad marknadsplats, internetbaserad sökmotor eller molntjänst.
OES	(Eng. Operator of Essential Service) Leverantör av samhällsviktig tjänst.
DSP	(Eng. Digital Service Provider) Leverantör av digital tjänst.
NIS-leverantör	Organisationer som omfattas av NIS-regleringen. Se vidare beskrivning i kapitel 2.2 i denna rapport.
NCA	(Eng. National Competent Authorities) Behöriga myndigheter som i relation till MSB:s föreskrifter om identifiering och anmälan av samhällsviktiga tjänster, informationssäkerhet och incidentrapportering, är tillsynsmyndigheter är tillsynsmyndigheter. I andra EU-medlemsstater behöver de behöriga myndigheterna inte nödvändigtvis ha tillsynsansvar i respektive sektor. I denna rapport används tillsynsmyndigheter då fokus är på incidentrapportering.
CSIRT	(Eng. Computer Security Incident Response Team) Sveriges nationella CSIRT är CERT-SE med uppgift att stödja samhället i arbetet med att hantera och förebygga it-incidenter.
SPOC	(Eng. Single Point of Contact) Nationell kontaktpunkt inom NIS-regleringen, den myndighet som har ett samordningsansvar och är kontaktpunkten in i ett land i frågor gällande NIS. I Sverige är MSB SPOC.
ENISA	European Union Agency for Cybersecurity Europeiska unionens cybersäkerhetsbyrå.
INEA	Innovation and Networks Executive Agency Europeiska unionens nätverk och innovationsbyrå, har till uppgift att finansiera projekt som stöttar innovation och ett sammankopplat Europa.
NIS-incident	En incident definieras som en händelse med faktiskt negativ inverkan på säkerheten i ett informationssystem eller nätverk. För att en incident ska rapporteras till MSB enligt NIS krävs att det uppstått en störning av leveransen av den samhällsviktiga eller digitala tjänsten samt att störningen har sitt ursprung i en incident i ett nätverk eller informationssystem. Begreppet NIS-incident används i rapporten för att benämna de it-incidenter som rapporterats i enlighet med uppsatta kriterier i NIS-regleringen. Se vidare beskrivning i kapitel 2.3 och 3.1 i denna rapport.

ICS	(Eng. Industrial Control Systems) Industriella informations- och styrsystem.
ICT	(Eng. Information and Communications Technology) Informations- och kommunikationsteknik.
Nätverks- och informationssystem	Nätverks- och informationssystem definieras enligt 2§ lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster som ett elektroniskt kommunikationsnät, en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra där digitala uppgifter som lagras, behandlas, hämtas eller överförs ska kunna driftas, användas, skyddas och underhållas.
Nätfiske	(Eng. Phishing) Nätfiske är idag den vanligaste metoden angripare använder för att komma åt lösenord eller bank- och kortuppgifter genom att skicka falsk e-post. Angriparen skickar ut ett massutskick via e-post till ett stort antal mottagare med förhoppning att någon klickar på den skadliga länken.
Utpressningsvirus	(Eng. Ransomware) Även kallat ”utpressningsprogram”, är benämningen på virus som krypterar hela eller delar av en verksamhets it-system och gör systemen eller informationen otillgänglig. Oftast finns krav på lösensumma för att (påstått) få tillbaka informationen och/eller undvika att informationen blir offentliggjord, därav utpressning.
IoT	(Eng. Internet of Things) Sakernas internet, ett begrepp som används för att beskriva föremål, både för privat- och industriellt bruk, som utrustas med möjligheten att anslutas till internet och andra nätverk.

Sammanfattning

Sammanfattning

EU:s NIS-direktiv[1] implementerades i Sverige under 2018 och riktar sig till leverantörer av samhällsviktiga och digitala tjänster, det vill säga verksamheter som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet. Genom NIS-direktivet vill EU-kommissionen öka informations- och cybersäkerheten över gränserna och således öka informationssäkerheten i hela unionen i syfte att stärka den inre marknadens funktion.

Sedan 2019 rapporterar leverantörer av samhällsviktiga och digitala tjänster in it-incidenter till MSB i enlighet med NIS-regleringen.

Med denna rapport vill MSB återföra kunskap till NIS-leverantörerna, tillsynsmyndigheterna och andra intressenter kring vilka typer av incidenter som varit vanligt förekommande under året och hur dessa kan motverkas. Vidare syftar rapporten till att ge en grundläggande förståelse för NIS-regleringen i Sverige men också beskriva ett europeiskt perspektiv för att visa på skillnader och likheter mellan ländernas implementering av NIS-direktivet. I rapporten återges även ett antal incidentexempel för att på ett tydligt sätt illustrera hur incidenter inträffar och förslag på hur dessa kan hanteras.

Trots att 2020 till stor del har präglats av covid-19-pandemin syns ingen tydlig pandemieffekt i årets incidentrapportering från NIS-leverantörerna. De slutsatser som kan dras av den samlade incidentrapporteringen som inkommit under året är bland annat hur nätverk eller system för kommunikation ofta drabbas av incidenter och orsakar störningar hos NIS-leverantörerna. Vidare visar rapporteringen att incidenterna ofta sker i en tjänst som tillhandahålls av en underleverantör, och att bristfälliga kontrakt kan leda till informationsbrist gällande incidenterna. En stor del av incidenterna har orsakats av systemfel, och i en del fall av handhavandefel. En mycket liten del av incidenterna anges ha orsakats av angrepp. Totalt rapporterade leverantörer av samhällsviktiga tjänster 88 incidenter 2020 vilket är en ökning från 2019.

Rapporten innehåller utöver incidentrapporteringen, även information om EU-satsningar, erfarenheter av NIS från andra EU-länder och en överblick av den svenska NIS-regleringen.

Rapporten är den första i sitt slag och kommer att publiceras årligen från och med 2021 för att höja kunskapen om de incidenter som drabbar samhällsviktiga och digitala tjänster i Sverige.

1. The Directive on Security of Network and Information Systems.

Inledning

Foto: Shutterstock

1. Inledning

NIS-direktivet berör leverantörer av samhällsviktiga och digitala tjänster, både inom den privata och offentliga sektorn. Direktivet ställer bland annat krav på säkerhet i nätverks- och informationssystem samt incidentrapportering.

1.1 Sverige år 2020

I takt med att samhället digitaliseras ökar även kraven på informations- och cybersäkerheten. Sverige placerar sig högt i flertalet mätningar vad gäller digital mognadsgrad, då det satsas mycket på digitala lösningar och på att ständigt utveckla den digitala infrastrukturen.[2] Regeringens vision är ett hållbart digitaliserat Sverige där det övergripande målet är en hög ambitionsnivå kring användandet av digitaliseringens möjligheter.[3] Samhällsviktiga tjänster, i synnerhet sådana som använder industriella styr- och kontrollsystem för att hantera fysiska processer såsom exempelvis dricksvattenförsörjning, elförsörjning och transporter, använder sig allt mer av sensorer och smarta enheter (Internet of Things) för att effektivisera sin verksamhet. Sådant som tidigare hanterades analogt har i högre grad blivit möjligt att sköta digitalt, vilket illustreras av automatiseringens successiva utveckling. Exempelvis har organisationer sedan millennieskiftet haft möjlighet att fjärrstyra ventiler som tidigare endast kunde öppnas och stängas manuellt på plats. Under 2000-talet övergick det manuella arbetet till att låta datorer öppna och stänga ventiler på basis av en uppsättning statiska regler. Sedan ett antal år tillbaka finns möjligheter att ersätta statiska regler med mer dynamiska system som utifrån skiftande omständigheter kan lära sig öppna och stänga ventilen efter behov. Övergången från en geografiskt lokaliserad manuell hantering till en nästan helt automatiserad styrning sker inom de flesta sektorer där fysiska processer hanteras.

Samtidigt som nya möjligheter skapas genom en ökad digitalisering, håller informations- och cybersäkerhetsarbetet inte samma takt. Med ett större beroende av digitala lösningar krävs en ökad robusthet för företag och leverantörer av samhällsviktiga och digitala tjänster, både nationellt och internationellt.

Under 2020 har spridningen av covid-19 påverkat samhället i stort vilket lett till en högre arbetsbelastning inom flertalet samhällsviktiga sektorer, framförallt inom hälso- och sjukvårdssektorn. Även cyberbrottsligheten har anpassats efter

2. https://digitaliseringsradet.se/sveriges-digitalisering/
3. https://www.regeringen.se/regeringens-politik/digitaliseringsstrategin/

de rådande omständigheterna. Flertalet internationella, och i viss utsträckning nationella rapporter, har beskrivit hur covid-19-relaterade cyberbrott förekommit under pandemin. Exempelvis genom nätfiske-kampanjer (phishing) med anspelningar på hälsorelaterad information och utpressningsattacker (ransomware) mot sjukvårdssektorn i olika delar av världen.[4] Pandemin har medfört att kraven på digitala lösningar växt genom att exempelvis distansarbete blivit vanligt förekommande och en nödvändighet. Händelserna under det gångna året har exponerat brister och sårbarheter i system men även belyst potentialen i organisationers digitala infrastruktur.

Denna rapport är den första i en serie av årliga rapporter som ska redovisa information ur inkommen incidentrapportering i enlighet med NIS-regleringen från samhällsviktiga och digitala tjänster i Sverige. Rapporten har ambitionen att öka kunskapen om NIS-direktivet, vanligt förekommande incidenter och Sveriges informations- och cybersäkerhet i stort.

1.2 En årsrapport över NIS-incidenter 2020

MSB tar emot incidentrapporter från självidentifierade svenska NIS-leverantörer vilket ger en ökad kännedom av vanligt förekommande incidenter som drabbar leverantörerna. Detta innebär inte att denna rapport ger en fullständig bild av alla de incidenter som sker hos samtliga leverantörer av samhällsviktiga tjänster, då de inte nödvändigtvis rapporterar alla incidenter som inträffat. Det kan även finnas leverantörer som inte anmält sig som NIS-leverantör ännu.

Denna rapport redovisar innehåll ur det totala antalet incidentrapporter som inkommit till MSB och beskriver anonymiserade exempel för att skapa en större förståelse kring hur incidenter kan hanteras och förebyggas. Exemplen illustrerar även hur en incident kan se ut för att öka medvetenheten kring vad som ska rapporteras och hur incidentrapporteringen går till. I de inkomna incidentrapporterna återfinns uppgifter om själva incidenten, den störning som skett samt potentiella konsekvenser av incidenten eller störningen. Även särskilda hanteringsåtgärder och förebyggande åtgärder beskrivs. Incidenterna redovisas i denna rapport på en aggregerad nivå och kategoriseras sektorsvis i begränsad utsträckning. MSB publicerar sedan ett antal år tillbaka en årsrapport över inkomna it-incidentrapporter från statliga myndigheter enligt *krisberedskapsförordningen* (2015:1052). Årsrapporten över NIS-leverantörers incidentrapportering skapar tillsammans med årsrapporten över statliga myndigheters it-incidenter en bredare förståelse för Sveriges informations- och cybersäkerhet.

Denna rapport riktar sig till en bred publik av såväl leverantörer av samhällsviktiga och digitala tjänster, men även övriga svenska organisationer och myndigheter i stort. Vidare syftar rapporten till att belysa kopplingen mellan informationssäkerhet, it-incidenter och störningar i samhället.

En förhoppning är att den samlade bilden ska kunna tydliggöra vikten av att rapportera incidenter och att de som ännu inte har inlett arbetet med incidentrapportering ska få kunskap och verktyg att påbörja arbetet.

4. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

Incidentexempel 1

En leverantör av dricksvatten fick problem med sina processtyrningssystem när VPN-servern hos deras systemleverantör drabbades av en incident. Flera funktioner påverkades, exempelvis bröts informationsflödet från fjärr-anläggningar (t ex vattentorn) under cirka fem timmar. Det förelåg ingen risk för människors hälsa under tiden för avbrottet.

Råd kring hantering:

För leverantörer av samhällsviktiga tjänster är det viktigt 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 upphandla tydliga serviceavtal om vilka krav som ställs på tjänsten. Förutom krav på kostnader, driftsäkerhet, antal fel och hastighet bör incidenthantering vara ett krav. Serviceavtalet bör även specificera vilka krav som måste garanteras i flera led. Kraven bör anges så att de blir mätbara.

Incidentexempel 2

Betalningstransaktioner påverkades under cirka fem timmar då en bank drabbades av nätverksproblem efter ett underhållsarbete. Störningarna påverkade såväl fysiska kontor som kundcenter, app och internetbank.

Råd kring hantering:

Det är viktigt att säkerställa att förändringar i it-miljön får det resultat som man förväntat sig, samt att alla förändringar är noga testade innan de går i drift. I det här fallet har inte leverantören angett vad bakgrunden till störningen var men generellt är det viktigt att ha redundanta miljöer så att det alltid finns alternativ om en störning inträffar.

NIS-direktivet

Foto: iStock

2. NIS-direktivet

NIS-direktivet, som antogs 2016 av EU, är en av de första unionsomfattande cybersäkerhetsregleringarna. Syftet med direktivet är att höja den gemensamma nivån gällande informations- och cybersäkerhet för de tjänster och system som anses vara centrala för medlemsstaternas ekonomi och befolkning. Samtidigt belyser direktivet hur säkerhetsincidenter blir allt vanligare, mer omfattande och får större inverkan på samhället vilket innebär ett allt större hot mot nätverks- och informationssystemens funktion.

Direktivet ställer fem övergripande krav på medlemsstaterna:

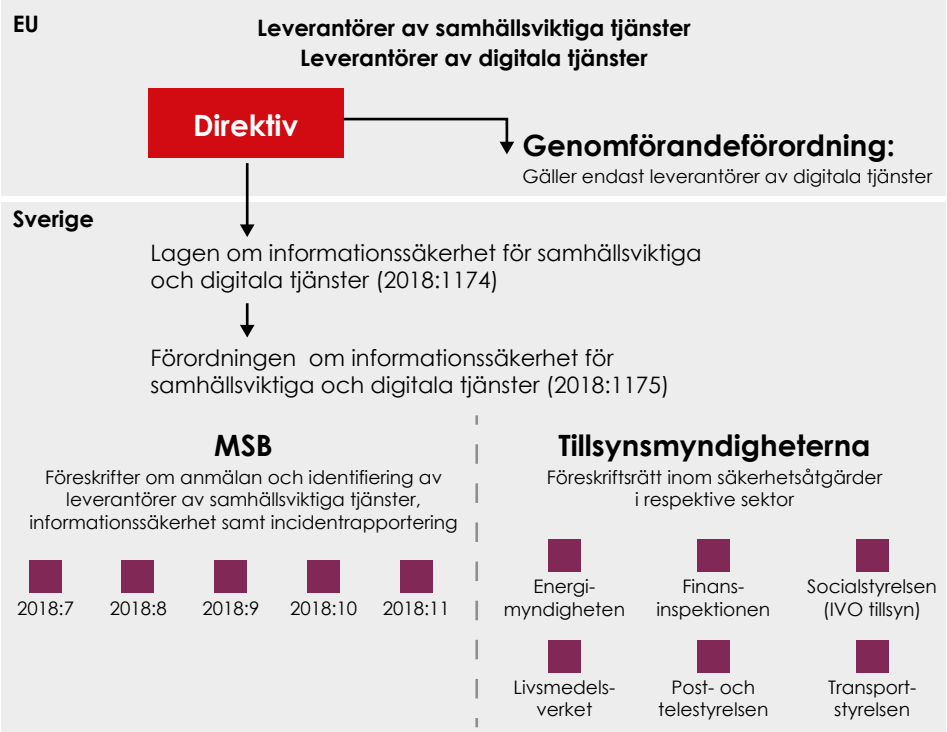
1. varje medlemsstat måste anta en nationell strategi för säkerhet i nätverks- och informationssystem
2. varje medlemsstat måste delta i en strategisk samarbetsgrupp som omfattar EU-medlemsstaterna (Cooperation group)
3. varje medlemsstat måste delta i ett nätverk för hantering av it-säkerhetsincidenter (CSIRT-nätverk)
4. varje medlemsstat måste fastställa säkerhets- och rapporteringskrav för leverantörer av samhällsviktiga tjänster och för leverantörer av digitala tjänster
5. varje medlemsstat måste utse behöriga myndigheter (NCAs) skapa en nationell kontaktpunkt (SPOC) samt utforma en CSIRT-enhet.

Implementeringen av direktivet skiljer sig något mellan olika medlemsstater, bland annat gällande framtagandet av tröskelvärden för identifiering av leverantörer och rapporteringspliktiga incidenter.

Under 2020 presenterades ett förslag på en revidering av NIS-direktivet vilket sannolikt kommer innebära förändringar inom europeisk och svensk lagstiftning inom de kommande åren.

2.1 Direktivet i svensk reglering

I Sverige har NIS-direktivet implementerats genom *lagen* (2018:1174) *om informationssäkerhet för samhällsviktiga och digitala tjänster*, ”NIS-lagen”. Lagen riktar sig till leverantörer av samhällsviktiga och digitala tjänster och ställer krav på bland annat systematiskt informationssäkerhetsarbete, riskanalyser och säkerhetsåtgärder. Lagen kompletteras av *förordningen* (2018:1175) o*m informationssäkerhet för samhällsviktiga och digitala tjänster*, ”NIS-förordningen”.



Figur 1. Förenklad visualisering av NIS-direktivet och den svenska NIS-regleringen.

MSB är Sveriges nationella kontaktpunkt (*SPOC – Single Point of Contact*) och därmed även Sveriges representant i den samarbetsgrupp som inrättats för EU:s medlemsstater och med EU-kommissionen på strategisk nivå (*Cooperation Group*). MSB är även Sveriges CSIRT-enhet, vars uppgifter utförs av funktionen CERT-SE, som är en del av MSB:s avdelning för cybersäkerhet och säkra kommunikationer. CERT-SE mottar incidentrapporter och arbetar operativt med att stödja samhället i arbetet med att hantera och förebygga bland annat NIS-incidenter. Utöver detta har Sverige sex sektoriella tillsynsmyndigheter som har i uppdrag att bedriva tillsyn över de identifierade leverantörerna i de respektive sektorerna.

Tillsynsmyndigheterna utgörs av Energimyndigheten, Finansinspektionen, Inspektionen för vård och omsorg/Socialstyrelsen,[5] Livsmedelsverket, Post- och telestyrelsen, samt Transportstyrelsen som har mandat att utfärda sektorsspecifika föreskrifter gällande säkerhetsåtgärder och riskanalyser. MSB har mandat att utfärda föreskrifter gällande identifiering och anmälan av samhällsviktiga tjänster, informationssäkerhet och incidentrapportering för NIS-leverantörer som gäller i samtliga sektorer. Tillsynsmyndigheterna utfärdar kompletterande och förtydligande föreskrifter inom respektive sektor.

Figur 2. MSB:s NIS-föreskrifter.

5. Inspektionen för vård och omsorg är tillsynsmyndighet men Socialstyrelsen har föreskriftsrätt inom hälso- och sjukvårdssektorn.

Liknande reglering för leverantörer av digitala tjänster finns på EU-nivå i en genomförandeförordning som är beslutad av EU-kommissionen. Genomförandeförordningen som även specificerar vilka incidenter som är rapporteringspliktiga för leverantörer av digitala tjänster kompletteras av MSB:s föreskrifter om incidentrapportering för leverantörer av digitala tjänster.

Under 2019 inleddes ett arbete hos tillsynsmyndigheterna med att ta fram föreskrifter inom respektive sektor som ställer krav på leverantörer av samhällsviktiga tjänster att vidta vissa säkerhetsåtgärder och hur genomförandet av riskanalyser ska ske. Flera av tillsynsmyndigheterna beräknas bli klara med föreskrifter under 2021.

2.2 Berörda aktörer

Då NIS-direktivet omfattar flera samhällsviktiga och digitala tjänster berörs både privata och offentliga aktörer av regleringen. De sju sektorer som omfattas gällande samhällsviktiga tjänster är:

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

Figur 3. Förenklad visualisering av sektorer och aktörer som ingår i kategorin leverantörer av samhällsviktiga tjänster, se MSBFS 2018:7 för ytterligare information.

Inom en del sektorer omfattas endast vissa delar av sektorns verksamheter (se Figur 3). Leverantörer av digitala tjänster omfattar internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster. Under september månad 2020 fanns det totalt 561 anmälda leverantörer av samhällsviktiga tjänster. Antalet anmälda aktörer stiger successivt då fler aktörer tillkommer över tid.

Leverantörer av samhällsviktiga tjänster som uppfyller kraven i föreskrifterna ska anmäla sig till sin sektors tillsynsmyndighet. Tillsynsmyndigheterna beslutar om att inleda tillsyn mot leverantörer som uppfyller kraven men som inte anmäler sig. MSB:s föreskrifter för identifiering och anmälan av leverantörer av samhällsviktiga tjänster (MSBFS 2018:7) fastställer kriterierna för vilka leverantörer som omfattas av NIS-regleringen samt hur anmälan till respektive sektors tillsynsmyndighet går till. De leverantörer som omfattas ska arbeta systematiskt och riskbaserat med informationssäkerhet, för att på så sätt minska riskerna för avbrott i tjänsten (MSBFS 2018:8).

2.3 Incidentrapportering: så fungerar det

Ökad kännedom om allvarliga incidenter är avgörande för att kunna mildra dess konsekvenser, identifiera hot och sårbarheter samt öka informations- och cybersäkerheten på samhällsnivå. Både leverantörer av samhällsviktiga och digitala tjänster ska rapportera incidenter till MSB som i sin tur delar informationen till ansvarig tillsynsmyndighet. Det är även möjligt för aktörer som inte omfattas av NIS-regleringen att frivilligt rapportera incidenter inom ramen för NIS (MSBFS 2018:11).[6,7] Incidentrapportering är, som tidigare nämnts, ett av de övergripande kraven i NIS-direktivet. I Sverige specificeras kraven på incidentrapporteringen i lagen (2018:1174) där det står att:

> 18 § Leverantörer av samhällsviktiga tjänster ska utan onödigt dröjsmål rapportera incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhandahåller.

I MSB:s föreskrift (MSBFS 2018:9) finns det tydliga kriterier för vilken typ av incident som respektive sektor ska rapportera utifrån den inträffade störningen.[8] För att en *incident* ska rapporteras i enlighet med NIS-regleringen krävs att den orsakat en *störning* med betydande inverkan på *kontinuiteten* i den samhällsviktiga tjänsten och att aktören är *rapporteringspliktig*. Störningen ska även ha sitt ursprung i ett nätverk eller informationssystem. I MSB:s vägledning (MSB 2018-13470) finns stöd som hjälper leverantören genom rapporteringsprocessen.

Ytterligare stöd för att uppfylla kraven på incidentrapportering och stöd gällande det faktiska ifyllandet av incidentformulären finns på MSB:s hemsida.[9]

---

6. MSBFS 2018:11 Föreskrifter och allmänna råd om frivilligrapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet.

7. Utöver incidentrapportering mottar MSB även it-incidentrapportering från Sveriges statliga myndigheter enligt förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (även kallad Krisberedskapsförordningen). Resultatet av den rapporteringen redovisas i MSB:s årsrapport om statliga myndigheters it-incidentrapportering som publiceras årligen. Rapporten *Årsrapport statliga myndigheters it-incidentrapportering 2020: Utmaningar för en säker och robust informationsdelning* finns att läsa på MSB:s hemsida msb.se.

8. MSB ger även ut en vägledning gällande incidentrapportering som både stöttar i att förstå vad som ska rapporteras, och hur en leverantör går till väga – *Vägledning för ifyllande av incidentrapporteringsformulären för samhällsviktiga respektive digitala tjänster* finns tillgänglig på MSB:s hemsida.

9. msb.se/NIS

2.4 Syftet med incidentrapportering

Incidentrapportering är viktig för att den rapporterande organisationen ska få en överblick av vad som inträffat vilket i sin tur kan utveckla det interna förebyggande arbetet. Vidare är det viktigt för samhället och andra aktörer då medvetenheten kring incidenter, störningar och hantering kan höjas. Incidenter och störningar kan ha spridningseffekter och på så sätt påverka flertalet aktörer, även om inte leverantörerna är medvetna om det själva.

MSB kan ge operativt stöd i det initiala skedet av en incident och även varna andra aktörer, samt andra EU-medlemsstater. De samlade incidentrapporterna ger MSB underlag till en strategisk analys och bidrar således till att kunna arbeta förebyggande och skapa gemensamma lösningar kring incidenter. Samtidigt får tillsynsmyndigheterna en tydligare bild av läget inom respektive sektor vilket ger underlag för att utforma stöd och tillsyn som kan bidra till minskad risk för incidenter och störningar.

Leverantörerna kan få en överblick av incidenten, dess kostnader och påverkan på verksamheten vilket i sin tur kan ligga till grund för hur verksamheten planeras framåt. Incidentrapporteringen kan, kombinerat med övrigt systematiskt informationssäkerhetsarbete inklusive övningar och träning, främja ett kontinuitetsarbete och ge översikt över vad som drabbar verksamheten.

Kunskap om incidenter ger leverantörerna, MSB och de utpekade tillsynsmyndigheterna bland annat:

- information om vilka incidenter som sker i samhället
- uppgifter om hur de hanteras
- övriga uppgifter såsom kostnader och spridningseffekter
- en möjlighet för leverantörerna att agera proaktivt.

NIS-direktivet, och dess krav på incidentrapportering, bidrar till en ökad kännedom över hur den enskilda organisationen drabbas av en incident. Vidare bidrar incidentrapporteringen till en ökad förståelse för hur en enskild incident kan vara en del i ett större sammanhang, som drabbar flera aktörer, både nationellt och internationellt. Kunskapen från incidentrapporteringen kan bidra till att åtgärder kan vidtas i god tid och eventuell skada begränsas – både för den enskilde aktören men även för att motverka att en liknande händelse inträffar igen. NIS-direktivet kan ses som en av åtgärderna för att skapa en gemensam grund för samhällets informations- och cybersäkerhet. Denna grund kan därefter vara en del i att höja nivån på den gemensamma information- och cybersäkerheten, både nationellt och på EU-nivå.

Rapportering 2020

Foto: Icon Photography

3. Rapportering 2020: Redovisning av inrapporterade NIS-incidenter

I följande del redovisas en sammanställning av de rapporter om NIS-incidenter som skett under 2020 och som MSB mottagit från leverantörer av samhällsviktiga och digitala tjänster. Formulären som fyllts i av leverantörerna ger MSB ett stort dataunderlag och möjliggör en detaljerad analys av de incidenter som skett inom ramen för NIS-regleringen under året som gått.

Leverantörer av samhällsviktiga tjänster är aktörer som i de flesta fall identifierat och anmält sig själva. I september 2020 fanns 561 anmälda leverantörer av samhällsviktiga tjänster. MSB har mottagit 88 incidentrapporter som avser incidenter som utspelats under 2020. Rapporterna är ojämnt fördelade över de olika sektorerna. Under året har främst hälso- och sjukvårdssektorn, men även dricksvattenförsörjningen, stått för en högre andel av rapporteringen. Leverantörer av digitala tjänster (internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster) ska enligt EU-gemensamma regler endast rapportera de incidenter som har *avsevärd* inverkan på tillhandahållandet av en digital tjänst. Några sådana rapporter har inte inkommit under 2020.

Många leverantörer av samhällsviktiga tjänster är beroende av exempelvis it-tjänster som levereras av en extern part. Vissa externa parter levererar ibland samma eller liknande it-tjänster till många leverantörer av samhällsviktiga tjänster, ibland inom en och samma sektor och vissa gånger till leverantörer inom olika sektorer. När en incident inträffar hos en sådan extern part kan det ge upphov till störningar hos många leverantörer samtidigt. Detta återspeglas i statistiken över antalet inrapporterade incidenter och störningar, då flera rapporterade NIS-incidenter kan ha sitt ursprung i samma incident hos en gemensam underleverantör. Leverantören av den samhällsviktiga tjänsten har skyldighet att rapportera incidenten oavsett var den skett och måste därför rapportera incidenten även om den har ursprung hos en annan aktör. Det redovisade resultatet baseras endast på inkomna rapporter och generaliserar inte bortom det inkomna materialet, vilket innebär att slutsatser och rekommendationer gäller för de inrapporterade incidenterna och inte nödvändigtvis för samtliga NIS-leverantörer.

Tills dess att ett digitalt rapporteringssystem med stödfunktioner för ifyllande av formulären framtagits, har PDF:er och papperskopior av formulären fyllts i och skickats in av leverantörerna till MSB enligt överenskommen process. I ett antal fall har den nuvarande manuella formen av inrapportering inneburit att underlaget ibland varit ofullständigt eller, i vissa delar, motstridigt. Detta kommer troligtvis avhjälpas genom det digitala rapporteringssystem som i större utsträckning kan stötta leverantören att fylla i de relevanta uppgifterna på ett korrekt sätt. Det digitala inrapporteringssystemet är beräknat att lanseras under 2021.

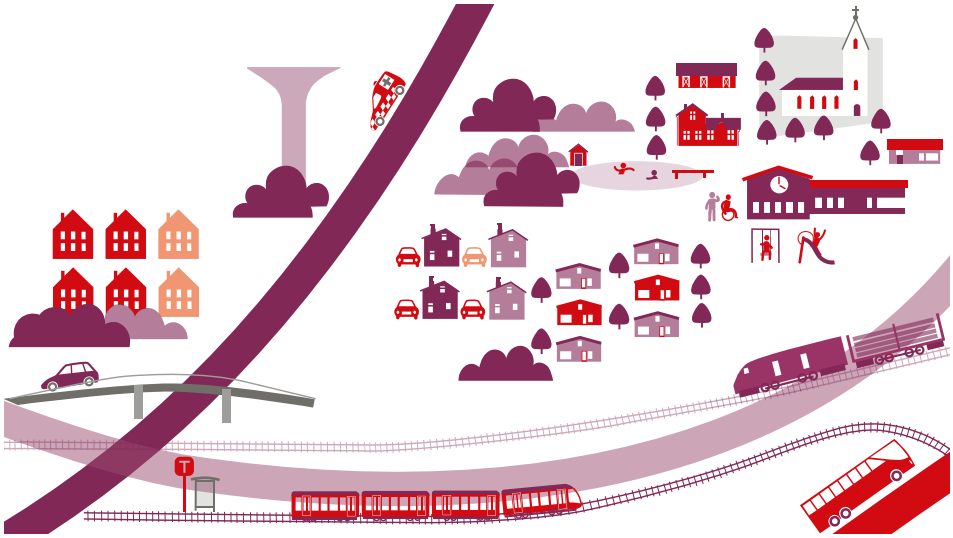
3.1 Incidentrapportering

I incidentrapporterna görs det skillnad på incident och störning:

- **Incidenter** definieras som händelser med en faktisk negativ inverkan på säkerheten i nätverks- och informationssystem. Incidenter kan därmed inträffa i informationssystem och nätverk (exempelvis genom att skadlig kod infekterar ett informationssystem) såväl som *runtomkring* informationssystem och nätverk (exempelvis genom att elförsörjning avbryts).
- En **störning** är en konsekvens av incidenten som innebär att den samhällsviktiga tjänsten inte levereras som normalt. För att rapporteringsplikt ska uppstå måste störningen ha en betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten. Detta utvecklas genom ett fiktivt exempel nedan.

3.1.1 Fiktivt exempel

Ett vattenverk i en fiktiv kommun har ett it-system som styr filtreringen av inpumpat vatten. När it-systemet som styr filtreringen drabbas av en incident och slutar fungera, kan vattenverkets pumpar fortsätta pumpa in vatten i det kommunala dricksvattennätet. Då it-systemet inte fungerar pumpas orent vatten ut i det kommunala nätet. I det här fallet är incidenten problemet i it-systemet som gör att filtreringen slutar fungera. Det krävs ofta personal med expertis inom sådana it-system för att lösa problemet.



Störningen som beskrivs i exemplet ovan är problemet med potentiellt orent vatten i vattennätet. Där behövs personal med expertis om bland annat dricksvattenförsörjning och VA-system för att lösa störningen precis som det krävs personal med expertis om det specifika it-systemet för att lösa incidenten. Det är viktigt att notera att störningen kan kvarstå när incidenten är löst och att störningen inte nödvändigtvis uppstår omedelbart i samband med incidenten. Det handlar med andra ord om två separata problem som pågår under varsin tidsperiod vilka kan, men inte måste, sammanfalla. Det kan även vara så att personalen som hanterar incidenten och störningen inte är den samma.

Om incidenten fortgår och inte upptäcks kan störningen förvärras, och om tillräckligt mycket orent vatten pumpas ut kan ett ökat antal sjukdomsfall ske inom kommunen. I detta fall kan störningen i sig få konsekvenser, så som exempelvis en förhöjd nivå av magsjuka, vilket ställer högre krav på allt från vård och skola till restaurangverksamhet. Det fiktiva exemplet belyser även att incidenten inte nödvändigtvis upptäcks först. Det kan vara en ökning av magsjuka i kommunen och i värsta fall dödsfall som leder till upptäckten av orent vatten, vilket i sin tur leder till upptäckten av en incident i it-systemet som styr filtreringen. I en organisation med bristande förmåga att upptäcka incidenter kan störningen behöva härledas från störningens konsekvenser, varpå incidenten kan härledas från störningen.

3.2 Typer av incidenter

När leverantörer ska rapportera om karaktären hos en incident får de först ta ställning till om incidenten har inträffat i ett informationssystem/nätverk, eller om den inträffat i miljön *runtomkring* ett informationssystem/nätverk (”kringmiljön”). Om incidenten har inträffat i ett informationssystem eller nätverk anger leverantören vad för slags system incidenten har inträffat i, samt vad som skett i informationssystemet eller nätverket (exempelvis om något har gått sönder eller om något som inte hör hemma i systemet har installerats i det). Om incidenten har inträffat i kringmiljön anger leverantören vad för slags händelse det är som har inträffat exempelvis avbrott i energiförsörjningen, i förbindelsen eller problem med kyla, värme eller fukt- och klimathållning.

I de fall där leverantörerna lyckats identifiera var incidenten skett, anger drygt 87 % av leverantörerna att incidenten inträffat i ett informationssystem eller nätverk (och således inte i kringmiljö). Av de som rapporterat att en incident skett i ett system eller nätverk, har incidenten ofta skett i ett system eller nätverk dedikerat för kommunikation (se Diagram 1). Ofta handlar incidenten om att kontinuerlig uppkoppling har brutits.

Av de som uppgett att det skett en incident i ett system eller nätverk uppger de flesta av de som kunnat klassificera sin incident som en förlustincident. Det vill säga en incident som uppstått genom att mjukvara eller hårdvara i systemet eller nätverket har tagits bort, raderats, slutat fungera eller förstörts.

I 68 % av rapporterna inträffar incidenten i en tjänst som tillhandahålls av en extern aktör, det vill säga en underleverantör till leverantören av den samhällsviktiga tjänsten. Detta visar att många leverantörer av samhällsviktiga tjänster, precis som resten av samhället, idag är beroende av it-tjänster som tillhandahålls av externa aktörer.

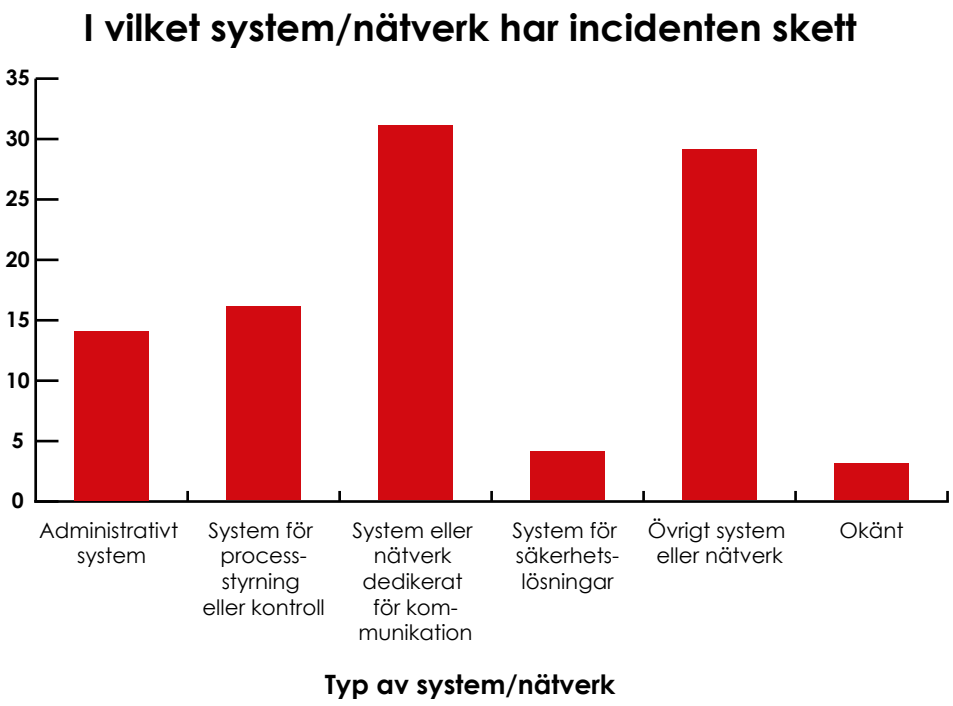


Diagram 1. Föredelning av antalet svar angående i vilket system eller nätverk incidenten inträffat.

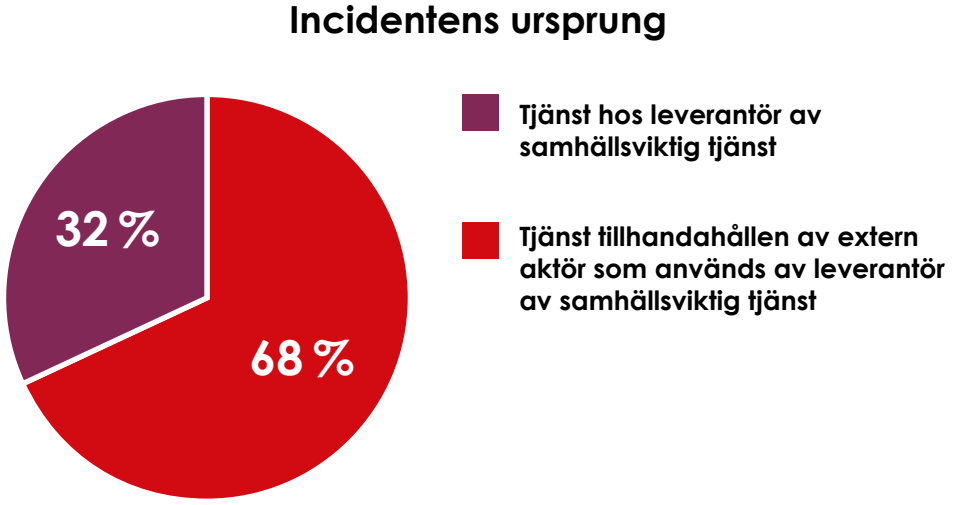


Diagram 2. Fördelningen av svar på frågan om incidenten inträffat i en tjänst tillhandahållen av extern aktör.

Tillgänglighet är den informationssäkerhetsaspekt som påverkats mest av incidenterna i den inkomna rapporteringen.[10] Ett fåtal leverantörer har angett att informationens riktighet har påverkats. Ytterst få av leverantörerna har uppgett att konfidentialitet hos informationen har påverkats negativt i någon form. Detta innebär att de flesta incidenterna som rapporterats handlar om att behöriga inte kan använda eller få tillgång till verksamhetskritisk information när det behövs, snarare än att känslig information röjts.

10. De tre aspekter som anges i svarsformulären och normalt inom informationssäkerhet är tillgänglighet, riktighet och konfidentialitet.

3.2.1 Tid och hur incidenten upptäcks

De rapporterade incidenterna som inträffar hos leverantörerna pågår i snitt 5–10 timmar. Tidsintervallet beskriver när incidenten inträffade (exempelvis när ett centralt system går ner), upptäcktes, hanterades och upphörde. Incidenten upptäcks ofta direkt, och i de flesta fall av egen personal, genom att personalen upptäcker att en tjänst de använder i sitt arbete inte är tillgänglig eller att tjänsten inte fungerar som vanligt. Detta går i linje med rapporteringen om att tillgänglighetsaspekten påverkats i högst utsträckning. I andra fall har incidenten upptäckts av interna detekteringssystem, detta är i rapporteringen vanligare bland bankverksamhet och dricksvattenförsörjning. I några få fall har det rapporterats att incidenten upptäckts av ett externt kontrakterat detekteringssystem.

Ett detekteringssystem kan vara och användas olika beroende på om det gäller upptäckten av en incident eller en störning. För att återvända till det fiktiva exemplet om vattenverket, kan ett detekteringssystem för en störning vara en sensor som upptäcker att vattnet är orent. Ett detekteringssystem för en incident verkar inom informationssystemet eller nätverket och känner av att systemet exempelvis inte kommunicerar som det ska. Det kan också vara ett system som ger indikation på intrång.

3.2.2 Störningen

Rapporterna beskriver att incidenten och störningen i tjänsten i de flesta fall uppkommer och avhjälps samtidigt, eller kort därefter. Dessutom svarar få leverantörer att incidenten orsakar störning för andra aktörer. Endast en incident bedöms ha orsakat en störning som inneburit konsekvenser för en annan eller flera medlemsstater. Detta ger en indikation på att det sker få incidenter med gränsöverskridande konsekvenser men det kan även indikera på begränsad kunskap om andra aktörers beroenden av tjänsten.

Däremot uppskattar leverantörerna sammantaget att störningen i tjänsterna påverkar privatpersoner i relativt hög grad, vilket i viss mån kan antas bero på att hälso- och sjukvårdssektorn står för en stor del av rapporteringen. Leverantörerna bedömer att negativ påverkan av störningarna (om en sådan angetts), gäller privatpersoners hälsa. Dock bedöms påverkan på privatpersoners hälsa oftast som liten. Framförallt bedöms oftast användarnas förtroende för den samhällsviktiga tjänsten vara det som påverkas mest av störningen, vilket inte är obetydligt då förtroende är en viktig del när det kommer till användandet av samhällsviktiga tjänster.

Leverantörerna bedömer i betydande utsträckning att incidenterna orsakade stora störningar på tjänsten. Sammanlagt anger 50 % att hela eller flera funktioner av tjänsten inte kunde tillhandahållas under störningen. I 29 % av fallen påverkades endast vissa funktioner av tjänsten. Samtidigt uppger 21 % att störningen endast påverkade tjänsten i begränsad utsträckning och att den samhällsviktiga tjänsten helt kunde tillhandahållas under tiden, vilket i flera fall beror på alternativa manuella rutiner.

3.2.3 Kostnader

I incidentformuläret får leverantörerna besvara frågor angående kostnader av incidenten. Detta innefattar separata kostnadsuppskattningar för incidenten, störningen samt potentiella förebyggande åtgärder. Leverantörerna får ange en uppskattad lägsta kostnad, en högsta kostnad och en mest sannolik kostnad.

Få av de rapporterande leverantörerna har angett svar över kostnader för incidenten och störningen, vilket kan indikera på att en sådan bedömning är svår att göra i det skedet. I 26 % av fallen uppger leverantörerna att organisationen slutgiltigt har fastställt incidentens kostnader, men ännu färre har presenterat kostnadsuppskattningar i rapporteringen. Utifrån de svar för mest sannolika kostnad som angetts spänner incidentkostnadernas intervall mellan 2 000–1 000 000 kr. Mediankostnaden för en incident bedöms vara 35 000 kr (medelvärde: 129 000 kr). Det är, utifrån sammanställd data, svårt att presentera en representativ kostnad för de inkomna incidentrapporterna. Samma gäller för de kostnadsberäkningar gällande den uppkomna störningen, där uppskattningarna sträcker sig mellan 2 000–5 000 000 kr, och mediankostnaden är 25 000 kr (medelvärde: 451 000 kr).

Utöver information gällande den uppskattade kostnaden, får MSB även information om hur leverantören ämnar täcka kostnaderna. Av de organisationer som är medvetna om hur incidenten ska bekostas, är det ungefär lika många som angett att pengar tas från en fast budget för incidenthantering som de som svarat att kostnader täcks med medel som äskas från annan budget. Kostnadsindikationer kan därför vara av betydelse för leverantörens möjligheter att avsätta en budget för incidentrapportering och få en förståelse för hur mycket en incident eller störning kan kosta. Att inte ange kostnader i incidentrapporten kan även indikera på att personen som fyller i formuläret inte kan göra en sådan beräkning, inte har tillgång till data, har tidsbrist eller inte får redogöra för sådana uppgifter. Det är viktigt att budgetera för säkerhetsarbete, däribland incidenthantering, då det kan planeras för och främja det förebyggande arbetet samt minska risken för nedprioriteringar av andra delar i verksamheten om budgeten måste omplaneras till följd av en incident.

3.2.4 Hantering

I 41 % av rapporterna uppger leverantörerna att de vid tidigare tillfälle har drabbats av en liknande incident. Av dessa hade nästan samtliga även drabbats av liknande störningar. I rapporterna har 29 % av leverantörerna angett att de hade med hjälp av en genomförd riskanalys innan den inträffade incidenten, identifierat att liknande incidenter skulle kunna inträffa. Utav dessa hade 81 % även på förhand bedömt att en sådan incident skulle kunna orsaka en liknande störning. Rapporteringen visar på att flera aktörer har en medvetenhet om vad som kan inträffa men mindre resurser att åtgärda eller förebygga förekomsten av återkommande incidenter.

I rapporteringen hade 55 % av leverantörerna en kontinuitetsplan för liknande incidenter varav 61 % aktiverade kontinuitetsplanen under incidenten. Något färre leverantörer (52 %) hade även en kontinuitetsplan för en liknande störning i den samhällsviktiga tjänsten (se Diagram 3). Av dessa aktiverade 65 % av leverantörerna sina kontinuitetsplaner för den aktuella störningen. Utifrån underlaget är det svårt att bedöma varför kontinuitetsplanerna inte använts vid de aktuella incidenterna. En möjlig orsak är att incidenterna och störningarna inte varit allvarliga nog för att nå de trösklar organisationen satt upp för att aktivera kontinuitetsplanen. En annan möjlighet är att kontinuitetsplanen inte varit praktisk tillämpbar, tillräckligt anpassad eller inövad för att effektivt kunna användas. Det är det är viktigt att betona att kontinuitetsplaner som tas fram är praktiskt tillämpbara och övas.

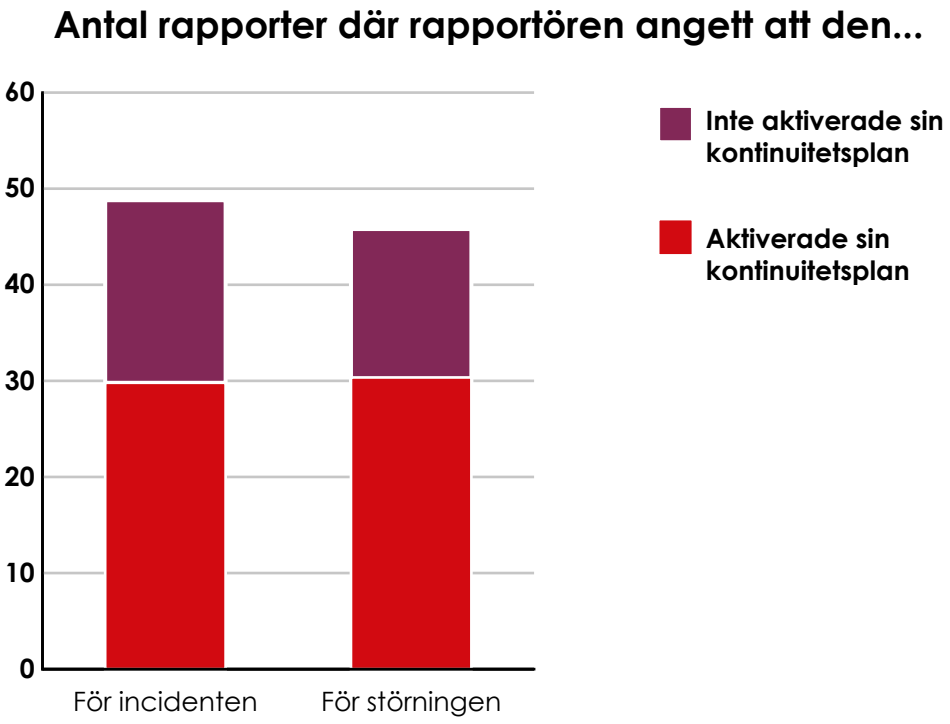


Diagram 3. Staplarna visar antalet rapporter där leverantören uppger att de haft kontinuitetsplaner för liknande incidenter respektive störningar samt vilka som aktiverades.

I drygt en tredjedel av de rapporterade incidenterna hade leverantörerna ett definierat mål för återställningstid vid incidenter. Flera leverantörer har mer generella än tydligt definierade mål. Det vanligaste målet för återställning vid incidenter är 4 timmar. För störningar i den drabbade samhällsviktiga tjänsten är målen längre, och i de fall det anges är det ofta ett dygn. Färre leverantörer har definierat återställningstid för störningar än för incidenter. Att färre har fastställda återställningstider för störningar kan möjligtvis bero på bristande analys av behoven av tjänsten utanför den egna organisationen.

3.2.5 Åtgärder

Mer än två tredjedelar av leverantörerna har eller planerar att genomföra särskilda förebyggande åtgärder med anledning av incidenten eller störningen. Det vill säga att leverantören utifrån incidenten och/eller störningen beslutat att ytterligare förebyggande åtgärder krävs. Syftena med de särskilda hanteringsåtgärderna är nästintill jämt fördelade på att åtgärda incidenten, störningen eller störningens konsekvenser. Drygt en tredjedel har vid rapporteringstillfället implementerat, eller angett att de ämnar implementera, förebyggande åtgärder för att undvika att liknande incidenter och/eller störningar inträffar igen. Dessa åtgärder kan i vissa fall bli dyra och leverantörernas uppskattningar för mest sannolika kostnad ligger mellan 16 000 kr och 2 500 000 kr (median 50 000 kr/medelvärde: 266 000 kr). Som i fallet med kostnader för incidenterna och störningarna, så bör de uppskattade kostnaderna för förebyggande åtgärder inte ser som representativt för alla rapporter då det är drygt en femtedel av rapporterna som anger kostnadsuppskattningar.

Incidentexempel 3

Ett akutsjukhus kunde inte bedriva vård under cirka två timmars tid på grund av nätverksstörningar. Dessa orsakades av överbelastning efter hårdvarufel på DNS-servern samt buggar i mjukvara. Det gick inte att få åtkomst till journalsystem för dokumentation av patienters vård utan detta fick skötas manuellt under tiden för störningen. Akuta operationer och elektiv vård fick ställas in och ambulanstransporter (inklusive prio 1-larm) fick styras om.

Råd kring hantering:

Sjukhusen har i regel reservrutiner så att verksamheten kan löpa på som vanligt även om it-stöd tillfälligt saknas. Det centrala vid den här typen av incidenter är att påminna om vikten av kontinuitetsarbete så att verksamheten kan säkras och påverkan av eventuella it-störningar kan minimeras.

3.2.6 Orsaker

NIS-leverantörerna har vid rapporteringstillfället ibland svårt att avgöra vad som orsakade incidenten och flera anger att orsaken är okänd. Detta kan delvis förklaras av att en stor andel har sitt ursprung i en tjänst som tillhandahålls av en underleverantör och därför saknar tillräcklig insyn. I 13 % av incidentrapporterna uppger leverantören att mänsklig handling orsakat incidenten vilket innebär att någon form av handhavandefel bedöms ha orsakat incidenten. I två rapporter uppger leverantören att syftet bedöms antagonistiskt, det vill säga att någon form av attack inträffat. I de fall leverantören av den samhällsviktiga tjänsten kunnat bedöma orsaken är systemfel den vanligaste kategorin med drygt en tredjedel av samtliga svar.

3.3 Slutsatser

Ett antal slutsatser kan dras utifrån sammanställningen av resultaten och presenteras tematiskt med tillhörande resonemang i detta kapitel.

Under 2020 har 88 rapporterade incidenter skett, vilket är en ökning i jämförelse med 2019, då antalet rapporterade incidenter var 55. Då incidentrapporteringen inte påbörjades förrän under mars 2019 är det svårt att göra jämförelser mellan åren 2019 och 2020, men rapporteringssnittet har ökat från 5,5 rapporter per månad 2019, till 7,3 rapporter per månad under 2020.

NIS-regleringen och de medföljande kraven på incidentrapportering är en relativt ny reglering vilket medför att rapportering från tidigare jämförelseår är ofullständig. Av denna anledning är det inte möjligt att dra konkreta slutsatser kring nivån av incidentrapportering. Det är däremot tydligt att det förekommer skillnader i rapporteringen mellan sektorer, där några sektorer har mycket låg eller ingen rapportering under 2020. Sektorsspecifika kriterier skiljer sig åt gällande vilka leverantörer som omfattas av NIS-regleringen samt vilka incidenter som är rapporteringspliktiga inom respektive sektor. Detta medför att det inte bör förväntas att samtliga sektorer rapporterar i lika hög utsträckning. En annan anledning kan vara att organisationer inom vissa sektorer saknar tillräcklig kunskap om NIS-regleringen, anser sig uppfylla rapporteringsplikt inom annat lagrum eller uppfattar att ansvaret för incidenten ligger hos underleverantör. Vidare kan en skillnad i mognadsgrad gällande informations- och cybersäkerhetsarbete, och därmed förmågan att uppmärksamma och rapportera incidenter, kunna ligga till grund för de skillnader som syns gällande rapporteringsgrad.

I it-incidentrapporteringen från statliga myndigheter (enligt krisberedskapsförordningen), har MSB tidigare dragit slutsatsen att det råder underrapportering av allvarliga it-incidenter. Totalförsvarets forskningsinstitut (FOI) har genom enkätsvar från statliga myndigheter dragit slutsatser kring att underrapporteringen i enlighet med krisberedskapsförordningen beror på flera orsaker, bland annat bristande interna rutiner för identifiering av it-incidenter samt rutiner för överföring av sekretessbelagd information, hög arbetsbelastning, svårigheter i att bedöma incidenters allvarlighetsgrad, bristande återkoppling från MSB samt bristande kunskaper rörande rapporteringsskyldigheten.[11] Det är inte möjligt i detta skede att avgöra huruvida detta gäller även för leverantörer av samhällsviktiga och digitala tjänster.

11. https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4815--SE

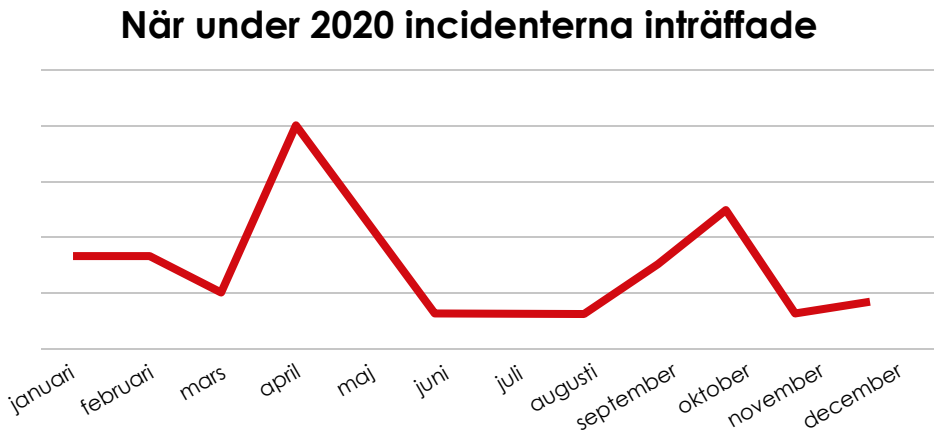


Diagram 4. Årsfördelning över när leverantören uppgett att incidenten inträffade

MSB bedömer utifrån de inkomna incidentrapporterna att det inte skett någon märkbar effekt på antalet incidenter till följd av covid-19-pandemin hos leverantörerna av samhällsviktiga och digitala tjänster. Bedömningen görs baserat på ett antal faktorer, dels när i tid incidentrapporterna inkommit, dels utifrån analys av rapporternas textmaterial vilket inte i någon betydande utsträckning ger indikationer på att pandemin i sig bidragit till en ökad mängd incidenter. Det som däremot kan uppstå som en effekt av rådande omvärldsläge, vilket är synligt i enstaka rapporter, är att störningarna som följer av incidenterna kan förvärras i tider av nedstängning och restriktioner då rutiner är förändrade både hos leverantörer och hos externa aktörer. En möjlig anledning till att återhämtningen efter en incident kan dröja kan exempelvis vara om fysisk teknisk service inte finns tillgänglig på grund av covid-19-relaterade rekommendationer i samhället eller policyer hos externa aktörer. Störningar kan därmed påverka på nya och oförutsägbara sätt givet 2020 års omvärldssituation.

Diagram 4 visar på en kraftig ökning av inrapporterade incidenter under april och även en mindre ökning i oktober, vilket kan ge sken av att det skulle sammanfalla med de restriktioner som infördes internationellt och nationellt till följd av covid-19-pandemins toppar under 2020. Topparna kan snarare förklaras av att det inom vissa sektorer är vanligt att många leverantörer (särskilt inom hälso- och sjukvård) använder en och samma it-infrastruktur eller tjänst som upprätthåller en funktion som är avgörande för leverantören. När denna it-infrastruktur eller tjänst drabbas av en incident uppstår en störning hos flera eller samtliga leverantörer samtidigt. Det innebär att vissa incidenter medför ett stort antal rapporter inkommer samtidigt. Vissa bakomliggande aktörer, som inte omfattas av NIS-regleringen, spelar av denna anledning en stor roll för många av Sveriges samhällsviktiga tjänster.

3.3.1 Antagonistiska hot

Flera internationella aktörer har betonat att den cyberrelaterade brottsligheten har ökat under pandemin och flera allvarliga exempel har fått medial spridning.[12] Mot bakgrund av den pressade situationen för vården och de problem som en utpressningsattack numera för med sig, tog MSB fram information riktad till it-säkerhetsarbetare i hälso- och sjukvårdssektorn och skapade ett forum för ett mer operativt informationsutbyte, från MSB men även vårdgivarna emellan.

12. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

De inkomna rapporterna indikerar inte en ökning eller betydande förekomst av cyberbrottslighet som orsak till NIS-incidenterna, vilket ses i den mycket låga rapporteringen av incidenter där antagonistiskt ursprung anges. Inkommen rapportering ger dock troligtvis inte en fullständig överblick av tillståndet inom sektorerna. Detta då brottslighet kan förekomma utan att leverantören upplever störning, eller av annan anledning inte upptäcker pågående eller genomfört angrepp eller intrång. Leverantörer kan även vara ovetande om incidentens ursprung vilket är vanligt förekommande i incidentrapporteringen. Leverantörer eller underleverantörer kan även avstå från att ange antagonistiskt ursprung eller avstå att rapportera sådana incidenter av andra anledningar. I två rapporter har leverantörer uppgivit att den troliga orsaken till incidenten är antagonistisk handling.

3.3.2 Underleverantörer

Många störningar har koppling till incidenter hos underleverantörer särskilt hos större bolag inom it-tjänster och hos leverantörer av kommunikationstjänster. I rapporteringen blir det tydligt att det finns centrala aktörer som vid störningar orsakar följdeffekter hos flertalet leverantörer av samhällsviktiga tjänster. Det finns i rapporteringen tydliga signaler på att leverantörer av samhällsviktiga tjänster inte alltid har tillräcklig information angående incidenterna vid rapporteringstillfällena, utan förlitar sig på informationsdelning från den externa aktören. Exempelvis illustreras detta i en av incidentrapporterna som inkommit: ”Inväntar leverantörens rapport (underleverantörens, reds. anm.), jag har svårt att fylla i dessa ’tekniska’ frågor då det är leverantören som ansvarar för systemet”. Det är svårt att ha överblick av en incident i ett tidigt skede, men citatet belyser de beroenden av externa aktörers informationsdelning, samt kunskap om it-infrastrukturen som den samhällsviktiga tjänsten förlitar sig på.

I vissa fall kan även underleverantören i sig ha en underleverantör, som NIS-leverantören i sin tur förlitar sig på för att få information om incidenten och störningen. Detta leder i några fall till kedjor av ovisshet kring hur och när incidenten och störningen kan upphöra och vilka åtgärder som vidtas för att störningen inte ska inträffa igen. Komplexa försörjningskedjor orsakar därför ett mindre detaljerat underlag gällande incidenterna, störningarna och leverantörernas hantering. Externa aktörer lyder sällan under NIS-regleringen och det kan därför finnas otydliga kontrakt angående i vilken takt eller i vilken mån information levereras tillbaka till NIS-leverantören. I nätverks- och informationssystem kan effekten av störningar i leveranskedjan orsaka stora störningar hos flera aktörer samtidigt. Detta ställer höga krav på skarpare kravställningar, SLA:er (*service level agreement*), kontaktvägar och regelbunden driftsinformation.

3.3.3 Informationssäkerhetsaspekter

Incidentrapporteringen visar att tillgänglighet är det mest förekommande av de tre informationssäkerhetsaspekterna angivna i formuläret.[13] Utifrån textunderlag i rapporteringen rör det sig ofta om att kontinuerlig uppkoppling brutits, det vill säga att system eller databaser som är uppkopplade gentemot varandra slutar kommunicera. Detta beskriver hur informationslandskapet ser ut och hur digitala tjänster fungerar. Databaser eller andra informationssystem

13. De tre informationssäkerhetsaspekterna är tillgänglighet, riktighet och konfidentialitet.

som leverantörerna behöver för att utföra samhällsviktiga tjänster kräver i högre grad ständig uppkoppling. Tidigare kunde det räcka för leverantörer av samhällsviktiga tjänster att koppla upp sig till exempelvis en databas vid ett givet antal tidpunkter. Rapporteringen visar att när kontinuerlig uppkoppling bryts uppstår störningar nästintill direkt, vilket indikerar att digitaliseringen har gett upphov till ett ökat beroende av kontinuerligt fungerande uppkopplingar. Detta kan ses som en stor del i det ständigt ökande beroendet som samhället har till robusta och digitala flöden.

3.3.4 Kostnader

Ett fåtal av de rapporterande leverantörerna uppger kostnader för incidenter eller störningar. Det kan troligtvis bero på att leverantörerna har svårt att bedöma kostnader, att personerna som rapporterar inte ges tillgång till sådan info, organisationen inte prioriterar att identifiera kostnader eller att de av olika anledningar inte vill uppge sådan information till andra aktörer. Denna rapport kan av denna anledning inte presentera en representativ kostnad för en incident, men den inkomna rapporteringen talar för att incidenter kan orsaka stora kostnader för leverantörerna.

Många leverantörer anger att de drabbas av samma incident eller störning mer än en gång. Detta inträffar som nämnt i redovisningen i fall där hot, sårbarheter och den aktuella störningen identifierats. Anledningarna till att incidenten sker på nytt kan vara flera, exempelvis att leverantörerna inte har råd att åtgärda hoten eller sårbarheterna, att medel för åtgärder är underprioriterat och att störningen därmed behöver accepteras. Andra orsaker kan vara beroendet av externa parter som av samma anledningar inte åtgärdar återkommande problem. De kostnader som uppstår för att helt eliminera hoten eller att åtgärda sårbarheterna är ibland bedömda att vara för stora, och ställer då leverantören mellan att åtgärda problemet eller att ta kostnaden för, och effektivitetsförlusten av, återkommande störningar. Detta bör ses som ett starkt incitament för att planera för och bekosta säkerhetsarbetet – både sett till säkerhet men även gällande effektivitets- och kostnadsbesparingar. Återigen är det viktigt att upprätta tydligare avtal och ha en tydlig kravställning på de underleverantörer som de samhällsviktiga tjänsterna är beroende av.

3.3.5 Rapporteringens vikt för totalförsvaret

Det är viktigt att betona att bilden som presenteras i redovisningen ibland är undermålig, då NIS-leverantörerna ibland saknar tillräcklig information gällande incidenten och störningen, såsom exempelvis incidenters ursprung. Ur ett totalförsvarsperspektiv är det viktigt att MSB, genom incidentrapportering bygger en förståelse för en normalbild i Sverige gällande incidenter och störningar hos samhällsviktiga och digitala tjänster. Detta för att förstå normalägets säkerhetsaspekter och de krav som ställs. Vid gråzonsproblematik, det vill säga ett tillstånd i gränslandet mellan krig och fred, samt i fall av höjd beredskap, är denna kunskap viktig för att bland annat bedöma utvecklingens riktning och vidta rätt åtgärder i tid. Vid ett förändrat omvärldsläge kan en god förståelse av normalläget hjälpa såväl MSB som andra myndigheter och aktörer att skapa mening av förändringen och därmed minska risken för över- eller undertolkning av händelser. Incidenter som drabbar verksamhet som lyder under säkerhetsskyddslagen ska inte ska rapporteras till MSB, men den samlade bilden av enskilda NIS-incidenter är viktig ur ett totalförsvarsperspektiv.

Utöver förändrad tolkning av förekommande incidenter kan en förändring av omvärldsläget skapa stress inom organisationen, behov av omfördelning av resurser från säkerhetsarbetet och på så sätt öka frekvensen av incidenter och förvärra störningarna. Utifrån nuvarande rapportering noteras att många leverantörer av samhällsviktiga tjänster är beroende av ett antal centrala underleverantörer vilket innebär att flera av de tjänster som är viktiga för det svenska samhället kan komma att drabbas vid händelse av storskaliga incidenter.

3.4 Rekommendationer

Följande del återger rekommendationer som baseras på den information som framkommit i incidentrapporteringarna under 2020. Flera av rekommendationerna är giltiga för samtliga leverantör av samhällsviktiga och digitala tjänster.

1. NIS-leverantörer bör se över kravställningar och SLA:er med externa aktörer.
   - Se över att underleverantörer har rutiner och bemanning för avvikelse- och incidenthantering samt hur rapportering sker mellan er organisation och externa aktörer. Detta är viktigt för att säkerställa att organisationen snarast får all relevant information om incidenter så att rapporteringsplikten kan uppfyllas.
   - Om ekonomin tillåter kan redundans byggas genom att ha en back-up lösning från annan aktör.
   - Om den externa aktören förändrar sina villkor måste även skrivningar mellan parterna uppdateras.
   - Inkludera skrivelser i SLA:er gällande att den externa parten måste kunna säkerställa att ytterligare underleverantörer bedriver ett ändamålsenligt informationssäkerhetsarbete med ovan beskrivna rutiner kring incidentrapportering.

2. NIS-leverantörerna bör ha tydliga rutiner gällande incidentrapportering där relevant information tagits fram och görs tillgänglig för den eller dem som rapporterar för organisationen.
   - Att organisationen har ett arbetssätt för incidenthantering är en viktig del i det systematiska informationssäkerhetsarbetet. Incidenthanteringsarbetet handlar om att förbättra organisationens förmåga att minimera risken för att incidenter uppstår, minska incidenters konsekvenser, utreda orsakerna till incidenten och därigenom förbättra skyddet så att liknande incidenter inte inträffar i framtiden.
   - Incidentrapporteringsprocessen måste kunna engagera rätt resurser och kompetens inom organisationen för att få tillgång till information för att kunna svara på formulärens frågor och uppfylla rapporteringsplikt. Rapportering bör ske på systematiskt och likvärdigt sätt och således sträva efter att undvika personberoenden.

3. Det är rekommenderat att ha mål för återställning då detta kan påskynda hanteringen av incidenten och höja ambitionsnivån.
   - Det är viktigt att dimensionera återställningstider efter inhämtning och analys hos andra parter i samhället utifrån aktuell samhällsviktig tjänst. Detta för att öka förståelsen kring externa aktörers beroende av tjänsten/tjänsterna.

4. Genom att budgetera för incidenter kan organisationen ha en beredskap för oväntade kostnader och minskar risken att övrig verksamhet påverkas.
   - Incidentrapporteringen kan visa att samma eller liknande incidenter ibland riskerar att ske återkommande och på så sätt motivera kostnader av säkerhetsåtgärder med en alternativ kostnad för upprepade incidenter som annars följer.

5. Att arbeta systematiskt och riskbaserat ger aktörerna en mer övergripande bild av vilka hot och sårbarheter verksamheten står inför, och minskar risken att drabbas av incidenter.
   - Viktiga moment i det riskbaserade och systematiska arbetet är bland annat att säkra ledningens engagemang gällande säkerhetsarbetet, riskanalyser, informationsvärdering och klassning, GAP-analyser, utformande av arbete och struktur, vidtagande av säkerhetsåtgärder, uppföljning och förbättringsinsatser.

Incidentexempel 4

Ett strömavbrott påverkade en samhällsviktig transportanläggning under cirka 2,5 timmes tid. Kameraövervaknings- och passagesystem, vaktbolagets larmcentral samt underliggande it-system var då ur funktion. Access till vissa områden påverkades också, då strömtillförsel saknades i grindar och dylikt. Störningen orsakades av ett fel mellan två närliggande ställverk och upphörde när strömmen återställdes.

Råd kring hantering:

Strömavbrott och elfel inträffar då och då, därför är det viktigt att ha kontroll över sina interna rutiner och dimensionera sin kapacitet i reservkraft. När det gäller samhällsviktig verksamhet och/eller tjänster är det av yttersta vikt att ha färdiga reservrutiner och redundanta system nära till hands, och redo för användning, för att minimera samhällsstörningen (eller risken för sådan) i tid och omfång.

Stöd från MSB

Foto: Kicki Nilsson/Icon Photography

4. Stöd från MSB

I följande avsnitt beskrivs en del av det stöd som MSB kan ge till aktörer gällande incidentrapportering och övrigt säkerhetsarbete.

4.1 CERT-SE

CERT-SE (Computer Emergency Response Team) har som uppgift att stödja samhället i arbetet med att hantera och förebygga it-incidenter, inte bara enligt NIS-regleringen utan även gällande andra typer av verksamheter. Ett exempel på vanligt förekommande ärenden är att bistå med rådgivning och stöd vid kapade e-postkonton, hantering av skadlig kod och överbelastningsattacker. En annan typ av ärende är att informera och uppmärksamma aktörer som använder sig av sårbar programvara, för att kunna avvärja angrepp. Vid ett flertal tillfällen under 2020 har CERT-SE identifierat allvarliga sårbarheter och kunnat ge stöd för att undvika eventuella angrepp. CERT-SE har även samverkat internationellt och varit involverat i hanteringen av internationella incidenter.

Vid en incident kan CERT-SE bistå med olika typer av stöd och rådgivning, inkluderat proaktivt stöd på plats i organisationens egen it-miljö (beroende på incidentens natur). CERT-SE kan nås dygnet runt via 010-240 40 40 och cert@cert.se.

4.2 Vikten av att arbeta systematiskt och riskbaserat

För att minimera effekterna av en incident är det av stor vikt att ha ett förebyggande arbete på plats inom organisationen. MSB ger ut stöd kring systematiskt informationssäkerhetsarbete som bidrar till att skapa en robust verksamhet vilket i sin tur kan medföra en större beredskap kring NIS-incidenter. NIS-regleringen gäller specifikt de nätverks- och informationssystem som den samhällsviktiga eller digitala tjänsten är beroende av, men grunderna i det systematiska och riskbaserade informationssäkerhetsarbete är detsamma oavsett vilken eller vilka verksamheter som omfattas. Om det redan finns ett informationssäkerhetsarbete i organisationen behövs inte ett separat arbete för den del av verksamheten som omfattas av NIS-kraven. Omvänt så kan också ett arbete som etableras för att möta NIS-kraven efter hand utvidgas till övriga delar av verksamheten om detta inte funnits tidigare.

För att uppnå och bibehålla en tillräcklig nivå av informationssäkerhet i en verksamhet är det viktigt att arbeta systematiskt, riskbaserat och långsiktigt. Ett sådant arbete gör det möjligt att skydda nätverks- och informationssystem även i takt med att krav och behov förändras. Det hjälper också organisationen att prioritera resurser och att kunna hantera och återhämta sig från incidenter.

Att arbeta systematiskt innebär att regelbundet analysera verksamhetens krav, att införa ändamålsenliga säkerhetsåtgärder utifrån dessa samt att kontinuerligt följa upp och förbättra skyddet. Med riskbaserat menas att säkerhetsåtgärderna ska vara anpassade till verksamhetens identifierade risker och behov, vilket ger ett ändamålsenligt skydd som inte kostar eller stör mer än nödvändigt.

MSB erbjuder ett metodstöd till stöd för organisationer i att bedriva ett systematiskt informationssäkerhetsarbete som bygger på de internationella standarderna i ISO/IEC 27000-serien. Metodstödet beskriver de delar som krävs för att kunna skapa en systematik i arbetet med informationssäkerhet – från hur analyserna kan genomföras till hur styrdokument kan utformas. Metodstödet är tillgängligt för alla, och går att applicera oavsett storlek eller organisationsform.

Tips om metodstödet för NIS-leverantörer

Du hittar metodstödet i sin helhet och fler verktyg på: www.informationssakerhet.se

Nedan följer ett antal råd och tips på hur en organisation kan arbeta systematiskt med stöd från metodstödet.

- **Ledningens ansvar:** Den högsta ledningen har det övergripande ansvaret för informationssäkerheten inom sin organisation, den behöver fatta nödvändiga beslut om inriktning och resurser samt följa upp resultaten. En ledning som är engagerad och införstådd med verksamhetsnyttan med informationssäkerhetsarbetet skapar goda förutsättningar för ett ändamålsenligt skydd.
- **Organiseringen av arbetet:** För att över tid kunna utveckla och upprätthålla informationssäkerhetsarbetet är det väsentligt att roller och ansvar är definierade och kända inom hela organisationen. Personer i dessa roller behöver också mandat och resurser för arbetet.
- **Internt regelverk:** Anvisningar och instruktioner är ofta omfattande och riktar sig till olika målgrupper. Tänk på att ta fram enkla anvisningar, anpassa dem till respektive grupp och i första hand lägga in dem i befintlig dokumentation som beskriver hur personalen ska utföra olika arbetsuppgifter.
- **Analysera informationstillgångar:** Identifiera de nätverk och informationssystem som den samhällsviktiga eller digitala tjänsten är beroende av. Kom ihåg att även externa informationstillgångar kan vara kritiska, t.ex. hos samarbetsparters eller systemleverantörer. Värdera tillgångarna utifrån olika skyddsbehov såsom skydd mot obehörig tillgång och behov av tillgänglighet.
- **Riskanalys.** Identifiera de hot och oönskade händelser som kan leda till negativa konsekvenser för verksamheten och analysera dem genom att undersöka sannolikhet och konsekvenser. Bedöm sedan hur allvarliga de olika riskerna är och gör en plan för hur de ska hanteras.
- **Kontinuitetshantering:** Analysera hur den samhällsviktiga eller digitala tjänsten kan upprätthållas om en incident eller annan störning inträffar. Identifiera, utforma och öva de åtgärder som behövs för att mildra konsekvenserna och snabbare återhämta sig från en störning, exempelvis alternativa arbetssätt eller dubblerade system.

I informationssäkerhetsarbetet är det viktigt att ta fram något som används och fungerar – inte blir en ”hyllvärmare”. Det är bättre att göra något enkelt till att börja med, som utformas på ett bra sätt och anammas i verksamheten. Genom det kontinuerliga arbetet kan arbetet sedan utökas efterhand. Om det redan finns relevanta eller besläktade arbetssätt i organisationen, exempelvis kring riskhantering eller systematiskt arbete på andra områden, kan dessa med fördel återanvändas och samordnas med informationssäkerhetsarbetet.

4.3 Arbetet framåt

MSB och andra myndigheter genomför ett antal satsningar som berör informations- och cybersäkerheten i samhället och har en inverkan på NIS-leverantörerna. Nedan följer ett axplock av de satsningar som inletts och som görs framöver:

- **Cybersäkerhetscentret:** I december 2020 beslutade regeringen att inrätta ett nationellt center för cybersäkerhet. Försvarsmakten, Försvarets radioanstalt (FRA), MSB och Säkerhetspolisen ska inrätta och bygga upp centret i nära samverkan med Post- och telestyrelsen (PTS), Polismyndigheten samt Försvarets materielverk (FMV) som ska ges möjlighet att medverka i centrets verksamhet. Det övergripande målet för Nationellt center för cybersäkerhet är att vara stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige och minska cybersårbarheterna. Samverkan med privata och offentliga aktörer ska utgöra en central del av uppdraget. Verksamheten i centret ska successivt byggas upp under en femårsperiod för att kunna ge full effekt 2025. Målet är att centret på sikt ska sammanställa gemensamma analyser och övergripande lägesbilder avseende hot och sårbarheter, sprida information mellan ingående myndigheter och andra aktörer samt koordinera arbetet vid it-incidenter och cyberangrepp. Läs mer om cybersäkerhetscentret och ta del av centrets publikationer på www.cfcs.se.
- **NIS-satsningar inom avtalet med INEA:** MSB har nått en överenskommelse med EU-organet INEA om medfinansiering av ett utvecklingsarbete kopplar till MSB:s roll som nationell kontaktpunkt för NIS i Sverige. Arbetet syftar till att stärka tillämpningen av den svenska NIS-regleringen. Ansökan beviljades våren 2020 och överenskommelsen blev klar under sommaren. Finansieringen sträcker sig fram till och med 2023. Överenskommelsen täcker sex aktiviteter som omfattar både ny och existerande verksamhet på MSB. Nya inslag är en årskonferens för NIS, leverantörsforum för NIS-leverantörer och denna årsrapport över incidentrapportering från NIS-leverantörer. I överenskommelsen ingår även revidering av NIS-föreskrifterna för identifiering och incidentrapportering, NIS samarbetsforum och NIS Cooperation Group vilka ingår i MSB:s uppdrag kopplat till NIS, men här används medlen för att stärka upp arbetet och till viss mån informationsspridning.
- **Digitalt system för incidentrapportering:** Under 2021 kommer MSB lansera ett digitalt sätt för incidentrapportering. Detta verktyg kommer att göra det enklare för leverantörer att uppfylla sin rapporteringsplikt gentemot nuvarande förfarande.

Europeiska erfarenheter

Foto: iStock

5. Europeiska erfarenheter

För att nå en ökad informations- och cybersäkerhet krävs samarbete mellan länder då it-incidenter kan ha spridningseffekter internationellt. För att motverka, samverka och hantera incidenter inom EU finns ett antal nätverk där information delas mellan medlemsstaterna. Att dra lärdom av andra länders erfarenheter gällande incidentrapportering och hantering är centralt för att förstå hur aktörer i längden kan hantera incidenter.

5.1 Utvecklingen av NIS-direktivet och cybersäkerheten på europeisk nivå

Inom CSIRT-nätverket, där nationella CSIRT-enheter från samtliga medlemsstater ingår, utbyts information om incidenter som kan få allvarliga eller gränsöverskridande konsekvenser. Gruppen bedriver också ett arbete för att kontinuerligt bevaka hot i unionen och skapa en gemensam lägesbild. Nationella CSIRT-enheter har funnits sedan 1990-talet, men när direktivet antogs saknade flertalet medlemsstater sådana enheter. Idag deltar CSIRT-enheter från samtliga medlemsstater i samarbetet inom nätverket vilket har skapat ett starkare förtroende och fördjupat samarbete som i sin tur bidrar till att förstärka arbetet mellan medlemsstaternas informationssäkerhetsmyndigheter.

NIS Cooperation Group är det forum och en samarbetsgrupp där policyfrågor diskuteras och beslut fattas och där Sverige representeras av MSB. I Cooperation Group finns även arbetsgrupper (så kallade work streams) som arbetar utefter tematiska områden i NIS-direktivet, men även andra frågor som är viktiga för utvecklingen inom informations- och cybersäkerheten, såsom 5G-frågor, säkerhetsåtgärder och storskaliga cyberincidenter. Samarbetsgruppen stödjer och underlättar det strategiska samarbetet, utbytet av information samt skapar förtroende och tillit mellan medlemsstaterna, allt i syfte att uppnå en hög gemensam nivå på säkerheten i nätverks- och informationssystem inom unionen.

NIS direktivet är en av flera delar i det arbete EU bedriver för att höja säkerheten i unionens nätverks- och informationssystem samt informations- och cybersäkerheten överlag. Utöver NIS-direktivet pågår ett antal andra satsningar.

5.1.1 Uppdaterat direktiv

Under 2020 har EU-kommissionen fortsatt arbetet med att förbereda den kommande revideringen av NIS-direktivet. Arbetet presenterades i december 2020, och förslaget innehöll flertalet förändringar i jämförelse med nuvarande direktiv. Till exempel föreslogs flertalet nya sektorer och delsektorer, likaså föreslår kommissionen ett uniformt identifieringsförfarande av leverantörer. Nu genomläses och analyseras förslaget i samtliga medlemsstater för att därefter förhandlas inom

unionen. Förhandlingen börjar under våren 2021 och det är Regeringskansliet som ansvarar för det arbetet för Sverige. När förhandlingarna är färdiga ska förslaget om ett nytt NIS-direktiv beslutas av EU-parlamentet och EU:s ministerråd.

> EU-kommissionens förslag på uppdaterat NIS-direktiv finns att läsa på:
> https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

I arbetet med uppdateringen har kommissionen sett paralleller med ECI direktivet om kritisk infrastruktur. Till exempel vad gäller problembild och upplägg. ECI direktivet administreras av generaldirektoratet för migration och inrikesfrågor (DG HOME) och NIS direktivet av generaldirektoratet för kommunikationsnät, innehåll och teknik (DG CNECT). Under hösten har samarbetet mellan DG HOME och DG CNECT intensifierats i samband med översynsarbetet. När kommissionen presenterade det nya förslaget till NIS direktiv presenterade de även ett nytt direktiv som ska ersätta det gamla ECI direktivet – Directive on the resilience of critical entities (CER Directive). Ett resultat av det är att det finns tydligare beröringspunkter mellan direktiven.

5.1.2 Cybersäkerhetsakten

Cybersäkerhetsakten trädde i kraft den i mitten av 2019. Den 28 juni 2021 kommer hela akten, inklusive de artiklar som kräver kompletterande bestämmelser på nationell nivå, att börja tillämpas. Det huvudsakliga syftet med förordningen är att säkerställa en väl fungerande inre marknad och samtidigt sträva efter att uppnå en hög nivå i fråga om informations- och cybersäkerhet, *cyberresiliens* och förtroende inom unionen. Förordningen är uppdelad i två delar. Den första delen gäller fastställandet av mål, uppgifter och organisatoriska frågor som rör ENISA vilket givit organisationen ett stärkt och permanent mandat. Den andra delen reglerar fastställandet av ett europeiskt ramverk för cybersäkerhetscertifiering. Skapandet av europeiska ordningar för cybersäkerhetscertifiering kommer att medföra att certifikat som utfärdas enligt dessa certifieringsordningar blir giltiga och erkända i alla medlemsstater. Den utredning som haft till uppgift att föreslå nationella anpassningar och en utpekad cybersäkerhetscertifieringsmyndighet har föreslagit att Försvarets materielverk (FMV) ska få den uppgiften i Sverige. Myndigheten kommer bland annat att få i uppdrag att övervaka och kontrollera organ för bedömning av överensstämmelse, innehavare av europeiska cybersäkerhetscertifikat och utfärdare av en EU-försäkran om överensstämmelse.

5.1.3 Ny EU-strategi på cybersäkerhetsområdet

Den 16 december 2020 presenterade kommissionen EU:s nya cybersäkerhetsstrategi – *The EU's Cybersecurity Strategy for the Digital Decade*. Strategin samlar flera av de initiativ som EU vill prioritera inom ramen för arbete med cybersäkerhet i unionen. Cybersäkerhet presenteras i strategin som en viktig del i EU:s större arbete med ökad säkerhet. Cybersäkerhet är en fråga som kommer in på flera olika politikområden och EU behöver bli en stakare aktör.

Den nya cybersäkerhetsstrategin innehåller tre grundpelare:

1. verka för resliens, teknisk suveränitet och ledarskap
2. bygga operativ förmåga att förhindra, avskräcka och besvara
3. främja en global och öppen cyberarena.

Inom ramen för vare grundpelare finns flera olika initiativ och strategiska prioriteringar. NIS-direktivet har en central roll som de regelverk som ska lägga grunden för och höja säkerheten i unionens nätverks- och informationssystem samt informations- och cybersäkerheten överlag. Ett annan viktig del i strategin är att kommissionen vill öka EU:s möjlighet att agera mer samlat i en kris och att dela information och lägesbildsuppfattning med varandra. Detta ska uppnås genom att utveckla och fördjupa flera befintliga delar. Strategin är en viktig utgångspunkt för fortsatt utveckling av cybersäkerhetsfrågorna inom EU och samlar ihop flera av de frågor som drivs inom EU.

5.1.4 EU:s långtidsbudget och återhämtningsplan

EU:s långtidsbudget för 2021–2027 uppgår till 1074 miljarder euro i åtaganden. Återhämtningspaketet, en del av långtidsbudgeten, är fördelat på 390 miljarder euro i bidrag och 360 miljarder euro i lån. I budgeten planeras betydande satsningar på informations- och cybersäkerhetsarbetet i unionen. Bland annat finansieringen av ett europeiskt kompetenscentrum och nationella samordningscenter inom cybersäkerhet.

5.1.5 Det europeiska kompetenscentret och nätverket av nationella samordningscenter

Förslaget till EU-förordning COM (2018) 630 ska stärka cybersäkerhetskapaciteten, cybersäkerhetskunskapen och cybersäkerhetsinfrastrukturen inom EU till förmån för näringsliv, offentlig sektor och forskarsamhället. Förordningen anger att ett europeiskt kompetenscenter för cybersäkerhet ska etableras och som ska knyta till sig ett nätverk av nationella samordningscenter (NCC). Kompetenscentret kommer att etableras i Bukarest under 2021. MSB har av regeringen blivit utsedd att i samarbete med Vinnova förbereda för etableringen av Sveriges nationella samordningscenter.

5.1.6 Joint Cyber Unit

Joint cyber unit (JCU) är en plattform och ett samarbete som ska kunna stödja och skydda EU från de mest allvarliga cybersäkerhetsincidenterna, särskilt de med gränsöverskridande konsekvenser. Grundtanken är att genom bättre informationsdelning inom EU och mellan nationella aktörer i medlemsstaterna kunna öka EU:s samlade förmåga att hantera risker och hot.
Uppbyggnaden ska ske stegvis. Först ska förmågor som redan finns definieras och beskrivas, därefter ska ett ramverk för strukturerat stöd och samarbete tas fram. När ramverket finns på plats ska ytterligare förmågor utvecklas tillsammans med industri och andra partners. Kommissionen kommer komma med ytterligare preciseringar gällande JCU under första delen av 2021.

5.2 Jämförelse mellan länder

För att öka förståelsen för NIS-direktivet på europeisk nivå och dess implementering inom andra medlemsstater återger detta kapitel ett antal exempel på hur länder arbetar med NIS-direktivet, vilka generella trender som setts samt exempel på incidenter som inträffat i respektive land. NIS-direktivet gäller över hela unionen och implementeringen av direktivet anpassas till respektive lands individuella lagar och nationella förutsättningar. Det innebär en del variation kring NIS-direktivet och dess utformning i medlemsstaterna, exempelvis gällande antalet tillsynsmyndigheter, NIS-leverantörer eller vilka incidenter som anses rapporteringspliktiga. En central skillnad är gällande kriterierna för vilka organisationer som identifieras som NIS-leverantörer samt kriterierna för vilka incidenter och störningar som är betydande nog att rapportera. Direktivet nämner att incidenter som har en betydande inverkan på kontinuiteten av den samhällsviktiga tjänsten ska rapporteras. Följande faktorer ska beaktas av medlemsstaterna när ”trösklar” för incidenter ska bestämmas av enskild medlemsstat:

1. antalet användare som påverkas av störningen av den samhällsviktiga tjänsten
2. hur länge incidenten varar
3. hur stort geografiskt område som påverkas av incidenten.[14]

Vissa länder har höga trösklar för vad som anses vara en rapporteringspliktig incident, medan andra har lägre trösklar. Av denna anledning är det svårt att jämföra antalet incidenter mellan länderna då det kan ge en missvisande bild. Att vissa länder rapporterar ett betydligt högre antal incidenter betyder inte är att det sker fler incidenter, utan det kan bero på vilka aktörer som är bundna att rapportera samt vilka trösklar för incidenter som landet har satt.

MSB har i arbetet med rapporten varit i kontakt med andra europeiska SPOC:ar för att utbyta erfarenheter och förstå hur implementeringen av NIS-direktivet arbetats med i respektive land.

5.3 Finland

Finlands SPOC och motsvarighet till MSB är finska nationella cybersäkerhetscentret (NCSC-FI) som är en del av Transport- och kommunikationsmyndigheten (Traficom). Till skillnad från MSB, som saknar tillsynsansvar, så bedriver Traficom tillsyn över sektorerna transport, digital infrastruktur och digitala tjänster. Landet har istället för att centralisera incidentrapporteringsföreskrifterna och kriterier för att rapportera en NIS-incident, ett dussintal olika sektoriella lagstiftningar. NCSC-FI är utöver SPOC, även Finlands CSIRT-enhet och mottar och hanterar all incidentrapportering.

Till skillnad från Sverige har Finland mottagit en mindre mängd NIS-incidentrapporter och utefter detta även sorterat vilka som anses vara betydande nog att vara en NIS-incident. I Sverige behandlas och räknas samtliga inrapporterade NIS-incidenter. Finland beskriver att de trösklar incidenter måste uppnå för att vara en NIS-incident är svåra att nå i skandinaviska länder då länderna är förhållandevis små i jämförelse med andra europeiska länder. Finland anser att direktivets begrepp gällande incidenters och störningars allvarlighetsgrad bör omformuleras så att fler incidenter kan inkluderas.

14. NIS-direktivet artikel 14 p. 4.

Incidentexempel från Finland

I juni 2019 infiltrerades ett centralt nätverk i den finska staden Lahti vilket ledde till att ett tusental arbetsstationer och servrar potentiellt kunde kontrolleras av infiltratören. Ett antal äldre ICT-system delades mellan staden och det regionala sjukhuset vilket bland annat medförde påverkan på sjukhussystemet. För att stoppa attacken och förhindra att servrarna togs över, stängdes stora delar av internetuppkopplingen ner under fem dagar vilket ledde till att tillgången till patientinformationssystem på flertalet ställen begränsades. Nedstängningen påverkade samhället brett och orsakade en betydande störning, men andra samhällsviktiga tjänster såsom dricksvattenförsörjning påverkades inte av nedstängningen. Information om händelsen delades inom interna forum för incidentrapportering. Hanteringen av incidenten orsakade i sig en stor störning i samhället, vilket klassades som en NIS-incident.

5.4 Tyskland

BSI (Bundessamt für Sicherheit in der Informationstechnik) är Tysklands SPOC och agerar under nationell NIS-lagstiftning men har även ett tillsynsansvar. BSI har sanktionsrätt över flera av sektorerna gällande de säkerhetsåtgärder som finns inom NIS-direktivet och incidentrapporteringsregleringen. BSI samarbetar med andra myndigheter som i sin tur har tillsyn över områdena finansiella tjänster och energi. Vidare bedriver BSI även ett operativt arbete och har ett ambulerande team som kan hjälpa leverantörerna på plats vid behov.

Likt den svenska regleringen identifierar och registrerar de tyska leverantörerna av samhällsviktiga tjänster sig själva som en NIS-leverantör enligt det som kallas ”operator driven approach”, vars motsats innebär att myndigheterna pekar ut de leverantörer som lyder under regleringen.

Fram till och med oktober 2020 har BSI mottagit 420 NIS-incidentrapporter, där hälso- och sjukvårdssektorn samt energisektorn står för flertalet av rapporterna. BSI understryker att året präglats av en högre grad av utpressningsvirus mot sjukvården än tidigare år. Många incidenter kan även länkas till föråldrade ICS-system. I likhet med MSB har BSI mottagit få rapporter från leverantörer av digitala tjänster.

En skillnad mellan Tyskland och flera EU-medlemsstater är att landets reglering inte kräver att en faktisk störning av tjänsten ska ha inträffat för att en incident ska vara rapporteringspliktig. Det finns därmed inga ”tröskelvärden” för incidenter, utan även incidenter som potentiellt skulle kunnat orsaka en störning i samhället ska rapporteras. Detta kan förklara Tysklands höga rapporteringsgrad, till skillnad från Finland, som har höga trösklar för att rapportera en incident.

BSI har ett starkt privat-offentligt perspektiv och ser samarbete mellan myndigheter och NIS-leverantörer som ett viktigt sätt att realisera NIS-direktivets mål kring höjandet av landets informations- och cybersäkerhet på. De arbetar med flertalet forum där kunskap kan delas mellan NIS-leverantörer men även med övriga intressenter som inte nödvändigtvis omfattas av NIS-regleringen.

Incidentexempel från Tyskland:

Universitetssjukhuset i Düsseldorf blev under 2020 utsatt för en utpressningsattack. Ett trettiotal servrar krypterades vilket bland annat medförde att all patientdata blev otillgänglig under en tid. Till följd av detta kunde sjukhuset inte ta emot nya akutfall. I förlängningen ledde detta till ett dödsfall, då en person som nekats vård på grund av störningen avled när personen istället behövde transporteras till ett sjukhus längre bort. Händelsen blev mycket omskriven och är ett av få fall där ett dödsfall tydligt kan kopplas till en incident.

5.5 Storbritannien

Då Storbritannien var en fullvärdig medlem av EU när NIS-direktivet antogs har landet implementerat direktivet till nationell lagstiftning. Storbritannien ämnar även behålla regleringen efter utträdet ur unionen. Storbritannien kommer däremot inte att automatiskt följa den framtida utvecklingen av direktivet som sker på EU-nivå, utan utveckla arbetet kring NIS enligt egna identifierade behov. I och med utträdet har landet även lämnat Cooperation Group och CSIRT-network, men fortsätter samarbetet och informationsutbytet gällande informations- och cybersäkerhet i andra forum.

I Storbritannien har the Department of Digital, Culture, Media and Sports (DCMS) samordningsansvaret över NIS-regleringen. National Cyber Security Centre (NCSC) som är del av Storbritanniens kommunikationshögkvarter (GCHQ), är landets CSIRT och SPOC. Eftersom landet har federala inslag har regleringen en blandning av sektoriella myndigheter på både nationell och regional nivå, så som i Nordirland, Wales och Skottland. Det är upp till varje sektorsmyndighet att föreskriva och det finns ingen central myndighet som har föreskriftsrätt inom NIS. NCSC producerar årligen en rapport som ger insikt i de cyberattacker som sker i Storbritannien. I 2020 års rapport beskriver NCSC att covid-19-pandemin har skapat nya möjligheter som hotaktörer har utnyttjat.[15]

Storbritannien inte delat något incidentexempel då väldigt få formella NIS-incidenter har nått de trösklar som de sektoriella regleringarna satt. De beskriver också att det är svårt för en incident att nå så pass höga nivåer och ser att en sådan incident troligtvis är gränsöverskridande. Landet har i likhet med Sverige och många andra länder ett krav på att en faktiskt negativ inverkan måste ha skett på tjänsten. Inom transportsektorn måste exempelvis 20 % av flygtrafiken på en flygplats (med mer än 350 000 flyg per år) bli inställda till följd av en enskild incidents störning under loppet av 24 timmar för att räknas som rapporteringspliktig enligt NIS. Även om mängden rapporteringspliktiga incidenter är låg så betonar NCSC att det sker flertalet incidenter hos NIS-leverantörer som rapporteras på annat vis, och att NCSC har hög prioritet kring incidenter hos NIS-leverantörer.

15. 2020 års rapport från National Cyber Security Centre finns tillgänglig på https://www.ncsc.gov.uk/news/annual-review-2020

Sammantaget kan ett antal jämförelser göras mellan de europeiska exempel som återgivits. Dels att tröskelvärdena varierar mellan medlemsstaterna vilket innebär en skillnad i antal inrapporterade incidenter, dels vilka aktörer och verksamheter som omfattas av rapporteringskraven. Det är ofta svårt att jämföra länder då både tröskelvärden och beskrivningen av samhällsviktiga aktörer varierar. I förhållande till exempelvis Finland och Storbritannien får MSB in ett stort antal incidentrapporter. Informations- och cybersäkerhet är en global, regional och nationell angelägenhet. Arbetet inom EU och unionens satsningar är viktiga för Sverige och samarbetet inom unionen är viktigt för att höja den unionsgemensamma och nationella ambitionen att stärka säkerheten hos flera av de mest samhällskritiska aktörerna inom våra allt mer digitaliserade samhällen.

Slutord

6. Slutord

NIS-direktivet och den svenska NIS-regleringen är en viktig grundstomme för att höja informations- och cybersäkerheten hos leverantörer av samhällsviktiga och digitala tjänster. Då digitaliseringen och automatiseringen av tjänster ökar kommer NIS-direktivet fortsätta vara viktigt för att skapa en bild av incidenter och störningar i samhällsviktiga och digitala tjänster och sträva mot en högre nivå av säkerhet.

I den incidentrapportering som inkommit under året ses ett antal teman som är centrala för den fortsatta kunskapshöjningen av NIS. Bland annat att incidenter kan drabba flertalet NIS-leverantörer samtidigt, och att bristfälliga kontrakt med underleverantörer kan leda till informationsunderskott gällande incidenter.

Utvecklingen av NIS-direktivet som sker på EU-nivå kommer möjligtvis att innebära en inkludering av fler sektorer och aktörer samt innebära en översyn gällande de skillnader i implementeringen av direktivet som synts över unionen. Flertalet satsningar för att höja informations- och cybersäkerheten i Sverige pågår där NIS-regleringen är en central del. Närmast kommer ett antal viktiga saker ske, dels förhandlingarna om ett uppdaterat NIS-direktiv på europeisk nivå, dels genom tillsynsmyndigheternas nya sektorsspecifika föreskrifter.

Sammantaget är det viktigt att incidentrapportera för att möjliggöra en så heltäckande bild som möjligt av de incidenter som sker i samhällsviktiga och digitala tjänster samt belysa vikten av systematiskt informationssäkerhetsarbete. Incidentrapporteringen är en central del i att öka förståelsen gällande Sveriges informations- och cybersäkerhet och redovisningen av NIS-leverantörers incidenter kommer över tid att utgöra en viktig källa för en förståelse för normalbilden i Sverige.

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 MSB1695 - februari 2021 ISBN 978-91-7927-106-0