Myndigheten för samhällsskydd och beredskap

Medfinansierat av Europeiska unionens fond för ett sammanlänkat Europa

ÅRSRAPPORT

It-incidenter som påverkar samhällsviktiga och digitala tjänster

NIS-leverantörers it-incidentrapportering 2021

It-incidenter som påverkar samhällsviktiga och digitala tjänster – NIS-leverantörers it-incidentrapportering 2021

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

Foto: Melker Dahlstrand
Produktion: Advant

Publikationsnummer: MSB1916 – februari 2022
ISBN: 978-91-7927-237-1

Begreppsförklaring

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

- **Informationssäkerhet:** Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.
- **Konfidentialitet:** Att endast behöriga har tillgång till informationssystemen eller informationen.
- **Riktighet:** Att informationssystemen eller informationen går att lita på.
- **Tillgänglighet:** Att informationssystemen eller informationen är tillgänglig för behöriga.
- **NIS:** NIS kommer utav direktivet The Directive on security of network and information systems – the NIS Directive. På svenska heter direktivet ”Åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen”.
- **NIS-regleringen:** Samlingsnamn på den lag (SFS 2018:1174) förordning (SFS 2018:1175) och föreskrifter som antagits i Sverige för att implementera NIS-direktivet (EU) 2016/1148.
- **NIS-leverantör:** Inkluderar både leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster.
- **Incident:** Händelse med faktisk negativ påverkan på säkerheten i informationssystem eller nätverk.
- **Störning:** En konsekvens av en incident som innebär att den samhällsviktiga tjänsten inte levereras som normalt.

Innehåll


Connected

Sammanfattning

Denna rapport behandlar inkomna it-incidentrapporter under 2021 från leverantörer av samhällsviktiga och digitala tjänster, så kallade NIS-leverantörer. NIS-leverantörer är några av de viktigaste organisationerna i Sverige då de tillhandahåller tjänster som är centrala för samhällets funktion. Arbetet med NIS har sitt ursprung i NIS-direktivet som antogs 2016 för att höja den gemensamma nivån på cybersäkerheten i några av den Europeiska unionens viktigaste funktioner. MSB är den myndighet som sedan 2019 tar emot incidentrapporter om incidenter med ursprung i nätverk och informationssystem som orsakat betydande respektive avsevärda störningar från leverantörer av samhällsviktiga och digitala tjänster. Denna rapports målgrupper är främst beslutsfattare, informations- och säkerhetsansvariga samt omvärldsbevakande och analyserande roller hos NIS-leverantörer, men de analyser, slutsatser och rekommendationer som presenteras kan vara betydelsefulla även för andra organisationer.

Rapporten redogör för incidenterna som inkommit på en övergripande nivå, men presenterar även djupare analys av incidenter inrapporterade av leverantörer inom hälso- och sjukvårds- samt dricksvattensektorn. Utöver detta beskriver rapporten regleringen, hur incidentrapporteringen går till samt ett antal rekommendationer till NIS-leverantörerna som baseras på inkomna incidentrapporter.

Några centrala slutsatser

- Antalet inrapporterade incidenter 2021 var 82 vilket är en liten minskning från 2020. Rapporteringen är fortsatt ojämn mellan sektorerna.
- Systemfel är fortsatt den vanligaste orsaken till incidenter, men MSB ser att incidenter i år orsakats av alla kategorier: systemfel, misstag, angrepp och naturhändelser. Andelen rapporterade angrepp 2021 har ökat från föregående år, men utgör fortsatt en liten del av orsakerna till rapporterade incidenter.
- Ett tema som framträder i rapporteringen är att förändringshantering ofta orsakar incidenter.
- En majoritet av incidenterna har fortsatt sitt ursprung hos en underleverantör till NIS-leverantören.
- Rapporterande organisationer har fortsatt svårt att uppskatta incidenters och störningars kostnader.
- Ofta är det system för kommunikation som drabbas, vilket är främst förekommande i hälso- och sjukvården.
- Flera leverantörer, särskilt inom hälso- och sjukvårdssektorn upplever incidenter, och även störningar som de tidigare drabbats av.

Ett digitalt samhälle

Leverantörer av samhällsviktiga och digitala tjänster, i denna rapport även kallade NIS-leverantörer, är de organisationer som levererar några av Sveriges viktigaste tjänster för samhällets funktionalitet. NIS-regleringen ställer, i korthet, krav på att organisationerna som identifierar sig som NIS-leverantörer bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete, gör riskanalyser och vidtar åtgärder samt rapporterar incidenter.

Sveriges viktigaste tjänster

År 2016 blev NIS-direktivet den första EU-regleringen som specifikt syftar till att höja informations- och cybersäkerheten i hela unionen genom att reglera en mininivå av säkerhet för informationssystem för vissa verksamheter.

Begreppet ”samhällsviktig tjänst”, som används i NIS-regleringen, täcker inte in alla tjänster som är viktiga för samhället, och är ett mer avgränsat begrepp än samhällsviktig verksamhet.[1] Sektorerna som levererar det som enligt NIS-regleringen är samhällsviktiga eller digitala tjänster är alla lika i det avseendet att de uppbär en funktion som är bedömd som viktig för samhället. Det är dock stor skillnad på de olika sektorernas verksamhet och även deras beroende till nätverk och informationssystem. Årets rapport strävar därför efter att försöka nyansera de olika förutsättningar och utmaningar som finns inom de olika sektorerna. Leverantörer av samhällsviktiga och digitala tjänster, även kallade NIS-leverantörer, inbegriper både offentliga och privata aktörer och många av de tjänster som ingår är under kommunernas ansvarsområde. Således utgör kommunerna en viktig del i samhällets informations- och cybersäkerhet.

Definitionen av samtliga samhällsviktiga och digitala tjänster inom NIS-regleringen bygger på att den samhällsviktiga eller digitala tjänsten är beroende av nätverk och informationssystem. Störningar som orsakats av incidenter i nätverk eller informationssystem kan dock utveckla sig väldigt annorlunda om den drabbade organisationen exempelvis är en lokal vårdinrättning, storbank eller om organisationen levererar en molntjänst. Hos den förstnämnda kan en omfattande incident i värsta fall orsaka stor inverkan på människors hälsa i lokalområdet,[2] i det andra exemplet kan en incident i värsta fall orsaka nationsomfattande betalningsstörningar som dessutom kan sprida sig utanför landets gränser, och i det

1. Med samhällsviktig verksamhet avses verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet. Se mer om samhällsviktig verksamhet på msb.se.

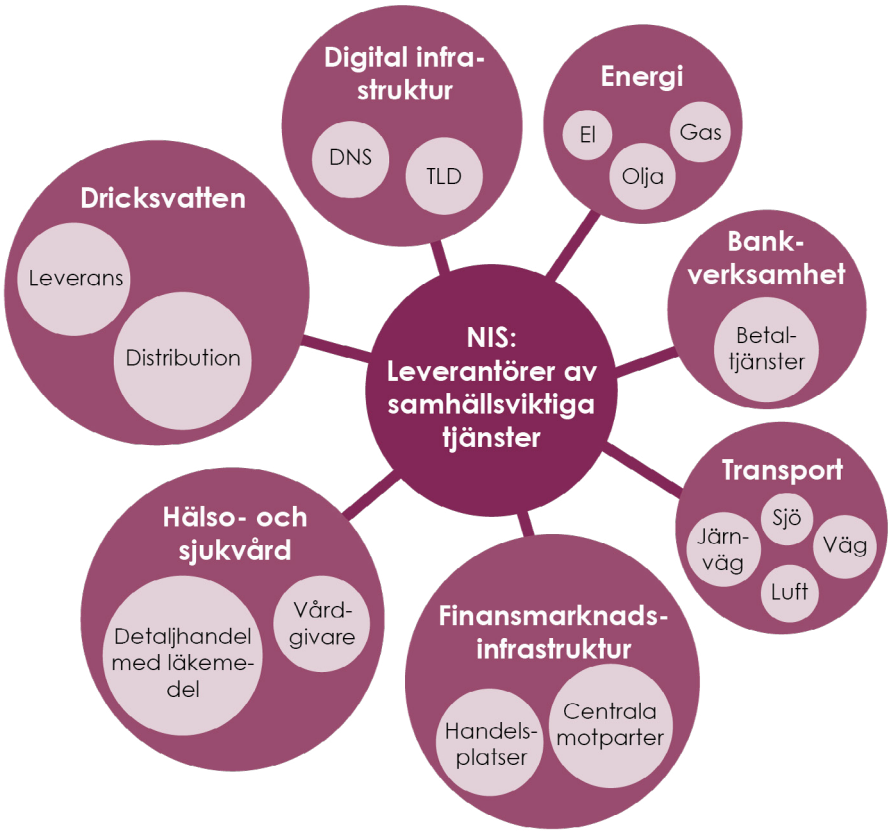
2. Indirekt inverkan genom till exempel inställda operationer och oförmåga att bedriva vård i samma utsträckning på grund av brist på tekniska stöd.

sistnämnda exemplet kan i värsta fall verksamheter i flera delar av världen påverkas samtidigt.[3] De samhällsviktiga tjänsterna som drivs med stöd från informationssystem har, i vissa fall, möjlighet att vid en incident tillfälligt ersätta stödet från informationssystemen med manuella rutiner till skillnad från de tjänster som inte bara tar stöd av digitala informationssystem, utan i sig själva utförs helt av eller genom informationssystem. De samhällsviktiga och digitala tjänsterna har med andra ord stor variation i vilken utsträckning tjänsten kan bedrivas utan stöd från nätverk och informationssystem och därför hur omfattande en störning kan bli.

Leverantörer av samhällsviktiga tjänster

Leverantörer av samhällsviktiga tjänster är de organisationer som bedriver verksamhet inom de sektorer som visas i figur 1. Det är dock inte samtliga organisationer inom sektorerna som omfattas utan inom respektive sektor finns det även förtydliganden av vilka delsektorer som omfattas. Samtliga organisationer inom dessa sektorer och delsektorer faller inte heller inom NIS-regleringen utan det varierar bland annat på grund av faktorer så som omsättning, antal kunder, antal anställda eller hur stort geografiskt område som skulle kunna påverkas av en störning till följd av incident.[4] Samhällsviktiga tjänster kan inom NIS-regleringen röra sig om till exempel leverans av kommunalt trygghetslarm eller en banks förmåga att hantera betalningar.

Figur 1. Figur som visar inom vilka sektorer leverantörer av samhällsviktiga tjänster bedriver verksamhet.



3. Exemplen är illustrativa och generella inte representativa för hela sektorerna.
4. Se mer i föreskrifterna för anmälan och identifiering av leverantörer av samhällsviktiga tjänster MSBFS 2018:7.

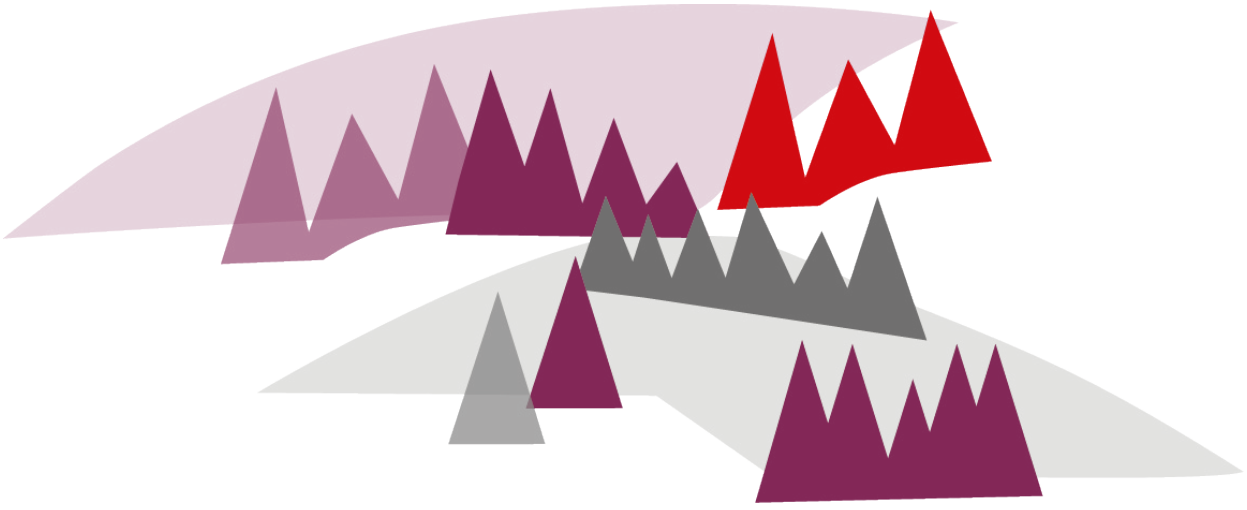
Antalet leverantörer av samhällsviktiga tjänster

Antalet leverantörer av samhällsviktiga tjänster sammanställs av MSB i samarbete med tillsynsmyndigheterna för NIS-regleringen: Energimyndigheten, Finansinspektionen, Inspektionen för vård och omsorg, Livsmedelsverket, Post- och telestyrelsen och Transportstyrelsen, vartannat år och uppgick vid den senaste redovisningen hösten 2020 till 561 stycken.

Leverantörer av samhällsviktiga tjänster skiljer sig mycket åt och således är även kriterierna på vilka som identifieras som leverantörer, och vilka incidenter som ska rapporteras i respektive sektor olika. I hälso- och sjukvårdssektorn finns andra typer av informationssystem och nätverk än i till exempel dricksvattensektorn, och banker bedriver en annan form av verksamhet och har andra behov än organisationer inom till exempel transportsektorn. I MSB:s föreskrifter om anmälan och identifiering av samhällsviktiga tjänster[5] beskrivs vilka kriterier som ska uppfyllas för att en organisation ska anmäla sig som leverantör av en samhällsviktig tjänst, och i föreskrifterna för incidentrapportering[6] står det vilka typer av incidenter inom vilken sektor som ska rapporteras.

Under våren 2022 kommer nya föreskrifter att träda i kraft för identifiering och anmälan av samhällsviktiga tjänster. De nya föreskrifterna innebär vissa förändringar av kriterierna för respektive sektor, bland annat förtydliganden av definitioner, justeringar av tröskelvärden, samt att det läggs till nya tjänster som omfattas, särskilt inom sektorerna energi- och bankverksamhet. Utöver MSB:s föreskrifter kan organisationer finna stödmaterial på sin sektors tillsynsmyndighets hemsida, eller kontakta sin tillsynsmyndighet för att få hjälp i att avgöra huruvida de omfattas av NIS-reglering, och anmäla sig som leverantör av samhällsviktig tjänst.

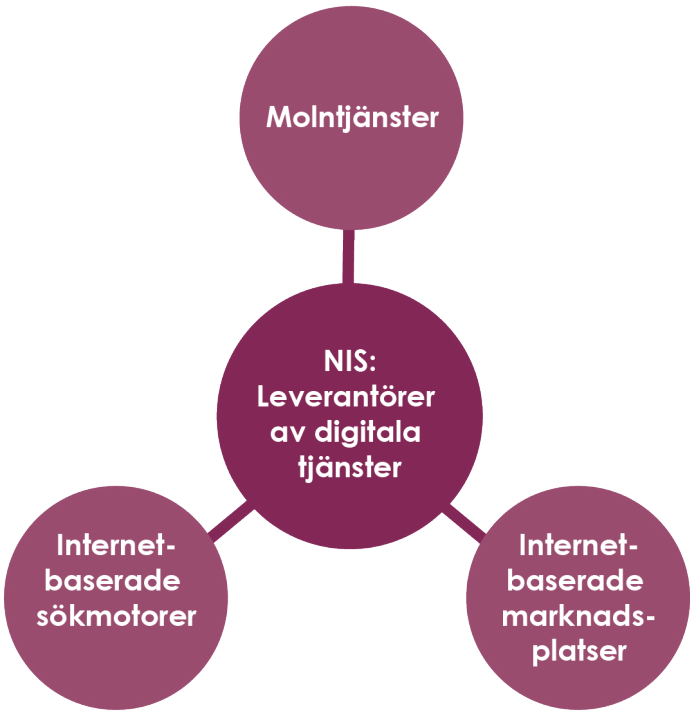
5. MSBFS 2018:7
6. MSBFS 2018:9



Leverantörer av digitala tjänster

Allt fler organisationer flyttar sin lagring till, eller på annat sätt använder sig av, molntjänster, allt fler handlar på digitala marknadsplatser och använder internetbaserade sökmotorer. Dessa tjänster har sedan länge varit en viktig del av den informationsekonomi som växt fram under 2000-talet. Beroendet av de ovan nämnda centrala delarna av internetinfrastrukturen är att betrakta som viktiga för funktionen av Sverige, samt EU:s inre marknad. Begreppet *digital tjänst* inom NIS-regleringen ska inte förväxlas med det vardagliga användandet av det bredare begreppet digital tjänst, det vill säga en tjänst som tillhandahålls med stöd av informationssystem, och ofta över internet. *Leverantör av digitala tjänster* är en avgränsad kategori tjänsteleverantörer definierade av NIS-regleringen och inbegriper sådana organisationer som tillhandahåller molntjänster, internetbaserade marknadsplatser, internetbaserade sökmotorer av en definierad storlek (se figur 2).

Figur 2. Figur som visar de tjänster som omfattas av NIS-regleringens begrepp leverantör av digitala tjänster.



Digitala tjänster är i högre grad än leverantörer av samhällsviktiga tjänster gränsöverskridande eller globala aktörer. Detta innebär att tjänster som används i exempelvis Sverige kan ha sitt huvudsakliga etableringsställe i en annan medlemsstat eller en annan världsdel. EU-kommissionen tillämpar kraven på leverantörer av digitala tjänster genom en genomförandeförordning (EU) 2018/151.[7] Kriterier för identifiering av leverantörer av digitala tjänster och kriterier för vad som är en rapporteringspliktig incident, finns i NIS-direktivet och vidare i tillhörande genomförandeförordning.

7. Kommissionens genomförandeförordning (EU) 2018/151 av den 30 januari 2018 om tillämpningsföreskrifter för Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

Under de år som NIS-lagen har gällt i Sverige har en mycket låg andel av de incidentrapporter MSB mottagit kommit från leverantörer av digitala tjänster. Det samma gäller i andra europeiska medlemsstater. En anledning till detta är att kriterierna/trösklarna för rapporteringspliktiga incidenter är höga. I regleringen står det att det är incidenter som orsakar *avsevärd* störning som ska rapporteras, till skillnad från en *betydande* störning hos leverantörer av samhällsviktiga tjänster. En skillnad mellan leverantörer av samhällsviktiga respektive digitala tjänster är att leverantörer av digitala tjänster inte behöver anmäla sig till sin tillsynsmyndighet. Således saknas en sammanställning av hur många organisationer det rör sig om. En annan skillnad i regleringen är att tillsyn endast kan genomföras efter att en incident inträffat. Tillsynsmyndigheten Post- och telestyrelsen har mer information om vad det innebär att vara en leverantör av digitala tjänster och bland annat en checklista för att hjälpa leverantörer att reda ut ifall organisationen faller under NIS-regleringen.[8]

Utvecklingen av NIS

I december 2020 presenterade EU-kommissionen ett förslag till nytt direktiv (som idag går under namnet NIS2) som ska ersätta nuvarande NIS-direktiv (EU) 2016/1148. Syftet med det nya förslaget är att uppdatera den befintliga rättsliga ramen för vilka åtgärder som ska vidtas för att motverka det ökade cybersäkerhetshotet. Förslaget utökar bland annat tillämpningsområdet till fler sektorer, utifrån deras betydelse för den ekonomiska och samhälleliga verksamheten. Nya sektorer som föreslås idag är avloppsvatten, offentlig förvaltning, rymd, post- och kurirtjänster, avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion och distribution av mat, tillverkning och digitala tjänster.[9] Förslaget skärper vidare säkerhetskraven genom att tillhandahålla en lista med minimikrav för åtgärder som ska tillämpas för att hantera riskerna kopplat till säkerheten i respektive verksamhets nätverk och informationssystem. Förslaget inför också strängare tillsynsåtgärder och strängare tillämpningskrav för att harmonisera sanktionssystemen i medlemsstaterna. Genom förslaget införs dessutom mer precisa rapporteringskrav. I början av 2022 pågår trilogförhandlingar om NIS2-förslaget mellan Europeiska unionens råd, Europaparlamentet och Europeiska kommissionen.

8. https://pts.se/sv/bransch/internet/Informationssakerhet-samhallsviktiga-och-digitala-tjanster-NIS/digitala-tjanster/

9. I förslaget görs inte längre någon skillnad mellan leverantörer av digitala tjänster och samhällsviktiga tjänster. Digitala tjänster föreslås också att utökas med fler typer av tjänster.

Om rapporten och incidentrapportering

Om denna rapport

Denna rapport är en fördjupningsrapport om den incidentrapportering MSB mottar från leverantörer av samhällsviktiga och digitala tjänster. MSB publicerar även en rapport som på ett samlat sätt redovisar inkomna incidentrapporter från både statliga myndigheter och NIS-leverantörer, samt innehåller omvärldsanalys med koppling till informations- och cybersäkerhet.

En inblick i Sveriges cybersäkerhet: årsrapport it-incidentrapportering 2021

Denna rapport syftar främst till att genom incidentrapporter ge en djupare inblick i vilka incidenter som drabbar NIS-leverantörer och hur dessa påverkar de tjänster som organisationerna levererar. Rapporten riktar sig främst till beslutsfattare, informations- och säkerhetsansvariga samt omvärldsbevakande och analyserande roller hos NIS-leverantörer, men de analyser, slutsatser och rekommendationer som presenteras kan vara betydelsefulla även för andra organisationer. Rapporten är skriven för att även vara tillgänglig för en bred publik.

Incidentrapporteringens fördelar

Incidentrapportering ska inte enbart ses som ett lagkrav utan bör ses som en viktig del i att få förståelse för brister hos enskilda organisationers och därmed brister i samhällets informations- och cybersäkerhet. Förståelse om sina brister är en förutsättning för att förbättra sig och på så sätt höja organisationens och samhällets informations- och cybersäkerhet. Att drabbas av en incident i nätverk och informationssystem är för en organisation en fråga om *när*, och i vilken omfattning, inte huruvida *om* det kommer att hända. Därför är det viktigt för organisationer att ha inarbetade rutiner för hur incidenter anmäls, att incidenter bedöms utifrån konsekvens, att organisationen har förmåga att åtgärda incidenten och utreda dess orsak. De incidentrapporteringsformulär som MSB tillhandahåller för rapporteringspliktiga incidenter inom NIS-regleringen kan således ses som en typ av checklista på flera av de frågor som organisationen bör kunna svara på vid sin bedömning av en incident. Med tanke på observerade trender med en större andel incidenter med ursprung hos

underleverantörer så kan organisationer även se det som något att ha vid kravställning inför upphandling.

För samhället i stort kan sammanställningar av de utmaningar som MSB ser i inrapporterade incidenter och de tips som MSB förmedlar bidra till ökad kunskap kring vad som sker och vilka förebyggande åtgärder som man kan införa för att undvika eller klara sig bättre undan en incident.[10]

MSB mottar incidentrapporter från leverantörer av samhällsviktiga och digitala tjänster via standardiserade formulär. Formulären finns tillgängliga här:

- **För leverantörer av samhällsviktiga tjänster**
- **För leverantörer av digitala tjänster**

Hur en incident rapporteras till CERT-SE

Incidentrapporteringen genomförs i tre skeden[11]:

Skede 1 – Inom sex timmar från att leverantören har identifierat att en incident är rapporteringspliktig ska leverantören underrätta CERT-SE vid MSB om incidenten via telefon 010-240 40 40.

Skede 2 – Inom 24 timmar från det att leverantören har identifierat att en incident är rapporteringspliktig ska skriftlig rapportering lämnas utifrån det första och andra skedet i incidentrapporteringsformuläret.

Skede 3 – Inom fyra veckor från det första rapporteringstillfället ska skriftlig rapportering lämnas utifrån det tredje skedet i incidentrapporteringsformuläret.

Förhållandet till andra krav på rapportering

Det finns fler lagstiftningar för organisationer att förhålla sig till rörande incidentrapportering varav några är sektorsspecifika. Två av de regleringar som gäller alla och som är mest centrala och omfattar incidenter i nätverk och informationssystem är säkerhetsskyddslagstiftningen[12] och dataskyddsförordningen (GDPR).

En organisation kan omfattas av både NIS och säkerhetsskyddslagen men vilken reglering som gäller vid en viss incident beror på vilken av regleringarna som gäller för det nätverket eller informationssystemet som drabbats. Det är upp till organisationen att identifiera vilken del av verksamheten som faller

10. MSB publicerade under 2021 även en rapport om hot mot digitala leveranskedjor som till del grundar sig på insikter från NIS-leverantörernas incidentrapportering. Rapporten heter Hoten mot de digitala leveranskedjorna – 50 rekommendationer för att stärka samhällssäkerheten och finns tillgänglig: https://www.msb.se/sv/publikationer/hoten-mot-de-digitala-leveranskedjorna--50-rekommendationer-for-att-starka-samhallssakerheten/

11. Varje skede har ett tillhörande frågeformulär tillgängligt på msb.se/NIS.

12. (2018:585)

inom säkerhetsskydd. Den del av verksamheten som omfattas av säkerhetsskyddslagstiftningen är undantagen i NIS-regleringen. När en incident sker inom verksamhet som bedöms vara under säkerhetsskyddslagstiftning så ska dessa rapporteras till Säkerhetspolisen. MSB erbjuder på sin hemsida en vägledning till stöd för organisationer i sin analys att förstå gränsdragningen mellan de två lagstiftningarna.[13]

Flera av NIS-leverantörerna behandlar stora mängder personuppgifter. Enligt dataskyddsförordningen (GDPR) finns det en skyldighet för organisationer att anmäla vissa typer av personuppgiftsincidenter till Integritetsskyddsmyndigheten (IMY). En personuppgiftsincident har inträffat om organisationen bedömer att uppgifter om en eller flera registrerade personer har blivit förstörda, gått förlorade eller kommit i orätta händer.[14]

13. På msb.se kan din organisation finna en vägledning för att förstå gränsdragningen mellan NIS och säkerhetsskyddslagen. Sidan går under titeln ”NIS-reglering och säkerhetsskyddslagen” https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/lag-forordning-och-foreskrifter/definiation-av-nis-regleringen-och-sakerhetsskyddslagen/

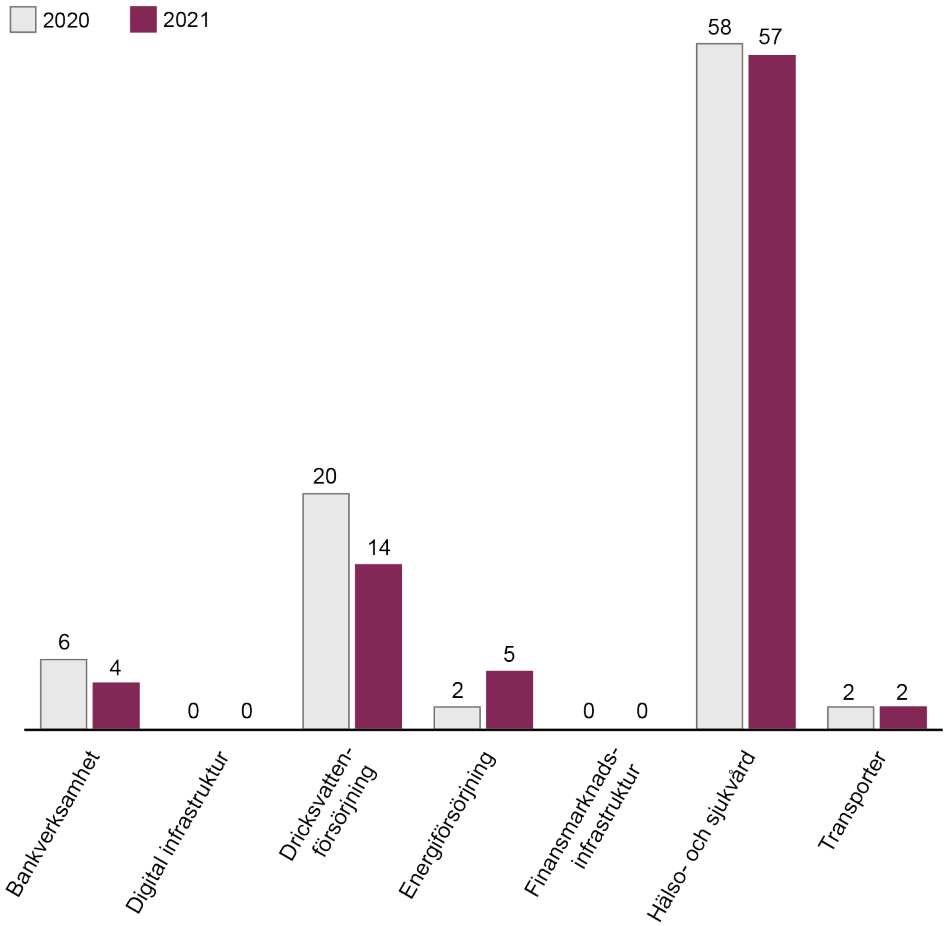
14. https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsincidenter/

Analys av inrapporterade incidenter

Analysen är uppdelad i två delar. Först presenteras en kortare analys av samtliga inkomna incidenter. Sedan följer två särredovisningar av de två sektorer från vilka leverantörer rapporterat tillräckligt mycket för att en analys ska kunna genomföras.

Årets incidenter

Diagram 1. Inkomna incidentrapporter från leverantörer av samhällsviktiga tjänster fördelat på sektorer 2021 & 2020.



Under 2021 inkom 82 incidentrapporter från leverantörer av samhällsviktiga tjänster. Fördelningen av incidentrapporter på sektorsnivå ser ut som i diagrammet (diagram 1). Fördelningen påminner om den bild som framträdde av 2020 års rapportering, där hälso- och sjukvårdssektorn står för den största delen, följt av sektorn leverans och distribution av dricksvatten. Att hälso- och sjukvård har hög rapportering kan bero på att leverantörerna inom sektorn utgör en stor del av det totala antalet NIS-leverantörer, samt att man inom sektorn har tradition av avvikelse- och incidentrapportering. Detta är en möjlig förklaring till att hälso- och sjukvårdssektorn har haft högst incidentrapportering under de år MSB mottagit rapporter, men det förklarar inte varför rapporteringen från de andra sektorerna är låg. Under året har ingen incident rapporterats från sektorerna digital infrastruktur, eller finansmarknadsinfrastruktur. Leverantörerna inom dessa sektorer är mycket färre. MSB har under året, i likhet med 2020, inte mottagit någon rapport från leverantörer av digitala tjänster gällande incidenter med avsevärda störningar på tillhandahållandet av den digitala tjänsten. Detta kan bero på det låga antalet leverantörer men också att leverantörer av digitala tjänster har annorlunda kriterier för incidentrapportering. Ytterligare resonemang kring detta finns i kapitlet om leverantörer av digitala tjänster.

Det som kännetecknar årets rapportering är att det inkommit fler incidentrapporter under sommaren än vad som inkom föregående år, och andra halvan av året hade betydligt högre rapportering än första.

Den minskning av antalet rapporterade incidenter som observeras har ingen enskild fastställd förklaring. Det kan delvis bero på att färre incidenter med spridningseffekter har rapporterats till MSB under 2021 jämfört med 2020. Under 2020 fanns det ett antal incidenter som hade orsakat störningar hos flera leverantörer vilket resulterade i fler rapporter. I år inkom endast enstaka sådana. En annan förklaring kan vara att årets incidentrapportering genomförts av en högre andel unika rapporterande organisationer. Bland de rapporter som rapporterades under 2020 fanns det ett antal leverantörer som rapporterade mer än en gång, ofta om liknande incidenter som var återkommande. Organisationer kan möjligtvis tolka att en liknande incident endast behöver rapporteras en gång, vilket är felaktigt. En rapporteringspliktig incident ska rapporteras varje gång den sker. MSB ser fortsatt en underrapportering, bland annat genom att incidenter som blivit offentligt kända inte alltid rapporteras. En annan möjlig förklaring är de förändringar i arbetssätt som skett under pandemin, med en högre andel av hemarbete. En följd av att många arbetar hemifrån kan vara att bland annat personal med it-ansvar fått förändrade eller utökade arbetsuppgifter kopplade till att möjliggöra hemarbete. Förflyttningen av en del av personalen från den fysiska arbetsplatsen kan även ha lett till att det funnits färre på plats för att uppmärksamma vissa typer av it-incidenter.

Incidenter hos underleverantörer (även kallade externa aktörer), kan leda till en-till-många incidenter där det sker flertalet incidenter samtidigt hos olika NIS-leverantörer med ursprung hos en gemensam underleverantör. Ovanstående resonemang om färre incidenter med spridningseffekter ska inte förstås som att leverantörskedjeproblematiken minskat. I 2021 års-rapportering är det fortsatt en majoritet (56 procent) av de inrapporterade incidenterna som har sitt ursprung hos en underleverantör som NIS-leverantören är beroende av för att bedriva den samhällsviktiga tjänsten.

Om något inträffar hos en underleverantör som NIS-leverantören är beroende av (om det exempelvis blir elavbrott, en fiberkabel går av, eller om externt tillhandahållen kommunikationstjänst går ner) och det leder till att NIS-leverantörens informationssystem eller nätverk inte fungerar som de ska och orsakar en störning, så är det en NIS-incident med ursprung hos extern aktör/underleverantör. Däremot så inbegriper detta inte leverantörer inom den egna koncernen.

Incidenter som har sitt ursprung hos underleverantörer kan flera gånger leda till att NIS-leverantören får otydlig eller för sen information angående incidenten och hur underleverantören åtgärdar incidenten, vilket försvårar det egna arbetet med incidenten. Detta är observerbart i årets rapportering och är något MSB konstaterat i tidigare rapporter. Informationsbristen inbegriper också information om vad incidentens orsak var, men mer centralt vad som görs av underleverantören för att undvika att liknande incidenter sker igen. Brister i information från underleverantörer syns även för 2021, även om det inte är lika stor andel av rapporterna.

Över hälften av de leverantörer som hade haft så stora störningar att de inte kunde bedriva den samhällsviktiga tjänsten under störningen hade haft en incident med ursprung hos underleverantör. I runt två tredjedelar av de incidenter som liknade incidenter som tidigare drabbat NIS-leverantörerna så hade incidenten ursprung hos en underleverantör.

Vad som orsakar en incident

Orsakerna till incidenterna är i linje med vad MSB tidigare år rapporterat. Nästan samtliga incidenter som rapporteras uppges ha skett i ett nätverk eller informationssystem, snarare än i kringmiljön. I analysen framkommer det dock att ytterligare ett litet antal bör kunna ses som incidenter i kringmiljön, så som incident i förbindelse- eller energitillförsel till NIS-leverantören.

Den största andelen av angivna orsaker till de rapporterade incidenterna bedöms ha orsakats av systemfel, vilket utgör omkring en tredjedel av rapporterna. Systemfel inbegriper en stor uppsättning orsaker med gemensamma nämnaren att systemet inte fungerar som det ska utan någon bedömd direkt påverkan från människor eller natur. Den näst vanligaste angivna orsaken är misstag[15], även kallade handhavandefel, vilket utgör en sjättedel av de rapporterade incidenterna.

Både andelen, och totala mängden angrepp har ökat något sedan 2020 från två till fem, men befinner sig fortsatt på en låg nivå sett till det totala antalet incidenter. I analysen av incidenternas orsaker skulle en del av de som bedömts orsakats av systemfel, och som bedömts ha okänd orsak mer korrekt vara klassade som misstag enligt MSB. De antagonistiska handlingarna är i mindre utsträckning något som i årets incidentrapportering riktat sig direkt mot den specifika leverantören utan har i fler fall uppkommit i samband med att någon underleverantör utsatts för angrepp. Det säger inget om hur många angreppsförsök som NIS-leverantörerna utsatts för. Om inte angreppet i sig själv skapar en störning, utan är till exempel intrång (spionage), så är det troligt leverantörens egen åtgärd för att hantera intrånget/intrångsförsöket som orsakar en störning. Det kan bland annat bero på att leverantören vid angreppsförsök stänger ner ett viktigt system för att förhindra eller avbryta ett intrång. Detta kan synas i en del av de inrapporterade incidenterna som bedöms ha antagonistiskt ursprung.

Jämfört med föregående år har fler naturhändelser orsakat incidenter. Ökningen är dock liten och kan inte bedömas som signifikant.

Orsak okänd

Runt en tredjedel av incidenterna uppges ha okänd orsak vilket är något fler än andelen rapporter där systemfel anges som orsaken. Detta liknar 2020 års rapportering, där andelen okända var ungefär lika stor. Vid en närmare analys av vilka incidenter där leverantören rapporterat okänd orsak framgår inte incidenterna i kategorin fördela sig på annat sätt än den övriga fördelningen av orsaker. Grundorsaker till incidenter kan i vissa fall vissa fall vara en tekniskt avancerad fråga som tar tid att utreda och leverantörer kan vid rapporteringstillfället ha en pågående incident eller störning. De incidenter som markerats som okänd orsak är inte i högre utsträckning pågående incidenter vid rapportering, det vill säga incidenterna är i de flesta fallen avslutade vid rapporteringen av incident med bedömd okänd orsak. Strax över hälften av alla som svarat okänt har haft en incident i en tjänst som tillhandahålls av extern aktör, och svaret på frågan om grundorsak är något som flera gånger besvaras med att de inväntar rapport från leverantör (underleverantör red. anm.). NIS-leverantörerna kan även välja att markera orsaken till incidenten som okänd då de fått en otydlig eller bristfällig

15. Misstag är mänskliga handlingar utan antagonistiskt syfte, även kallat handhavandefel.

incidentrapport av sin underleverantör, eller inte kunnat avgöra om det var ett systemfel eller ett misstag och därför rapporterar det som okänd. Ibland kan incidentrapporten beskriva ett samspel mellan mänskliga misstag och systemfel eller incidenter i kringmiljön, vilket kan göra den rapporterande organisationen osäker på vad som orsakat vad.

Kostnader

I en majoritet av rapporterna meddelar NIS-leverantörerna att de vid rapporteringstillfället inte slutgiltigt fastslagit varken incidentens eller störningens kostnader. Bland de som rapporterar hur de ska täcka för kostnaderna rapporterar de flesta att pengar kommer från fasta eller rörliga medel för incidenthantering. Ett lägre antal svarar att pengar kommer tas från äskade medel. Ingen rapporterar att de ämnar täcka kostnader med lån eller försäkring, vilket liknar rapporteringen från 2020. Privata aktörer kan ha det lättare att vid en incident beräkna till exempel uteblivna intäkter än offentliga aktörer. Även om det inte uppstår någon direkt kostnad av incidenten, så kan det ofta innebära lägre effektivitet eller produktivitet och behov av extra personal eller längre arbetstimmar för befintlig personal vilket kan leda till kostnader som organisationen ser som normala och inte som direkta konsekvenser utav de incidenter som sker. Likt förra årets rapportering är det relativt få NIS-leverantörer som kan rapportera någon numerisk kostnadsuppskattning för incidenterna och/eller störningen, eller de åtgärder som vidtas i efterhand för att förhindra upprepning av incidenten. Således publiceras ingen data gällande kostnader. Allmänt sagt kan vi konstatera att de kostnadsuppskattningar som rapporterats för incidenter och störningar som var bland de högsta, under både 2021 och 2020 kommer från organisationer som vid en incident bedömer att it-miljön är föråldrad, och där incidenten lett till insikter kring behov av större investeringar som vid det laget behöver bli omfattande. Förståelsen för NIS-incidenters kostnader hade troligtvis ökat om incidentrapporteringen var mer utspridd på sektorerna.[16]

16. Som del i att öka förståelsen för kostnader i samband med incidenter i nätverk och informationssystem samarbetar MSB med forskare kring ekonomiska perspektiv på cybersäkerhetsfrågor, inklusive kostnadsberäkningar för incidenter, störningar och åtgärder som utgår ifrån anonymiserade kostnadsberäkningar i NIS-rapporteringen.

Sektorsfokus

För att öka förståelsen för olika sektorers speciella förutsättningar presenteras därför två sektorers rapportering separat. För att kunna göra sektorsspecifika analyser krävs ett tillräckligt stort antal inrapporterade incidenter, vilket under 2021 gäller två sektorer.

Hälso- och sjukvård

Hälso- och sjukvårdssektorn har i jämförelse med de andra sektorerna påverkats av pandemin mer direkt, med ett högt tryck på flera tjänster som är samhällsviktiga och således på sektorn i stort. Organisationer inom hälso- och sjukvården har under en lång tid genomgått en digitaliseringsprocess. Pandemin har gjort att vissa delar av organisationernas verksamheter i högre grad fått ställa om till och ytterligare möjliggöra digitala lösningar, till exempel digitala samtal med läkare, psykolog eller kurator, och olika typer av självmonitorering. Fortsatt är dock många delar av verksamheten inte möjliga att bedriva på distans. Samtidigt fortsätter utvecklingen av digitala tjänster inom hälso- och sjukvården, där så kallade e-hälsotjänster och välfärdsteknik växer fram.[17] Den digitala utvecklingen av tjänster beskrivs som en av lösningarna på den demografiska utvecklingen med en stigande andel äldre i befolkningen.

Sektorn kännetecknas av många organisationer som är utspridda i landet i både små och stora kommuner och regioner. Hälso- och sjukvårdstjänster särskiljer sig också åt gällande graden av direktkontakt med medborgare som tar del av tjänster. Således kan många av de störningar som sker märkas av vanliga medborgare och även påverka deras hälsa på ett mer direkt vis, vilket ställer höga krav på organisationer inom sektorn. Som nämnt i föregående kapitel så har leverantörerna inom hälso- och sjukvårdssektorn varit den sektor som rapporterar flest incidenter under 2020 respektive 2021. Organisationerna inom sektorn har en lång erfarenhet av att bland annat rapportera avvikelser.

17. Socialstyrelsen definierar e-hälsa som ” E-hälsa är att använda digitala verktyg och utbyta information digitalt för att uppnå och bibehålla hälsa” och välfärdsteknik som ” Digital teknik som syftar till att bibehålla eller öka trygghet, aktivitet, delaktighet eller självständighet för en person som har eller löper förhöjd risk att få en funktionsnedsättning” https://www.socialstyrelsen.se/globalassets/sharepoint-dokument/artikelkatalog/ovrigt/2021-5-7384.pdf s.20.

Av MSB:s föreskrifter (MSBFS 2018:7) framgår att de organisationer som omfattas av NIS rörande hälso- och sjukvård avses:

1. hälso- och sjukvård som bedrivs av en vårdgivare och som omfattas av hälso- och sjukvårdslagen (2017:30), tandvårdslagen (1985:125) eller detaljhandel med läkemedel enligt lagen (2009:366) om handel med läkemedel
   a) där antalet anställd legitimerad vårdpersonal eller på annat sätt anlitad legitimerad vårdpersonal överstiger 50 årsarbetskrafter, eller
   b) är minst 20 000 expedieringar av receptbelagda läkemedel utförs per år.

Detta omfattar ett flertal olika verksamheter som bland annat tandvård, apotek och kommunal hälso- och sjukvård. Hälso- och sjukvårdssektorn inbegriper således en bred samling tjänster i privat, kommunal och regional regi.

För att bedöma huruvida en incident är rapporteringspliktig ska leverantörerna följa ett antal kriterier.

Av MSB:s föreskrifter (MSBFS 2018:9) framgår att leverantörer inom hälso- och sjukvård ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som:

1. innebär att anmälningsskyldighet inträder enligt 3 kap. 5 § första stycket patientsäkerhetslagen (2010:659),
2. har påverkat tillhandahållandet av ambulans och ambulanssjukvård enligt 7 kap. 6 § hälso- och sjukvårdslagen (2017:30)
3. innebär att sådan hälso- och sjukvård som baseras på system som insamlar, bearbetar, lagrar eller distribuerar och presenterar information inte kan tillhandahållas i minst två timmar, eller
4. har pågått i minst sex timmar.

Incidenten

En typisk incident och störning hos leverantörer av hälso- och sjukvård pågår under mindre än en arbetsdag, vilket utgör ungefär två av tre av de rapporterade incidenterna från sektorn. Ungefär en av tre pågår fram till dagen efter, och en liten andel pågår i en handfull dagar och i mycket få fall något längre. Incidenten upptäcks ofta av den egna personalen genom att en störning har uppkommit snarare än genom något tekniskt detekteringssystem. I vissa fall har ett detekteringssystem (internt eller externt) fungerat som planerat och varnat för en incident, men det har på grund av brist i bemanning och beredskap eller rutiner i larmkedjan inte funnits någon som hanterat det, vilket resulterat till att incidenten orsakat en störning.

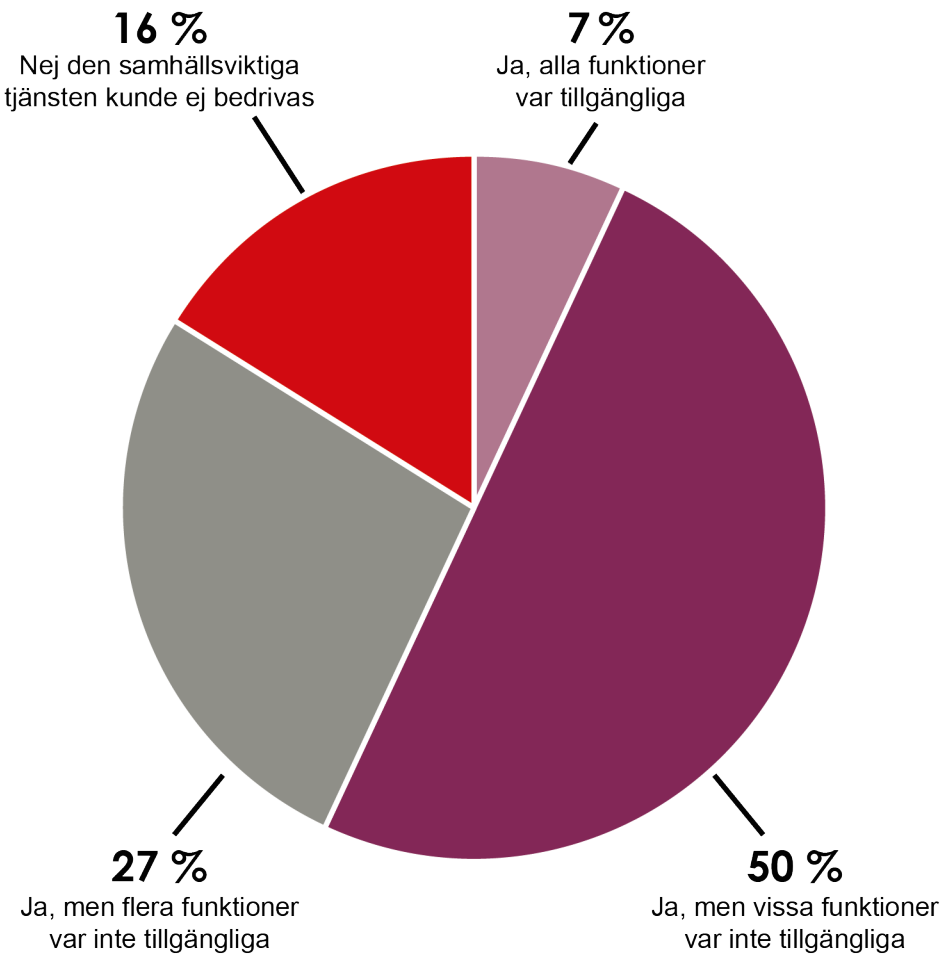
Från listan ovan, så är det fjärde kriteriet som åberopas vid incidentrapporteringen, alltså att incidenten orsakat en störning som pågått minst sex timmar. Det näst vanligaste kriteriet att åberopa i rapporteringen är det tredje, det vill säga att en typ av informationssystem som är viktigt för tillhandahållande av tjänsten har gått ner eller minskat i kapacitet under minst två timmar. Omkring en femtedel av leverantörerna har inte tydligt kategoriserat incidenten enligt ett av de angivna kriterierna, men bedömer att incidenten är rapporteringspliktig. Majoriteten av incidenter bedöms ha orsakats av systemfel och har skett i kommunikationssystem, följt av administrativa system. Två tredjedelar av de rapporterade incidenter som inträffat inom sektorn har sitt ursprung hos en underleverantör.

Ett tema som framträder i en del av årets rapportering är att ett antal incidenter inträffat i samband med planerade uppdateringar, eller planerade avbrott både internt och från extern aktör. Det som skett i dessa fall är att information inte nått fram till relevanta personer eller funktioner så att förberedelser inte funnits. Alternativt har backup-lösningar inte fungerat som planerat vilket orsakat att incidenter inträffar med störningar som konsekvens trots att förberedelser på avbrott funnits.

Störningen

Störningen, det vill säga konsekvensen på den samhällsviktiga tjänsten av incidenten i nätverk eller informationssystem, kan vara allvarlig på olika vis. I incidentrapporteringen finns ett antal sätt att bedöma allvarlighetsgraden av störningen. Bland annat svarar leverantörerna på i vilken utsträckning den samhällsviktiga tjänsten var möjlig att bedriva under störningen (se diagram 2).

Diagram 2. Andel svar från leverantörer inom hälso- och sjukvård på om den samhällsviktiga tjänsten gick att tillhandahålla under störningen.



Hälso- och sjukvårdssektorn uppvisar aningen högre påverkan på tjänsten än vad de andra sektorernas leverantörer gör.
I sexton procent av fallen kunde tjänsten inte tillhandahållas under störningen som följde incidenten, och i strax under en tredjedel av fallen bedömer leverantörerna att tjänsten saknade flera funktioner under störningen. Som framgår av diagrammet är den vanligaste konsekvensen av incidenterna att *vissa* funktioner av den samhällsviktiga tjänsten saknas under störningen, men att det går att bedriva den i viss utsträckning, med bland annat alternativa manuella rutiner.

Ett annat sätt att bedöma en störnings allvarlighetsgrad är att analysera och värdera de *skyddsvärden*[18] som påverkades, vilket främst behandlar på vilket sätt användarna[19] påverkades. Samtidigt som det i sexton procent av sektorns incidentrapporter uppges att tjänsten inte gick att bedriva under störningen, så är omkring tio procent av alla rapporter från sektorn där leverantören bedömer att störningen orsakat betydlig påverkan på människors hälsa.[20] Leverantörerna bedömer oftast att störningen fick liten eller ingen sådan påverkan alls på människors hälsa. Det av skyddsvärdena som istället påverkas mest är, likt förra året, förtroendet för tjänsten där omkring tjugo procent av rapporterna bedömer att det skett en betydlig påverkan på förtroendet för den samhällsviktiga tjänsten.

Störningarna inom sektorn påverkar med få undantag på kommunal nivå, och bedöms inte påverka andra NIS-leverantörer vilket innebär att störningarna oftast inte bedöms vara sektorsöverskridande. Däremot påverkas privatpersoner av förklarliga skäl i en hög grad. Likt ovan nämnt, så har leverantörerna inom sektorn i stor utsträckning en direkt kontakt med de som brukar tjänsterna, och en incident kan således ge en märkbar störning för användare kort inpå att den inträffat.

Det har under pandemiåren talats om att antagonistiska aktörer och cyberkriminella med ökande intensitet riktat sig mot särskilt hälso- och sjukvårdsaktörer. I rapportering som MSB mottagit under 2021, syns ingen markant ökning av angrepp mot just denna sektor. Med tanke på det omskrivna ransomware-angreppet som riktades mot Kalix kommun i slutet av året är det

18. I incidentrapporteringsformuläret är de tre *skyddsvärdena* människors hälsa, användares ekonomi och användarnas förtroende för den samhällsviktiga tjänsten.

19. Här avser användare både leverantörens egna anställda och men även brukare.

20. ”Betydlig” är den högsta menbedömningen.

värt att notera att även om frekvensen av inrapporterade angrepp är låg jämfört med andra orsaker så säger det inte något om hur omfattande eller allvarlig en störning till följd av ett specifikt angrepp som genomförs kan bli. Det är därför viktigt att ha ett allriskperspektiv till incidenter och att se till samtliga orsakskategorier och deras möjliga konsekvenser i sitt systematiska och förebyggande informationssäkerhetsarbete.

Riktat stöd till hälso- och sjukvårdssektorn

Hösten 2020 inleddes en särskild satsning mot den svenska hälso- och sjukvårdssektorn, efter varningar från den amerikanska cybersäkerhetsmyndigheten CISA att det förekom ransomware riktat mot sjukvårdsinrättningar. MSB/CERT-SE inledde samverkan med it-säkerhetspersonal (i huvudsak operativ personal, men även på strategisk och/eller ledningsnivå), dels för att skapa kontaktytor och kunna samla in och dela relevant information, dels för att finnas tillgängliga för tekniskt stöd och rådgivning vid behov. Initiativet har medfört höjd it-säkerhetsförmåga samt ökad motståndskraft för att undvika it-incidenter under det kritiska läge som pandemin innebar, samt även bidragit till samhällets generella förmåga att hantera pandemin.

Hantering och åtgärder

I 2020 års rapport över inkomna incidenter konstaterades det att flera leverantörer av samhällsviktiga tjänster drabbas av liknande incidenter som den de rapporterar om. Under 2021 uppger strax under hälften av leverantörerna inom hälso- och sjukvård att incidenten de rapporterar om liknar incidenter som skett förut. Utav dessa har 75 procent även upplevt en liknande störning i den drabbade samhällsviktiga tjänsten. I organisationernas riskanalyser ska de identifiera de relevanta risker som kan orsaka incidenter och störningar hos organisationen. Utav de organisationer som drabbats utav både en liknande incident och störning har en bit över hälften av dessa leverantörer identifierat och analyserat en sådan incident i sin riskanalys. Även om analysunderlaget i frågan är litet, så är det värt att belysa vikten av att tidigare incidenter och störningar analyseras för att finna grundorsakerna samt att leverantörerna tar med sig relevanta lärdomar från inträffade incidenter. Detta bör sedan användas i kommande riskanalysarbete för att identifiera och vidta nödvändiga säkerhetsåtgärder för att minska identifierade risker, konsekvenser och sannolikheter.

En kontinuitetsplan är en i förhand dokumenterad plan som har till syfte att minska konsekvenserna av en incident genom att kunna upprätthålla en tolerabel nivå av leverans av verksamhetens tjänster vid störning. I rapporteringsformuläret får leverantörer svara på frågor gällande kontinuitetsplaner för både incidenter och störningar. Utav incidentrapporter från leverantörerna inom hälso- och sjukvårdssektorn så hade ungefär hälften en kontinuitetsplan för att hantera en incident och störning[21] som liknar den inträffade. Utav de som hade en kontinuitetsplan valde nästintill samtliga att aktivera den, det vill säga genomföra de särskilda åtgärder som organisationen planerat i förhand.

En stor del av de rapporterande leverantörerna genomförde vid incidenten en eller flera särskilda åtgärder för att hantera incidenten och dess konsekvenser.

21. Fler av leverantörerna hade en kontinuitetsplan för att hantera en liknande störning.

Det vill säga att de bedömde att situationen krävde åtgärder utöver det normala arbetet. Vid genomläsning vad åtgärderna består i kan de grovt klustras enligt fem huvudsakliga kategorier. Byte av hårdvara, felsökning, se över rutiner, rapportera till och ha uppföljning med leverantör, övergång till manuella rutiner som ofta innebär en ökad bemanning.

Se över rutiner, och *uppföljning med leverantör* är båda mer långsiktiga arbeten snarare än direkta svar på en incident och störning. Detta kan ha att göra dels med att incidenterna och störningarna generellt är kortvariga och att färre rapporterar incidenten medan problemen är pågående. Detta kan påverka att de även svarar på vad organisationen kommer att införa för säkerhetsåtgärder mer generellt och på längre sikt.

Just uppföljning, eller rapportering till underleverantör är dock åtgärder som flera organisationer ser som enda alternativ. Det vill säga att uppmärksamma underleverantören och hoppas att de åtgärdar incidenten så snart som möjligt. Den vanligaste åtgärden från NIS-leverantörerna vid störning i tjänsten är att gå över på manuella rutiner och då gå upp i ökad bemanning, eller tillsätta någon sorts särskild grupp för att hantera situationen. Inom hälso- och sjukvårdssektorn finns det en tradition och möjlighet av att ha manuella rutiner, samt möjlighet att bedriva vissa tjänster utan tekniska stöd. Dessa manuella arbetssätt fungerar i flera fall som en relativt bra kontinuitetshantering, i vissa fall av ren slump andra gånger enligt kontinuitetsplan och rutin. Ökad bemanning tas i rapporteringen ofta inte in i kostnadsuppskattningar eller bedöms vara en särskild åtgärd utifrån störningen utan verkar mer som ett standardförfarande. En NIS-leverantör i sektorn skriver i en rapport dock att manuell hantering leder till ”ökad belastning, vilket ger ökad risk för avvikelse”.

Leverans och distribution av dricksvatten

I Sverige står de kommunala vattenverken för ca 85 % av den totala dricksvattenförsörjningen, vilket kompletteras av flera mindre och ibland privata aktörer.[22] Leverantörerna är utspridda i hela landet och deras produktionsställen i hemkommunen är ofta uppdelade på olika geografiska platser med allt från mätstationer, pumpstationer och distributionsanläggning. Informationssystem och olika typer av digitala tjänster krävs i många fall för att kunna övervaka och kommunicera med de delar av verksamheten som är geografiskt utspridda.

Sektorn karaktäriseras i hög grad av industriella processer, och man använder därför i stor utsträckning industriella styr- och kontrollsystem (ICS). Inom sektorns verksamheter finns det en uppdelning mellan informationsteknik (it) och *operational technology* (ot). OT innefattar de system och delsystem som behövs för att styra och övervaka en fysisk process. It-system är det som organisationen använder i den övriga och den mer kontorsnära verksamheten. Historiskt har det varit normalt att separera ICS och övrig it, men precis som i samhället i stort så innebär digitaliseringen både möjligheter och utmaning inom sektorn, där det i högre utsträckning sker sammankopplingar mellan de olika nätverken. Till exempel för att ge behörig möjlighet att arbeta på distans av olika anledningar. Att koppla OT-miljön mot kontorsnätverket, särskilt utan tillräckliga skyddsmekanismer riskerar att exponera delar eller hela av de industriella styr- och regleringssystemen som styr vattenproduktionen mot internet.

22. https://www.livsmedelsverket.se/produktion-handel--kontroll/dricksvattenproduktion

Av MSB:s föreskrifter (MSBFS 2018:7) framgår att de organisationer som omfattas av NIS inom leverans och distribution av dricksvatten tillhandahåller:[23]

1. 1. leveranser av dricksvatten som en huvudman enligt 2 § lagen (2006:412) om allmänna vattentjänster tillhandahåller[24]
   a) minst 20 000 personer, eller
   b) akutsjukhus.

Av MSB:s föreskrifter (MSBFS 2018:9) framgår att leverantörer inom leverans och distribution av dricksvatten ska rapportera incidenter som orsakat störning i den samhällsviktiga tjänsten som:[25]

1. har pågått i minst två timmar och som
   a) kan antas ha påverkat minst 2 000 personer,
   b) har påverkat akutsjukhus, eller
2. har påverkat styrning och övervakning av tjänsten.

23. Första mars 2022 kommer nya föreskrifter för identifiering och anmälan för leverantörer av samhällsviktiga tjänster att träda i kraft vilket bland annat påverkar definitionen av en leverantör inom dricksvattensektorn.

24. 8 kap §1 MSBFS:7

25. 8 kap §1 MSBFS:9

Incidenter & störningar

Leverantörerna inom sektorn har 2020 och 2021 varit de som rapporterar näst flest incidenter. Likt hälso- och sjukvårdssektorn, behöver inte detta betyda att det sker fler incidenter i denna sektor, utan att organisationerna i högre grad än flera andra sektorer har en vana att rapportera incidenter, samt utgör en betydande del av de rapporteringspliktiga organisationerna. Underlaget är för litet för en mer genomgripande analys men i relation till 2020 års rapportering ser trenderna i rapporteringen stabila ut. Nedan följer några generella observationer.

Den vanligaste incidenten inom sektorn rapporteras enligt punkt två i listan ovan, det vill säga att incidenten har påverkat styrning och övervakning av tjänsten. Det vanligaste incidenterna inom sektorn bedöms i likhet med samtliga inkomna incidentrapporter ha orsakats av systemfel, och det är tillgänglighet hos tjänsten som drabbats, exempelvis genom att ett övervakningssystem i sig själv, eller via en stödtjänst till den, inte varit tillgänglig. Det är vanligast att en leverantör inom sektorn rapporterar att det är ett system för processtyrning som drabbats, och incidenter i kommunikationstjänster eller administrativa system utgör endast en liten del av rapporteringen inom sektorn.

Inom sektorn så är det mindre vanligt att en incident orsakar en extern störning i den bemärkelsen att det blir märkbart hos användare av tjänsten, det vill säga konsumenter av dricksvatten. Det är ingen av leverantörerna som anger att incidenten orsakat en sådan störning som gjort att tjänsten inte alls kunnat bedrivas (jämför med diagram 2). Det är dock en betydande minoritet av leverantörerna som rapporterar att flera av tjänstens funktioner saknades under störningen. De flesta anger att endast vissa eller inga funktioner saknades. Leverantörerna bedömer därför oftast att dessa incidenter inte har lett till någon märkbar störning utanför organisationen och att de inte drabbat varken privatpersoner eller andra organisationer. Manuella rutiner, och redundans i form av hög kapacitet leder ofta till att störningen i tillhandahållandet av tjänsten inte påverkar samhället märkbart. Störningen bedöms av leverantörerna främst ha påverkat på lokal nivå vilket följer av att dricksvatten i stor utsträckning produceras och distribueras lokalt.

Det förekommer även i denna sektor att liknande incidenter inträffar igen, samt att störningarna, om de uppstår, också liknar tidigare störningar. De leverantörer som har rapporterat mer än en gång under 2021 har oftast rapporterat om olika typer av incidenter. Detta skiljer sig aningen från 2020 års rapportering då ett antal leverantörer inom sektorn rapporterade återkommande liknande incidenter.

Leverantörerna i sektorn är i mindre utsträckning (än hälso- och sjukvården) drabbade av incidenter i underleverantörers tjänster, men incidenter med ursprung hos underleverantör utgör ändå runt hälften av de rapporterade incidenterna inom sektorn.

Krav, rekommendationer & stöd

NIS-direktivet syftar till att höja den gemensamma nivån av säkerhet i nätverk och informationssystem hos några av unionens viktigaste tjänster. I den svenska NIS-regleringen ställs krav på att leverantörerna ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Detta innebär att NIS-leverantörerna ska införa ändamålsenliga och proportionella säkerhetsåtgärder för att skydda sina informationssystem och nätverk.

Baserat på den incidentrapportering MSB mottagit framträder ett antal problemområden som ofta leder till incidenter. Dessa områden berör både sådant som det redan ställs krav på i MSB:s och tillsynsmyndigheternas föreskrifter och sådant som det inte ställs krav på. Att uppmärksamma och förbättra arbetet inom dessa områden är därför viktigt inte bara för att undgå att drabbas av incidenter som hade kunnat undvikas men också för att uppfylla de krav som organisationerna måste uppfylla enligt föreskrifter. Av de krav som NIS-leverantörer ska uppfylla i enlighet med lag, förordning och MSB:s samt tillsynsmyndigheternas föreskrifter är dessa av särskild betydelse att arbeta vidare med utifrån vad som framkommit i våra analyser.

- Analysera informationstillgångar och identifiera de nätverk och informationssystem som den samhällsviktiga eller digitala tjänsten är beroende av. Kom ihåg att även externa informationstillgångar kan vara kritiska, till exempel hos samarbetsparters eller systemleverantörer. Värdera tillgångarna utifrån olika skyddsbehov såsom skydd mot obehörig tillgång och behov av tillgänglighet.
- Värdera tillgångarna utifrån vilka konsekvenser otillräckligt skydd mot obehörig påverkan på konfidentialitet, tillgänglighet och riktighet kan få. Inkludera i era analyser vilka konsekvenser utomstående organisationer får om er tjänst inte levereras.
- Etablera tydliga kontaktvägar med underleverantörer gällande informationsdelning vid incidenter, och kravställ ett systematiskt och riskbaserat informationssäkerhetsarbete inklusive de säkerhetsåtgärder som är specifika för den information och de informationssystem som era underleverantörer hanterar.
- Budgetera för incidenter för att inte undvika att medel tas från annan verksamhet. Säkerställ även att de resurser som krävs för att hantera incidenten finns tillgängliga om en incident skulle uppstå och att den redundans som krävs finns under tiden incidenten hanteras.

Utifrån de incidentrapporter MSB mottagit behöver **leverantörer inom hälso- och sjukvård** särskilt arbeta med att

- Förbättra arbetssätten för att åtgärda identifierade risker så att inte identifierade risker fortsätter att realiseras.
- Upprätta kontinuitetsplaner som är rätt dimensionerade och fungerar vid olika incidenter och störningar.
- Ha beredskap att hantera planerade avbrott, så som uppdatering av centrala tjänster, elavbrott, internetbortfall, och ha beredskap för att planerade förändringar kan gå fel.
  - Ha etablerade kanaler för hur information delas inom organisationen inför förändringar så att rätt information når dem som berörs.
  - Ha etablerade informationskanaler med underleverantörer gällande förändringshantering.
- Kravställ att underleverantörer agerar på incidentinformation och har fungerande rutiner och beredskapskedjor vid incidenter.
  - Etablera rutiner för om hur incidentinformation ska utbytas med underleverantör.
- Etablera redundans av kritiska funktioner så som anslutningar, eltillförsel.

Utifrån de incidentrapporter MSB mottagit behöver **leverantörer inom leverans och distribution av dricksvatten** särskilt arbeta med att

- Säkerställa redundans i övervakning av tjänsten.

Slutligen måste det betonas att det mest centrala för att organisationer ska kunna uppnå och bibehålla en tillräcklig nivå för sin informations- och cybersäkerhet är att de bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete. Det innebär bland annat att värdera hur viktig information är för organisationen utifrån behov av tillgänglighet, riktighet och konfidentialitet samt bedöma och hantera risker med informationshanteringen. Utifrån resultatet av värderingen av information, riskbedömningen kan organisationen prioritera och välja och införa ändamålsenliga och proportionella säkerhetsåtgärder.

Till stöd för NIS-leverantörerna erbjuder MSB även ett antal vägledningar.

- **Vägledning för systematiskt och riskbaserat informationssäkerhetsarbete (metodstödet)**
- **Förebyggande stöd för att bygga upp organisationens incidenthantering**
- **Vägledning för anmälan och identifiering av leverantörer av samhällsviktiga tjänster enligt NIS-regleringen**
- **Stöd för ifyllande av incidentrapporteringsformulären för samhällsviktiga respektive digitala tjänster**
- **Vägledning om rapportering av incidenter för leverantörer av samhällsviktiga tjänster enligt NIS-regleringen**

Samtliga vägledningar återfinns på MSB:s hemsida. Utöver detta erbjuder alla tillsynsmyndigheter stöd på sina hemsidor för leverantörer inom respektive sektor.

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 MSB1916 - februari 2022 ISBN 978-91-7927-237-1