ÅRSRAPPORT

NIS-leverantörers it-incidentrapportering 2020

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

NIS-incidenter och äventyr

Rekommendationer och press

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

© Myndigheten för samhällsskydd och beredskap (MSB)

Foto omslag: iStock
Tryck: DanagårdLiTHO
Produktion: Advant

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


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.


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

<table>
<thead>
<tr>
<th>Begrepplista</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sammanfattning</td>
<td>9</td>
</tr>
<tr>
<td>1. Inledning</td>
<td>11</td>
</tr>
<tr>
<td>1.1 Sverige år 2020</td>
<td>11</td>
</tr>
<tr>
<td>1.2 En årsrapport över NIS-incidenter 2020</td>
<td>12</td>
</tr>
<tr>
<td>Incidentexempel 1</td>
<td>13</td>
</tr>
<tr>
<td>Incidentexempel 2</td>
<td>13</td>
</tr>
<tr>
<td>2. NIS-direktivet</td>
<td>15</td>
</tr>
<tr>
<td>2.1 Direktivet i svensk reglering</td>
<td>15</td>
</tr>
<tr>
<td>2.2 Berörda aktörer</td>
<td>17</td>
</tr>
<tr>
<td>2.3 Incidentrapportering: så fungerar det</td>
<td>18</td>
</tr>
<tr>
<td>2.4 Syftet med incidentrapportering</td>
<td>19</td>
</tr>
<tr>
<td>3. Rapportering 2020: Redovisning av inrapporterade NIS-incidenter</td>
<td>21</td>
</tr>
<tr>
<td>3.1 Incidentrapportering</td>
<td>22</td>
</tr>
<tr>
<td>3.1.1 Fiktivt exempel</td>
<td>22</td>
</tr>
<tr>
<td>3.2 Typer av incidenter</td>
<td>23</td>
</tr>
<tr>
<td>3.2.1 Tid och hur incidenten upptäcks</td>
<td>25</td>
</tr>
<tr>
<td>3.2.2 Störningen</td>
<td>25</td>
</tr>
<tr>
<td>3.2.3 Kostnader</td>
<td>25</td>
</tr>
<tr>
<td>3.2.4 Hantering</td>
<td>26</td>
</tr>
<tr>
<td>3.2.5 Åtgärder</td>
<td>27</td>
</tr>
<tr>
<td>Incidentexempel 3</td>
<td>28</td>
</tr>
<tr>
<td>3.2.6 Orsaker</td>
<td>29</td>
</tr>
<tr>
<td>3.3 Slutsatser</td>
<td>29</td>
</tr>
<tr>
<td>3.3.1 Antagonistiska hot</td>
<td>30</td>
</tr>
<tr>
<td>3.3.2 Underleverantörer</td>
<td>31</td>
</tr>
<tr>
<td>3.3.3 Informations säkerhetsaspekter</td>
<td>31</td>
</tr>
<tr>
<td>3.3.4 Kostnader</td>
<td>32</td>
</tr>
<tr>
<td>3.3.5 Rapporteringens vikt för totalförsvaret</td>
<td>32</td>
</tr>
<tr>
<td>3.4 Rekommendationer</td>
<td>33</td>
</tr>
<tr>
<td>Incidentexempel 4</td>
<td>35</td>
</tr>
</tbody>
</table>
4. Stöd från MSB

4.1 CERT-SE

4.2 Vikten av att arbeta systematiskt och riskbaserat

4.3 Arbetet framåt

5. Europeiska erfarenheter

5.1 Utvecklingen av NIS-direktivet och cybersäkerheten på europeisk nivå

5.1.1 Uppdaterat direktiv

5.1.2 Cybersäkerhetsakten

5.1.3 Ny EU-strategi på cybersäkerhetsområdet

5.1.4 EU:s långtidsbudget och återhämtningsplan

5.1.5 Det europeiska kompetenscentret och nätverket av nationella samordningscenter

5.1.6 Joint Cyber Unit

5.2 Jämförelse mellan länder

5.3 Finland

5.4 Tyskland

5.5 Storbritannien

6. Slutord
**Begreppslista**

<table>
<thead>
<tr>
<th>Begrepp</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samhällsviktig tjänst</td>
<td>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.</td>
</tr>
<tr>
<td>Digital tjänst</td>
<td>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.</td>
</tr>
<tr>
<td>OES</td>
<td>(Eng. Operator of Essential Service) Leverantör av samhällsviktig tjänst.</td>
</tr>
<tr>
<td>DSP</td>
<td>(Eng. Digital Service Provider) Leverantör av digital tjänst.</td>
</tr>
<tr>
<td>NIS-leverantör</td>
<td>Organisationer som omfattas av NIS-regleringen. Se vidare beskrivning i kapitel 2.2 i denna rapport.</td>
</tr>
<tr>
<td>SPOC</td>
<td>(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.</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Union Agency for Cybersecurity Europeiska unionens cybersäkerhetsbyrå.</td>
</tr>
<tr>
<td>INEA</td>
<td>Innovation and Networks Executive Agency Europeiska unionens nätverk och innovationsbyrå, har till uppgift att finansiera projekt som stöter innovation och ett sammankopplat Europa.</td>
</tr>
<tr>
<td>NIS-incident</td>
<td>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 benämnas 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.</td>
</tr>
</tbody>
</table>
| **ICS** | (Eng. Industrial Control Systems)  
Industriella informations- och styrsystem. |
| **ICT** | (Eng. Information and Communications Technology)  
Informations- och kommunikationsteknik. |
| **Nätfiske** | (Eng. Phishing)  
| **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 lösen- summa 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
2. 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.


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.

---

Inledning
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


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/
Inledning

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. 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 nödvändigvis rapporterar all incidenter som inträffat. Det kan även finnas leverantörer som inte anmält sig som NIS-leverantör ännu.


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 inlet arbetet med incidentrapportering ska få kunskap och verktyg att påbörja arbetet.

---

**Incidentexempel 1**

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

**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
2. NIS-direktivet


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 informationsäkerhet 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) om informationsäkerhet för samhällsviktiga och digitala tjänster, ”NIS-forordningen”.

NIS-leverantörer - II-incidentrapportering 2020 15
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 utförs av Energimyndigheten, Finansinspektionen, Inspektionen för vård och omsorg/Socialstyrelsen, Livsmedelsverket, Post- och telestyrelsen, samt Transportstyrelsen som har mandat att utfärda sektorspecifika 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.

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

---

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 utförs av Energimyndigheten, Finansinspektionen, Inspektionen för vård och omsorg/Socialstyrelsen, Livsmedelsverket, Post- och telestyrelsen, samt Transportstyrelsen som har mandat att utfärda sektorspecifika 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.

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.

### 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 incidentrapportering 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 MSBs 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 MSBs 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 MSBs hemsida.\(^9\)

---

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


8. MSB ger även ut en vägledning gällande incidentrapportering som både stöttar att förstå vad som ska rapporteras, och hur en leverantör går till väga – Vägledning för ifyllandet av incidentrapporteringssformulären för samhällsviktiga respektive digitala tjänster finns tillgänglig på MSBs 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 analyser 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 informations-säkerhetsarbete 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.

Rapportering
2020
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 leverantöre x ger MSB ett stort dataunderlag och möjliggör en detaljerad analys av de incidenter som skett inom ramen för NIS-regleringen under året som gått.


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, motsstridigt. Detta kommer troligtvis avhjälpas genom det digitala rapporteringssystem som i större utsträckning kan stöta 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


Om incidenten fortgår och inte upptäcks kan störningen förvärras, och om tillräckligt mycket orent vatten pumpas ut kan ett ökat antal sjuksdomsfall 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 nödvändigvis 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 styra 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 kringmiljön). Av de som rapporterat att en incident skett i ett system eller nätverk, har incidenten ofta inträffat i ett system eller nätverk dedikerat för kommunikation (se Diagram 1). Ofta handlar incidenten om att kontinuerlig uppkoppling har brutits.

Av de som uppgivit att det skett en incident i ett system eller nätverk uppgår 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, slutfunget eller förstörtats.

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.
Tillgänglighet är den informationssäkerhetsaspekt som påverkats mest av incidenterna i den inkomna rapporteringen.\textsuperscript{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 röjs.
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 dricksvattenförortning. I några få fall har det rapporterats att incidenten upptäckts av ett externt kontrakterat detekteringssystem.


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 anges), 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 uppgör leverantörerna att organisationen slutgiltigt har fastställt incidentens kostnader, men ännu färre har presenterat kostnadsuppskattningsar 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 uppskattningsarna sträcker sig mellan 2 000–5 000 000 kr, och mediankostnaden är 25 000 kr (medelvärde: 451 000 kr).


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.


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 förebryggande åtgärder krävs. Syftena med de särskilda hanteringsåtgärderna är nästintill jämt fördelade på att åtgärda incidenten, störningen eller störningens konsekvenser. Drygt en tredjedel har vid rapporteringstillsfallet 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 (medelvärde: 266 000 kr). Som i fallet med kostnader för incidenterna och störningarna, så bör de uppskattade kostnaderna för förebryggande 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 patients 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.


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

---

Diagram 4. Årsfördelning över när leverantören upptagit att incidenten inträffade


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. 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.

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 följddefekter 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 rapporterings tillfällena, utan förlitar sig på informationsdelning från den externa aktören. Exempelvis illustreras detta i en av incidentrapporterna som inkommit: ”Inväntar leverantörens rapport (underleverantörens, reds. ann.), 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 in 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 orydliga 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 brutton, 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

---

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 uppgir kostnader för incidenter eller störningar. Det kan troligtvis bero på att leverantörerna har svårt att bedöma kostnader, att personer som rapporterar inte ges tillgång till sådan info, organisationen inte prioriterar att identifiera kostnader eller att de av olika anledningar inte vill uppgöra 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.


### 3.3.5 Rapporteringens vikt för totalförsvaret

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, utförande 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
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. Omvänd 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 riskbaserad 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.


**Tips om metodstödet för NIS-leverantörer**
Du hittar metodstödet i sin helhet och fler verktyg på: [www.informationssakerhet.se](http://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.

- **Analysa informationstillgångar:** Identifiera de nätverk och informationsystem som den samhällsviktiga eller digitala tjänsten är beroende av. Kom ihåg att även externa informationstillgångar kan vara kritiska, t.ex. hos samarbetspartners 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.

4.3 Arbetet framåt

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

- **Cybersäkerhetscentret:** I december 2020 beslutade regeringen att inrätta ett nationellt centrum 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 centrum för cybersäkerhet är att vara stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige och minska cybersäbarheterna. 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.


- **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
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 länder 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**


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. Samarbetetsgruppen stödjer och underlättar det strategiska samarbetet, utbytet av information samt skapa 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 uniformalt identifieringsförfarande av leverantörer. Nu genomläsas och analyseras förslaget i samtliga medlemsstater för att därefter förhandlas inom
unionen. Förhandlingarna 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.


5.1.2 Cybersäkerhetsakten


5.1.3 Ny EU-strategi på cybersäkerhetsområdet

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 samlad 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 återhämningsplan**


**5.1.5 Det europeiska kompetenscentret och nätverket av nationella samordningscenter**


**5.1.6 Joint Cyber Unit**

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 trendar 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 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


Till skillnad från Sverige har Finland mottagit en mindre mängd NIS-incident-rapporter 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**


---

**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.


Incidentexempel från Tyskland:
Universitetssjukhuset i Düsseldorf blev under 2020 utsatt för en utpressningsattack. Ett trettiotal servrar krypterades vilket bland annat medförde att all patient-data blev otillgänglig under en tid. Till följd av detta kunde sjukhuset inte ta emot nya akutfall, och denna avbrottet ledde 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

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, såsom 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

Storbritanniens rapporter av incidenter är begränsade, och har nätt 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.

---

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 syns 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.