Myndigheten för samhällsskydd och beredskap

Årsrapport it-incident-rapportering 2018

En sammanställning och analys av de statliga myndigheternas it-incidentrapportering

Titel

Enhet: Enheten för verksamhetssamordning och strategisk analys

Produktion: Advant

Publikationsnummer: MSB1334 – April 2019
ISBN: 978-91-7383-907-5

Innehåll

Bilaga 1 Rapporteringspliktiga myndigheter och antal inlämnade rapporter
(sekretess med stöd av OSL 15:2 (försvarssekretess) och 18:8 (säkerhets- eller bevakningsåtgärd))

Bilaga 2 Underlag från Säkerhetspolisen och Försvarsmakten
(sekretess med stöd av OSL 15:2 (försvarssekretess))

Bilaga 3 Om bevakningsansvariga myndigheter
(sekretess med stöd av OSL 15:2 (försvarssekretess) och 18:8 (säkerhets- eller bevakningsåtgärd))

Bilaga 4 Rapporterade incidenter under 2018
(sekretess med stöd av OSL 15:2 (försvarssekretess) och 18:8 (säkerhets- eller bevakningsåtgärd))

Sammanfattning

Statliga myndigheter ska rapportera it-incidenter som de själva bedömer som allvarliga[1]. Rapporteringen görs till Myndigheten för samhällsskydd och beredskap (MSB) som utfärdar föreskrifter för detta. Den här rapporten innehåller en sammanställning och analys av de statliga myndigheternas rapportering av it-incidenter som de bedömt som allvarliga 2018. Syftet med rapporteringen är att den ska vara ett stöd för arbetet med samhällets informations- och cybersäkerhet samt att rapporteringen ska bidra till arbetet med en lägesbild för samhällets informations- och cybersäkerhet.

Under 2018 har 87 myndigheter rapporterat 297 allvarliga it-incidenter till MSB. MSB ser positivt på att fler myndigheter nu rapporterar it-incidenter, något som indikerar att medvetenheten ökar. Rapporteringsgraden varierar över året, men har sedan starten i april 2016 inte förändrats i någon större omfattning. MSB bedömer att fler it-incidenter hos statliga myndigheter borde betraktas som allvarliga och därmed rapporteras. Denna bedömning grundar sig bland annat på de it-incidentrapporter som inkommit och den vidare omvärldsbevakningen hos MSB.

Myndigheternas ledningar ska snarast säkerställa att myndigheten fullt ut följer MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1) samt MSB:s föreskrifter om statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2).

Baserat på rapporteringen av allvarliga it-incidenter och andra underlag kan MSB konstatera att flera myndigheter inte följer MSB:s föreskrifter om ett systematiskt och riskbaserat arbetssätt gällande informationssäkerhet. Detta gäller såväl utifrån antalet rapporterande myndigheter, antalet incidenter och beskrivningen av incidenternas orsaker och konsekvenser. Arbetet med informations- och cybersäkerhet måste ske systematiskt, baseras på analyser och tillföras resurser för att analyserna ska kunna genomföras och resultatet av analyserna omsättas i åtgärder.

De statliga myndigheternas medvetenhet har ökat, men de måste också ha med säkerhetsperspektivet i digitaliseringsprocesserna. Allvarliga it-incidenter riskerar på sikt att få allt större konsekvenser för medborgarnas förtroende för digitaliseringsprocessen och de myndigheter som genomför den.

1. Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2).

Arbetet med informations- och cybersäkerhet måste genomsyra hela myndighetens arbete, inte enbart hanteras av it- eller säkerhetsavdelningar. En ökad digitalisering medför att behovet av säkra cyberfysiska system och it-system ökar än mer. MSB kan konstatera att myndigheternas it-incidentrapportering indikerar att statliga myndigheter har ett stort arbete kvar att göra gällande säkra tekniska lösningar och arbetet med att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.

Myndigheter är beroende av tjänster via externa system och infrastruktur och måste i förväg veta hur de ska agera vid störningar i dessa tjänster. En del av myndigheternas arbete bör bestå i att genomföra övningar i syfte att pröva och utveckla myndighetens säkerhetsåtgärder för kontinuitetshantering avseende informations- och cybersäkerhet.

It-incidentrapporteringen från statliga myndigheter behöver öka, vilket också kommer kunna ske med hjälp av de utökade medel som regeringen tilldelat MSB. Under 2019 kommer MSB att skärpa kraven på och öka stödet till statliga myndigheter i syfte att förbättra informations- och cybersäkerheten hos statliga myndigheter. MSB arbetar med att revidera och förtydliga kraven på rapportering av it-incidenter som allvarligt kan påverka säkerheten i myndigheternas informationshantering. Genom att MSB tilldelats ytterligare medel finns det bättre förutsättningar att utöka stödet till myndigheterna. Det innefattar bland annat utökad återkoppling och ett nytt metodstöd. MSB kommer även att fördjupa samarbetet med centrala aktörer.

Inledning

1. Inledning

Alla statliga myndigheter ska enligt 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap *skyndsamt rapportera it-incidenter som inträffat i myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation.* Rapporteringen ska ske till Myndigheten för samhällsskydd och beredskap (MSB), i enlighet med MSB:s föreskrifter om statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2).

MSB ska årligen lämna en rapport till regeringen avseende den it-incidentrapportering som skett till myndigheten.[2]

Inför sammanställningen av rapporten ska MSB enligt sin instruktion även inhämta upplysningar från Säkerhetspolisen och Försvarsmakten om de incidenter som rapporterats in till dessa myndigheter enligt 10 a § säkerhetsskyddsförordningen (1996:633).[3]

Syftet med den här rapporten är att presentera en sammanställning och analys av de it-incidentrapporter som inkommit under 2018[4]. Rapporten innehåller även slutsatser och rekommendationer som förväntas bidra till en ökad kunskap inom informations- och cybersäkerhetsområdet och utgöra ett stöd i det förbyggande arbetet med att förhindra it-incidenter. Hemlig alternativt sekretessbelagd information gällande myndigheternas rapportering redovisas till regeringen i fyra hemliga bilagor, se innehållsförteckningen.

Huvuddelen av informationen i de inkomna it-incidentrapporterna omfattas av sekretess med stöd av 18 kap 8 § 3 p. offentlighets- och sekretesslagen (2009:400).[5]

2. Enligt 11 a § 2 st förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap,

3. Från 1 april 2019 gäller ny lagstiftning för säkerhetsskyddet, men eftersom rapporten och incidenterna avser 2018 och MSB:s begäran om underlag från Säkerhetspolisen och Försvarsmakten är gjord före 1 april 2019 hänvisar MSB fortfarande till den gamla lagstiftningen.

4. I enlighet med kravet på årlig rapport i 11 a § 2 st förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

5. Tillämpningen har prövats flera gånger i Kammarrätten, där domsluten stöder MSB:s ställningstagande till sekretessbedömningen. Se bland annat dom från Kammarrätten i Göteborg, mål nr 5032-16.

Om rapporteringen

2. Om rapporteringen

2.1 Rapporterings-skyldiga myndigheter

Enligt 20 § i förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap gäller rapporteringsskyldigheten för it-incidenter alla statliga myndigheter under regeringen, med undantag för Regeringskansliet, kommittéväsendet, Säkerhetspolisen, Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt och Totalförsvarets forskningsinstitut enligt 3 § i samma förordning.

För utlandsmyndigheterna tillämpas bestämmelserna endast i den utsträckning som bestäms i föreskrifter som meddelas av Regeringskansliet (Utrikesdepartementet).

Rapporteringsskyldigheten omfattar inte sådana incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen (1996:633).[6]

I mars 2018 uppgick antalet rapporterings-skyldiga myndigheter till 256 stycken, vilket är en ökning med 12 myndigheter sedan föregående år.

2.2 Vad myndigheterna ska rapportera

Statliga myndigheter ska ha rutiner för att identifiera, rapportera, bedöma, hantera och dokumentera incidenter som kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation.[7] Myndigheterna ska skyndsamt rapportera it-incidenter som inträffat i myndighetens informationssystem och som *allvarligt* kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation.[8] Det är upp till myndigheterna själva att bedöma vilka incidenter som är tillräckligt allvarliga för att omfattas av rapporteringsskyldigheten.

Rapporteringen av allvarliga it-incidenter till MSB ska innehålla uppgifter om bland annat tidpunkter för upptäckt, när incidenten inträffade och om den är pågående eller avslutad. Myndigheterna ska också uppge eventuell sekretess för uppgifterna i rapporten samt om händelsen är polisanmäld. Myndigheterna ska därutöver bedöma vilken eller vilka kategorier som it-incidenten faller inom, liksom en beskrivning av vad som inträffat och en initial bedömning och beskrivning av it-incidentens konsekvenser.[9]

6. Från 1 april 2019 gäller undantag med motsvarande innebörd utifrån 2 kap 10 § säkerhetsskyddsförordningen (2018:658).
7. 10 § MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1).
8. Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.
9. MSB:s föreskrifter för obligatorisk it-incidentrapportering för statliga myndigheter (MSBFS 2016:2).

It-incident-rapporteringen under 2018

3. It-incidentrapporteringen under 2018

I detta kapitel redovisas den rapportering som skett under 2018. Jämförelser görs även med tidigare års rapporteringar.

I enstaka fall har myndigheterna lämnat en preliminär rapport som sedan kompletterats. I de fallen har detta endast räknats som en rapport. Däremot kan en och samma samhällsstörning generera it-incidentrapporter från flera myndigheter om flera myndigheter berörts, exempelvis vid elavbrott eller störningar i elektroniska kommunikationer.

Rapporterna räknas utifrån det datum som de rapporterats till MSB, även om incidenten har upptäckts eller inträffat vid ett tidigare datum.

3.1 Antal rapporterade incidenter

Under 2018 har 87 myndigheter lämnat in totalt 297 it-incidentrapporter till MSB.[10] Detta innebär att 169 myndigheter inte lämnat in någon it-incidentrapport till MSB under 2018.

Jämfört med tidigare år har fler myndigheter rapporterat it-incidenter. Vissa myndigheter som tidigare lämnat ett större antal rapporter per år har under 2018 minskat sin rapportering.

Andelen rapporterande myndigheter av de som är rapporteringspliktiga har ökat marginellt. Flera myndigheter har påbörjat rapportering under 2018, men samtidigt har även ett tjugotal myndigheter som rapporterat under 2017 inte lämnat någon rapport under 2018.

Av de rapporterande myndigheterna har 17 stycken lämnat fem rapporter eller fler, vilket är samma siffra som i föregående års rapportering. Det är dock inte samma myndigheter som rapporterat mest under 2018 jämfört med 2017.

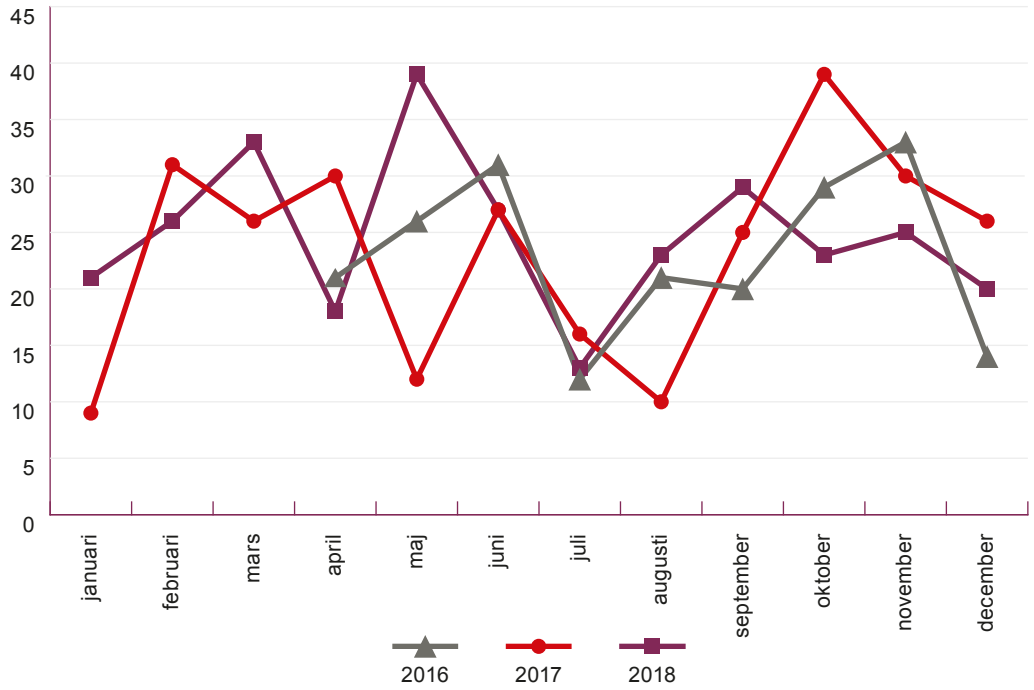
Rapporteringsgraden varierar över året, men har sedan starten i april 2016 inte förändrats i någon större omfattning.

10. Rapporteringsgraden kan fortfarande vara påverkad av undantaget i rapporteringsskyldigheten i de fall en myndighet har utkontrakterat delar av sin it-drift innan ikraftträdandet av föreskrifterna. Detta i enlighet med 9 § i MSB:s föreskrifter om statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2).

Tabell 1. Antal rapporteringspliktiga myndigheter, antal rapporterande myndigheter och antalet lämnade rapporter för 2016-2018.

	2016	2017	2018
Antal rapporteringspliktiga myndigheter	244	244	256
Antal (andel) rapporterande myndigheter	77 (32 %)	79 (32 %)	87 (34 %)
Antal inlämnade it-incidentrapporter	214 (285)[11]	281	297

Figur 1. Antal inkomna it-incidentrapporter per månad 2016 – 2018.



3.2 Skyndsam rapportering

En it-incidentrapport ska enligt krisberedskapsförordningen lämnas skyndsamt. MSB har i föreskrifterna för rapporteringen preciserat detta till att rapportering ska ske inom 24 timmar efter att incidenten upptäckts.

Det är även möjligt att inom dessa 24 timmar lämna en preliminär rapport som sedan kompletteras. I de allmänna råden kopplade till föreskrifterna specificerar MSB att den rapporterande myndigheten anses ha upptäckt it-incidenten när information om den hanteras i utpekad intern process för hantering av it-incidenter eller när säkerhetsansvarig eller motsvarande fått kännedom om incidenten.

11. Då incidentrapporteringen startade först i april 2016 har det redovisade antalet it-incidentrapporter även justerats för brutet räkenskapsår.

En incident blir heller inte rapporteringspliktig förrän den bedöms som allvarlig. Varje myndighet gör en självständig bedömning av vilka it-incidenter som omfattas av rapporteringsskyldigheten i 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

En minoritet av de allvarliga it-incidenter som myndigheterna rapporterade till MSB under 2018 lämnades inom 24 timmar efter att de upptäckts, utifrån vad som går att utläsa från rapporteringen. Ungefär 15 % av rapporterna lämnades till MSB över en vecka efter att incidenten upptäckts. Angrepp rapporteras i regel snabbare än andra typer av incidenter. Det som inte framgår av rapporteringen är om det finns en tidsfördröjning från det att myndigheterna anger att en incident upptäcks till att den bedöms som så allvarlig att den är rapporteringspliktig. Eftersom vissa incidenter kan ha ett utdraget förlopp eller att orsaker eller konsekvenser kan vara svåra att överblicka i ett inledande skede skulle detta kunna förklara en del av fördröjningen i rapportering till MSB.

3.3 Kategorier av incidenter som rapporteras

Vid rapportering av en it-incident går det att ange flera incidentkategorier för varje rapport. Exempelvis kan en it-incident i driftmiljön orsakas av ett angrepp som leder till hindrad tillgång till information. Därmed kan tre olika kategorier anges vid rapportering.

Rapporterade incidenter har av MSB bedömts huvudsakligen tillhöra en incidentkategori. Enligt denna bedömning har rapporterna varit fördelade enligt nedanstående tabell.

Tabell 2. Rapporterade allvarliga it-incidenter per kategori

Kategori	Antal
Angrepp	73
Oönskad eller oplanerad störning i kritisk infrastruktur	59
Störning i driftmiljö	47
Handhavandefel	42
Störning i mjukvara eller hårdvara	38
Informationsläckage eller –förlust	21
Säkerhetsbrist i produkt	14
Annan plötslig oförutsedd händelse som lett till skada	3
Informationsförvanskning	0
Hindrad tillgång till information	0
Totalt	297

Angrepp utgör den största incidentkategorin med ungefär en fjärdedel av de rapporterade it-incidenterna. Därefter följer *Oönskad eller oplanerad störning i kritisk infrastruktur* samt *Störning i driftmiljö* och *Handhavandefel.*

Vid en separat genomgång av konsekvenskategorierna *Informationsläckage* eller *-förlust, Informationsförvanskning* och *Hindrad tillgång till information* framgår det av rapporteringen att *Hindrad tillgång till information* och *Informationsläckage* eller *-förlust* anges som en aktuell kategori i vardera 20 % av rapporterna. *Informationsförvanskning* förekommer betydligt mer sällan.

För exempel på inrapporterade incidenter, se kapitel 4.

3.4 Angreppens avsikt och effekt

MSB har gjort en särskild analys av de av myndigheterna inrapporterade it-incidenter från 2016 till 2018 som kategoriserats som angrepp. I analysen har MSB använt en taxonomi och utifrån den gjort en bedömning av vad som är den troliga avsikten med angreppet, samt en bedömning av angreppets effekt på den myndighet som drabbats.[12]

Den typ av angrepp, enligt taxonomin, som oftast lyckats är de som gjorts med avsikt att förhindra förmedling av nytta för den angripne, exempelvis genom att allmänheten inte kunnat använda e-tjänster eller att myndighetens handläggning fördröjts. Ett konkret exempel på sådana angrepp, som även är vanligt förekommande, är överbelastningsattacker. Sådana angrepp får myndigheters webbsidor eller tjänster att gå ner under en tidsperiod, vilket därmed förhindrar dem från att tillhandahålla tjänster eller information.

Den vanligaste kategorin av angrepp, de fall där angreppen syftat till att orsaka nytta för den som angriper, har effekten ofta inte blivit vad angriparen troligen tänkt sig.

Exempel på detta är när angriparen försökt komma över information eller tjäna ekonomiskt på angreppet, men istället snarare förhindrat förmedling av nytta för den angripne, enligt resonemanget ovan. Ett vanligt förekommande exempel på sådana angrepp är utpressningstrojaner, så kallad *ransomware*.

It-incidentrapporteringen från statliga myndigheter 2016 till 2018 visar att även om ett angrepp misslyckats, givet vad angriparen troligen försökte uppnå, kan det ofta ha ställt till med skadliga effekter för den angripna myndigheten, om än i varierande omfattning. Sådana skador är huvudsakligen ekonomiska, samt i viss mån data- respektive förtroendeförluster.

3.5 Angrepp och polisanmälan

Vid angrepp, eller vid misstanke om att it-incidenten har sitt ursprung i en brottslig gärning, uppmanar MSB den rapporterande myndigheten att göra en polisanmälan. Av antalet incidenter som anges som kategori *Angrepp* polisanmäldes cirka 11 % utifrån vad myndigheterna uppgett i sina rapporter. Detta är i princip samma nivå som för 2017. I kategori *Angrepp* ingår cyberangrepp, exempelvis dataintrång, bedrägeri och överbelastningsattacker. Bland it-incidenterna som rapporterats till MSB under 2018 förekommer även försök till utpressning.

Fysiska tillgrepp t.ex. inbrott och stöld där exempelvis datorer eller mobiltelefoner förlorats rapporteras oftast i kategorin *Informationsförlust*. Av det totala antalet rapporterade it-incidenter, oavsett kategori, så uppgav myndigheterna att ungefär 7 % polisanmäldes, vilket är en liten ökning jämfört med föregående år.

Beroende på vilken typ av informationssystem som angripits[13] ska anmälan om misstänkt brott göras antingen till Polisen eller Säkerhetspolisen. I det senare fallet handlar det om en it-incident i myndighetens informationssystem och där incidenten allvarligt kan påverka säkerheten i ett informationssystem där hemliga uppgifter behandlas i en omfattning som inte är ringa, enligt 10 a § säkerhetsskyddsförordningen (1996:633). I det fall Försvarsmakten är tillsynsmyndighet ska rapporteringen ske till dem, och Säkerhetspolisen ska skyndsamt informeras.[14] Sådana anmälningar till Säkerhetspolisen och Försvarsmakten behandlas i bilaga 2 (sekre-

12. Analysen är gjord utifrån en bedömning från MSB:s sida givet den information som finns i myndigheternas incidentrapporter. Bedömningen innebär antaganden om angriparens avsikt, vilket är mycket svårt att ens med djupare efterforskningar dra slutsatser kring. MSB har därför utgått från angreppssättet (val av metod) hos angriparen för att göra sådana antaganden. Det utesluter inte fler eller andra avsikter med angreppen.

13. Fram till 31 mars 2019. Från 1 april 2019 gäller ny säkerhetsskyddslagstiftning med något ändrade formuleringar kring vad som omfattas av rapporteringsskyldigheten utifrån 2 kap 10 § säkerhetsskyddsförordningen (2018:658).

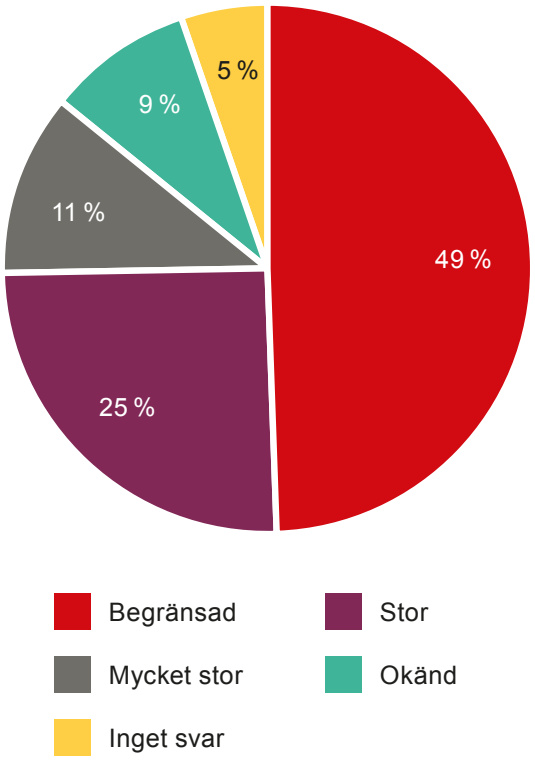
14. Reglering med motsvarande innebörd finns även i den nya lagstiftningen i 2 kap 10 § säkerhetsskyddsförordningen (2018:658).

tessbelagd).

3.6 De rapporterade it-incidenternas omfattning och konsekvenser

Omfattningen av konsekvenserna bedöms av den rapporteringsskyldiga myndigheten. Över hälften av de rapporterade it-incidenterna anges ha fått begränsade konsekvenser, vilket är en ökning jämfört med både 2016 och 2017. Samtidigt fortsätter trenden från 2017 med en minskad andel incidenter där myndigheterna inte ger något svar om bedömd konsekvens eller anger att omfattningen av konsekvenserna är okända (totalt 14 % av fallen 2018).

Figur 1. Figur 2 Fördelning av omfattning av konsekvenser för rapporterade it-incidenter under 2018



Värt att notera är att ytterst få incidenter som rapporterats i kategorin Angrepp har fått stora eller mycket stora konsekvenser enligt myndigheterna. De allra flesta angrepp uppges istället fått begränsade konsekvenser. De kategorier som ger mest omfattande konsekvenser (stora eller mycket stora) är Störning i driftmiljö respektive Oönskad eller oplanerad störning i kritisk infrastruktur.

3.7 Särskilt om större myndigheter

MSB har i år valt att mer specifikt undersöka rapporteringsgraden hos större myndigheter, vilket vi definierat som myndigheter med mer än 1 000 anställda under 2018. Utifrån Ekonomistyrningsverkets (ESV) uppgifter[15] består denna grupp av närmare 40 myndigheter[16], där ca 80 % av myndigheterna lämnat minst en incidentrapport under 2018. En stor andel av de större rapporteringsskyldiga myndigheterna (över 40 %) är universitet.

Större myndigheter rapporterade överlag färre it-incidenter i kategorin Angrepp under 2018 jämfört med hur det ser ut för alla myndigheter gemensamt. Istället har man rapporterat något fler it-incidenter inom kategorierna Störning i driftmiljö respektive Störning i mjuk- eller hårdvara.

De större myndigheternas rapporterade antal polisanmälda it-incidenter utgör en mindre andel i jämförelse med den totala andelen polisanmälda it-incidenter för samtliga myndigheter.

I bedömningen av omfattningen på it-incidenternas konsekvenser skiljer det sig inte nämnvärt mellan de större myndigheterna i jämförelse med den totala rapporteringen från samtliga myndigheter.

15. Hämtad från https://sromyndigheter.esv.se/ per den 9 januari 2019. Datat uppdateras kontinuerligt, här har MSB använt siffrorna som anges för 2018, vilket resulterar i samma lista på myndigheter som för 2017.

16. I denna siffra ingår inte de myndigheter som är undantagna från rapporteringsplikten, vilka är Regeringskansliet, Försvarsmakten och Försvarets materielverk.

Exempel på rapporterade it-incidenter

4. Exempel på rapporterade it-incidenter

Nedan presenteras några exempel på incidenter som rapporterats till MSB under 2018, utifrån de fyra mest förekommande kategorierna i rapporteringen. Flera av incidenterna är även exempel på andra kategorier än den primära. I flera av fallen har MSB/CERT-SE varit med och stöttat myndigheterna i arbetet med hanteringen av incidenterna. Sådant stöd är inte alltid nödvändigt eftersom de flesta av it-incidenterna som rapporteras till MSB inte innebär något sådant behov. Rapporteringen kan dock tjäna som en indikator på när flera aktörer blir drabbade samtidigt, exempelvis liknande angrepp i närtid, eller för att identifiera mönster av bredare och mer storskaliga attacker. De drabbade kan då även vara exempelvis kommuner eller företag.

I sammanhanget är det viktigt att påpeka att MSB/CERT-SE behandlar ett stort antal ärenden varje år där olika aktörer vänder sig till funktionen för att få stöd. De it-incidentrapporter som kommer in till följd av statliga myndigheters it-incidentrapportering är endast en delmängd av detta.

Det finns inga krav på myndigheterna att i rapporteringen till MSB lämna information om myndighetens uppföljning av inträffade it-incidenter. I de fall MSB fått in information om vidtagna åtgärder i de olika exempelfallen återges detta. För vissa incidentkategorier finns även en beskrivning av vad MSB brukar vidta för generella stöttande åtgärder till drabbade myndigheter.

4.1 Angrepp

I kategorin *angrepp* ingår incidenter där en utomstående part genom aktiv handling avsett, och ibland lyckats, påverka en myndighets informationshantering och informationstillgångar negativt.

Under året har flera myndigheter rapporterat it-incidenter där myndighetens anställda fått e-post med försök till nätfiske samt e-postbedrägerier[17]. Rapporter har även inkommit om olika överbelastningsattacker mot myndigheters it-system och -tjänster där behörig åtkomst till organisationernas it-miljö hindrats.

17. E-postbedrägerier innebär att falsk e-postkorrespondens bl.a. riktas till ekonomiansvariga om att göra felaktiga överföringar mellan konton.

4.1.1 Nätfiske

Nätfiske (från engelskans phishing), eller så kallat lösenordsfiske, är en form av bedrägeri där en användare lockas att uppge lösenord, kreditkortsnummer eller annan personlig information. Nätfiske utformas ofta som ett e-postmeddelande med ambitionen att efterliknautskick från en bank, kreditkortsbolag eller en systemleverantör och innehåller en uppmaning till användaren att klicka på en länk i e-postmeddelandet som går till en falsk webbsida. På denna falska webbsida finns ett inloggningsformulär där användaren uppmanas logga in genom att ange sina mejlkontouppgifter och liknande. Detta möjliggör åtkomst till uppgifterna för den som satt upp den falska sidan. Den falska webbsidan är ofta mycket lik originalet.

I ett fall fångades e-postmeddelanden med nätfiske inte helt upp av den aktuella myndighetens spamskydd utan gick igenom till myndighetens medarbetare, som uppmanades att registrera sina användaruppgifter på en webbsida för att deras användarkonto inte skulle stängas ner. Minst en medarbetare registrerade sina uppgifter. Medarbetarens konto användes sedan för att logga in på myndighetens webbmail där över 2000 e-postmeddelanden skickades ut från kontot, till både interna och externa mottagare. Meddelandena innehöll nya länkar för nätfiske.

MSB/CERT-SE har under året återkommande publicerat rekommendationer och föreslagit åtgärder för drabbade aktörer. Hösten 2018 påbörjades ett arbete vid MSB/CERT-SE med att samla in information från drabbade aktörer under pågående nätfiske. Arbetet syftade till att skapa en bättre bild av händelserna, uppmärksamma drabbade organisationer på att deras e-postkonton användes för nätfiske samt bidra till att ta ner infrastrukturen för de falska webbsidorna.

I dialogen med berörda har vidare kartläggning möjliggjorts och flera organisationer har blivit uppmärksammade på dessa intrång i deras it-miljö.

4.1.2 Överbelastningsattacker

Vid så kallade överbelastningsattacker angrips det utsatta systemet på ett sådant sätt att i stort sett samtliga resurser används för att exempelvis hantera ett stort antal anrop till en hemsida, det vill säga själva överbelastningen. Attacken kan utgöras av en enskild dator (DoS – Denial of Service), men ofta deltar ett stort antal tillgängliga datorer på olika geografiska platser för att skapa ett större genomslag på nätverket eller systemet (DDoS – Distributed Denial of Service). Hanteringen av överbelastningen i det senare fallet försvåras av att trafiken inte kan begränsas utifrån att stoppa trafik från enskilda IP-adresser, eftersom det är många som deltar.

Vid en inrapporterad it-incident hade en myndighet fått ett stort antal förfrågningar riktade mot en av sina externa tjänster. Med den stora mängden anrop kunde tjänsten inte levereras under ett antal timmar. CERT-SE var i kontakt med myndigheten och bistod med råd och stöd i hanteringen av incidenten.

MSB/CERT-SE har bistått med råd och stöd vid hantering av överbelastningsattacker under året. Vid denna typ av händelser söker MSB/CERT-SE kontakt med berörda, eftersöker ytterligare information för att få klarhet i det som sker samt bistår drabbade med analys, tekniskt kunnande och samverkan med till exempel nättjänsteleverantörer. Efter en DDoS-attack kan MSB/CERT-SE stödja med analys kring vad som bidrog till angreppet. För detta arbete kan bland annat utdrag från händelseloggar innebära att information kan sammanställas och delges berörda samtidigt som informationen kan bidra till att it-incidenter kan avvärjas och begränsas hos andra.

4.2 Oönskad eller oplanerad störning i kritisk infrastruktur

Gällande *Oönskad eller oplanerad störning i kritisk infrastruktur* förekommer ofta olika varianter på avbrott. Det kan handla om elförsörjning, elektroniska kommunikationer (exempelvis telefoni och internetförbindelser) eller kylsystem. Under året har rapporter inkommit om störningar som haft negativ påverkan på verksamhetskritiska system för bland annat mobiltelefoni, fast telefoni, kylsystem och elförsörjning.

4.2.1 Störningar i telefoni

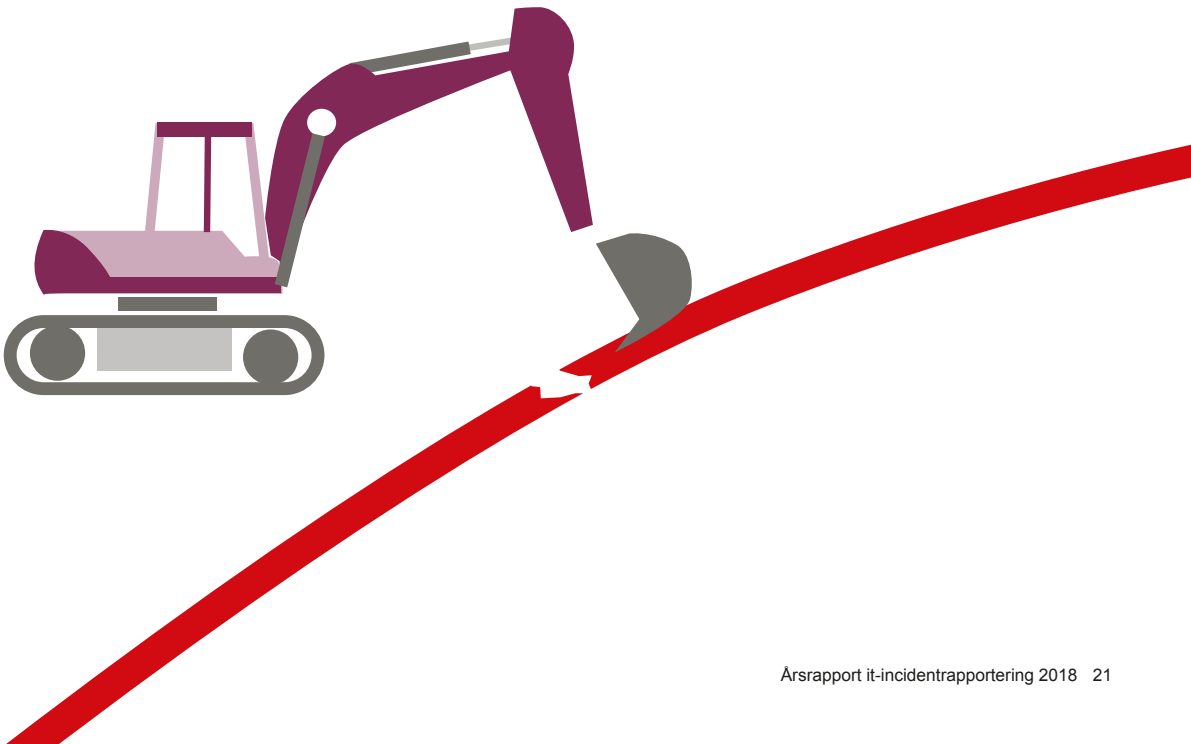
Myndigheter är i hög grad, liksom övriga verksamheter i samhället, beroende av olika elektroniska kommunikationer för att kunna upprätthålla den dagliga verksamheten. Mobilkommunikation och fast telefoni är exempel på detta. Störningar i telefoni kan inträffa till följd av handhavandefel, it-relaterade driftproblem eller genom angrepp och sabotage. Telefoni kan också störas genom avbrott i en operatörs infrastruktur till följd av exempelvis strömavbrott, bortfall av synkroniseringsinformation, avgrävda kablar eller överbelastningsattacker.

Under 2018 fick MSB in en rapport om en incident där myndigheten inte kunde nås via mobiltelefoni till följd av problem hos en operatör. Det gick vare sig att nå myndigheten eller för myndigheten att nå ut under störningen. Incidenten påverkade även möjligheten till tvåfaktorsautentisering via SMS. Myndigheten i fråga bedömde att incidenten haft stor konsekvens för verksamheten.

4.2.2 Störningar i kylning av it-utrustning

Alla verksamheter med it-drift är beroende av kylningskapacitet för sin it-utrustning. Via antingen intern kapacitet eller extern leverans av kyla (exempelvis fjärrkyla) behöver myndigheter kunna upprätthålla kontinuitet i sin kylförmåga. It-utrustning, såsom servrar, nätverksutrustning, switchar etc., kan skadas allvarligt vid överhettning. Om det plötsligt uppstår ett behov av att stänga ner system i syfte att förhindra detta riskerar istället snabbt tillgänglighetsproblem att uppstå i myndighetens informationshantering.

En myndighet rapporterade under året en allvarlig it-incident där kylkapaciteten minskade kraftigt i ett utrymme för it-drift. Otillräcklig reservförmåga att fortsätta kyla utrymmet medförde att myndigheten fick stänga ned utrustning och vidta manuella rutiner för att säkerställa viss kylning. Den senare åtgärden gjorde att ytterligare resurser fick läggas på att upprätthålla hallens fysiska säkerhet.



4.3 Störning i driftmiljö

Störning i driftmiljö omfattar bland annat när it-system av olika anledningar inte fungerar som de ska. Det kan gälla allt från en servermiljö till olika webbtjänster. Ibland kan det vara svårt att avgöra vad som orsakat störningen, vilket innebär att incidenten även kan kategoriseras som störning i mjuk- eller hårdvara.

4.3.1 Omfattande störning i driftmiljö som påverkar flera myndigheter

I de fall myndigheter delar system kan en störning i driftmiljön få spridning till flera myndigheter.

Vid en rapporterad incident drabbades flera system av avbrott och intermittenta fel[18], som drabbade flera myndigheter samtidigt. Det gällde både interna system och system för extern kommunikation och e-tjänster. Problemen uppstod under morgonen och förmiddagen, hade till viss del åtgärdats senare under dagen, och systemen var helt i drift igen vid lunchtid dagen därpå. Enligt incidentrapporten bedömde den rapporterande myndigheten att denna incident resulterat i mycket stora konsekvenser.

4.3.2 Avsaknad av rutiner hos leverantör ger problem med tillgänglighet till system

Vid utkontraktering av it-drift till externa aktörer finns alltid en risk att störningar eller avsaknad av rutiner hos leverantören drabbar verksamheten. Ofta resulterar sådana störningar i problem med tillgänglighet på olika sätt.

Exempelvis hade en myndighet under slutet av en period med lågt utnyttjande problem med just tillgängligheten i sina system. Det visade sig bero på att leverantören av systemen hade minskat resurserna för tjänstens databas till följd av lågt utnyttjande. Leverantören saknade dock övervakning för att notera och åtgärda när behovet av resursutnyttjande ökade igen. Myndigheten kontaktade leverantören vid upprepade tillfällen under två dagar för att leverantören skulle öka åtkomsten igen, vilket slutligen gjordes.

4.4 Handhavandefel

It-incidenter gällande *handhavandefel* handlar oftast om att uppdateringar inte fungerat som det var tänkt på grund av felkonfigurering. Det kan även röra sig om incidenter som uppstått till följd av att personal gjort felaktiga inställningar i system som sedan gör att hela eller delar av systemen inte fungerar som de ska.

4.4.1 Misstänkt angrepp var felkonfiguration

I vissa fall är det svårt att inledningsvis veta vad orsaken till en störning är. Att utreda frågan kan vara påkallat både för att kunna avhjälpa felet, men också för att ta reda på om det handlar om ett medvetet angrepp. Att utreda orsaken ger ett underlag till hur liknande incidenter ska kunna förebyggas i framtiden.

Hos en myndighet uppstod störningar i interna nätverk, vilka även påverkade myndighetens externa tjänster. Problemet upptäcktes då nätverket för både interna och för externa tjänster var instabilt. Därefter påbörjas felsökning direkt.

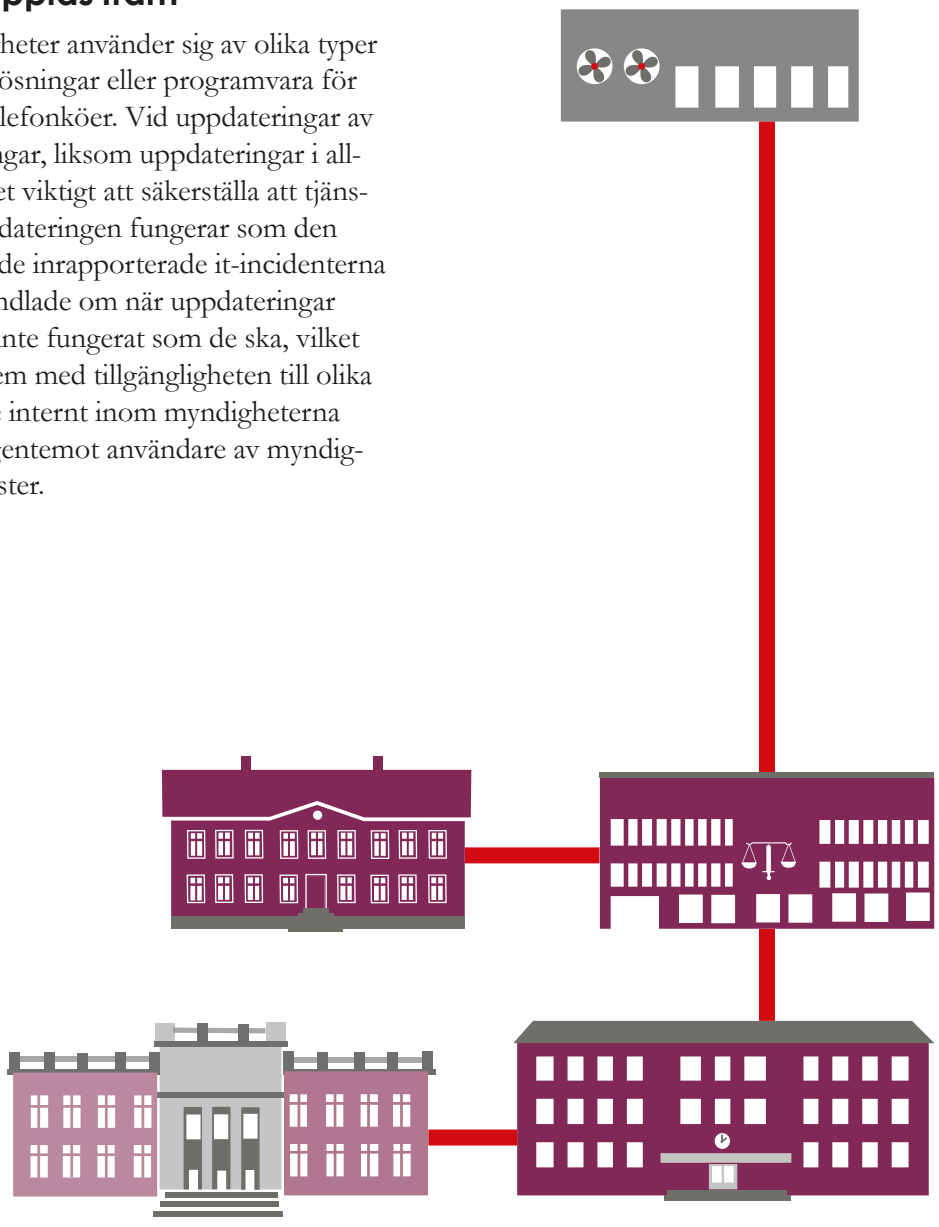
18. Fel som återkommer men inte pågår konstant.

Misstankar föll först mot ett virusangrepp via e-post vilket föranlett behov av ominstallation av en dator kort tid innan instabiliteten i nätverken upptäcktes. Den fortsatta incidenthanteringen visade dock att det första antagandet var felaktigt och orsaken var en felkonfiguration från att myndigheten uppdaterade en infrastrukturkomponent. Myndigheten uppgav i sin it-incidentrapport till MSB att man avsåg att utreda orsaken för felkonfigurationen.

4.4.2 Säkerhetsuppdatering ledde till att telefonsamtal inte kunde kopplas fram

Flera myndigheter använder sig av olika typer av callcenterlösningar eller programvara för att hantera telefonköer. Vid uppdateringar av sådana lösningar, liksom uppdateringar i allmänhet, är det viktigt att säkerställa att tjänsten efter uppdateringen fungerar som den ska. Flera av de inrapporterade it-incidenterna från 2018 handlade om när uppdateringar av olika skäl inte fungerat som de ska, vilket lett till problem med tillgängligheten till olika tjänster, både internt inom myndigheterna och externt gentemot användare av myndigheternas tjänster.

I samband med en säkerhetsuppdatering av en myndighets callcenterlösning upptäcktes att inga samtal kom fram. Samtalen fastnade i systemets köhantering och reservlösningar fungerade inte. Avbrottet varade i en halvtimme innan myndigheten lyckades lösa problemet. Efter incidenten har myndigheten uppdaterat sina rutiner för att säkerställa att samtliga nödvändiga tjänster i callcenterlösningen är aktiva efter uppdateringar eller omstarter.



Slutsatser, krav och rekommendationer

5. Slutsatser, krav och rekommendationer

Nedan följer MSB:s slutsatser utifrån 2018 års it-incidentrapportering från statliga myndigheter. I anslutning till slutsatserna återges ett urval av regleringen i MSB:s föreskrifter för statliga myndigheters informationssäkerhet (MSBFS 2016:1) samt MSB:s föreskrifter för statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2). Detta för att öka tydligheten om vad MSB har föreskrivit och vad som är relevant för varje slutsats som dragits.

Myndigheternas ledningar ska snarast säkerställa att myndigheten fullt ut följer MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2016:1) samt MSB:s föreskrifter om statliga myndigheters rapportering av it-incidenter (MSBFS 2016:2).

5.1 Fler kan rapportera mer

MSB bedömer att det är för få myndigheter som rapporterar allvarliga it-incidenter och att antalet rapporterade incidenter borde vara fler.

MSB kan konstatera att fler myndigheter har rapporterat it-incidenter under 2018 än tidigare år, oaktat de nya rapporteringspliktiga myndigheter som tillkommit för 2018.

Av de myndigheter som har rapporterat lämnade en tredjedel endast en rapport under hela 2018.

Av de rapporter som inkommit är det en stor andel som lämnats mer än en vecka efter att incidenten har upptäckts, givet det datum för upptäckt som myndigheterna angett i sina rapporter till MSB. MSB bedömer att fler it-incidenter hos statliga myndigheter borde betraktas som allvarliga och därmed rapporteras. Denna bedömning grundar sig bland annat på de it-incidentrapporter som inkommit och den vidare omvärldsbevakningen hos MSB. Bedömningen av vilka incidenter som är att betrakta som allvarliga och därmed rapporteringsskyldiga görs av varje enskild myndighet. Detta medför att dessa bedömningar görs på olika sätt hos olika myndigheter. För att påverka rapporteringen krävs därför bland annat en ändring av MSB:s föreskrifter för att förtydliga vad som är att betrakta som allvarlig it-incident.

Varje myndighet ska rapportera en it-incident senast 24 timmar efter det att myndigheten upptäckt den rapporteringspliktiga incidenten. (MSBFS 2016:2, § 4)

I de fall en myndighet anlitar en annan myndighet för att fullgöra uppgifter som regleras i denna författning ska de berörda myndigheterna tydligt dokumentera sitt samarbete. Det ska i dokumentationen tydliggöras vilken myndighet som är ansvarig för att uppfylla kraven som ställs i denna författning. (MSBFS 2016:1, § 3)

MSB har svårt att bedöma omfattningen på mörkertalet när det gäller it-incidenter som aldrig upptäcks och av den anledningen inte rapporteras. De incidenter som är enkla att upptäcka gäller framför allt problem med tillgänglighet, då det ofta innebär svårigheter att nå myndigheternas information och möjligheten att arbeta påverkas. Att upptäcka problem med riktighet[19] eller konfidentialitet[20] är ofta svårare, vilket också avspeglas i myndigheternas rapportering där hindrad tillgång till information förekommer betydligt oftare i incidentrapporterna än förlust, läckage eller förvanskning av information.

Flera myndigheter har sin it-drift utlokaliserad till någon annan myndighet eller en privat aktör. Detta fråntar dem inte ansvaret att rapportera allvarliga it-incidenter som drabbar den egna verksamheten.[21]

Vid utlokalisering krävs nödvändig kompetens för att hantera informationssäkerhetsaspekter vid upprättandet och i uppföljningen av avtal och överenskommelser. MSB tillhandahåller en vägledning för hur myndigheter kan inkludera krav på informations- och cybersäkerhet i upphandlingar av exempelvis it-drift.[22]

MSB vill särskilt påtala att myndigheter enligt 2 kap. 6 § säkerhetsskyddslagen (2018:585) ska använda säkerhetsskyddad upphandling med säkerhetsskyddsavtal (SUA) när det i upphandlingen förekommer säkerhetsskyddsklassificerade uppgifter i klassen konfidentiell eller högre.

Det samma gäller när myndigheter ger leverantören tillgång till säkerhetskänslig verksamhet av motsvarande betydelse. I vissa fall krävs samråd med Säkerhetspolisen.

19. Såsom att konfigurationer har lagts till, ändrats, tagits bort eller gjorts otillförlitliga i it-system, eller att informationsmängder har gjorts otillförlitliga (exempelvis för att det inte går att utröna när, hur eller av vem de har ändrats) eller manipulerats så att information har lagts till, ändrats eller tagits bort.

20. Såsom att behöriga användare har fått för höga behörigheter till system eller nätverk, att tillgång för obehöriga användare kan eller har upprättats till system eller nätverk, eller att obehöriga användare kan konfigurera system eller nätverk, eller att få system eller nätverk att utföra uppgifter.

21. Undantag från detta finns om myndigheten har avtal om it-drift som trätt i kraft innan nuvarande föreskrifter kommit på plats, om ingått avtal inte reglerat detta.

22. *MSB, Upphandla informationssäkert: en vägledning,* 2018, länk: https://www.msb.se/RibData/Filer/pdf/28742.pdf (hämtad 2019-01-09)

5.2 Rapportering kräver ett systematiskt och riskbaserat arbetssätt

Baserat på rapporteringen av allvarliga it-incidenter kan MSB konstatera att många myndigheter inte följer MSB:s föreskrifter om ett systematiskt och riskbaserat arbetssätt gällande informationssäkerhet. Detta gäller såväl utifrån antalet rapporterande myndigheter, antalet incidenter och beskrivningen av incidenternas orsaker och konsekvenser.

> *Varje myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. (MSBFS 2016:1, § 5)*
>
> *Myndigheten ska ha rutiner för att identifiera, rapportera, bedöma, hantera och dokumentera incidenter som kan påverka säkerheten i den informationshantering som myndigheten ansvarar för eller i tjänster som myndigheten tillhandahåller åt en annan organisation. Myndigheten ska ha rutiner för att lära av sådana inträffade incidenter och utförda åtgärder. (MSBFS 2016:1, § 10)*

För att förebygga, såväl som att upptäcka och hantera, incidenter krävs ett systematiskt och riskbaserat arbetssätt. Detta är också en förutsättning för en fungerande incidentrapportering.

Utifrån arbetet med att analysera och bedöma bevakningsansvariga myndigheters informationssäkerhet[23] har MSB sedan tidigare konstaterat att få bevakningsansvariga myndigheter följer MSB:s föreskrifter till fullo. Incidentrapporteringen från statliga myndigheter indikerar att även övriga myndigheter har brister i sitt systematiska och riskbaserade informationssäkerhetsarbete.

Stöldskyddsföreningen har tillsammans med bland annat MSB tagit fram en norm för cybersäkerhet.[24] Normen innehåller en rad krav på grundläggande it-säkerhet. Normen utgör en basnivå för främst små och medelstora företag och ligger under den nivå som MSB föreskriver att statliga myndigheter ska upprätthålla genom systematiskt och riskbaserat informationssäkerhetsarbete. MSB anser att flera myndigheter inte ens når upp till basnivån i Stöldskyddsföreningens norm.

För att få en fungerande incidenthantering behöver myndigheterna säkerställa en fungerande incidenthanteringsprocess. En fungerande incidenthantering förutsätter att medarbetarna vet när och var de ska anmäla problem, att de som mottar incidentanmälan kan göra korrekta bedömningar av konsekvensen för organisationen och att åtgärder vidtas för att återställa och återgå till normal drift. Som vägledning i arbetet finns stöd att få via Informationssäkerhet.se och MSB:s metodstöd. Stödet utvecklas kontinuerligt.

23. *Bevakningsansvariga myndigheters informations- och cybersäkerhet,* dnr MSB2017-07165. Rapporten utgjorde svar på regeringsuppdrag Ju2017/05787/SSK där MSB hade i uppgift att sammanställa och analysera redovisningar från de bevakningsansvariga myndigheterna utifrån ett regeringsuppdrag gällande deras egen informationssäkerhet.

24. *SSF, Norm avseende cybersäkerhet,* SSF 1101 utgåva 1, september 2018

I en fungerande incidenthanteringsprocess ingår att händelser i nätverk och it-system, inklusive cyberfysiska system såsom till exempel fastighetsautomation, loggas för att det ska gå att spåra var ändringar har skett samt vilken information obehöriga har fått tillgång till. För detta krävs även kompetens och avsatta resurser för att följa upp och analysera loggarna.

5.3 Medvetenheten om hotbilden behöver öka och skyddet anpassas

De statliga myndigheternas medvetenhet har ökat, men de måste mer aktivt integrera säkerhetsperspektivet i digitaliseringsprocesserna. Arbetet med informations- och cybersäkerhet måste genomsyra hela myndighetens arbete, inte enbart hanteras av it- eller säkerhetsavdelningar.

Genom ledningssystemet ska myndigheten

1. tydliggöra myndighetsledningens och den övriga organisationens ansvar för myndighetens informationssäkerhetsarbete,

2. tilldela nödvändiga befogenheter för de roller som arbetet med informationssäkerhet kräver, detta gäller särskilt för den eller de som ska utses för att leda och samordna arbetet. (MSBFS 2016:1, § 6)

Myndigheten ska eftersträva en god säkerhetskultur där alla i organisationen har kunskap om och förståelse för behoven av säker informationshantering, genom att

1. informera medarbetare om krav på säker informationshantering och relevanta regler inom området,

2. regelbundet, och enligt en beslutad utbildningsplan, genomföra utbildningar rörande informationssäkerhet som är anpassade till medarbetarnas uppgifter. (MSBFS 2016:1, § 8)

Dagens myndigheter är, liksom samhället i övrigt, beroende av fungerande tekniska system för att kunna utföra sina uppgifter. En ökad digitalisering medför att behovet av säkra it- och cyberfysiska system ökar än mer. Medvetenheten och förståelsen för detta släpar dock efter, och därmed även skyddet. Digitaliseringen av samhället har kommit långt och kommer under de närmsta åren att omdana fler verksamheter och funktioner i den offentliga sektorn. I takt med denna utveckling riskerar allvarliga it-incidenter att få allt större konsekvenser för medborgarnas förtroende för digitaliseringsprocessen och de myndigheter som genomför den.

Säkerhetspolisen har påtalat det växande gapet mellan hot och säkerhet, där myndigheter och företag med skyddsvärd verksamhet har brister i sin informationssäkerhet och därmed, i kombination med otillräckliga säkerhetsskyddsåtgärder, är sårbara.[25] Många organisationer har enligt MSB:s bedömning bristande kontroll över vilken information de har, vilket värde den har och var den finns.

MSB kan konstatera utifrån myndigheternas it-incidentrapportering att statliga myndigheter har ett stort arbete kvar att göra gällande säkra tekniska lösningar och arbetet med att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. MSB ser positivt på att fler myndigheter nu rapporterar it-incidenter, något som kan indikera att medvetenheten ökar. Även FRA har i sin årsrapport för 2018 rapporterat om en väsentligt ökad medvetenhet hos svenska myndigheter och statliga bolag om risken för it-angrepp och vikten av informationssäkerhetsfrågor.[26]

25. Säkerhetspolisen, *Årsbok 2018,* https://sakerhetspolisen.se/download/18.6af3d1c916687131f1fae5/1552543607309/Arsbok-2018.pdf hämtad 2019-03-15.

26. FRA (2018), *Årsrapport 2018,* https://fra.se/download/18.69cf97cd167832fc038250/1548773731405/FRA-arsrapport-2018.pdf

Andelen allvarliga it-incidenter som har rapporterats från statliga myndigheter till MSB under 2018 som beror på den mänskliga faktorn är relativt hög. Handhavandefelen är många och därutöver skulle flera av angreppen ha kunnat undvikas, alternativt inte fått lika omfattande konsekvenser, om individer haft en större medvetenhet om informationssäkerhet och säkerhetsrutiner. Genom att höja kompetensen och bygga en god säkerhetskultur på myndigheterna kan informationssäkerheten också förbättras.

För att stärka informations- och cybersäkerheten vid statliga myndigheter behöver respektive myndighetsledning ta ansvar för, och bidra till, en ökad medvetenhet kring dessa frågor. Säkerhetsarbetet måste ske systematiskt, baserat på analyser som ger kunskap om informationens värde och risker förknippande med hanteringen. Resurser måste tillföras för att resultatet från analyserna ska kunna omsättas i åtgärder. Vid digitaliseringsprocesser behöver det systematiska informationssäkerhetsarbetet tillföras de resurser som krävs för att detta arbete ska bedrivas tillräckligt väl.

MSB uppmanar skyndsamt, enligt krav i 20 § förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, statliga myndigheter att polisanmäla it-incidenter som har sin grund i en brottslig gärning, såsom bedrägerier och intrång. I de fall det inträffat en it-incident i ett informationssystem som verksamhetsutövaren är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet ska detta skyndsamt rapporteras till Säkerhetspolisen. Om verksamhetsutövaren tillhör Försvarsmaktens tillsynsområde ska anmälan också göras till Försvarsmakten.[27]

5.4 Kontinuitetshantering och övning gör stor skillnad

Myndigheterna är beroende av tjänster via externa system och infrastruktur och måste i förväg veta hur de ska agera vid störningar i dessa tjänster. För att upprätthålla en god informations- och cybersäkerhet är regelbunden övning och arbete med kontinuitetshantering en nödvändighet.

Myndigheten ska ha rutiner för kontinuitetshantering som tydliggör hur verksamhetens informationshantering upprätthålls vid större störningar och avbrott. Förhållanden som kan uppstå i samband med fredstida kriser och under höjd beredskap ska beaktas. (MSBFS 2016:1, § 11)

Myndigheten ska eftersträva en god säkerhetskultur där alla i organisationen har kunskap om och förståelse för behoven av säker informationshantering, genom att regelbundet, och enligt en beslutad övningsplan, genomföra övningar för att pröva och utveckla myndighetens säkerhetsåtgärder för kontinuitetshantering avseende informationssäkerhet. (MSBFS 2016:1, § 8)

Årets it-incidentrapportering visar på fortsatt stort behov av att reducera konsekvenserna av oönskade eller oplanerade störningar i it-miljöer och då främst i kritisk infrastruktur. Det gäller exempelvis kylningen av datahallar där sommarens värmebölja gjorde att otillräcklig eller utebliven kylning snabbt kunde bli ett kritiskt problem för att upprätthålla it-drift och därmed tillgång till information.

27. 2 kap 10 § säkerhetsskyddsförordningen (2018:658). Före 1 april 2018 fanns en motsvarande bestämmelse i 10 a § säkerhetsskyddsförordningen (1996:633).

Kontinuitetshantering och -planering handlar om att skapa en förmåga att fortsätta bedriva sin verksamhet på en acceptabel nivå oavsett vilken typ av störning som organisationen utsätts för. I vissa fall kan detta innebära att mindre prioriterade delar av verksamheten måste stängas ner på ett kontrollerat sätt. Kontinuitetshantering kräver att alla aspekter inom kontinuitet hanteras – från att analysera hur olika grupper påverkas om olika verksamheter inte fungerar normalt, via incidenthantering till krishantering. Det är upp till den egna organisationen att planera på ett sådant sätt att störningar i verksamheten och kritisk infrastruktur kan hanteras så att den verksamhet som måste fungera fungerar.

Vid den här typen av planering är det viktigt att beakta totalförsvarsperspektivet. Situationen vid höjd beredskap skiljer sig mycket från normalläget och detta påverkar både hotbild och sårbarheter då andra hot behöver hanteras och situationer som organisationen klarar av i normalläget kan bli svårare eller omöjliga att hantera.

En vägledning för kontinuitetshantering och -planering har getts ut av Standardiseringsinstitutet (SIS). MSB bekostar standarden för offentliga och privata aktörer som bedriver samhällsviktig verksamhet, och som finns att hämta via SIS hemsida.[28] MSB tillhandahåller även en vägledning för upphandling till samhällsviktig verksamhet.[29]

Särskilt om kylning av datahallar

MSB tillhandahåller en vägledning för den fysiska informationssäkerheten i förvaring och användning av it-utrustningar.[30] I kapitel 2 i vägledningen ges särskilt stöd i arbetet med att säkra kylningen av datahallar. Generellt behöver myndigheter och andra aktörer ha teknisk övervakning och larm på plats för att kunna upptäcka störningar i kylningen av it-utrustning samt reservkapacitet om det sker avbrott i de primära systemen.

Särskilt om robust telekommunikation

MSB har gett ut en vägledning för säker och robust samverkan, vars syfte är att stödja organisationer som ska identifiera vilka verktyg som ska användas för säker och robust samverkan utifrån organisationers respektive behov. Vägledningen är inriktad på de verktyg som MSB tillhandahåller, exempelvis Rakel, SGSI och WIS.[31] Post- och telestyrelsen, PTS, har gett ut en vägledning för anskaffning av robust elektronisk kommunikation för användare.[32] Vägledningen kommer uppdateras utifrån ett arbete med att ta fram stöd för anskaffning av robust elektronisk kommunikation som aviserats i den samlade informations- och cybersäkerhetshandlingsplanen för åren 2019-2022.[33] PTS arbete fokuserar på kommersiella lösningar .

28. *SiS, Vägledning för kontinuitetshantering,* SS 22304:2014, länk: https://www.sis.se/MSB_bekostar_standarden_kontinuitetshantering (hämtad 2019-01-09)

29. *MSB, Upphandling till samhällsviktig verksamhet – en vägledning,* 2018, länk: https://www.msb.se/RibData/Filer/pdf/28720.pdf (hämtad 2019-01-10)

30. *MSB, Vägledning för fysisk informationssäkerhet i it-utrymmen,* 2013, länk: https://www.msb.se/RibData/Filer/pdf/27280.pdf (hämtad 2019-01-09) – se särskilt avsnitt 2.5 och 2.9

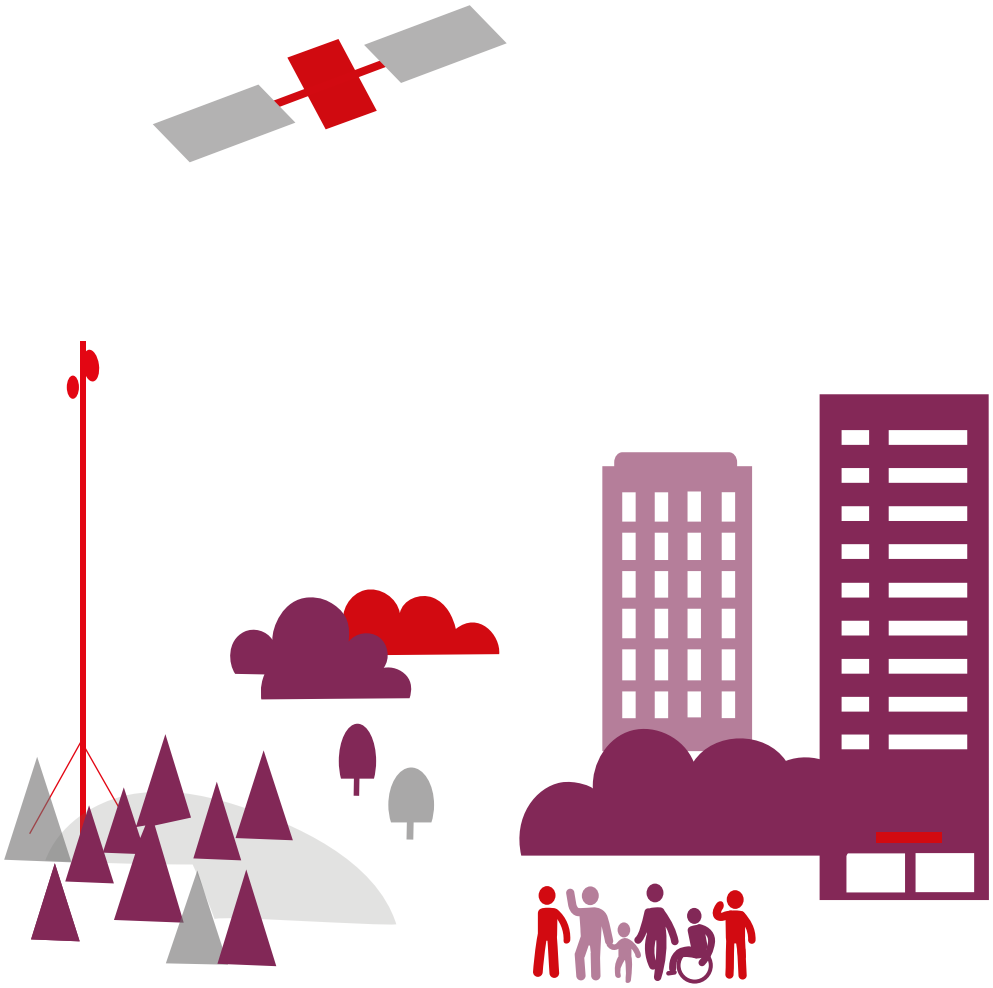
31. *MSB, Vägledning för säker och robust samverkan,* MSB1285 - november 2018, länk: https://www.msb.se/RibData/Filer/pdf/28747.pdf (hämtad 2019-03-28)

32. *PTS, Robust elektronisk kommunikation - vägledning för användare vid anskaffning,* 2011 https://www.pts.se/globalassets/startpage/dokument/icke-legala-dokument/rapporter/2011/internet/rapport--pts--vagledning-for--anskaffning-av-robust-elektronisk-kommunikation.pdf 2-19

33. *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019-2022,* MSB, FRA, FMV, Försvarsmakten, PTS, Polismyndigheten och Säkerhetspolisen, MSB1351 – mars 2019.

I februari 2018 genomförde MSB den nationella informationssäkerhetsövningen NISÖ 2018. Övningen syftade till att stärka samhällets förmåga att hantera nationella it-relaterade kriser, främst genom att utveckla förmågan till samarbete och samordning mellan privata och offentliga aktörer inom utpekade sektorer. Utvärderingen av övningen pekade på två övergripande utvecklingsområden – samverkan och systemförståelse, samt informationsdelning och lägesbild.[34]

Vid större kriser behöver olika organisationer kunna arbeta tillsammans, ofta under stor tidspress. En aspekt i detta arbete blir att kunna säkerställa kontinuitet i den egna förmågan att kommunicera med omvärlden. Att då ha övat sin organisation internt är en förutsättning för en god krishantering.



34. *MSB, NISÖ 2018 – Erfarenhetsrapport,* MSB1326 - december 2018

MSB:s åtgärder

6. MSB:s åtgärder

Under 2019 kommer MSB att skärpa kraven på och öka stödet till statliga myndigheter i syfte att förbättra informations- och cybersäkerheten hos statliga myndigheter. MSB arbetar med att revidera och förtydliga kraven på rapportering av it-incidenter som allvarligt kan påverka säkerheten i myndigheternas informationshantering. Det utökade stödet till myndigheterna innefattar bland annat utökad återkoppling och ett nytt metodstöd. MSB kommer även att fördjupa samarbetet med centrala aktörer.

Syftet med it-incidentrapporteringen för statliga myndigheter är att stödja arbetet med samhällets informations- och cybersäkerhet. Rapporteringen är tänkt att bidra till MSB:s övergripande lägesbild av vilka it-incidenter som inträffar, när de sker och vilka orsaker de har, samt vilka konsekvenser de får. En väl fungerande it-incidentrapportering skulle avsevärt förbättra MSB:s möjligheter att stötta och stödja myndigheterna. Dels kan MSB:s förmåga att stödja myndigheterna i det operativa arbetet med it-incidenter stärkas. Resultatet av en väl fungerande it-incidentrapportering stärker även MSB:s förmåga att stötta myndigheterna i det förebyggande arbetet.

Nedan redovisar MSB ett urval av de pågående och planerade åtgärder som syftar till att stödja statliga myndigheters arbete med informations- och cybersäkerhet, inklusive it-incidentrapporteringen. Åtgärderna är även tänkta att stödja och stärka andra aktörers arbete med dessa frågor och därmed samhällets informations- och cybersäkerhet i stort. Under varje del finns också en kort beskrivning av ett urval av åtgärder från den samlade informations- och cybersäkerhetshandlingsplan för åren 2019-2022 som presenterades den 1 mars 2019.[35] De deltagande myndigheterna i Samverkansgruppen för informationssäkerhet (SAMFI)[36] har sedan hösten 2018 särskilt samarbetat kring ett regeringsuppdrag för att ta fram denna handlingsplan.

6.1 Nya och skärpta krav på statliga myndigheter – MSB reviderar och kompletterar nuvarande föreskrifter

MSB kommer att öka kraven på myndigheternas it-incidentrapportering genom förändringar i flera regelverk. Föreskrifterna för statliga myndigheters it-incidentrapportering (MSBFS 2016:2) skärps ytterligare avseende krav på vad som ska rapporteras och när.

35. *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019-2022,* MSB, FRA, FMV, Försvarsmakten, PTS, Polismyndigheten och Säkerhetspolisen, MSB1351 – mars 2019.

36. I SAMFI ingår Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Polisen, Post- och telestyrelsen, Säkerhetspolisen och MSB.

Dessutom kommer föreskrifterna justeras för att förbättra förutsättningarna för MSB att stödja vid hanteringen av it-incidenter. Föreskrifterna kommer att träda i kraft den 1 januari 2020.

MSB kommer även att skärpa kraven på myndigheternas informationssäkerhetsarbete. I detta ingår en tydligare kravställning på myndigheternas interna incidenthanteringsprocess genom nya föreskrifter om säkerhetsåtgärder samt revidering av nuvarande föreskrifter om systematiskt och riskbaserat informationssäkerhetsarbete (MSBFS 2016:1).

Där så är lämpligt kommer en harmonisering ske med MSB:s föreskrifter kopplade till lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen).

Åtgärderna finns även beskrivna under punkten *1.1.8. Revidering och komplettering av MSB:s föreskrifter för statliga myndigheter* i den samlade informations- och cybersäkerhetshandlingsplanen för 2019-2020.

6.2 MSB kommer arbeta mer riktat med återkoppling till statliga myndigheter gällande deras informationssäkerhetsarbete, inklusive it-incidentrapportering

Återkoppling pågår redan idag utifrån MSB:s sammanställning och analys från 2018 av bevakningsansvariga myndigheters informationssäkerhet. Bland annat har MSB:s generaldirektör påbörjat en turné för att träffa bevakningsansvariga myndigheter. Turnén kommer fortsätta under 2019. MSB har även inlett en närmare dialog med Länsstyrelsen i Västra Götalands län gällande länsstyrelsernas rapportering.

Återkoppling till myndigheterna gällande inlämnade it-incidentrapporter sker dels månatligen, dels i samband med funktionen CERT-SE:s operativa arbete där incidentdrabbad myndighet får stöd i de fall det finns behov av det.

MSB kommer under 2019 att i större utsträckning arbeta med återkoppling till myndigheterna för att ytterligare förbättra informations- och cybersäkerheten i den statliga sektorn. Återkopplingen behandlas separat från årsrapporten och kommer att pågå i olika former under 2019, i syfte att etablera och upprätthålla en mer kontinuerlig dialog med myndigheterna om deras systematiska informationssäkerhetsarbete och it-incidentrapportering.

6.3 MSB utvecklar nytt metodstöd och tar fram koncept för grundläggande säkerhetsåtgärder

MSB har under 2018 nylanserat metodstödet som ges via Informationssäkerhet.se. Metodstödet riktar sig till såväl myndigheter som andra aktörer, och baseras på SS-EN ISO/IEC 27 001 och 27002, en internationell standard för arbetet med informationssäkerhet. Stödet utvecklas löpande. Metodstödet kommer fortsätta att utvecklas under de närmaste åren, bland annat gällande metoder för att klassa information med koppling till säkerhetsåtgärder, riskanalys och incidenthantering, i enlighet med åtgärd *1.1.11. Utveckla MSB:s metodstöd för systematiskt informationssäkerhetsarbete* i den samlade informations- och cybersäkerhetshandlingsplanen för 2019-2020.

Med hänsyn till de brister som idag finns i flera aktörers systematiska och riskbaserade informationssäkerhetsarbete behövs ytterligare stöd. Ett sådant stöd kan exempelvis ges i form av att ytterligare tydliggöra säkerhetsåtgärder som måste genomföras. Både kommande arbete med reviderade och kompletterade föreskrifter enligt ovan och framtaget stöd i form av koncept för grundläggande informations- och it-säkerhetsåtgärder planeras under 2019 och 2020. Det senare i enlighet med åtgärd *1.1.12 Ta fram koncept för grundläggande säkerhetsåtgärder för informationssäkerhet* i den samlade informations- och cybersäkerhetshandlingsplanen för 2019–2020.

MSB kommer också under 2019-2020 tillsammans med berörda aktörer genomföra en nationell satsning på ökad säkerhet i cyber-fysiska system för att stärka samhällets samlade förmåga att förebygga och hantera såväl brister som felaktigheter som it-angrepp i sådan samhällsfunktionalitet som är beroende av industriella informations- och styrsystem (ICS), i enlighet med åtgärd *2.5.3. Genomföra en nationell satsning på ökad säkerhet i cyberfysiska system* i den samlade informations- och cybersäkerhetshandlingsplanen för 2019–2020.

6.4 MSB ställer krav på it-incidentrapportering från leverantörer av samhällsviktiga och digitala tjänster – ger ökad kunskap och erfarenhet

I och med NIS-regleringen[37] ska leverantörer av samhällsviktiga och digitala tjänster, från och med 1 mars 2019, rapportera it-incidenter till MSB. MSB har etablerat tekniskt stöd och utvecklat nya processer för incidentrapportering. En prioriterad uppgift har varit att säkerställa hög kvalitet på informationen i it- incidentrapporterna. Arbetet bidrar till att underlätta återkoppling och aggregerad analys. Erfarenheterna kommer att användas i utvecklingen av de statliga myndigheternas it-incidentrapportering.

Rapporteringen utifrån NIS-regleringen kommer att bredda, fördjupa och utveckla lägesbilden för svensk informations- och cybersäkerhet. Den nya lägesbilden kommer ge MSB bättre förutsättningar att stödja vid hanteringen av it-incidenter. Den samlade kunskapen kan även ligga till grund för förbättringen av råd i det förbyggande arbetet, mer preciserade åtgärder och förbättrad tillsyn inom bland annat NIS-området. MSB är nationell kontaktpunkt och nationell CSIRT-enhet utifrån NIS-regleringen. I dessa roller deltar MSB även fortsättningsvis i EU-samarbetet för att harmonisera genomförandet av NIS-direktivet samt gällande incidenthantering, i enlighet med åtgärd *6.2.2. Fortsätta delta i samarbetsgruppen och CSIRT-nätverket inom ramen för NIS-direktivets genomförande och tillämpning* i den samlade informations- och cybersäkerhetshandlingsplanen för 2019–2020.

6.5 Fortsatt utveckling av samarbetet med andra aktörer

Arbetet med den samlade informations- och cybersäkerhetshandlingsplanen har utgjort en möjlighet till utveckling av existerande samverkan mellan de deltagande myndigheterna. Handlingsplanen är också ett instrument för fortsatt fördjupad samverkan.

I den samlade informations- och cybersäkerhetshandlingsplanen för åren 2019-2022 finns ett antal åtgärder listade som syftar till ökat samarbete mellan myndigheter, liksom med andra aktörer. Några av de viktigaste som berör statliga myndigheter är fördjupat samarbete mellan FRA, Säkerhetspolisen, Försvarsmakten och MSB (åtgärd 1.3.4.), skapa förutsättningar för samverkan inom

37. Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

ramen för MSB:s CSIRT-verksamhet (åtgärd 3.1.5.), etablera ett samarbetsforum för olika myndigheters incidenthanteringsfunktioner (åtgärd 3.2.3.) och stärkt samarbete vid incidentrapportering rörande brottslig verksamhet (åtgärd 4.1.1.). Därutöver ska ett antal övningar genomföras, bland annat delmoment i Totalförsvarsövning 2020 (TFÖ 2020) och NISÖ 2021 (åtgärd 5.4.1. – 5.4.4.).

MSB kommer att ha fortsatt dialog med Polismyndigheten gällande antalet rapporterade allvarliga it-incidenter som polisanmäls. MSB kommer också tillsammans med de andra cybersäkerhetsmyndigheterna, inklusive Polismyndigheten, under 2019 genomföra arbete för att utveckla operativ samverkan och informationsdelning sinsemellan samt även påbörja arbetet med att skapa förutsättningar för en samordnad hantering mellan berörda myndigheter vid allvarliga it-relaterade kriser.

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB1334 – April 2019 ISBN 978-91-7383-907-5