Myndigheten för samhällsskydd och beredskap

EU förändrar cybersäkerhetsområdet

Årsrapport it-incidentrapportering 2023

EU förändrar cybersäkerhetsområdet – Årsrapport it-incidentrapportering 2023

Foto omslag: Adobe Stock
Foto: Melker Dahlstrand sida 3, Adobe Stock sida 8–56
Tryck: By Wind AB
Produktion: Advant

Publikationsnummer: MSB2341 – mars 2024
ISBN: 978-91-7927-494-8

Förord

Vi står inför händelserika år inom informations- och cybersäkerhetsområdet. Nya EU-regleringar kommer att ställa högre krav på hur berörda organisationer arbetar med informations- och cybersäkerhet. Kraven kommer i rätt tidpunkt. Under 2023 ökade antalet rapporterade cyberangreppsförsök mot statliga myndigheter kraftigt. Bilden av många angrepp står i kontrast till tidigare år, då systemfel och misstag var de vanligaste orsakerna till rapporterade it-incidenter. Som ni vet befinner vi oss i ett försämrat säkerhetspolitiskt läge och det syns nu på allt fler områden. Därför är det viktigt att säkerställa motståndskraften i våra samhällsviktiga informationssystem.

Årsrapporten har sin grund i den it-incidentrapportering MSB mottar från både statliga myndigheter och från leverantörer av samhällsviktiga och digitala tjänster. I likhet med tidigare år har vi ett tema som har präglat MSB:s arbete. Vi fördjupar oss i EU:s växande roll med anledning av erfarenheter från det svenska ordförandeskapet i det Europeiska rådet, och med anledning av den stora mängd nya EU-regleringar som är på väg. Regleringar som stärker området samtidigt som högre krav kommer att ställas på de organisationer som berörs. Genom samordning av krav och funktioner i regleringarna ges organisationer bästa möjliga förutsättningar. Samtidigt behöver organisationer tillsätta resurser i ett tidigt skede för en lyckad implementering.

Närmare hälften av alla it-incidenter som rapporterats har skett hos en leverantör, vilket föranleder en kartläggning av problem i digitala leveranskedjor inom beredskapsområdena. Rapportens slutsatser och rekommendationer handlar även om hur det förebyggande säkerhetsarbetet hos organisationer ska stärkas.

Slutligen, vill jag framhäva att det bästa sättet att förebygga it-incidenter är att arbeta systematiskt och riskbaserat med helheten utifrån allriskperspektivet. Min förhoppning är att denna rapport inte bara informerar utan även inspirerar till ökade studier för ett proaktivt arbete med skydd för att förebygga it-incidenter, säkerställa efterlevnad av regleringar inom området och på så vis bidra till samhällets motståndskraft.

Stockholm, 2024-03-14

Åke Holmgren

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

Innehåll

Begreppsförteckning

I detta kapitel förklaras rapportens centrala begrepp och akronymer.

Allriskperspektiv: Att sträva efter att bedöma alla typer av risker för något som ska skyddas och att analysera alla möjliga orsaker till att en risk realiseras.

Aktörsgrupp: En grupp aktörer med gemensamma karaktärsdrag eller ansvarsområden. Centrala aktörsgrupper för denna rapport är statliga myndigheter och NIS-leverantörer.

CERT: En förkortning för ”Computer Emergency Response Team”. En funktion med uppgift att stödja samhället i arbetet med att hantera och förebygga it-relaterade incidenter.

CSIRT: En förkortning för ”Computer Security Incident Response Teams”. CSIRT-nätverket, som etablerades genom NIS-direktivet (EU) 2016/1148, är ett nätverk av nationellt utpekade CERT-funktioner för hantering av it-säkerhetsincidenter. MSB/CERT-SE vid MSB är Sveriges nationella CSIRT.

Cyberangrepp: En interaktion mellan en angripare och ett mål som I) angriparen inte har rätt att utföra mot målet, ii) medför ett utbyte av information som resulterar i en interaktion, konfigurering, installation/sparande, avinstallation/raderande eller överbelastning i något av målets informationssystem, iii) resulterar i minst en för målet oönskad konsekvens i termer av konfidentialitet riktighet eller tillgänglighet för målet eller för andra via målet och vi) som angriparen utför i ett antagonistiskt syfte.

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

ECCC: En förkortning för “European Cybersecurity Competence Centre”. EU:s kompetenscentrum för cybersäkerhet vars uppdrag är att främja europeisk innovation och industripolitik inom informations- och cybersäkerhetsområdet.

ENISA: En förkortning för “European Union Agency for Network and Information Security”. Europeiska unionens byrå för nät- och informationssäkerhet.

Entitet: En fysisk eller juridisk person som bildats och erkänts som sådan enligt nationell rätt där den etablerats och som i eget namn får utöva rättigheter och ha skyldigheter. Begreppet används i flera EU-regleringar.

EU-CyCLONe: En förkortning för ”the European Cyber Crisis Liaison Organisation Network”. Nätverket ska stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser på operativ nivå och säkerställa ett regelbundet utbyte av relevant information mellan medlemsstaterna och unionens institutioner, organ och byråer. Inrättades genom direktiv (EU) 2022/2555, NIS2-direktivet.

IKT-leverantör: En organisation som levererar informations- och kommunikationsrelaterade tjänster.

Incident: En inträffad oönskad händelse. Vid incidentrapportering delas orsak in enligt mänskliga hot (både antagonistiska hot i form av angrepp och icke-antagonistiska hot i form av misstag), tekniska hot (i form av systemfel) eller naturhot (såsom väderfenomen, jordbävningar et cetera).

Informationssystem: System för att samla in, lagra, bearbeta och distribuera information för ett givet ändamål.

Konfidentialitet: En aspekt av informations- och cybersäkerhet som innebär att endast behöriga kan ta del av informationen.

Monoberoende: En organisation har ett monoberoende av (exempelvis) en tjänst när den är beroende av den tjänsten och det inte finns några alternativa tjänster att använda ifall den tjänst organisationen redan använder upphör.

NCC-SE: Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet.

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

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

Riktighet: En aspekt av informations- och cybersäkerhet som innebär att information och informationssystem är korrekta eller fungerar korrekt och inte ändras på ett felaktigt sätt.

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

Systematisk informationssäkerhet: Förebyggande och kontinuerlig anpassning av skydd utifrån behov och risker. Det innefattar arbetssätt baserat på en metodik för verksamhetsrisk, som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet, det vill säga skydd av informationstillgångar avseende konfidentialitet, riktighet och tillgänglighet.

Tillgänglighet: Tillgänglighet är aspekten att information eller informationssystem ska finnas tillgängligt när de behövs.

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

Överbelastningsangrepp (engelska Denial of service/Distributed denial of service): Angreppsmetod som bygger på att stora mängder datatrafik skickas mot en server eller annan nätverkskomponent i syfte att begränsa dess förmåga att bearbeta data och därmed blockera åtkomst för annan, legitim datatrafik. Datatrafiken kan skickas från en, ett fåtal, respektive ett stort antal av angriparen kontrollerade enheter. I det senare fallet brukar angreppet benämnas som ett DDoS-angrepp.

Sammanfattning

Sammanfattning

Under 2023 ökade antalet cyberangreppsförsök mot statliga myndigheter och leverantörer av samhällsviktiga tjänster kraftigt, trots detta har inte antalet inkomna it-incidentrapporter ökat. I kontrast till tidigare år, som dominerats av systemfel och misstag, var angrepp den största orsakskategorin till rapporterade it-incidenter. Rapportens temadel påvisar att nya EU-regleringar inom informations- och cybersäkerhet stärker området, samtidigt som högre krav kommer att innebära ökade kostnader för de organisationer som berörs.

Denna årsrapport har sin grund i den it-incidentrapportering som MSB tar emot från både statliga myndigheter och från leverantörer av samhällsviktiga och digitala tjänster. Med anledning av erfarenheter från det svenska ordförandeskapet i det Europeiska rådet och med anledning av den stora mängd nya EU-regleringar som är på väg handlar rapportens tema om EU-regleringar inom informations- och cybersäkerhetsområdet.

Under 2023 har totalt 334 it-incidenter rapporterats till MSB från 136 enskilda organisationer. Av dessa har 189 rapporter inkommit från statliga myndigheter och 145 från leverantörer av samhällsviktiga och digitala tjänster. Det totala antalet inkomna it-incidenter skiljer sig minimalt från hur många som rapporterades under 2021 och 2022. Detta trots att det under 2023 rapporterats betydligt fler cyberangrepp. I kontrast till tidigare år, som dominerats av systemfel och misstag, utgjorde angrepp den största orsakskategorin under 2023. Att rapporterade angrepp ökade beror bland annat på att det rapporterats betydligt fler överbelastningsangrepp än normalfallet. Majoriteten av överbelastningsangreppen rapporterades mellan januari till maj och inträffade under samma period som en serie manifestationer där heliga skrifter skändades och väckte uppmärksamhet. Flera av dessa angrepp orsakade att tillgängligheten till webbsidor och e-tjänster begränsades under en tid.

Statistiken indikerar att närmare hälften av alla it-incidenter har sitt ursprung hos en leverantör till den rapporterade organisationen. De flesta av it-incidenterna resulterade även här i att tillgängligheten till berörda informationssystem förlorades under en tidsperiod. I många fall har bortfallet påverkat tillgången till verksamhetskritisk information. MSB bedömer samtidigt att det är få av dessa som har resulterat i större samhällskonsekvenser då eventuellt bortfall i den drabbade samhällsviktiga tjänsten ofta kunnat kompenseras för.

Som tidigare nämnts, inkluderas ett särskilt kapitel om EU-regleringar inom informations- och cybersäkerhetsområdet. Dessa regleringar betonar vikten av att underhålla och ytterligare stärka den nationella kapaciteten för att bemöta cyberhot och it-incidenter. Genom att utvidga samarbete och informationsutbyte mellan medlemsstater och unionens institutioner, organ och byråer ska medlemsstaternas och organisationernas kapacitet och beredskap stärkas. Initiativen förväntas påverka såväl svensk som europeisk säkerhet liksom roller och krav på myndigheter och organisationer i medlemsstaterna.

Infosäkkollen 2023 (som från 2024 går under namnet Cybersäkerhetskollen) visar att en majoritet av alla organisationer inom offentlig sektor saknar de mest grundläggande delarna i det systematiska informations- och cybersäkerhetsarbetet. Det kombinerat med ett oroligt omvärldsläge och en föränderlig angreppsbild mot samhällsviktig verksamhet gör att Sverige sammantaget behöver ta nya tag om informations- och cybersäkerhetsområdet. Kommande EU-regleringar kan bidra till det arbetet, om den svenska implementeringen görs enhetligt och resurser i ett tidigt skede allokeras för att bemöta utökade säkerhetskrav.

MSB:s slutsatser och rekommendationer i denna rapport handlar om hur det förebyggande säkerhetsarbetet hos organisationer ska stärkas. Framför allt inom de områden där större brister påvisats, såsom ledningens engagemang, incident-, kontinuitets- och ändringshantering, kompetensförsörjning samt digitala leveranskedjor. De kommande EU-regleringarna omfattar en mängd olika initiativ med fokus på stärkt informations- och cybersäkerhet. MSB bedömer att en lyckad implementering kräver att organisationer som omfattas av regleringarna i ett tidigt skede tillsätter de resurser som behövs. Rekommendationerna till regeringen handlar om att uppmuntra genomförande av Cybersäkerhetskollen, kartläggning av digitala leveranskedjor, samt om vikten att sträva efter samordning vid implementering av EU-reglering.

Rapporten är framtagen på uppdrag av regeringen i enlighet med MSB:s instruktion, men riktar sig också till beslutsfattare, informations- och säkerhetsansvariga, samt omvärldsbevakande och analyserande funktioner hos både statliga myndigheter och NIS-leverantörer. Innehållet kan även vara värdefullt för motsvarande roller hos andra organisationer.

MSB informerar

MSB informerar

I detta kapitel summeras några nyheter inom informations- och cybersäkerhetsområdet från MSB under 2023.

Informations- och cybersäkerhet står högt upp på regeringens agenda.[1] Nedan ges en insyn i en del av det arbete som bedrivs på MSB inom området.

Infosäkkollen och It-säkkollen 2023

På uppdrag av regeringen genomför MSB Infosäkkollen och It-säkkollen, som är ett verktyg som både mäter och stödjer informations- och cybersäkerheten hos deltagande organisationer. Syftet kan sammanfattas som tvådelat, nämligen att ge organisationerna stöd med återkoppling om nivån på deras informations- och cybersäkerhetsarbete och förslag på förbättringar, samt att ta fram en samlad bedömning till regeringen.

Mellan 17 maj och 29 september 2023 genomfördes Infosäkkollen för andra gången. 291 organisationer, 53 procent, av organisationerna i offentlig förvaltning deltog[2] och bland dem var det endast 31 procent som nådde upp till någon av modellens fyra nivåer. Nivåer som visar hur långt en organisation kommit i säkerhetsarbetet. Resten, 69 procent, av organisationerna saknar de mest grundläggande delarna i ett systematiskt informations- och cybersäkerhetsarbete. Motsvarande procentsiffra 2021 var dock ännu högre, nämligen 82 procent. Endast fyra av 120 myndigheter når det samlade resultat som MSB har definierat som en indikation över huruvida en organisation uppfyller MSB:s föreskriftskrav om statliga myndigheters informationssäkerhet[3]. Den första utgåvan av föreskrifterna trädde ikraft 2009.

211 organisationer har deltagit vid båda undersökningstillfällena 2021 och 2023. Mätt i antalet genomförda åtgärder motsvarar utvecklingen en 6 procentig förbättring gällande deras resultat i Infosäkkollen 2023 jämfört med 2021. Vid en jämförelse mellan de organisationer som deltagit enbart 2021 eller 2023 framkommer det dock att många organisationer med svagare resultat 2021 inte deltagit 2023 och att de organisationer som deltog 2023 hade betydligt bättre resultat än de som enbart deltog 2021. En del av det ”förbättrade” resultatet för Infosäkkollen 2023 kan därför förklaras genom att de svagare organisationerna från 2021 helt enkelt inte deltog 2023.

---

1. Regeringskansliet. *Nationell strategi för samhällets informations- och cybersäkerhet.* https://www.regeringen.se/regeringens-politik/krisberedskap/nationell-strategi-for-samhallets-informations--och-cybersakerhet/ (Hämtad 01–2024).

2. Domstolsverket svarade för alla domstolar, vilket påverkar antalet deltagande organisationer.

3. Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

Resultatet inom arbetsområdet för *Ledningens styrning och kontroll visar* tyvärr på bristande engagemang från organisationernas ledningar. Medan ett visst skydd kan uppnås utan aktiv inriktning och uppföljning av ledningen är MSB:s bedömning att det är svårt att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete utan ledningens löpande engagemang. För att kunna arbeta systematiskt över tid måste informations- och cybersäkerhetsarbetet prioriteras och tilldelas resurser.

I resultatredovisningen av Infosäkkollen 2021 konstaterades att ”den mest centrala slutsatsen från MSB:s analys är att det behövs en generell satsning på att stärka det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen”[4]. Att offentliga förvaltningar inte hörsammat tidigare slutsatser och resurssatt informations- och cybersäkerhetsarbetet, stärker MSB nu sin rekommendation ytterligare. MSB bedömer att en särskild satsning gällande finansiering till de organisationer i offentlig förvaltning som genomfört Infosäkkollen och It-säkkollen, och där brister föreligger, bör övervägas. Detta för att tillföra de resurser som behövs för att höja organisationens nivå i den utsträckning som krävs för att kunna garantera säkerhet och tillförlitlighet i samhällsviktiga tjänster. It-incidenter är dessutom kostsamma och ur ett samhällsperspektiv torde det vara mer ekonomiskt att förekomma de incidenter som kan förebyggas.

267 organisationer från offentlig förvaltning deltog i It-säkkollen 2023. It-säkkollen 2023 är en självskattningsundersökning och kommer vidareutvecklas för att få samma metodologiska robusthet som Infosäkkollen inför mättillfället 2025. Resultatet för 2023 ligger på en förhållandevis god nivå, nästan motsvarande nivå 3 av 4 i modellen, vilket motsvarar ”visst skydd”. Resultatet visar på små skillnader mellan organisationerna för såväl helheten som inom varje enskilt arbetsområde. Myndigheterna presterar lite bättre än regionerna, följt av kommunerna som är marginellt svagast.

För mer information och slutsatser och rekommendationer hänvisas till resultatredovisningen på MSB:s webbplats.[5]

Användarnära stöd i informationssäkerhetsarbetet

I juli 2022 gav regeringen MSB i uppdrag att utveckla och förenkla det stöd som myndigheten lämnar inom informations- och cybersäkerhetsområdet. Detta resulterade i ett användarnära stöd i två delar, en rådgivningstjänst och en webbinarieserie, som båda startade i mindre skala under 2022 och etablerades på allvar under 2023. Det användarnära stödet ska hjälpa aktörerna att lättare hitta till det stöd som MSB tillhandahåller, ge vägledning till hur stödet kan användas och hjälpa organisationer att anpassa informationssäkerhetsarbetet till deras verksamhet.

Rådgivningstjänsten är en tjänst där aktörerna via ett webbformulär kan boka rådgivning och få hjälp med sina frågor. Tjänsten samlar också in feedback och information om användarnas behov, som används för att utveckla och förbättra MSB:s stödmaterial på området. I juni 2023 utvärderades tjänsten och resultaten visar på en hög effektivitet och en kvalitativ hantering av ärendena. Förutom

4. MSB. *Det systematiska informationssäkerhetsarbetet i den offentliga Förvaltningen – Resultatredovisning Infosäkkollen 2021*. https://rib.msb.se/filer/pdf/30002.pdf (Hämtad 02–2024)

5. MSB. *Det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen – Resultatredovisning av Infosäkkollen och It-säkkollen 2023.* https://rib.msb.se/filer/pdf/30598.pdf (Hämtad 03–2024)

effekten ute i organisationerna som söker stöd har tjänsten även hjälpt MSB att få en tydligare bild av användarnas behov, vilket i sin tur gett bättre möjligheter att utforma relevant stöd.

Webbinarieserien ”Informationssäkerhet i fokus” består av korta föreläsningar med frågestund till expertpanel. Serien har behandlat olika teman inom informationssäkerhet med olika föredragande från MSB, och varje tema har sänts två gånger. I samband med varje sändning har deltagarna fått ställa frågor till de föredragande – ett mycket uppskattat inslag. Varje webbinarium har haft plats för 200 deltagare och har snabbt blivit fullbokade.

MSB/CERT-SE

MSB/CERT-SE har under året genomfört ett flertal åtgärder inom ramen för regeringsuppdraget till MSB om att stärka funktionen MSB/CERT-SE, samt utveckla och förenkla det stöd som lämnas inom informations- och cybersäkerhetsområdet.

En ny webbplats lanserades under 2023 i syfte att mer effektivt kunna informera om it-säkerhet, incidenter och åtgärder. MSB/CERT-SE har även vidareutvecklat interna processer och organisationen i sin helhet. Resultatet är en utvecklad förmåga att förebygga och ge stöd och information till samhället vid inträffade incidenter, samt stöd att upptäcka och förstå sårbarheter genom direkta varningar avseende system.

Datadriven CERT (DDC), är ett EU-finansierat projekt med syfte att stärka den nationella förmågan att förebygga och hantera it-säkerhetshändelser genom en ökad grad av automatisering av omvärldsbevakning och datadrivna åtgärder avseende it-säkerhetshändelser. Projektet skapar bättre förutsättningar för MSB/CERT-SE att hantera de stora volymer av information om sårbarheter och hot på it-säkerhetsområdet som finns tillgängliga. Projektet ökar även förmågan att bearbeta och analysera information, samt att MSB/CERT-SE bättre kan inrikta sin verksamhet och kommunicera råd, varningar eller analyser till olika samhällsaktörer som i sin tur kan vidta nödvändiga åtgärder för att förebygga eller hantera it-incidenter.

MSB/CERT-SE har även lanserat en funktion för automatiska notifieringar avseende tekniska sårbarheter (ANTS). Syftet med funktionen är att med en högre grad av automatisering uppmärksamma MSB/CERT-SE:s intressenter då information om tekniska företeelser som kan behöva åtgärdas har påträffats hos dem. För att identifiera sådana företeelser bedriver MSB/CERT-SE kontinuerlig omvärldsbevakning med verktyg, via kontakter och nätverk i Sverige och via informationsutbyte med sina motsvarigheter i andra länder. Sedan lanseringen i augusti har drygt 2 500 notifieringar skickats ut via ANTS till anslutna organisationer.

Under året har MSB/CERT-SE även förnyat sin certifiering som CSIRT-funktion enligt den europeiska standarden Trusted Introducer (TI), som säkerställer kvalitet och utveckling hos, och samarbete mellan, europeiska organisationer som arbetar med it-relaterad incidenthantering. MSB/CERT-SE har varit certifierade sedan 2011 och uppnådde under 2023 kraven för certifiering för tredje gången.

De ovan nämnda åtgärderna under 2023 har sammantaget ökat MSB/CERT-SE:s förmåga att snabbt identifiera samt direkt informera svenska verksamheter om sårbarheter, vilket bidragit till att stärka den totala it-beredskapen i Sverige. Ett annat fokus under 2023 har varit att säkerställa ett bättre informationsflöde

till representanter inom offentlig samt privat sektor genom informationsdelning i MSB:s olika samarbetsforum. Dessa har sedan dess genomförts löpande varannan vecka. Vid mötena presenterar representanter från MSB/CERT-SE den senaste versionen av MSB/CERT-SE lägesuppfattning, som sammanställs varannan vecka. Lägesuppfattningen ger en samlad bedömning av läget i den svenska it-sfären, samt ett urval av it-säkerhetsrelaterade händelser och företeelser under perioden som bedöms relevanta för svenska aktörer.

MSB/NCC-SE

MSB driver i enlighet med myndighetens instruktion Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE) sedan 2022. Uppdraget för NCC-SE är att bidra till att stärka Sveriges förmåga och konkurrenskraft inom cybersäkerhet inom ramen för den EU-förordning som reglerar EU:s kompetenscentrum för cybersäkerhet (ECCC) och nätverket av nationella samordningscenter. NCC-SE knyter ihop svenska och europeiska forskare och företag, underlättar för svenska aktörer att svara på europeiska forsknings- och innovationsutlysningar inom cybersäkerhet och stöttar ECCC med expertis inklusive inspel gällande svenska behov och prioriteringar till kommande EU-finansieringsprogram. NCC-SE erbjuder även rådgivning i hur man söker EU-finansiering för forskning och cybersäkerhetslösningar som kan bidra till stärkt förmåga. Under 2023 har NCC-SE fortsatt uppbyggnaden av centret och den nationella kompetensgemenskapen i samarbete med RISE/Cybernoden, samt vidareutvecklat och fördjupat samarbetet med ECCC och det europeiska NCC-nätverket. NCC-SE förbereder också för att genomföra nationella cybersäkerhetsrelaterade utlysningar riktade mot små och medelstora företag under 2025.

Rapporterade it-incidenter under 2023

Rapporterade it-incidenter under 2023

Statliga myndigheter och leverantörer av samhällsviktiga tjänster ska enligt lag rapportera it-incidenter som drabbat dem. Kapitlet redogör för rapporterade it-incidenter 2023, samt dess orsaker och konsekvenser.

Om it-incidentrapportering

Ur ett samhälls- och organisationsperspektiv är det fördelaktigt att rapportera it-incidenter. Ju mer information som tillhandahålls kring incidenter, desto bättre kan det förebyggande arbetet utvecklas och struktureras. Incidentdata bidrar även till MSB:s nulägesbild liksom till den långsiktiga strategiska analysen. Vissa organisationer har krav på sig att rapportera eftersom den verksamhet de bedriver anses särskilt kritisk för samhällets funktionalitet. De organisationer som har krav på sig att rapportera it-incidenter till MSB är statliga myndigheter[6] och leverantörer av samhällsviktiga och digitala tjänster (NIS-leverantörer)[7].

Under särskilda omständigheter kan en och samma it-incident behöva rapporteras till flera olika myndigheter. Incidenter relaterade till brott ska exempelvis anmälas både till MSB (it-incidenten) och Polismyndigheten (brottsanmälan). Om en incident innefattar påverkan på personuppgifter är den rapporteringspliktig enligt dataskyddsförordningen (GDPR) och ska, utöver rapportering till MSB, rapporteras till Integritetsskyddsmyndigheten. En incident som faller under rapporteringsskyldighet enligt säkerhetsskyddsförordningen ska rapporteras till Säkerhetspolisen eller Försvarsmakten. MSB uppmanar alla organisationer att proaktivt se över vilka rapporteringskrav som gäller för olika typer av it-incidenter för att kunna agera snabbt och korrekt om och när en incident inträffar.

6. Sveriges riksdag. *Förordning (2022:524) om statliga myndigheters beredskap*. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-2022524-om-statliga-myndigheters_sfs-2022-524/ (Hämtad 01/2024).

7. Sveriges riksdag. Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174/ och Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-20181175-om-informationssakerhet-for_sfs-2018-1175/ (Hämtade 02–2024).

Rapporterade it-incidenter

Under 2023 har totalt 334 it-incidenter rapporterats till MSB. Av dessa har 189 inkommit från statliga myndigheter och 145 från leverantörer av samhällsviktiga och digitala tjänster.[8] Den stora majoriteten av it-incidentrapporter som inkommit från NIS-leverantörer har rapporterats av organisationer inom hälso- och sjukvårdssektorn (76,5 procent). Därefter har 13 procent inkommit från transportsektorn och tio procent från leverantörer av dricksvatten. Resterande sektorer står sammanlagt för mindre än en procent av inkomna it-incidenter från NIS-leverantörer. Totalt har 72 statliga myndigheter och 64 NIS-leverantörer rapporterat minst en it-incident vardera.[9]

Tabell 1. Antal inrapporterade it-incidenter 2021–2023

Organisation	2023	2022	2021
Statliga myndigheter	189	231	261
NIS-leverantörer	145	99	82
Totalt	**334**	**330**	**343**

Tabellen beskriver antal it-incidenter som rapporterats till MSB per år mellan 2021–2023. Antalet it-incidenter som rapporterats in av statliga myndigheter respektive NIS-leverantörer redogörs för separat såväl som ihop.

Som *Tabell 1* visar är förändringen mellan åren minimal. Under 2023 har antalet rapporterade it-incidenter ökat minimalt i jämförelse med föregående år och minskat i jämförelse med 2021. Under hela perioden har genomsnittet för hur många it-incidenter som rapporterats varje månad varit ungefär detsamma. Däremot syns tydliga skillnader i antalet it-incidenter som rapporterats från statliga myndigheter respektive NIS-leverantörer. Medan antalet inkomna it-incidentrapporter från NIS-leverantörer konsekvent ökat under perioden har antalet från statliga myndigheter, även om de fortfarande står för merparten av rapporter, minskat. Att det totala antalet rapporterade it-incidenter inte skiljer nämnvärt från år till år kan således ses som en konsekvens av dessa två trender sammanfaller i statistiken.

Statliga myndigheter har alltid inkommit med fler it-incidentrapporter per år än NIS-leverantörer. En förklaring till detta är att statliga myndigheter har bredare rapporteringskrav och behöver därav rapportera fler typer av it-incidenter. Skillnaden kan dock delvis också förklaras av att rapporteringsbenägenheten bland statliga myndigheter generellt bedöms vara större än bland NIS-leverantörer. MSB har tidigare år gjort bedömningen att en ökning i antalet inkomna it-incidenter som rapporteras av NIS-leverantörer delvis reflekterar en ökad rapporteringsbenägenhet

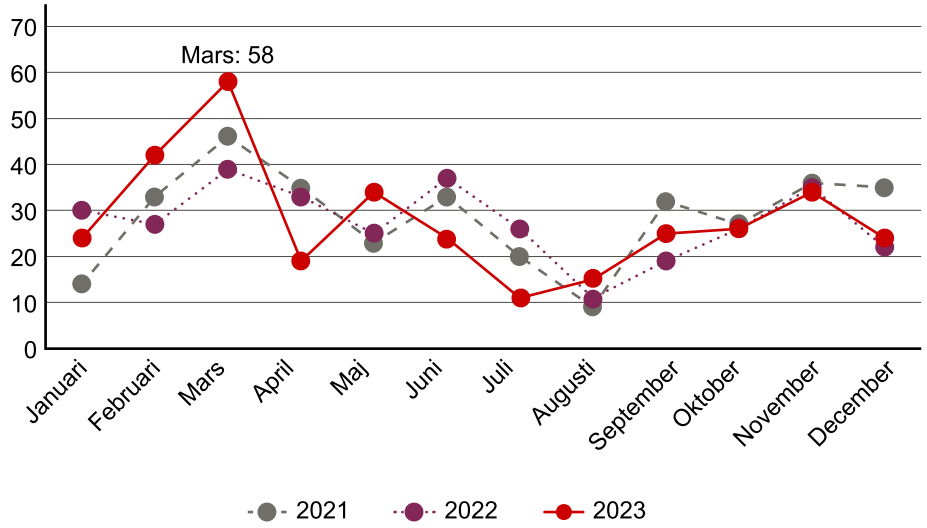
8. Vissa it-incidenter som rapporteras till MSB återkallas av rapporterande organisation. Dessa inkluderas inte i statistiken. I MSB:s årsredovisning för 2023 redovisades två it-incidenter från NIS-leverantörer som i ett senare skede återkallades. Det gör att den redovisade siffran över antalet rapporter inkomna från NIS-leverantörer, och således totalsiffran, inte överensstämmer med det som tidigare uppgavs i årsredovisningen.

9. Statistiken över rapporterade it-incidentrapporter baseras på när it-incidenten *rapporterades* och inte när den *inträffade*. Det förekommer således ett eftersläp som bland annat påverkar redovisningen av antalet it-incidenter som inkommit per månad. Det påverkar även till viss del hur många it-incidenter som uppges inkomma per år. Detta då it-incidenter som inträffat i slutet av 2022 och i slutet av 2023 potentiellt inkluderas respektive exkluderas beroende på när aktören rapporterar it-incidenten. En it-incident som exempelvis inträffat i december 2023 men inte rapporteras förrän januari 2024 redovisas i nästa årsrapport.

inom aktörsgruppen.[10] Något som tyder på att det fortfarande gäller är att det under 2023 inkommit fler rapporter från aktörer inom sektorer där mörkertalet bedöms vara stort. Samtidigt har dock både andelen och antalet rapporter som mottagits från aktörer inom hälso- och sjukvården, den sektor som generellt har störst rapporteringsbenägenhet, ökat under året. Sammantaget ökade antalet inkomna it-incidentrapporter från hälso- och sjukvårdssektorn med cirka 70 procent jämfört med 2022, något som sannolikt indikerar att det förekommit ett ökat antal it-incidenter inom den sektorn.

Att ökningen bland NIS-leverantörer kan kontrasteras med en konsekvent minskning bland statliga myndigheter är anmärkningsvärt. Minskningen av rapporterade it-incidenter inom aktörsgruppen kan bero på en kombination av en (i) generellt avtagande rapporteringsvilja, (ii) minskad benägenhet att rapportera in it-incidenter som inte resulterat i störningar och (iii) förbättrade skydd och säkerhetsrutiner. Den sistnämnda förklaringen bör vägas mot att Infosäkkollen 2023 fortsatt visar på stora brister i statliga myndigheters systematiska informationssäkerhetsarbete.

Diagram 1. Inrapporterade it-incidenter per månad 2021–2023



Linjediagram som beskriver antalet it-incidenter som rapporterats av rapporteringspliktiga aktörer per månad under åren 2021, 2022 respektive 2023.

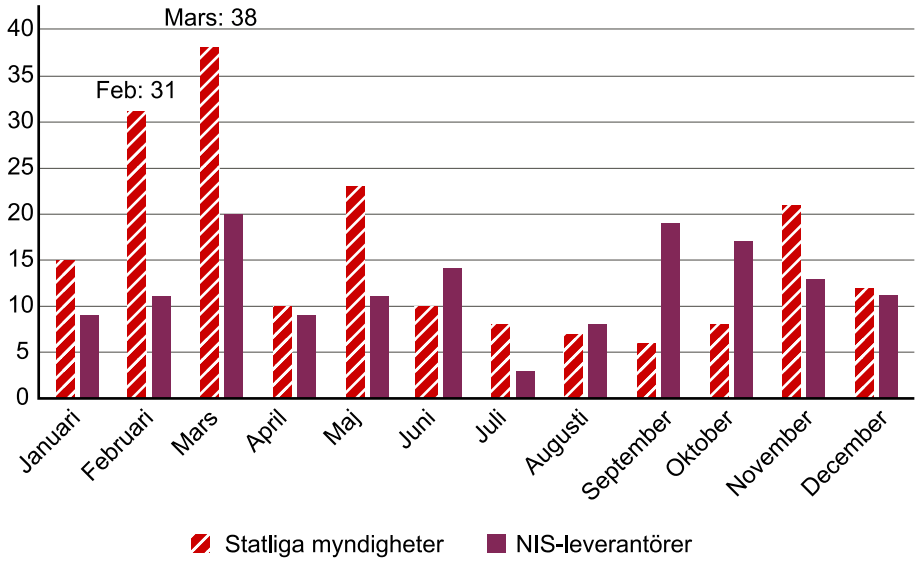
Årscykeln för antalet rapporterade it-incidenter per månad under 2023 skiljer sig inte drastiskt från vad som observerats tidigare år. Liksom tidigare år inkom majoriteten av it-incidentrapporter under årets första halva, även om skillnaden är mer påtaglig under 2023. Som *Diagram 1* illustrerar rapporterades flest it-incidenter under 2023, liksom under 2021 och 2022, i mars. Mars 2023 utmärker sig dock sett till antalet, då totalt 58 it-incidentrapporter inkom under månaden. Det gör det till den månad då flest it-incidentrapporter mottagits mellan 2021 och 2023. Det bör noteras att det även under februari 2023 sammanlagt rapporterades 42 it-incidenter, vilket är mer än vad som rapporterades under en enskild

10. MSB har länge bedömt att det förekommer ett mörkertal i it-incidentrapporteringen. Även om ett mörkertal förekommer ser MSB att it-incidentrapporteringen ger en bra överblick sett till fördelningen av rapporterade orsaker och konsekvenser. MSB bedömer därmed att underlaget är fullgott för extrapolering. En bekymrande aspekt är dock att mörkertalet bedöms vara mycket stort inom vissa NIS-sektorer, exempelvis finansmarknadsinfrastruktur och bankverksamhet, som rapporterar in ytterst få it-incidenter. Det gör att underlaget inte är representativt för dessa delar av populationen. MSB tar hänsyn till detta inom ramen för de analyser som är baserade på it-incidentrapporteringen.

månad under 2022. Samtidigt rapporterades det färre it-incidenter i april, juni och juli. Minst antal it-incidenter under 2023 rapporterades i juli, då MSB endast mottog tio stycken it-incidentrapporter från rapporteringspliktiga aktörer.

Gemensamt för alla åren är att antalet rapporterade it-incidenter minskar under sommarmånaderna. Det kan bero på att det inträffar färre rapporteringspliktiga it-incidenter då, exempelvis på grund av att aktiviteten inom organisationer generellt minskar. Mer sannolikt är dock att organisationers rapportering avtar i samband med en förändrad och ofta lägre bemanning under semestertider. En förändrad bemanning kan tänkas negativt påverka organisationers förmåga att både upptäcka och utreda inträffade it-incidenter. Det kan också tänkas resultera i att rapporteringsbenägenheten generellt minskar i de fall organisationen saknar en väletablerad rutin för att rapportera it-incidenter.

Diagram 2. Inrapporterade it-incidenter per månad 2023 – Statliga myndigheter och NIS-leverantörer



Stapeldiagram som visar antalet it-incidenter som rapporterats av statliga myndigheter respektive NIS-leverantörer per månad under år 2023.

Som *Diagram 2* visar uppstod toppen under februari och mars 2023 framförallt på grund av att statliga myndigheter rapporterade in fler it-incidenter. Statliga myndigheter rapporterade 38 it-incidenter under mars och 31 under februari. Ökningen beror framförallt på att en större mängd överbelastningsangrepp utfördes och rapporterades under det första halvåret, vilket närmare redogörs för i nästkommande avsnitt under rubriken *Ökat antal rapporterade överbelastningsangrepp*.

Antalet it-incidenter som rapporterats av NIS-leverantörer har fluktuerat mindre. Det högsta antalet it-incidenter rapporterades under mars (20 fall) tätt följt av september (19 fall). Till skillnad från de rapporter som inkom från statliga myndigheter uppstod dessa toppar inte som en konsekvens av ett ökat antal rapporterade överbelastningsangrepp. De är istället bland annat en konsekvens av att flera leveranskedjeincidenter, som påverkade flera rapporteringspliktiga aktörer samtidigt, inträffade under perioderna. Incidenterna kan härledas till både misstag och systemfel, såväl som angrepp. I mars rapporterades ett ovanligt stort antal NIS-leverantörer en it-incident till följd av att en gemensam leverantör utsattes för ett dataintrång.

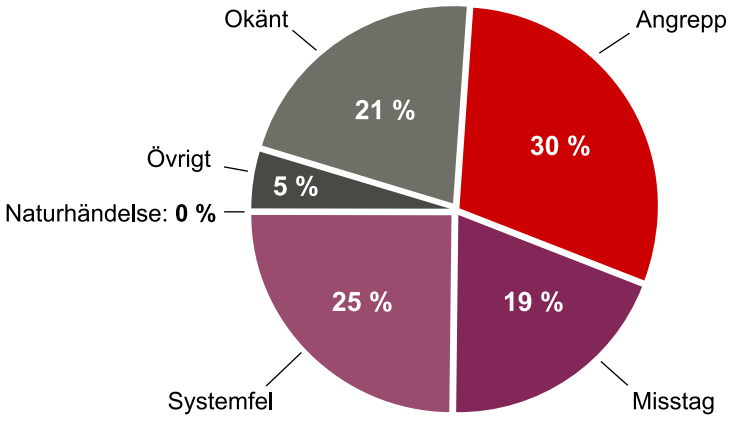
Angrepp den vanligaste orsaken till rapporterade it-incidenter

En it-incident kan orsakas av flera olika typer av händelser. MSB delar övergripande in dessa händelser i kategorierna (i) misstag, (ii) angrepp, (iii) systemfel och (iv) naturhändelse. Misstag och angrepp förutsätter mänsklig intervention. Systemfel och naturhändelse är tvärtom it-incidenter som triggats av en händelse som saknar en tydlig mänsklig intervention.

Cyberangrepp får ofta stor uppmärksamhet, särskilt i jämförelse med andra it-incidenter, men i termer av konsekvenser spelar det dock ingen roll om det är ett angrepp, misstag eller systemfel som gör att exempelvis ett livsuppehållande informationssystem slutar att fungera. Om systemet inte repareras eller ersätts kan patienter avlida. Det är därför viktigt att tillämpa allriskperspektivet för att upprätthålla samhällsviktiga verksamheter och tjänster.

I *Diagram 3* redogörs för fördelningen av rapporterade orsaker under 2023.[11] Diagrammet inkluderar kategorierna ”övrigt” och ”okänt” vid sidan av de ovan nämnda. I denna kontext innebär en rapporterad ”övrig” orsak att rapportör bedömt att orsaken inte överensstämmer med någon av de etablerade kategorierna.

Diagram 3. Fördelning av inrapporterade orsaker till it-incidenter 2023



Cirkeldiagram som redogör för fördelningen av inrapporterade orsaker till it-incidenter utifrån kategorierna Angrepp, Misstag, Systemfel, Naturhändelse, Övrigt samt Okänt under år 2023. I 18 it-incidentrapporter har frågan ej besvarats och fördelningen är således baserad på 316 inkomna rapporter. Ett fåtal rapportörer har angett mer än en orsakskategori som bakomliggande orsak.

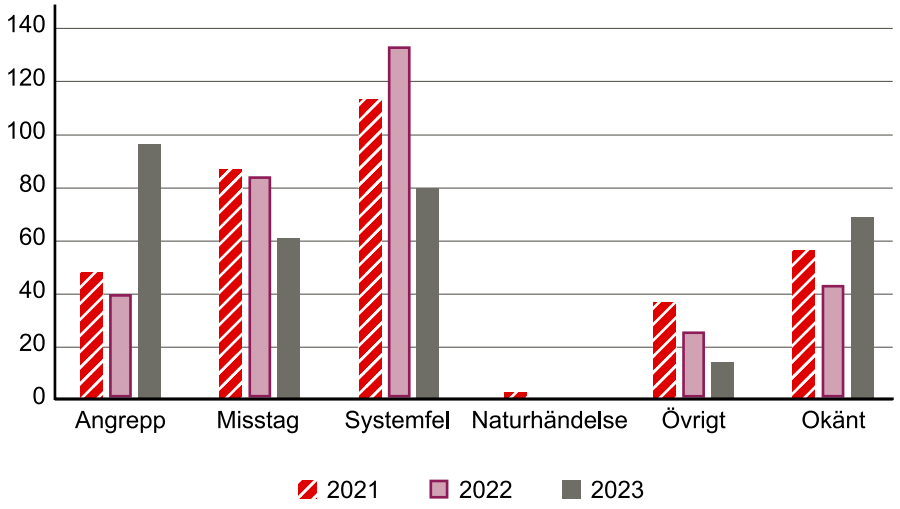
År 2023 utmärker sig från tidigare år då det rapporterats betydligt fler angrepp som bakomliggande orsak. Under 2023 går cirka 30 procent av rapporterade it-incidenter att härleda till ett angrepp. Systemfel, som tidigare utgjort den största orsakskategorin, har angetts vara den bakomliggande orsaken i 25 procent av rapporterna. Därefter är det 21 procent av rapportörer som angett att den bakomliggande orsaken är okänd. 19 procent har angett att it-incidenten orsakats av ett misstag och 5 procent har angett att it-incidenten har en övrig orsak. Liksom föregående år är det ingen rapportör som angett en naturhändelse som bakomliggande orsak.

11. Vissa it-incidentrapporter som inkommer är ofullständiga. I de fall statistiken redovisas i procent inkluderas mer information om storleken på underlaget i förklaringstexten under diagrammet.

Att naturhändelser sällan rapporteras vara en bakomliggande orsak skulle kunna bero på att det är ovanligt att sådana händelser påverkar infrastruktur som försörjer informationssystem. Det kan dock förekomma en underrapportering som en konsekvens av att organisationer själva sällan ansvarar för fysiskt underhåll av it-komponenter.

Trots den markanta ökningen av antalet rapporterade angrepp skiljde sig, som tidigare nämnt, det totala antalet it-incidenter som rapporterades under 2023 inte nämnvärt från varken 2022 eller 2021. Det har sannolikt flera förklaringar, men bottnar i att det har rapporterats betydligt färre it-incidenter med andra bakomliggande orsaker under 2023. *Diagram 4* redogör för antalet rapporterade it-incidenter tillhörande respektive orsakskategori har förändrats mellan 2021 och 2023.

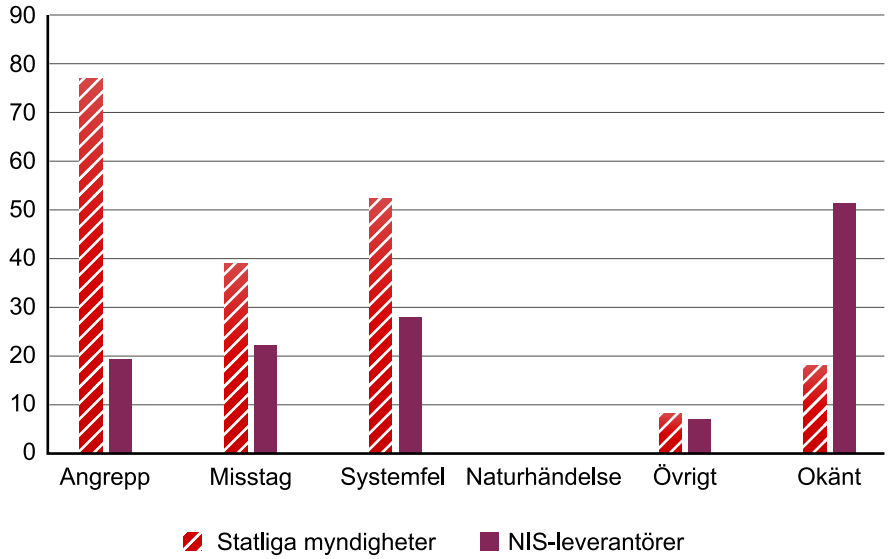
Diagram 4. Inrapporterade orsaker till it-incidenter 2021, 2022 och 2023



Stapeldiagram som redogör för antalet inrapporterade it-incidenter som beskriver incidentens orsak som Angrepp, Misstag, Systemfel, Naturhändelse, Övrigt respektive Okänt för åren 2021, 2022 och 2023. Ett fåtal rapportörer har angett mer än en orsakskategori som bakomliggande orsak.

Diagrammet visar tydligt att antalet rapporterade angrepp har ökat under år 2023 i jämförelse med tidigare år samtidigt som framförallt rapporteringen av systemfel har minskat. Antalet rapporterade angrepp har ökat från 48 och 40 fall 2021 respektive 2022 till 96 år 2023. Det utgör en dryg fördubbling. Det enda andra svarsalternativet där det går att observera en absolut, men även en relativ, ökning är orsakskategorin ”okänt”. Antalet rapporterade systemfel, som i normalfall brukar vara den största orsakskategorin, har samtidigt minskat från 133 rapporterade fall 2022 till 80 rapporterade fall 2023. Antalet rapporterade misstag har likväl minskat från cirka 85 fall under 2021 och 2022 till 61 år 2023.

Diagram 5. Fördelning av incidenter med avseende på orsak för statliga myndigheter och NIS-leverantörer



Stapeldiagram som redogör för fördelningen av rapporterade systemfel, misstag, angrepp, och naturhändelser samt de som angett svarsalternativ övrigt respektive okänt. Fördelningen presenteras som antal it-incidentrapporter som inkommit från NIS-leverantörer respektive statliga myndigheter inom respektive kategori. Ett fåtal rapportörer har angett mer än en orsakskategori som bakomliggande orsak.

Diagram 5 visar att majoriteten av rapporterade angrepp har inkommit från statliga myndigheter. Sammanlagt anges angrepp vara den bakomliggande orsaken i 77 fall, sammanlagt cirka 41 procent, av rapporter inkomna från statliga myndigheter medan det endast representerar 19 fall, sammanlagt 13 procent, av rapporter inkomna från NIS-leverantörer. Liksom tidigare år står även statliga myndigheter för den största andelen av rapporterade systemfel och misstag. Den oftast angivna kategorin bland NIS-leverantörer är istället ”okänt”, något som angetts i 51 fall, totalt 35 procent av inkomna rapporter från aktörsgruppen.

Att många NIS-leverantörer rapporterar it-incidentens bakomliggande orsak som okänd följer normalbilden. Det bedöms bland annat bero på att en stor andel av de it-incidenter som rapporteras av aktörsgruppen har sitt ursprung hos en leverantör. Det är en vanligt förekommande situation att rapporterande organisation inte har fått tillräckligt med information från leverantören för att kunna specificera den bakomliggande orsaken.

Att färre misstag och systemfel rapporteras in sammanfaller med en generellt minskande trend av rapporter inkomna från statliga myndigheter. Som redogörs för i början av avsnittet kan det finnas flera bakomliggande förklaringar, inklusive att rapporteringsbenägenheten har minskat.

Ökat antal rapporterade överbelastningsangrepp

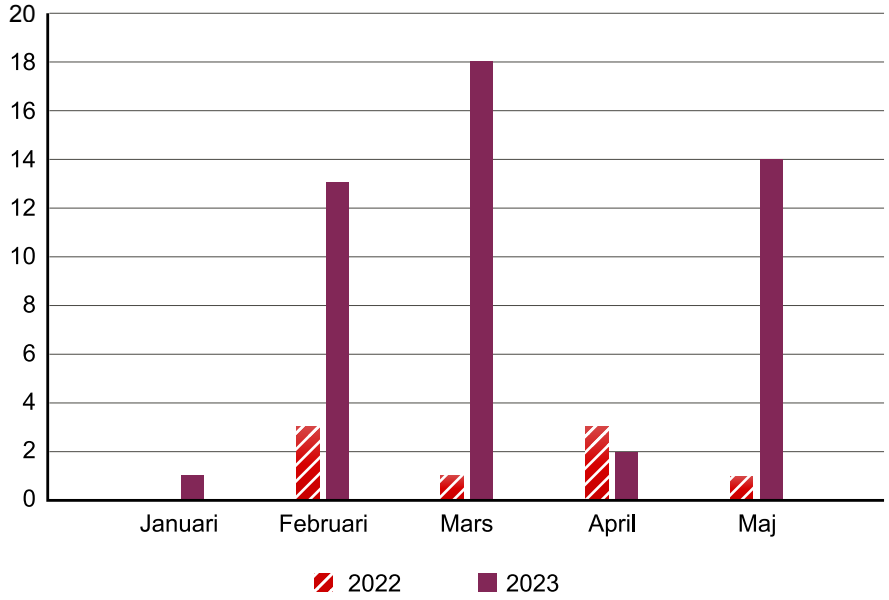
Att angrepp utgör den största orsakskategorin bland statliga myndigheter är anmärkningsvärt, då orsaker till it-incidenter tidigare år har dominerats av systemfel och misstag. Ökningen beror till stor del på att det under årets första månader rapporterades in fler överbelastningsangrepp än normalfallet. Ett förhöjt antal rapporterade överbelastningsangrepp kunde observeras mellan januari till maj och inträffade under samma period som flera manifestationer där koranen skändades väckte uppmärksamhet både nationellt och internationellt. Över 70 procent av de it-incidentrapporter som beskriver angrepp som bakomliggande orsak under 2023 rapporterades mellan januari och maj. Totalt

rapporterades det under den perioden fyra gånger fler överbelastningsangrepp än under hela 2022. Frekvensen illustreras i *Diagram 6*. Det bör noteras att då det förekommer en viss fördröjning i rapporteringen har vissa överbelastningsangrepp som inträffat under en månad inte rapporterats förrän månaden efter.

Vid ett överbelastningsangrepp skickas stora mängder datatrafik mot en webbsida eller liknande i syfte att blockera åtkomst för legitim trafik. Överbelastningsangrepp drabbar oftast webbsidor och e-tjänster, vilka under tiden för angreppet blir helt eller delvis otillgängliga för användare om effekten inte kan mitigeras.

Till skillnad från mer avancerade typer av cyberangrepp, exempelvis utpressningsangrepp, innebär ett lyckat överbelastningsangrepp inte att it-miljöns integritet har kompromitterats eller att skyddad information blivit tillgänglig för obehöriga. Mer avancerade cyberangrepp har, till skillnad från överbelastningsangrepp, inte rapporterats i större utsträckning under 2023, även om flera fall blivit medialt uppmärksammade. Det bör dock återigen noteras att statistiken endast bygger på it-incidenter rapporterade av rapporteringspliktiga organisationer.

Diagram 6. Antalet överbelastningsangrepp som rapporterats mellan januari och maj 2023



Stapeldiagram som redogör för antalet överbelastningsangrepp som rapporterades mellan januari och maj 2022 och 2023.

De överbelastningsangrepp som rapporterats har i de flesta fall inte uppgetts påverka organisationens möjlighet att fullfölja sitt uppdrag i någon större utsträckning. Det är sannolikt på grund av att effekten inte blir lika omfattande som NIS-leverantörer, med deras högre kriterier för inrapportering, rapporterat in få liknande it-incidenter. Samhällskonsekvenserna av att ett ökat antal överbelastningsangrepp genomfördes under perioden bedöms därmed sammantaget vara mycket ringa, samtidigt som antalet ”lyckade” överbelastningsangrepp avslöjar en viss sårbarhet mot mindre sofistikerade angreppsmetoder. Att många cyberangrepp som rapporteras karaktäriseras av relativt osofistikerade angreppsmetoder är något som vidare lyfts i MSB:s nyligen publicerade rapport *Cyberangrepp mot samhällsviktiga informationssystem.*[12]

12. En fördjupad redogörelse för hur angreppsbilden mot statliga myndigheter och NIS-leverantörer utvecklats under åren finns i MSB:s nyligen publicerade rappo*rt Cyberangrepp mot samhällsviktiga informationssystem.* https://rib.msb.se/filer/pdf/30558.pdf (Hämtad 02–2024).

Utpressningsangrepp mot svenska organisationer

Under 2023 skedde ett antal utpressningsangrepp som uppmärksammades medialt på grund av dess konsekvenser för de drabbade organisationerna och användare av deras tjänster. Det inkluderar bland annat utpressningsangreppen som utfördes mot Svenska kyrkan, Coop Värmland och Härjedalens kommun under senare delen av året. Vid ett utpressningsangrepp installerar angripare programvara i målets informationssystem och den krypterar sedan alla eller delar av de informationstillgångar som behandlas eller lagras i målets it-miljö. Syftet är att kräva den drabbade organisationen på en lösensumma i utbyte mot nycklar som kan dekryptera informationen igen. I vissa fall exfiltreras information med hot om publicering i syfte att pressa målet att betala ännu mer.[13]

Vid alla de nämnda incidenterna har organisationen förlorat tillgång till informationssystem som används inom den dagliga verksamheten till följd av angreppet. Angreppet mot Svenska kyrkan resulterade i att stora delar av deras it-miljö blev otillgänglig. Bland annat påverkades kyrkans webbplatser och vissa församlingars förmåga att utföra sin begravningsverksamhet.[14] Angreppet mot Coop Värmland resulterade i att kortterminaler i ett flertal butiker inte gick att använda under ett antal timmar.[15] I Härjedalens kommun uppgavs hela kommunens it-miljö vara påverkad vilket gjorde att kommunen bland annat inte kunde skicka eller ta emot fakturor[16] och fick övergå till reservrutiner inom äldreomsorgen. Invånare kunde heller inte använda sig av kommunens e-tjänster.[17] Det är bekräftat att angripare haft tillgång till system som behandlar personuppgifter i samband med intrånget hos Svenska kyrkan[18] och Coop Värmland. I det sistnämnda fallet publicerade angripare viss information på darknet, inklusive personuppgifter tillhörande medlemmar och anställda.[19]

Återställningsarbetet efter det att en organisation blivit utsatt för ett utpressningsangrepp kan ta lång tid och vara kostsam. Det tog exempelvis närmare två månader innan svenska kyrkans webbsida återfick full funktionalitet.[20] Som en del av återställningsarbetet behöver bland annat en forensisk genomsökning av system göras för att fastställa hur stor del av it-miljön angripare haft tillgång till samt om det finns någon skadlig kod kvar.

It-incidentens ursprung

En stor majoritet av de rapporterade it-incidenterna har, liksom tidigare år, inträffat i ett informationssystem inom organisationens eller en leverantörs it-miljö. En mindre andel har inträffat i det som kallas kringmiljön.

13. Mer information om utpressningsangrepp går att hitta på MSB/CERT-SE:s webbsida. https://www.cert.se/tema/ransomware/ (Hämtad 02–2024).

14. Karin Lindström, Computer Sweden. *Svenska Kyrkan bekräftar – drabbat av ransomewareattack.* https://computersweden.idg.se/2.2683/1.780522/svenska-kyrkan-bekraftar-drabbat-av-ransomwareattack (Hämtad: 02–2024).

15. SVT. *Coop-anställda hängs ut på darknet efter cyberattack.* https://www.svt.se/nyheter/lokalt/varmland/coop-anstallda-hangs-ut-pa-darknet-efter-cyberattack (Hämtad 02-2024).

16. Härjedalens kommun. *Uppdatering om IT-attack 2 januari 2024.* https://www.herjedalen.se/nyhetsarkiv/nyhetsarkiv/nyheter/2024-01-02-uppdatering-om-it-attack-2-januari-2024.html (Hämtad 02–2024).

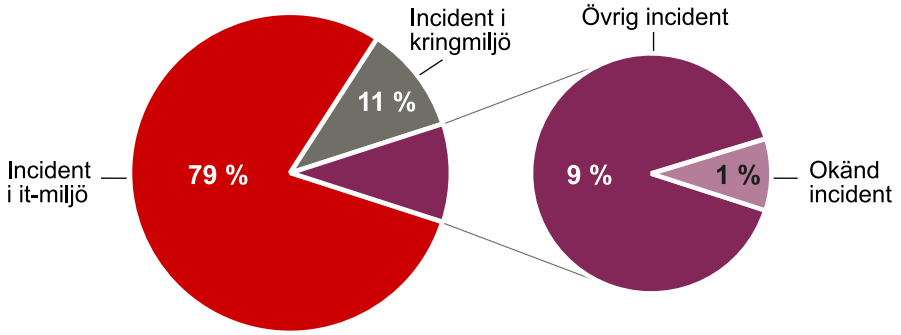
17. Karin Lindström, Computer Sweden. *Efter cyberattacken: Härjedalens kommun kämpar med att återställa it-systemen.* https://computersweden.idg.se/2.2683/1.780708/efter-cyberattacken-harjedalens-kommun-kampar-med-att-aterstalla-it-systemen (Hämtad 02–2024).

18. Alice Aveshagen och Johan Carlström, Svenska Dagbladet. *Kyrkan: ”Kan inte veta vad de fått fram”.* https://www.svd.se/a/0QmbAG/it-attacken-mot-svenska-kyrkan-personuppgifter-lackte (Hämtad 02-2024)

19. SVT. *Coop-anställda hängs ut på darknet efter cyberattack.* https://www.svt.se/nyheter/lokalt/varmland/coop-anstallda-hangs-ut-pa-darknet-efter-cyberattack (Hämtad 02-2024).

20. Katarina Lagerwall, Dagens nyheter. *Svenska Kyrkans hemsida uppe igen efter hackerattack*. https://www.dn.se/direkt/2024-01-23/svenska-kyrkans-hemsida-uppe-igen-efter-hackerattack/ (Hämtad 02–2024).

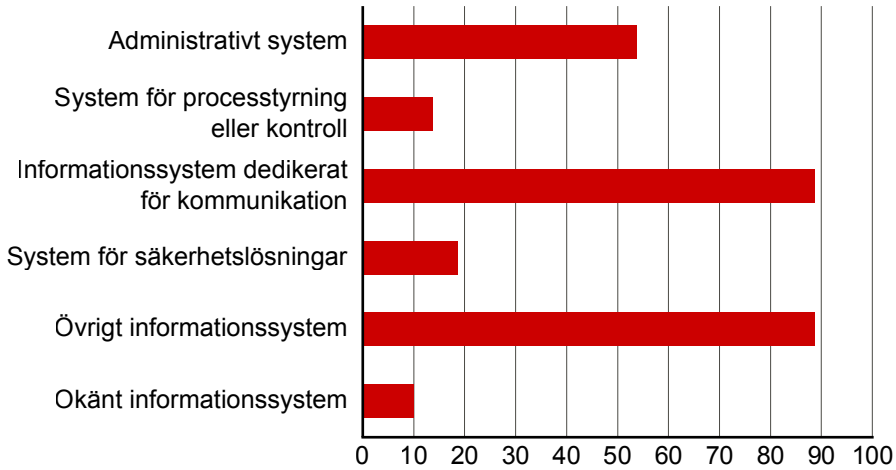
Diagram 7. Typ av it-incident under 2023



Cirkeldiagram som redogör för andelen it-incidentersom inträffat inom it-miljön respektive kringmiljön. De som rapporterat att incidenten inträffat i en övrig eller okänd miljö, vilket tillsammans motsvarar tio procent av it-incidentrapporterna, redovisas i det högra cirkeldiagrammet. I 25 av de inkomna it-incident-rapporterna har frågan inte besvarats och underlaget bygger således på totalt 309 it-incidentrapporter.

Som framgår i *Diagram 7* har 79 procent av it-incidenterna år 2023 sitt ursprung inom it-miljön, det vill säga inom ett informationssystem eller andra it-komponenter. Elva procent av it-incidenterna har inträffat i kringmiljön och resterande tio procent uppges ha inträffat i en övrig eller okänd miljö. Kringmiljön inkluderar infrastruktur såsom exempelvis förbindelser, lokaler och energiförsörjningen. När en it-incident har inträffat i kringmiljön har detta oftast orsakats av att en förbindelse upphört, ofta i samband med att en fiberkabel av misstag har skadats vid ett grävarbete. Det är mycket sällan som det inkommer rapporter som beskriver att infrastruktur skadats till följd av sabotage och ännu mer ovanligt, som tidigare framkommit, att det orsakats av en naturhändelse.

Diagram 8. Typ av informationssystem som påverkats när it-incidenten inträffat i ett informationssystem 2023



Liggande stapeldiagram som redogör för vilken typ av informationssystem som påverkats när it-incidenten inträffat i ett informationssystem. Kategorier som informationssystem är uppdelade i inkluderar Administrativt system, System för processtyrning eller kontroll, Informationssystem dedikerat till kommunikation, system för säkerhetslösningar, övrigt informationssystem och/eller okänt informationssystem. Rapportör kan ange fler än en typ av informationssystem.

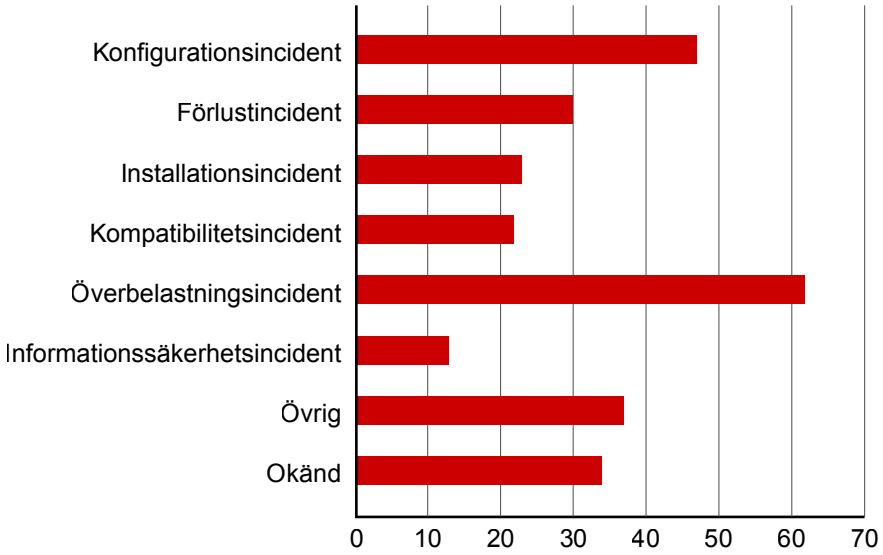
Som *Diagram 8* visar så har sammanlagt har incidenten uppgetts inträffat, och därav påverkat, ett informationssystem dedikerat till kommunikation i 89 fall. Det motsvarar drygt 36 procent av de it-incidenter som inträffat inom it-miljön. Det kan röra sig om både informationssystem dedikerat specifikt till extern

kommunikation, såsom konton på sociala medier, men även e-post och lösningar för säker kommunikation internt. Lika många har angett att ett ”övrigt” informationssystem påverkats. Med ”övrigt” menas ett informationssystem som inte specificerats bland de andra svarsalternativen som redogörs för i diagrammet. Statliga myndigheter står för en majoritet av it-incidenter där ett sådant informationssystem angetts. Det handlar ofta om att det påverkat webbsidor eller e-tjänster som används för specifika syften alternativt organisationens VPN-lösning.

Därefter har rapportörer i 54 fall (22 procent) uppgett att incidenten inträffat i ett administrativt system. Det inkluderar exempelvis system för lön- och personalhantering samt schemaläggning. När en NIS-leverantör rapporterat att ett administrativt system har påverkats rör det sig ofta om ett journalsystem, något som reflekterar det faktum att majoriteten av it-incidenter rapporteras av aktörer inom hälso- och sjukvårdssektorn.

Det är mindre vanligt att it-incidenten inträffat inom ett informationssystem för säkerhetslösningar eller processtyrning. 19 rapportörer har uppgett att it-incidenten inträffat och påverkat ett system för säkerhetslösningar medan endast 14 har uppgett ett system för processtyrning och kontroll. En stor majoritet av dessa har rapporterats av NIS-leverantörer. När ett system för processtyrning och kontroll angetts är det framförallt ett system för övervakning, och inte processen i sig, som påverkats. Ett sådant scenario beskrivs ofta av leverantörer av dricksvatten och transport. Det innebar i de flesta fall att leverantören varit tvungen att vidta reservrutiner för att garantera säkerheten, men att den samhällsviktiga tjänsten fortsatt kunde levereras under störningen.

Diagram 9. Typ av it-incident som inträffat när it-incidenten inträffat i ett informationssystem 2023



Liggande stapeldiagram som redogör för vilken typ av it-incident som har uppstått när incidenten inträffat i ett informationssystem. Inkluderade kategorier är Konfigurationsincident, Förlustincident, Installationsincident, Kompatibilitetsincident, Överbelastningsincident, Informationssäkerhetsincident, Övrig incident och eller Okänd incident. Av de 246 rapportörer som angett att it-incidenten inträffat inom it-miljön är det totalt 240 som besvarat frågan. Ett antal rapportörer har angett mer än en kategori.

När it-incidenten inträffat inom ett informationssystem uppges det oftast ha inträffat på grund av en överbelastnings- eller konfigurationsincident. Som redogörs i *Diagram 9* uppges 62 it-incidenter ha inträffat som konsekvens av ett informationssystem blivit överbelastat. Det gör att 25 procent av de it-incidenter med ursprung

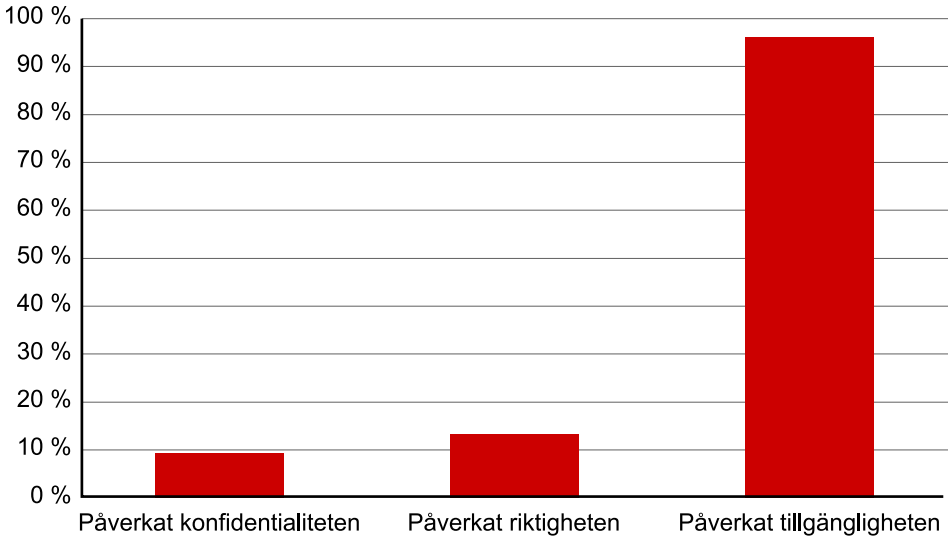
inom it-miljön har orsakats av en överbelastning. Det näst vanligaste är att it-incidenten orsakats av en felkonfiguration (47 fall). 37 rapportörer har uppgett att it-incidenten har en annan, övrig orsak, som inte specificeras i de svarsalternativ som redogörs för i diagrammet.

Majoriteten av överbelastningsincidenterna går att koppla till de överbelastningsangrepp som rapporterats av statliga myndigheter under inledningen av året. Fördelningen skiljer sig från tidigare år då både konfigurationsincidenter, förlustincidenter och installationsincidenter förekom oftare än överbelastningsincidenter. Likt föregående år är det dock få som rapporterat händelsen som en informationssäkerhetsincident. Det innebär att incidenten sällan bedömts vara kopplad till att information går förlorad, ändras eller blir tillgänglig för obehöriga.

It-miljöpåverkan

De flesta it-incidenter som rapporteras till MSB resulterar i att delar av organisationens it-miljö påverkas negativt. En it-incident kan resultera i it-miljöpåverkan om händelseförloppet inte kan mitigeras och eventuellt bortfall kompenseras för. Incidenten kan då resultera i att tillgängligheten, riktigheten eller konfidentialiteten inom ett informationssystem påverkas negativt. Det kan i nästa led få negativa följdeffekter för den drabbade organisationen.

Diagram 10. Andel inrapporterade it-incidenter 2023 som påverkat tillgängligheten, riktigheten eller konfidentialiteten inom ett informationssystem



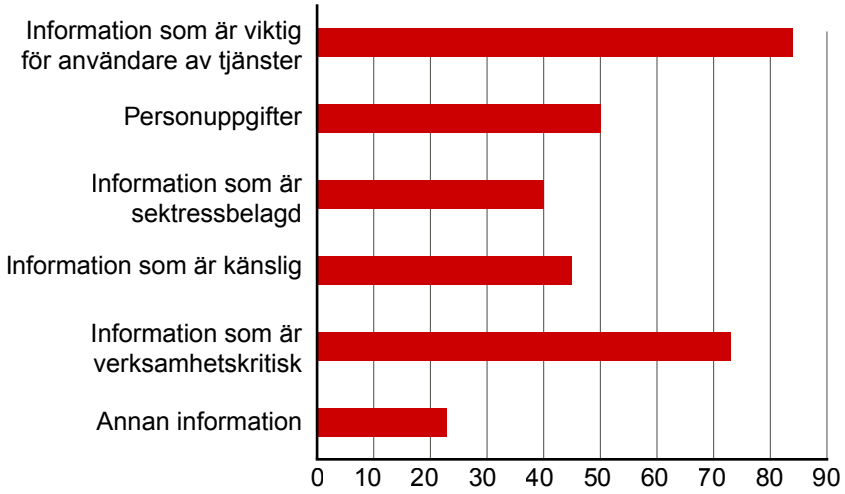
Stapeldiagram som redogör för andelen it-incidenter som påverkat tillgängligheten, riktigheten respektive konfidentialiteten inom ett informationssystem. Rapportören kan ha svarat att fler än ett av värdena har påverkats. Frågan har lämnats obesvarad i 33 it-incidentrapporter och statistiken bygger således på 301 fall.

Diagram 10 visar att det absolut vanligaste är att den rapporterade it-incidenten påverkat tillgängligheten till eller inom ett informationssystem. Informationssystemets riktighet och konfidentialitet uppgavs endast ha påverkats i tolv respektive åtta procent av fallen. Att tillgängligheten påverkas kan bestå i allt från långa svarstider och kortare avbrott till längre, mer omfattande och långvariga effekter. Störningar i tillgängligheten är den vanligaste formen av påverkan bland både statliga myndigheter och NIS-leverantörer. I de flesta fall består störningen under en kortare tid med begränsad påverkan på organisationen. I samband med

det höga antalet överbelastningsangrepp som utfördes under första halvan av året var det flera myndigheter, och andra organisationer, vars webbsidor blev otillgänglig under kortare perioder.

Konsekvensen av att tillgängligheten till eller inom ett informationssystem påverkas är att organisationen förlorar tillgången till funktioner och information som är viktig för deras verksamhet eller på annat sätt känslig. I cirka 43 procent av alla it-incidentrapporter har rapportören angett att it-incidenten har påverkat organisationens information. Oftast handlar det om att information blivit otillgänglig i samband med ett avbrott i ett informationssystem. Cirka 11 procent har svarat att det är okänt om information har påverkats och resterande och 46 procent har angett att informationstillgångar inte har påverkats.[21]

Diagram 11. Typ av påverkade informationstillgångar under 2023.



Liggande stapeldiagram som redogör för antalet it-incidenter som uppges ha påverkat olika informationskategorier. Ett stort antal har svarat att mer än en form av information har påverkats.

I majoriteten av it-incidentrapporter där information påverkats har rapportören uppgett att det rör sig om mer än en typ av information. Som redogörs för i *Diagram 10* är det vanligast att det rör sig om information som är viktig för användare av organisationens tjänster och verksamhetskritisk information. Dessa typer av informationstillgångar har vardera påverkats i mer än en femtedel av rapporterade it-incidenter. Att information som är viktig för organisationens funktionalitet ofta drabbas visar på vikten av att organisationer arbetar aktivt med kontinuitetsplanering. Minst antal rapportörer har angett att it-incidenten påverkat ”annan information” än de kategorier i diagrammet.

Samhällspåverkan

Det digitala samhället kan beskrivas som relativt redundant utifrån bemärkelsen att det ofta finns fler leverantörer av en digital tjänst. Samma tjänster kan generellt levereras av andra i händelse av att en fallerar eller blir komprometterad. Att en samhällsviktig aktör på grund av en inträffad it-incident inte längre kan leverera

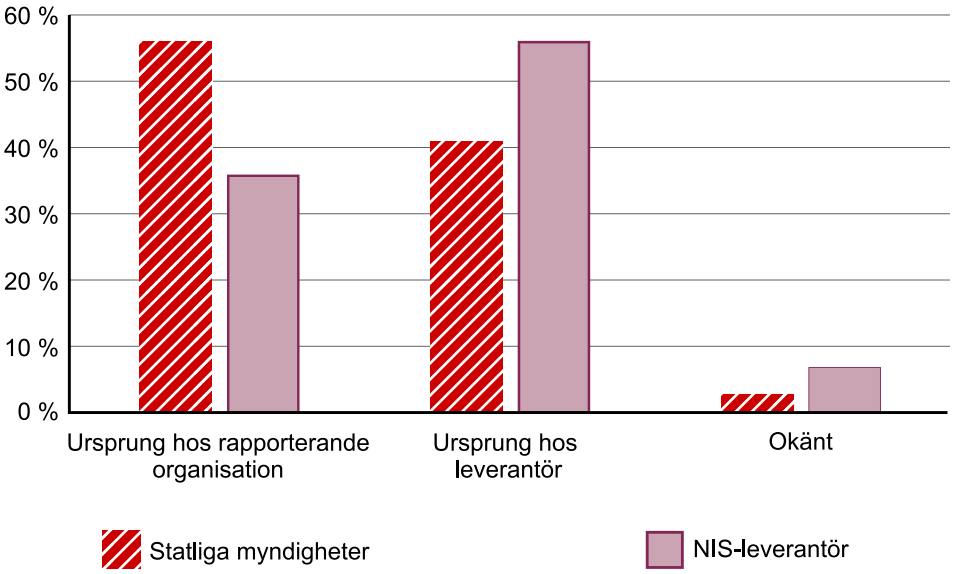
21. I 23 it-incidentrapporter har frågan lämnats obesvarad. Underlaget utgörs därmed av totalt 313 it-incidentrapporter.

sin tjänst innebär således inte nödvändigtvis att följande störning kommer att få samhällspåverkan. Betalsystemet kan sägas exemplifiera denna strukturella redundans då betalningar som inte kan genomföras via en aktörs tjänster ofta kan genomföras via en annan vid en eventuell störning, även långvariga sådana.

Det finns dock situationer då en eller flera it-incidenter, trots en generellt redundant infrastruktur, kan få samhällskonsekvenser. Generellt kan en it-incident resultera i samhällspåverkan om den (i) påverkar en samhällsviktigtjänst som levereras till andra negativt och (ii) denna tjänst i sin tur inte kan levereras alls, eller med samma kvalitet, av andra. I dessa fall kan ett så kallat monoberoende i den digitala leveranskedjan sägas ha etablerats. Monoberoenden kan uppstå inom en eller flera segment av den digitala leveranskedjan och därmed vara ett problem som uppstår nära eller mer avlägset slutanvändaren. MSB bedömer att incidenter som uppstår i digitala leveranskedjor som försörjer samhällsviktig verksamhet, och som besitter monoberoenden, är den typ av it-incidenter som kan leda till mest omfattande samhällspåverkan. I föregående årsrapport *När kriget kom nära*[22] efterlyste MSB ett uppdrag att kartlägga monoberoenden som kan påverka samhällsviktig verksamhet.

Det framkommer i it-incidentrapporteringen att det är mycket sällan it-incidenter som påverkar rapporteringspliktiga aktörer får samhällskonsekvenser i enlighet med beskrivningen ovan. De flesta incidenter som resulterar i organisationspåverkan påverkar sällan leveransen av den samhällsviktiga tjänsten i någon större utsträckning under längre perioder. Det är ännu mer sällan som it-incidenter påverkar ett stort antal leverantörer av samhällsviktiga tjänster på samma gång. Samtidigt är det vanligt att rapporteringspliktiga it-incidenter inträffar till följd av en incident hos en leverantör.

Diagram 12. Andel inrapporterade it-incidenter 2023 som inträffat hos en leverantör åt rapporterade organisation – Statliga myndigheter och NIS-leverantörer.



Stapeldiagram som beskriver andelen rapporter där incidenten uppges ha sitt ursprung hos en leverantör, hos den egna organisationen respektive ha ett okänt ursprung. Myndigheter respektive NIS-leverantörer redogörs för separat. Frågan har besvarats av alla NIS-leverantörer men endast i 171 av 198 incidentrapporter mottagna av myndigheter.

22. *När kriget kom nära: Årsrapport it-incidentrapportering 2022*. https://rib.msb.se/filer/pdf/30339.pdf (Hämtad: 02–2024).

Som *Diagram 12* visar har en majoritet, totalt 56 procent, av it-incidenter som rapporterats av NIS-leverantörer sitt ursprung hos en leverantör till den rapporterande organisationen. För statliga myndigheter är siffran lägre, men omfattar ändå cirka 41 procent av alla rapporterade it-incidenter.

Att it-incidenter hos NIS-leverantörer ofta har sitt ursprung hos en leverantör kan ha flera förklaringar. Då majoriteten av dessa it-incidenter rapporteras av aktörer inom hälso- och sjukvårdssektorn skulle det potentiellt kunna påvisa att det inom sektorn finns en bristande redundans vid händelse av avbrott i utkontrakterade tjänster. Förklaringen skulle således vara att det är vanligare att incidenter som uppstår hos en leverantör till rapporterande organisation blir rapporteringspliktiga. Det är något som på en strukturell nivå skulle kunna utgöra en betydande risk i händelse av att en it-incident påverkar flertalet mottagare av en tjänst inom hälso- och sjukvårdssektorn. En annan potentiell förklaring, kopplat till att MSB bedömer att det finns ett större mörkertal, skulle kunna vara att en it-incident med sitt ursprung hos en leverantör till rapporterande organisation upplevs vara mindre känsliga att rapportera.

Cyberangrepp mot larmleverantör

I början av 2023 uppstod en storskalig incident till följd av ett cyberangrepp mot en larmleverantör inom hälso- och sjukvårdssektorn. Leverantören, Careium, har en stor marknadsandel och levererar trygghetslarm som används av hemtjänster i drygt häften av alla Sveriges kommuner. Cyberangreppet gjorde att larmtjänsten blev otillgänglig och därmed att brukare inte längre kunde larma sjukvården som vanligt om en händelse skulle uppstå. Störningen påverkade ett stort antal verksamheter som fick övergå till reservrutiner. Sammanlagt påverkades cirka 100 000 trygghetslarm under tiden för störningen.[23]

Som tidigare poängterat har antalet it-incidenter som rapporterats från hälso- och sjukvårdssektorn ökat med närmare 70 procent i jämförelse med föregående år. 30 procent av alla it-incidenter rapporterade av aktörer från hälso- och sjukvårdssektorn bedöms ha en betydande eller en viss påverkan på människors hälsa. Därtill är det 34 procent av NIS-leverantörer, varav majoriteten utgör aktörer inom hälso- och sjukvårdssektorn, som bedömer att störningen haft en betydande eller viss påverkan på förtroendet för den samhällsviktiga tjänsten.[24] Då informationen behöver förmedlas till MSB i ett tidigt skede (6 timmar efter det att it-incidenten identifierats som rapporteringspliktig) ger svaret på frågan huruvida störningen påverkat människors liv och hälsa ofta uttryck för en uppfattad risk istället för något inträffat. Det indikerar oavsett att flera aktörer inom hälso- och sjukvårdssektorn under 2023 upplevt att det funnits en betydande eller viss risk för liv och hälsa i samband med att organisationen behövt övergå till reservrutiner och alternativ drift.

23. Dagens samhälle, *It-attack slog ut 100 000 trygghetslarm*, https://www.dagenssamhalle.se/samhalle-och-valfard/digitalisering/it-attack-slog-ut-100-000-trygghetslarm/ (Hämtad: 02–2024).

24. Rapportör kan ange att störningen resulterat i i) en betydande, ii) en viss, iii) en liten eller iv) ingen påverkan på *människors liv och hälsa* respektive *förtroende för den samhällsviktiga tjänsten*. Ett tredje skyddsvärde som inkluderas i formulären är användares ekonomi. Det är dock endast cirka 1 procent av rapporterade it-incidenter som har resulterat i en sådan störning.

Tema: EU förändrar cybersäkerhets-området

Tema: EU förändrar cybersäkerhetsområdet

EU har aviserat nya regleringar och andra satsningar med bäring på informations- och cybersäkerhetsområdet under de kommande åren. Redan idag har stora delar av den svenska regleringen på informations- och cybersäkerhetsområdet sitt ursprung i EU-reglering. Förståelse för hur dessa regleringar påverkar organisationer i Sverige gör det enklare att möta kraven som ställs och att hitta rätt stöd.

Nya EU-regleringar och andra satsningar med bäring på informations- och cybersäkerhetsområdet förväntas påverka såväl svensk som europeisk säkerhet i stor utsträckning. I det här kapitlet inkluderas i) en introduktion till några av de EU-regleringar som MSB bedömer redan har eller kommer att få stor betydelse inom området, ii) en översikt över vilka organisationer som kommer att omfattas av de olika regleringarna och slutligen iii) en analys av hur regleringarna kan komma att påverka organisationer och Sverige i stort.

EU-regleringar översikt

Under de kommande åren görs en tydlig prioritering inom EU för att stärka unionen som en säkerhetspolitisk aktör, främja en säker digitalisering och minska sårbarheter i samt säkerställa kontinuiteten i samhällsviktiga tjänster. Frågorna drivs som en del i Europas ”digitala agenda” i syfte att stärka EU:s digitala suveränitet. Som en del i detta har EU-kommissionen lagt fram en mängd olika initiativ med fokus på stärkt informations- och cybersäkerhet, samt ökad konkurrenskraft.

EU-reglering tas fram gemensamt av EU:s medlemsstater. Nedan informationsruta beskriver de olika typerna av reglering som EU kan anta.[25]

25. Sveriges Riksdag. EU:s lagar och regler. https://www.riksdagen.se/sv/sa-fungerar-riksdagen/sa-fungerar-eu/en-eu-lag-blir-till/eus-lagar-och-regler/#olika-typer-av-eu-regler-00 (Hämtad 02/2024) och EU, Typer av EU-rättsakter, https://commission.europa.eu/law/law-making-process/types-eu-law_sv#types-of-eu-legal-acts (Hämtad 03/2024).

Om EU:s reglering

Förordning

En EU-förordning är reglering som gäller enhetligt i alla EU-länder och börjar gälla direkt i medlemsstaterna när den har trätt i kraft. Förordningar införs inte i svensk lagstiftning, men ibland kan en svensk lag behöva ändras eller kompletteras för att det inte ska bli en regelkrock när en förordning börjar gälla.

Direktiv

Ett EU-direktiv är en EU-rättsakt som sätter upp ett mål som ska uppnås, ett slags ramlagstiftning. Medlemsländerna avgör sedan själva vilka åtgärder som ska vidtas för att målet ska uppnås. I Sverige stiftar riksdagen de lagar som krävs för att nå målet. När den svenska lagstiftningen är anpassad till direktivet anmäler regeringen det till EU-kommissionen. Medlemsländerna har ofta två år på sig att implementera ett direktiv i svensk lagstiftning.

Beslut

Ett EU-beslut riktar sig ofta speciellt till en eller flera personer, företag eller organisationer. Därför lämpar de sig bäst för administrativa syften eller för att genomföra lagar som redan finns. Beslut används till exempel ofta inom EU:s konkurrenslagstiftning och kan då vända sig till företag. Det är bindande för den eller dem beslutet riktar sig till.

Rekommendationer och yttranden

Rekommendationer och yttranden från EU är inte bindande rättsakter. I en rekommendation föreslår en EU-institution förändringar för en annan institution eller för medlemsländerna. Ministerrådet ger till exempel EU-länderna rekommendationer som gäller ländernas ekonomiska politik. I ett yttrande kan EU-institutionerna uttala sig om en aktuell situation eller ärende.

En rättsakt som inte är bindande behöver inte följas av medlemsländerna. Men rättsakten kan få följder ändå. Det kan till exempel vara att EU-domstolen använder den som stöd vid tolkning av EU-rätten.

Genomförandeakter

Genomförandeakter ska säkerställa att EU:s rättsakter tillämpas på samma sätt i hela EU. Men på områden där det krävs enhetliga villkor för att genomföra reglerna antar kommissionen en genomförandeakt i samråd med en kommitté, där alla EU-länder är representerade. Det här kallas kommittéförfarandet och är till för att EU-länderna ska kunna kontrollera kommissionens genomförandebefogenheter. Uppdraget till kommissionen att ta fram genomförandeakter ges av Europaparlamentet och rådet i en rättsakt, exempelvis ett direktiv.

Delegerade akter

Delegerade akter kompletterar eller ändrar befintlig lagstiftning för att lägga till nya mindre väsentliga bestämmelser. Den delegerade akten får inte ändra väsentliga delar av grundrättsakten. Grundrättsakten måste ange mål, innehåll, omfattning och varaktighet för delegeringen. Europaparlamentet och rådet kan återkalla delegeringen eller göra invändningar mot en delegerad akt. Kommissionen föreslår och antar delegerade akter efter samråd med expertgrupper av företrädare från alla EU-länder.

Nedan presenteras en översikt av gällande EU-regleringar och regelverk som antingen börjar direkt gälla i Sverige (EU-förordningar) eller ska implementeras i svensk lagstiftning (EU-direktiv) under 2024 eller 2025. Vissa av de kommande regleringarna är fortfarande under förhandling. Med de nya EU-regleringarna tillkommer nya myndighetsroller och samverkansformer. EU väljer även i många fall att ge existerande myndighetsroller nya eller utvidgade uppgifter.[26] Tabellen ger även en översiktlig redogörelse för dessa.

26. Exempelvis ges den nationella CISRT-enheten som etablerades genom NIS-direktivet, ett utvidgat uppdrag genom både NIS2-direktivet och DORA-förordningen.

Gällande regleringar

Dataskyddsförordningen (GDPR)

Reglering och tidsram

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) även förkortad GDPR. GDPR började gälla i Sverige den 25 maj 2018.

Vad innebär det?

Förordningen reglerar behandlingen av personuppgifter och utgör grunden för skyddet för fysiska personers integritet vid behandling av personuppgifter inom unionen. En grundläggande princip är att personuppgifter endast får behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. GDPR ställer även krav på att den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta lämpliga tekniska och organisatoriska åtgärder vid behandling av personuppgifter för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.[27] I det fall regleringen inte efterlevs innebär GDPR en möjlighet att utdöma administrativa sanktionsavgifter på upp till 10 000 000 EUR eller, om det gäller ett företag, på upp till 2 procent av den totala globala årsomsättningen under föregående budgetår.[28]

Myndighetsroller och samverkan

Efterlevnaden omfattas av tillsyn som i Sverige utförs av Integritetsskyddsmyndigheten (IMY).

Tillsynsmyndigheterna ska övervaka tillämpningen av bestämmelserna i denna förordning och bidra till att tillämpningen blir enhetlig över hela unionen. För detta ändamål ska medlemsstaternas tillsynsmyndigheter samarbeta såväl sinsemellan som med kommissionen.

NIS-direktivet

Reglering och tidsram

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. NIS-direktivet[29] implementerades i svensk lagstiftning den 1 augusti 2018 genom lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster samt tillhörande förordning och myndighetsföreskrifter. Kommer att ersättas av NIS2-direktivet.

Vad innebär det?

Direktivet innebär både krav på medlemsstaterna och leverantörer av samhällsviktiga[30] respektive digitala tjänster[31] i medlemsstaterna. Medlemsstaterna är bland annat skyldiga att ha en nationell strategi för säkerhet i nätverks- och informationssystem, att utse tillsynsmyndigheter och en nationell kontaktpunkt för samordning och gränsöverskridande samarbete.

Medlemsstaterna ska även ha en organisation för hantering av it-incidenter och lämna en rapport till EU-kommissionen över inrapporterade it-incidenter.

Medlemsstater ska därför säkerställa att de har väl fungerande nationella CSIRT-enheter.[32] Den nationella CSIRT-enheten ska samverka med unionens CSIRT-nätverk.

---

27. Artikel 32 GDPR.

28. Artikel 83 GDPR.

29. Namnet NIS-direktivet kopplar till EU-direktivets engelska namn Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

30. De sju sektorerna är: bankverksamhet, digital infrastruktur, energi, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten och transport.

31. Med digitala tjänster avses internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster.

32. Dessa kallas även för incidenthanteringsorganisationer, Computer Emergency Response Teams, (CERT).

Leverantörer av samhällsviktiga och digitala tjänster omfattas av tillsyn och är skyldiga att vidta olika säkerhetsåtgärder för sådana nätverk och informationssystem som de använder för sin samhällsviktiga eller digitala tjänst. De ska även rapportera incidenter som påverkar säkerheten i nätverken och informationssystemen.

I Sverige har direktivet implementerats genom lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, samt förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. I lagen ställs krav på leverantörer av samhällsviktiga och digitala tjänster och förordningen specificerar myndighetsroller och uppgifter med mera närmare. Utöver lag och förordning ges i myndighetsföreskrifter från MSB närmare regler om vilka tjänster som omfattas, vilka incidenter som ska rapporteras och hur systematiskt informationssäkerhetsarbete ska bedrivas och i myndighetsföreskrifter från tillsynsmyndigheterna och Socialstyrelsen närmare regler om vilka säkerhetsåtgärder som ska vidtas.

Myndighetsroller och samverkan

Energimyndigheten, Finansinspektionen, Inspektionen för vård och omsorg, Livsmedelsverket, Post- och telestyrelsen och Transportstyrelsen har som behöriga myndigheter i NIS i uppgift att utöva tillsyn över respektive sektor samt mandat att utfärda föreskrifter rörande säkerhetsåtgärder.

MSB som nationell kontaktpunkt har en samordnande roll kopplat till regleringen som bland annat innefattar föreskriftsrätt för identifiering av samhällsviktiga tjänster, systematiskt informationssäkerhetsarbete och incidentrapportering, men ska även samordna det nationella arbetet. Den nationella kontaktpunkten samverkar med motsvarande kontaktpunkter i andra medlemsstater i NIS Cooperation Group och dess undergrupper. MSB representerar även Sverige i nätverket för cyberkriser EU-CyCLONe.

CERT-SE hos MSB är Sveriges nationella CSIRT-enhet och mottar incidentrapporter samt stödjer leverantörer av samhällsviktiga och digitala tjänster vid incidenter. CSIRT-enheten samverkar med motsvarande funktioner i andra medlemsstater i CSIRT-nätverket.

Cybersäkerhetsakten

Reglering och tidsram

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten). Cybersäkerhetsakten började gälla i Sverige den 28 juni 2021.Tillägg i Cybersäkerhetsakten förhandlas för närvarande, se avsnitt nedan under rubriken ”Regleringar som förhandlas”.

Vad innebär det?

Cybersäkerhetsakten har som mål att säkerställa en väl fungerande inre marknad genom att främja cyberresiliens, säkerhet och förtroende genom att inrätta ett ramverk för cybersäkerhetscertifiering i fråga om att säkerställa en tillfredsställande nivå av cybersäkerhet för IKT-produkter, IKT-tjänster och IKT-processer i unionen.

EU-förordningen kan sägas ha två huvuddelar. Det handlar om att

1. stärka Enisas, den europeiska cybersäkerhetsbyrån, mandat och tydliggöra dess uppdrag,[33] samt
2. etablera ett nytt ramverk för cybersäkerhetscertifiering och att utveckla certifieringsordningar avseende cybersäkerheten i kommersiella IT-produkter och IT-tjänster. Sådana produkter och tjänster kan därefter certifieras mot dessa krav.

Syftet med ramverket för cybersäkerhetscertifiering är att säkerställa en tillfredsställande nivå i fråga om cybersäkerhet för informations- och kommunikationsteknik (IKT) i unionen samt att undvika en fragmentering av den inre marknaden när det gäller certifieringsordningar i unionen. Skapandet av europeiska ordningar för cybersäkerhetscertifiering kommer att medföra att certifikat som utfärdas enligt dessa certifieringsordningar blir giltiga och erkända i alla medlemsstater.

33. Enisa ska bland annat att stödja nationella myndigheter och EU:s institutioner, organ och byråer i arbetet med att förbättra cybersäkerheten, tjäna som referenspunkt för vetenskaplig och teknisk rådgivning och sakkunskap om cybersäkerhet.

Medlemsstaterna ska utse en eller flera nationella myndigheter för cybersäkerhetscertifiering med tillräckliga resurser och befogenheter för att övervaka, kontrollera och verkställa reglerna för de europeiska certifieringssystemen, exempelvis så att de som utfärdar certifikat enligt de europeiska certifieringsordningarna gör det på ett korrekt sätt.

Det är frivilligt för tillverkare eller leverantörer av IKT-produkter, IKT-tjänster eller IKT-processer att certifiera sina tjänster eller produkter enligt cybersäkerhetsakten men det finns exempelvis möjlighet enligt NIS2-direktivet för både medlemsstater och kommissionen kräva certifiering för vissa produkter och tjänster i vissa verksamheter, till exempel viss samhällskritisk verksamhet.[34]

Myndighetsroller och samverkan

I Sverige är Försvarets materielverk (FMV) nationell myndighet för cybersäkerhetscertifiering.[35] Inom FMV är det Inspektionen för cybersäkerhetscertifiering, ICC som utför tillsyn[36] och som bland annat representerar Sverige i Europeiska kommissionens rådgivande grupp European Cybersecurity Certification Group, ECCG.

Vid FMV finns även Sveriges Certifieringsorgan för IT-säkerhet, CSEC,[37] som har uppdrag kopplade till certifiering enligt vissa internationella samarbeten samt medverkar i arbetet med FMV:s uppdrag enligt EU:s cybersäkerhetsakt.

CCCN-förordningen

Reglering och tidsram

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum. CCCN-förordningen[38] började gälla i Sverige den 28 juni 2021.

Vad innebär det?

EU-förordningen reglerar och beskriver huvudsakligen tre delar i ett ekosystem för cybersäkerhetsforskning, innovation och kapacitetsutveckling inom EU:

- ett europeiskt kompetenscentrum för cybersäkerhet, ECCC;
- ett nätverk av nationella samordningscentrum;
- en europeisk kompetensgemenskap.

ECCC, som är ett EU-organ i Bukarest, utformar och genomför cybersäkerhetsutlysningar inom forsknings- och innovations-programmet Horizon Europe och tillämpningsprogrammet Digital Europe samt leder nätverket av nationella samordningscenter och den europeiska kompetensgemenskapen bestående av behovsägare, forskare och leverantörer inom cybersäkerhet.

Myndighetsroller och samverkan

Det svenska nationella samordningscentret (NCC-SE) är etablerat hos MSB.[39] NCC-SE ska främja de europeiska cybersäkerhetsprogrammen, ge rådgivning till aktörer i Sverige gällande EU:s cybersäkerhetsprogram, främja kompetensutveckling, skapa synergier med policyutveckling i medlemsstaten, samverka med europeiska digitala innovationshubbar (EDIH), samt följa upp och synliggöra EU-finansierade projekt. NCC-SE samordnar bland annat den svenska kompetensgemenskapen Cybernode.se som i sin tur ingår i en europeisk kompetensgemenskap. Cybernoden är en plattform där akademin, näringslivet och offentlig sektor bygger upp samarbeten med målsättningen att initiera forskning och innovation inom cybersäkerhet.

---

34. Artikel 24 NIS2-direktivet.
35. https://www.fmv.se/verksamhet/ovrig-verksamhet/ncca/ (Hämtad 02–2024).
36. https://www.fmv.se/verksamhet/ovrig-verksamhet/icc/ (Hämtad 02–2024).
37. https://www.fmv.se/english/supplier-information/csec/ (Hämtad 02–2024).
38. Namnet CCCN-förordningen kopplar till förordningens engelska namn Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.
39. Regeringen gav MSB i uppdrag att i samverkan med Vinnova och DIGG, inrätta ett nationellt samordningscenter för cybersäkerhetsforskning och innovation.

Regleringar som antingen börjar gälla direkt i Sverige (EU-förordningar) eller ska implementeras i svensk lagstiftning (EU-direktiv) under 2024 eller 2025

NIS2-direktivet

Reglering och tidsram

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet). Ersätter det första NIS-direktivet och ska ha implementerats av medlemsstaterna senast den 17 oktober 2024 och börja tillämpas den 18 oktober 2024.[40]

Vad innebär det?

NIS2-direktivet har samma övergripande syfte som det första NIS-direktivet, det vill säga att uppnå en hög gemensam cybersäkerhetsnivå inom unionen för att förbättra den inre marknadens funktion. NIS2-direktivet utvecklar och skärper NIS-regleringen och ska dessutom implementeras samordnat med CER-direktivet[41] vilket säkerställer ett allriskperspektiv.

I NIS2-direktivet ställs, precis som i NIS-direktivet, krav på att medlemsstaterna antar nationella strategier[42] för cybersäkerhet och utser behöriga myndigheter för bland annat tillsyn, en gemensam kontaktpunkt med samordningsuppgifter och en CSIRT-enhet för hantering av it-säkerhetsincidenter. En ny roll som följer av NIS2 är dock att medlemsstaterna ska utse en cyberkrishanteringsmyndighet, EU-nätverket för cyberkriser EU-CyCLONe formaliseras och varje medlemsstat ska ha en nationell cyberkrishanteringsplan.

Dessutom ges CSIRT-enheten ytterligare uppgifter för att stödja verksamhetsutövare som omfattas av regleringen och nya verktyg, såsom proaktiv skanning.[43] CSIRT-enheten ska också samordna rapporteringar av sårbarheter.[44]

Genom NIS2-direktivet utvidgas regleringen till att gälla fler verksamhetsutövare[45] och kraven vad gäller vilka säkerhetsåtgärder som ska vidtas respektive hur och när incidenter ska rapporteras specificeras i direktivet i syfte att få en mer ensad implementering i medlemsstaterna. Bland annat ställs uttryckliga krav på säkerhet i leveranskedjor.[46] En annan skillnad mot NIS-direktivet är istället för att endast gälla de nätverk och informationssystem som användes för den samhällsviktiga eller digitala tjänsten som omfattades av regleringen gäller nu NIS2-direktivet för hela organisationen hos de verksamhetsutövare som omfattas. Dessutom har sanktionsavgifterna justerats på ett sådant sätt att de går i linje med de som kan aktualiseras vid bristande efterlevnad av GDPR, exempelvis kan vissa verksamhetsutövare vid brister påföras administrativa sanktioner på upp till 10 000 000 EUR eller högst 2 procent av den totala globala årsomsättningen under det föregående räkenskapsåret.[47] En annan nyhet är ett tydligare uttalat ansvar för ledningen att styra arbetet och utbilda sig samt en möjlighet för en tillsynsmyndighet att vid överträdelser och tillfälligt förbjuda en person på nivån verkställande direktör och motsvarande att utöva ledningsfunktion, en förutsättning är dock att andra åtgärder är ineffektiva.[48]

Direktivet är ett minimidirektiv så det står medlemsstater fritt att utvidga tillämpningsområdet.

---

40. Det kan noteras att pågående lagstiftningsprocess med stor sannolikhet inte kommer att hunnit slutföras i tid för att ny reglering ska börja tillämpas på utsatt tid, direktivet kommer troligtvis att implementeras i svensk lagstiftning under 2025.

41. Se nedan.

42. Varje medlemsstat ska anta en nationell strategi för cybersäkerhet som tillhandahåller strategiska mål, de resurser som krävs för att uppnå dessa mål och relevanta politiska och reglerande åtgärder, i syfte att uppnå och upprätthålla en hög cybersäkerhetsnivå.

43. Artikel 11 och artikel 23 NIS2-direktivet.

44. Artikel 12 NIS2-direktivet.

45. NIS2-direktivet gäller verksamhetsutövare inom sektorerna Energi, Transport, Bankverksamhet, Finansmarknadsinfrastruktur, Hälso- och sjukvård, Dricksvatten, Avloppsvatten, Digital infrastruktur, Förvaltning av IKT-tjänster (mellan företag), Offentlig förvaltning, Rymden, Post- och budtjänster, Avfallshantering, Tillverkning, produktion och distribution av kemikalier, Produktion, bearbetning och distribution av livsmedel, Tillverkning (medicinska produkter), Digitala leverantörer och Forskning som med några undantag, uppfyller vissa krav på storlek och omsättning.

46. Artikel 21, 22 och 23 NIS2-direktivet.

47. Artikel 34 NIS2-direktivet.

48. Artikel 20 och artikel 32 NIS2-direktivet.

Myndighetsroller och samverkan

Det är ännu inte klart hur den slutliga fördelningen av myndighetsroller och uppgifter kommer att utformas men MSB kommer sannolikt ha fortsatta samordningsuppgifter på nationell och EU-nivå som nationell kontaktpunkt, CERT-SE hos MSB fortsatt nationell CSIRT-enhet samt nuvarande tillsynsmyndigheter enligt NIS fortsatta tillsynsuppdrag. Det är dessutom sannolikt att ytterligare myndigheter tilldelas tillsynsuppdrag enligt NIS2. Utredningen om genomförande av NIS2- och CER-direktiven har lämnat förslag på implementering av NIS2-direktivet i sitt delbetänkande SOU 2024:18 Nya regler om cybersäkerhet.

Utöver att etablerade NIS-roller som nationell kontaktpunkt, behöriga myndigheter för bland annat tillsyn och CSIRT-enhet inrättas genom NIS2 en ytterligare roll som cyberkrishanteringsmyndighet.

CER-direktivet

Reglering och tidsram

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG. CER-direktivet[49] ska ha implementerats av medlemsstaterna senast den 17 oktober 2024 och börja tillämpas den 18 oktober 2024. (Det kan noteras att pågående lagstiftningsprocess med stor sannolikhet inte kommer att hunnit slutföras i tid för att ny reglering ska börja tillämpas på utsatt tid, direktivet kommer troligtvis att implementeras i svensk lagstiftning under 2025). Genom CER-direktivet upphävs ECI-direktivet.[50]

Vad innebär det?

Direktivet syftar till att hjälpa medlemsstaterna att öka kritiska entiteters övergripande motståndskraft och samtidigt stärka samordningen på unionsnivå med syftet att säkerställa ett oavbrutet tillhandahållande av tjänster som är väsentliga för ekonomin och samhället som helhet. CER-direktivet kan jämföras med NIS-direktivet avseende vilken potentiell skillnad det kommer att innebära för det nationella arbetet med motståndskraft i samhällsviktig verksamhet. CER-direktivet ska implementeras samordnat med NIS2-direktivet vilket säkerställer ett allriskperspektiv.

CER-direktivet innebär samtidigt krav på identifiering av sådana verksamhetsutövare som bedriver den typ av samhällsviktig verksamhet som omfattas av direktivet. De som omfattas ska vidta åtgärder som ska stärka deras motståndskraft och förmåga att tillhandahålla sina tjänster, samt rapportera incidenter. De omfattas även av tillsyn. De sektorer som omfattas av CER-direktivet överensstämmer i många delar med NIS2-sektorerna men är något färre.[51] Alla verksamhetsutövare som omfattas CER-direktivet omfattas också av kraven i NIS2-direktivet.

Direktivet är ett minimidirektiv så det står medlemsstater fritt att utvidga tillämpningsområdet.

Myndighetsroller och samverkan

Det är ännu inte klart hur den slutliga fördelningen av myndighetsroller och uppgifter kommer att utformas men precis som enligt NIS-regelverket ska det finnas behöriga myndigheter med tillsynsuppdrag respektive uppdrag att vara nationell kontaktpunkt. Ett ingångsvärde i pågående lagstiftningsprocess är att det bör vara samma tillsynsmyndigheter som ansvarar för tillsynen enligt NIS2. Utredningen om genomförande av NIS2- och CER-direktiven kommer att lämna förslag på implementering av CER-direktivet i sitt slutbetänkande vilket ska redovisas den 16 september 2024.

49. Namnet CER-direktivet kopplar till direktivets engelska namn Critical Entities Resilience Directive.

50. RÅDETS DIREKTIV 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (ECI-direktivet), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114.

51. De sektorer som omfattas av CER-direktivet är: Energi, Transport, Bankverksamhet, Finansmarknadsinfrastruktur, Hälso- och sjukvård, Dricksvatten, Avloppsvatten, Digital infrastruktur, Offentlig förvaltning, Rymden, Produktion, bearbetning och distribution av livsmedel .

DORA

Reglering och tidsram

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011. DORA[52] börjar gälla i Sverige den 17 januari 2025.

Vad innebär det?

Syftet med DORA är att stärka digital operativ motståndskraft inom EU:s finanssektor och dess kritiska IKT- (informations- och kommunikationsrelaterade) tjänster, genom att inrätta ökad robusthet, resiliens och redundans för informations- och cybersäkerhet inom finanssektorn.

Förordningen ställer krav på (den finansiella enhetens) ledningens ansvar för IKT-risker, vilket i sin tur ställer krav på organisation och ledningens kontroll över hur verksamheten hanterar risker och sårbarheter i sina system.

DORA kommer att gälla för organisationer som tillhandahåller revisionstjänster, försäkringstjänster, bank- och finanstjänster, kryptotjänster, värdepapperstjänster samt förtredjepartsleverantörer för IKT-tjänster. Dessa kallas för finansiella enheter. De finansiella enheterna omfattas av krav på dokumentation och förhållningssätt till ett IKT-riskramverk. I detta ramverk ingår strategier, processer, IKT-protokoll och verktyg som är nödvändiga för att säkerställa att all relevant infrastruktur, inklusive servrar, lokaler, datacenter och hårdvara, är tillräckligt skyddade för att förhindra fysisk skada eller obehörig åtkomst.

De finansiella enheterna ska även testa sina IKT-system, bland annat genom avancerade penetrationstester[53].

Idag incident rapporterar finansiella enheter till MSB i enlighet med NIS-direktivet. Vid ikraftträdandet av DORA behöver de finansiella enheterna endast rapportera incidenter till Finansinspektionen.

Myndighetsroller och samverkan

Finansinspektionen är behörig myndighet och har tillsyn över att finansiella entiteter följer bestämmelserna i förordningen. Finansinspektionen ska besluta om vilka finansiella entiteter som ska genomföra hotbildsstyrd penetrationstestning.[54] De beslutar även hur ofta en finansiell enhet ska genomföra sådan testning. Det är Riksbanken som övervakar och samordnar dessa tester.

Finansinspektionen ska samarbeta med andra relevanta instanser vid it-incidenter. Finansinspektionen ska anmäla allvarliga IKT-relaterade incidenter[55] till den nationella CSIRT-enheten och nationella kontaktpunkten på MSB i enlighet med NIS-direktivet, till den nationella dataskyddsmyndigheten IMY (Integritetsskyddsmyndigheten) och brottsbekämpande myndigheter.

52. Namnet är kopplat till förordningens engelska namn Digital Operational Resilience Act.

53. Avancerade penetrationstester innebär att en cyberattack under kontrollerade former simuleras mot en organisations anställda, processer och teknik. Dessa tester är inte utformade för att godkänna eller underkänna ett företags kapacitet, utan syftar till att identifiera brister för att sedan kunna förbättra motståndskraften. Regeringskansliet Faktapromemoria 2020/21:FPM16.

54. Artikel 26 DORA.

55. Vid en gränsöverskridande incident, ska Finansinspektionen även informera europeiska bankmyndigheten (Eba), europeiska värdepappers- och marknadsmyndigheten (Esma) eller europeiska försäkrings- och tjänstepensionsmyndigheten (Eiopa) beroende vilken sektor som berörs, samt Europeiska centralbanken (ECB).

Regleringar som förhandlas

Förslag till AI-förordning

Reglering och tidsram

Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om harmoniserade regler för artificiell intelligens (rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter (COM) 2021/0106. Förhandlingarna är i slutskedet och som stöd för arbetet enligt det nya regelverket har kommissionen i januari 2024 inrättat den Europeiska byrån för artificiell intelligens.[56]

Vad innebär det?

Syftet med förordningsförslaget är att utforma etiska riktlinjer för utvecklingen av AI, och säkerställa att AI-system används i enighet med grundläggande rättigheter. Genom att inrätta omfattande krav på riskhantering, dokumentation, transparens, mänsklig insyn och informations – och cybersäkerhet, skapas en säkrare inre marknad för lagliga, säkra och pålitliga AI-system.

Förslaget etablerar en strukturerad uppdelning mellan olika typer av AI-system, där vissa är förbjudna, andra tillåtna men med restriktioner och krav i form av bland annat tillsyn och registrering hos ansvarig myndighet. De AI-system som inte innebär någon eller liten risk får användas utan restriktioner. CE-märkning krävs på AI-system som karaktäriseras av hög riskfaktor.

Leverantörer av AI-system med hög risk ska enligt förslaget på begäran förse en utpekad tillsynsmyndighet med all information och dokumentation som krävs för att påvisa att systemet överensstämmer och efterlever kraven i förordningen. AI-system som utvecklas för militärt bruk omfattas inte av förordningsförslaget.

Det ska enligt förslaget upprättas en databas på unionsnivå som ska katalogisera AI-system som definieras som högrisk. Denna databas ska vara tillgänglig för allmänheten och ansvaras av medlemsstaterna och kommissionen.

Förslaget riktar skärpta krav mot tillhandahållare, importörer, tillverkare, distributörer (och i viss mån användare) av AI-system som innebär riskhantering, dokumentation och kvalitetskontrollsystem. Vid överträdelser av nationell lagstiftning eller unionslagstiftning, har leverantörerna rapporteringsskyldighet till behörig myndighet.

Användning av förbjudna AI-system kan enligt förslaget leda till sanktionsavgifter, tvångsnedstängning av tjänster och system samt avsättande av personer i chefsställning.

Myndighetsroller och samverkan

Varje medlemsstat ska enligt förslaget utse en eller flera nationella behöriga myndigheter för att övervaka tillämpningen och genomförandet av förordningen genom tillsyn. Det föreslås även inrättas marknadskontrollmyndigheter med uppgift att kontrollera marknaden och undersöka efterlevnaden av skyldigheterna och kraven för alla AI-system med hög risk som redan släppts ut på marknaden.

Den nationella tillsynsmyndigheten ska också fungera som gemensam kontaktpunkt och företräda Sverige i den europeiska nämnden för artificiell intelligens.

56. *COMMISSION DECISION of 24 January 2024 establishing the European Artificial Intelligence Office* (C/2024/1459). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024D01459.

Förslag till Cyberresiliensakt

Reglering och tidsram

Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020. Förväntas träda ikraft i början av 2024 och ska börja tillämpas 36 månader senare.[57]

Vad innebär det?

Syftet med förslaget är att skapa förutsättningar för utvecklingen av säkra produkter med digitala element genom att säkerställa att hårdvaru- och programvaruprodukter har färre sårbarheter när de släpps ut på marknaden och att tillverkarna tar säkerheten på allvar under produktens hela livscykel.

CRA ställer särskilt krav på aktörer som tillhandahåller, producerar, distribuerar eller nyttjar högriskprodukter med it-funktionalitet (inklusive omfattande krav på riskhantering, dokumentation, transparens, kvalitetskontrollsystem, standardisering, och CE-märkning). Genom CE-märkning av produkter får användaren ett intyg på att produkten lever upp till EU:s grundläggande hälso-, miljö- och säkerhetskrav.

Tillverkare är enligt förslaget skyldiga att upprätta incidentsanmälan vid kännedom om incident eller sårbarhet i komponent. Tillverkare föreslås efter upptäckt av en sårbarhet eller incident, utan onödigt dröjsmål, anmäla detta till Enisa. Om en sårbarhet i en produkt med digitala element aktivt utnyttjas måste tillverkaren enligt förslaget anmäla det inom 24 timmar efter att de fått kännedom om det. Anmälan ska omfatta uppgifter om sårbarheten och, i förekommande fall, de korrigerande eller riskreducerande åtgärder som vidtagits. Enisa ska sedan utan onödigt dröjsmål, vidarebefordra denna anmälan till berörd nationell CSIRT-enhet.[58]

Myndighetsroller och samverkan

Medlemsstaten ska utse en redan befintlig eller etablera en ny marknadskontrollsmyndighet.

För att säkerställa en effektiv efterlevnadskontroll av de skyldigheter som fastställs i förordningen har marknads-kontrollmyndigheten befogenhet att påföra eller begära administrativa sanktionsavgifter.

Samverkan ska enligt förslaget bland annat ske med både den nationella myndigheten för cybersäkerhetscertifiering enligt cybersäkerhetsakten (i Sverige FMV) och den nationella tillsynsmyndigheten över dataskydd (i Sverige IMY).

Förslag till Cybersolidaritetsakt

Reglering och tidsram

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents COM(2023) 209[59]. Förslaget är fortsatt under förhandling.

Vad innebär det?

Syftet med akten är att stärka medlemsstaternas solidaritet och samordnande insatskapacitet kring gränsöverskridande cyberhot och incidenter.[60] Förslaget är en del i genomförandet av EU:s strategi för cybersäkerhet[61] för inrättandet av en europeisk cybersköld som ska stärka den befintliga samarbetsramen och förbättra förmågan att upptäcka och hantera cybersäkerhetshot. Målsättningen som beskrivs i akten ska genomföras genom följande åtgärder:

57. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (Hämtad 03 2024).

58. Artikel 11 Förslaget till cyberresiliensakt.

59. https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-cyber-solidarity-act, se även Regeringskansliet. Gemensamt meddelande om en cyberförsvarspolicy för EU, 2022/23:FPM30. https://www.regeringen.se/contentassets/effbdd2a6c7c41c1875edb012ad97414/gemensamt-meddelande-om-en-cyberforsvarspolicy-for-eu-202223fpm30/

60. Förslaget till en ny förordning benämnd Cybersolidaritetsakten ingår i Cybersolidaritetsinitiativet som även inkluderar inrättandet av en cybersäkerhetskompetensakademi.

61. Gemensamt meddelande till Europaparlamentet och rådet, EU:s strategi för cybersäkerhet för ett digitalt decennium, JOIN(2020)18 final) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018.

1. Inrättandet av en europeisk så kallad ”cybersköld” bestående av nationella cyber-hubbar. I tidigare versioner av förslaget användes istället cybersäkerhetscentrum, SOC (Security Operation Centre) men eftersom användningen av begreppet orsakade otydlighet i denna kontext ändrades det på medlemsstaternas begäran. Det nya begreppet blev cyber-hubb. Cyberhubben syftar till att stärka situationsmedvetenheten och den samordnade kapaciteten för upptäckt av hot och incidenter.
2. Inrättandet av en europeisk så kallad ”cybernödmekanism”. Akten avser att stödja en gradvis uppbyggnad av en gemensam cybersäkerhetsreserv på unionsnivå med tjänster från betrodda privata leverantörer, redo att ingripa på medlemsstaternas begäran vid omfattande antagonistiska cyberincidenter. Dessa leverantörer föreslås väljas ut på grundval av ett antal kriterier som listas i förordningen och upphandlas genom kommissionen. Cybersäkerhetsreserven ska kunna aktiveras för att stödja medlemsstaterna i att stärka beredskapen för, svara på, samt skyndsamt återhämta sig från storskaliga cybersäkerhetsincidenter. Förslaget innehåller även initiativ om att inrätta cybersäkerhetscertifikat för betrodda privata företag.
3. Inrättandet av europeisk incidentutvärderingsmekanism för att utvärdera betydande eller storskaliga cybersäkerhetsincidenter. Det är Europeiska unionens cybersäkerhetsbyrå Enisa, som på begäran av kommissionen, EU-CyCLONe eller CSIRT-nätverket ska utvärdera, granska och bedöma hot, sårbarheter och hanteringen avseende en betydande eller storskalig cybersäkerhetsincident.

Myndighetsroller och samverkan

För att ingå i den gemensamma cyberskölden ska varje medlemsstat på frivillig basis etablera en nationell cyberhubb. Denna cyberhubb kan utgöras av den nationella CSIRT-enheten eller etableras som egen plattform under berörd myndighet. Cyberhubben ska stärka den gemensamma förmågan att detektera och upprätta lägesbilder.

En gemensam unionsstruktur ska etableras bestående av flera samverkande gränsöverskridande cyberhubbar med syfte att gemensamt utnyttja den senaste tekniken för datainsamling och informationsutbyte.

Begäran om stöd från cybersäkerhetsreserven sker genom den nationella cyberkrishanteringsmyndigheten som ska utses i enlighet med NIS2-direktivet. Det är Cyberkrishanteringsmyndigheten som har mandat att beställa, tillsätta och inrikta användningen av cybersäkerhetsreserven vid storskaliga cyberincidenter.

Förslag på tillägg till Cybersäkerhetsakten

Reglering och tidsram

Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om ändring av förordning (EU) 2019/881 vad gäller hanterade säkerhetstjänster COM (2023)208.[62] Förslaget är fortsatt under förhandling.

Vad innebär det?

Förslag till ändringar i EU:s cybersäkerhetsakt utgör en del av Cybersolidaritetsinitiativet tillsammans med förslaget om en ny förordning benämnd Cybersolidaritetsakten. Förslaget innebär att leverantörer av cybersäkerhetstjänster ska kunna certifieras enligt ramverket för cybersäkerhetscertifiering. Det innebär att utveckla cybersäkerhetscertifiering på EU-nivå för cybersäkerhetsbranschen och privata företag (utöver de leverantörer för IKT-produkter, tjänster och processer som redan omfattas av cybersäkerhetsakten).

Certifieringen av leverantörer av cybersäkerhetstjänster säkerställer att leverantören har kompetens att hantera datalagring och dataöverföring och i de processerna kan skydda sig mot oavsiktlig tillgång till eller förlust av data. Detta ska kunna möjliggöra återställning av data, service och funktioner i händelse av incident. De föreslagna ändringarna syftar till att även komma till rätta med fragmentiseringen av kravspecifikationer på den inre marknaden för dessa leverantörer.

62. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2019/881 as regards managed security service https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A208%3AFIN.

Organisationer som omfattas

Med de EU-regleringarna tillkommer olika krav på organisationer i Sverige. Tabell 2 ger en översiktlig redogörelse hur olika organisationer kan komma att omfattas av regleringarna med störst påverkan på organisationsnivå.

Tabell 2. Översikt över hur kommuner, regioner, statliga myndigheter och företag kan komma att omfattas av olika EU-regleringar.

Reglering/ Organisation	Kommun	Region	Statlig myndighet	Företag
GDPR	Ja, vid hantering av personuppgifter.	Ja, vid hantering av personuppgifter.	Ja, vid hantering av personuppgifter.	Ja, vid hantering av personuppgifter.
NIS	Ja, för de nätverk och informationsystem som används vid leverans av samhällsviktiga eller digitala tjänster enligt NIS-regleringen.	Ja, för de nätverk och informationssystem som används vid leverans av samhällsviktiga eller digitala tjänster enligt NIS-regleringen.	Med några få undantag omfattas inte statliga myndigheter av kraven inom NIS-regleringen. Däremot utövar flera myndigheter uppdrag rörande samordning och tillsyn kopplat till NIS-regleringen.	Ja, för de nätverk och informationsystem som används vid leverans av samhällsviktiga eller digitala tjänster enligt NIS-regleringen.
Cybersäkerhetsakten	Endast om de tillverkar eller levererar IKT-produkter, IKT-tjänster eller IKT-processer som de certifierar enligt en europeisk ordning för cybersäkerhetscertifiering.	Endast om de tillverkar eller levererar IKT-produkter, IKT-tjänster eller IKT-processer som de certifierar enligt en europeisk ordning för cybersäkerhetscertifiering.	Endast om de tillverkar eller levererar IKT-produkter, IKT-tjänster eller IKT-processer som de certifierar enligt en europeisk ordning för cybersäkerhetscertifiering. Försvarets materielverk utgör nationell myndighet för cybersäkerhetscertifiering och innehar tillsynsuppgifter.	Endast om de tillverkar eller levererar IKT-produkter, IKT-tjänster eller IKT-processer som de certifierar enligt en europeisk ordning för cybersäkerhetscertifiering.
NIS2	Ja, krav på cybersäkerhet omfattar all verksamhet i kommunen (med vissa undantag såsom säkerhetsskydd).	Ja, krav på cybersäkerhet omfattar all verksamhet i kommunen (med vissa undantag såsom säkerhetsskydd).	Ja, krav på cybersäkerhet omfattar all verksamhet i myndigheten (med vissa undantag såsom säkerhetsskydd). Vissa myndigheter undantas med verksamhet inom exempelvis nationell säkerhet och brottsbekämpning. Dessutom kommer sannolikt fler statliga myndigheter tilldelas tillsynsuppdrag med koppling till NIS2-regleringen jämfört med NIS1-regleringen. Bakgrunden är utökningen av antalet sektorer.	Ja, krav på cybersäkerhet omfattar all verksamhet i företaget (med vissa undantag såsom säkerhetsskydd) förutsatt att företaget uppfyller storleks- och omsättningskrav för att utgöra verksamhetsutövare i de sektorer som omfattas av NIS2-direktivet[63] samt att de inte omfattas av något undantag, exempelvis för nationell säkerhet.

63. Energi, Transporter, Bankverksamhet, Finansmarknadsinfrastruktur, Hälso- och sjukvård, Dricksvatten, Avloppsvatten, Digital infrastruktur, Förvaltning av IKT-tjänster (mellan företag), Offentlig förvaltning, Rymden, Post- och budtjänster, Avfallshantering, Tillverkning, produktion och distribution av kemikalier, Produktion, bearbetning och distribution av livsmedel, Tillverkning (medicinska produkter), Digitala leverantörer och Forskning

Reglering/ Organisation	Kommun	Region	Statlig myndighet	Företag
CER	Ja, all verksamhet kommer att omfattas av krav på motståndskraft (med vissa undantag såsom säkerhetsskydd) om kommunen 1. bedriver verksamhet som ingår i de sektorer som omfattas av direktivet, 2. verksamheten bedrivs inom unionen och dess kritiska infrastruktur finns inom unionen, samt 3. en incident skulle innebära en betydande störning vid tillhandahållandet av tjänsten.	Ja, all verksamhet kommer att omfattas av krav på motståndskraft[64] (med vissa undantag såsom säkerhetsskydd) om regionen 1. bedriver verksamhet som ingår i de sektorer som omfattas av direktivet, 2. verksamheten bedrivs inom unionen och dess kritiska infrastruktur finns inom unionen, samt 3. en incident skulle innebära en betydande störning vid tillhandahållandet av tjänsten.	Ja, all verksamhet i den statliga myndigheten kommer att omfattas av krav på motståndskraft (med vissa undantag såsom säkerhetsskydd). Därutöver utövar myndigheter uppdrag rörande samordning och tillsyn av CER-regleringen. Inriktningen är att samma myndighet ska utöva tillsyn enligt både NIS2- och CER- regleringen.	Ja, all verksamhet kommer att omfattas av krav på motståndskraft (med vissa undantag såsom säkerhetsskydd) om företaget 1. bedriver verksamhet som ingår i de sektorer som omfattas av direktivet, 2. verksamheten bedrivs inom unionen och dess kritiska infrastruktur finns inom unionen, samt 3. en incident skulle innebära en betydande störning vid tillhandahållandet av tjänsten.
DORA	Omfattas inte.	Omfattas inte.	Statliga myndigheter omfattas inte av regleringen men Finansinspektionen är behörig myndighet och kommer att utöva tillsyn över de företag och övriga organisationer som omfattas. Övriga myndigheter kan komma att få särskilda ansvarsroller inom ramen av förordningen bland annat Riksbanken.	Ja, förordningen gäller säkerhet i nätverks- och informationssystem som stöder finansiella entiteters affärsprocesser hos finansiella aktörer, leverantörer och verksamhetsutövare såsom Revisionstjänster, Försäkringstjänster, Bank- och finanstjänster, Leverantör av kryptotjänster, Värdepapperstjänster och Tredjepartsleverantörer för IKT-tjänster. Vissa aktörer inom finansiella sektorn kommer att undantas på grund av storlekskrav med mera.
Förslag till AI-förordningen	Ja, förslaget till AI-förordning innehåller harmoniserade regler för utveckling, utsläppande på marknaden och användning av AI-system.	Ja, förslaget till AI-förordning innehåller harmoniserade regler för utveckling, utsläppande på marknaden och användning av AI-system.	Ja, förslaget till AI-förordning innehåller harmoniserade regler för utveckling, utsläppande på marknaden och användning av AI-system. En eller flera statliga myndigheter kan komma att få uppgifter enligt AI-förordningen, exempelvis som nationell tillsynsmyndighet marknadskontrollsmyndighet.	Ja, förslaget till AI-förordning innehåller harmoniserade regler för utveckling, utsläppande på marknaden och användning av AI-system.
Förslag till Cyber-resiliensakten	Endast i rollen som utvecklare, tillverkare, importörer eller distributörer av produkter med digitala element.	Endast i rollen som utvecklare, tillverkare, importörer eller distributörer av produkter med digitala element	I rollen som utvecklare, tillverkare, importörer eller distributörer av produkter med digitala element. Därutöver innebär förslaget att en eller flera myndigheter får uppgifter som exempelvis marknadskontrollmyndighet eller anmälande myndighet.	Ja, exempelvis utvecklare, tillverkare, importörer eller distributörer av produkter med digitala element, såsom mjuk- och hårdvaruprodukter och lösningar för fjärrbehandling av data.

64. Mot bakgrund av regionernas uppdrag och verksamhet är utgångspunkten de omfattas. Detta kommer att tydliggöras först vid den nationella implementeringen av CER-direktivet.

Vad innebär det för Sverige

Den nya informations- och cybersäkerhetsregleringen från EU kommer att ändra hur vi i Sverige arbetar med frågorna i grunden. Sverige har historiskt haft en modell som i mångt och mycket bygger på samverkan, samarbete och samförstånd. Med de nya EU-regleringarna sker ett paradigmskifte där kraven på organisationer ökar påtagligt, samtidigt som mandatet och uppgiften att sanktionera organisationer som inte möter kraven också stärks.

Aktörernas behov behöver tillgodoses

MSB samverkar brett och ofta med organisationer i Sverige och har identifierat några faktorer som genomgående anses nödvändiga av aktörerna:

1. **En samlad kravbild:** För att göra arbetet med regelefterlevnad hanterligt, förutsägbart och möjligt att överblicka behövs en samlad kravbild. Kravbilden behöver inkludera alla, eller så många som möjligt, av kraven på informations- och cybersäkerhetsområdet *och* kraven inom andra säkerhetsområden. Kravbilden ska helst tillhandahållas av *en* myndighet, och den myndigheten ska ha i uppgift att säkerställa att kraven är förenliga, koherenta och att sammanställningen av krav hela tiden är uppdaterad.
2. **En samlad tjänst för åtaganden och kontakter med myndigheter:** EU-regleringarna ställer krav på anmälan, rapportering av incidenter, tillbud, cyberhot och sårbarheter, informationsdelning, rätt att begära stöd vid incidenter, rätt att begära stöd med förebyggande insatser (såsom skanningar av nätverk), (eventuellt) rätt att begära ”beredskapsstärkande” insatser såsom PEN-tester, (eventuellt) rätt att begära stöd av EU:s cyberreserv, och mycket annat. Kraven på att rapportera till olika myndigheter, och rätt utifrån olika rättsakter att begära stöd, är svåra att överblicka. Aktörerna önskar sig därför en samlad tjänst där de kan genomföra sina åtaganden, men också utnyttja sina rättigheter, gentemot myndigheterna.
3. **En samlad rapportering av incidenter:** Många av EU-regleringarna innebär krav på incidentrapportering, och därmed ifyllande av olika slags formulär. För att kunna besvara formulären behöver ansvarig dessutom ofta samla in en större mängd information. Det finns en risk för att samma information ska rapporteras flera gånger i olika formulär, och det finns en risk att organisationer, när en incident har inträffat, missar att rapportera in i enlighet med någon av alla regleringar som är tillämpliga i det aktuella fallet. För att slippa utföra mer arbete än vad som är nödvändigt önskar de sig en säker internetbaserad tjänst där de genom val i tjänsten får svara på alla de frågor som de måste besvara, utifrån kraven i alla de tillämpliga regelverken, varpå tjänsten i sin tur ser till att all och endast den information respektive ansvarig myndighet ska ha kommer den myndigheten tillhanda.
4. **En samlad katalog över tjänster staten tillhandahåller inom informations- och cybersäkerhetsområdet med information om vem som kan utnyttja dem:** Med regleringarna kommer flertalet tjänster tillkomma. Exempelvis utökas CSIRT-enhetens utbud av tjänster gentemot organisationer som omfattas av NIS2-direktivet. Sådana organisationer får rätt att begära individualiserad återkoppling på inrapporterade incidenter inom 24 timmar, och de kan också begära ”proaktiva skanningar” av sina nätverk i syfte

att identifiera hot och sårbarheter. På motsvarande sätt etableras genom CCCN-förordningen en utökad möjlighet att få stöd att söka medel från EU för att bedriva forskning och utveckling på informations- och cybersäkerhetsområdet. För att berörda organisationer lätt ska kunna få en överblick önskar de kunna ta del av information om tjänsterna samlat.

5. **Möjlighet att implementera kraven utan att ytterligare reglering tillkommer under implementeringens gång:** Den stora mängden nya krav innebär att organisationer har en mycket komplex kravbild att förhålla sig till. Det är svårt att hinna med alla anpassningar som krävs under den relativt korta tid som de har på sig framöver. Det finns därför en önskan om att de regleringar som nu kommer på plats ska gälla utan ändringar under den förutsebara framtiden, så att organisationer har ett stabilt ramverk att förhålla sig till.

Makroutmaningar behöver analyseras och hanteras

MSB bedömer att det finns skäl att se över de makroeffekter som den samlade regleringen leder till. Det försämrade säkerhetspolitiska läget och ett ökande antal cyberangrepp aktualiserar vikten av att stärka svenska organisationers informations- och cybersäkerhet. Kommande regleringar kan bidra till detta. Den utökade kravställningen såväl som introduktionen av mer omfattande sanktioner riskerar dock att även resultera i stora kostnadsökningar för berörda organisationer. I värsta fall kan detta göra att antalet organisationer som kan verka på marknaden minskar. Det ökar risken för att monoberoenden etableras i digitala leveranskedjor och därmed för att enskilda it-incidenter orsakar omfattande störningar.

De ökade kostnaderna kan också ha en hämmande effekt på Sveriges framtida ekonomiska säkerhet. När kostnaderna för att verka, forska och innovera inom EU ökar kan det bli mer lockande att flytta någon annanstans. Skyddet för det skyddsvärda vi redan har stärks, men framtida skyddsvärda innovationer kanske uteblir.

Sverige behöver bli bättre på att utnyttja möjligheterna EU erbjuder

De nya regelverken på informations- och cybersäkerhetsområdet medför också möjligheter – och Sverige har hittills inte utnyttjat dem i en sådan utsträckning som MSB bedömer hade varit önskvärt.

Med stöd av CCCN-förordningen avsätts och kanaliseras omfattande medel från EU för cybersäkerhetstillämpningar och kompetensutveckling till stöd för implementering av EU-lagstiftning hos såväl offentliga som privata organisationer. Sverige behöver öka sitt engagemang i arbetet med att hämta hem medel till svenska organisationer som utvecklar framtidens informations- och cybersäkerhetslösningar och till svenska organisationer som ska efterleva EU-lagstiftningen. Sverige behöver också stärka sitt engagemang för ökad kompetensförsörjning inom informations- och cybersäkerhet och dra nytta av de möjligheter som CCCN-förordningen medför i sammanhanget.

Samtidigt möjliggör de nya regelverken att mekanismer etableras för utbyten av expertis och experter, sakkunnigbedömningar, informationsdelning och annat. Det finns många områden där andra medlemsstater har kommit minst lika långt som Sverige i arbetet med olika informations- och cybersäkerhetsutmaningar. Möjligheterna att lära av varandra finns, men det är upp till medlemsstaterna att utnyttja dem.

Slutsatser och rekommendationer

Slutsatser och rekommendationer

Det oroliga säkerhetspolitiska läget, insikterna om att en stor majoritet av svensk offentliga organisationer saknar de mest grundläggande delarna i ett systematiskt informations- och cybersäkerhetsarbete och att även mindre sofistikerade cyberangrepp får påverkan på organisationer, kombinerat med nya krav från EU-regleringar, gör att Sverige behöver utveckla sitt informations- och cybersäkerhetsarbete. MSB:s slutsatser och rekommendationer till regeringen och organisationer presenteras i detta kapitel.

De senaste åren har samhället ställts inför stora utmaningar. Den ökade digitaliseringstakten och gapet mellan digitalisering och informations- och cybersäkerhet har blivit påtaglig. Samtidigt har vikten av motståndskraft inom säkerhetsarbetet blivit mer angeläget på grund av det oroliga säkerhetspolitiska läget. Säkerheten i våra informationssystem måste prioriteras och för att minska risken för it-incidenter med samhällspåverkan gäller detta särskilt samhällsviktiga verksamheter. Samtidigt påvisar Infosäkkollen 2023 att 69 procent av organisationerna saknar de mest grundläggande delarna i ett systematiskt informations- och cybersäkerhetsarbete. I det förebyggande arbetet är det viktigt att organisationer arbetar systematiskt och riskbaserat med helheten utifrån allriskperspektivet. Utifrån denna rapport och insamlat underlag[65] är det främst följande områden som behöver förbättras:

- **Ledningens engagemang:** Kommande EU-regler inom informations- och cybersäkerhet kommer att ställa högre krav på hur organisationers ledningar agerar och tar ansvar för att skydda digitala system, tjänster och data. Resultatet inom arbetsområdet för ”Ledningens styrning och kontroll” i Infosäkkollen 2023 visar tyvärr på bristande engagemang från organisationernas ledningar. Medan en viss säkerhet kan uppnås utan aktiv inriktning och uppföljning av ledningen är förutsättningarna för en god säkerhetskultur och ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete svår att uppnå utan ledningens engagemang.

65. MSB. *Det systematiska informationsoch cybersäkerhetsarbetet i den offentliga förvaltningen – Resultatredovisning av Infosäkkollen och It-säkkollen 2023.* https://rib.msb.se/filer/pdf/30598.pdf (Hämtad 03–2024).

- **Incidenthantering:** Det framkommer av it-incidentrapportering att organisationer behöver förbättra och anpassa sitt arbete med incidenthantering. Det faktum att flera rapportörer har angett att den bakomliggande orsaken är ”okänd” vid tidpunkten för rapportering indikerar på att det tar lång tid för organisationer att fastställa vad det är som inträffat. Dessutom visar den ökade förekomsten av tillgänglighetsstörningar till följd av överbelastningsangrepp att många it-incidenter inte hanteras tillräckligt snabbt. Detta utgör incitament för att införa skärpta rutiner och öva incidenthantering.
- **Kontinuitetshantering:** De flesta av it-incidenterna resulterar i att tillgängligheten till drabbade delar av it-miljön förloras. Att tillgången till informationssystem och information, däribland verksamhetskritisk sådan, ofta påverkas när en it-incident uppstått ställer krav på organisationer att ha en väl utvecklad kontinuitetshantering så att verksamheten kan fortsätta fungera även vid störningar.
- **Ändringshantering**: It-incidentrapporteringen har under flera år visat att organisationers sätt att genomföra ändringar i sina informationssystem har varit en vanligt återkommande orsak till incidenter. Av it-incidentrapporteringen från 2023 framkommer att drygt 20 procent av it-incidenterna har orsakats av misstag. Det är mindre än föregående år, men likväl en vanligt förekommande orsak till att it-incidenter inträffar. Statistiken visar även att it-incidenter uppstår till följd av felkonfigurering. Många av dessa incidenter hade kunnat förebyggas med robusta arbetssätt för att hantera ändringar.
- **Digitala leveranskedjor:** En majoritet av alla NIS-leverantörer rapporterar att it-incidenten har inträffat hos en leverantör. Det har även förekommit ett antal it-incidenter under 2023 som drabbat mer än en mottagare av en tjänst. Dessa incidenter kan orsakas av angrepp, systemfel eller misstag, men får likväl stora konsekvenser i den mån det påverkar mottagare av organisationens tjänster.

De kommande EU-regleringarna omfattar en mängd olika initiativ med fokus på stärkt informations- och cybersäkerhet. Regleringarna innebär inte bara nya uppgifter och krav på offentliga förvaltningar utan även på företag. Resurser behöver tillsättas och arbetssätt kan komma att behöva ses över för att möta kraven. Några krav som företag och organisationer kommer att behöva ta hänsyn till gällande regleringarna sammanfattas i nedan punkter:

- **Cybersäkerhetsakten:** Med akten kommer en EU-omfattande ram införas för cybersäkerhetscertifiering för IKT-produkter, IKT-tjänster och IKT-processer. Certifieringen kommer att vara frivillig för organisationer som bedriver verksamhet i EU, men det kommer att finnas incitament för företag att certifiera sina produkter, tjänster och processer. De organisationer som vill be certifierade kommer därför behöva implementera nya arbetssätt för att ansöka om certifiering.
- **NIS2/CER:** Implementering av NIS2 kommer innebära att organisationer som omfattas behöver delge information om sårbarheter, incidentrapportering, skärpta säkerhetskrav, strängare tillsynsåtgärder och höjda sanktionsavgifter. Med CER direktivet kommer dessutom krav på fysisk säkerhet och kontinuitet för samhällsviktiga verksamheter i de elva sektorer som omfattas av direktivet. Alla sektorer som omfattas CER-direktivet omfattas också av NIS2-direktivet. För många organisationer innebär detta att nya eller utvecklade arbetssätt

behövs bland annat för hantering av sårbarheter och incidenter, riskbedömning riskhanteringsåtgärder, utbildning och uppföljning.

- **DORA:** Med förordningen ska den digitala motståndskraften stärkas inom finanssektorn och dess kritiska IKT-tjänster. Förordningen ställer krav på (den finansiella enhetens) ledningens ansvar för IKT-risker, vilket i sin tur ställer krav på organisation och ledningens kontroll över hur verksamheten hanterar risker och sårbarheter i sina system. För de organisationer som omfattas kommer arbetssätt för risk och sårbarhetshantering behövas.
- **Cyberresiliensakten:** Akten ställer krav på berörda organisationer, i synnerhet om de tillhandahåller, producerar, distribuerar eller nyttjar högriskprodukter med it-funktionalitet (inklusive omfattande krav på riskhantering, dokumentation, transparens, kvalitetskontrollsystem, standardisering, och CE-märkning). CE-märkta produkter intygar att produkten lever upp till EU:s grundläggande hälso-, miljö- och säkerhetskrav. De organisationer som omfattas kommer att behöva arbetssätt för riskhantering, dokumentation, transparens, kvalitetskontrollsystem, standardisering och leva upp till hälso-, miljö- och säkerhetskrav för att uppnå CE-märkning.
- **AI-förordningen:** Förordningen syftar till att skapa en strukturerad uppdelning mellan olika typer av AI-system, där vissa är förbjudna medan andra är tillåtna, men med restriktioner och krav i form av bland annat tillsyn och registrering hos ansvarig myndighet. De AI-system som inte innebär någon eller liten risk får användas utan restriktioner. CE-märkning krävs på AI-system som karaktäriseras av hög riskfaktor. Leverantörer av AI-system ska rapportera in allvarliga incidenter eller överträdelser av nationell lagstiftning och unionslagstiftning. Användning av förbjudna AI-system kan leda till sanktionsavgifter, tvångsnedstängning av tjänster och system samt avsättande av personer i chefsställning. Organisationer kommer bland annat att behöva implementera arbetssätt för registrering av AI-system, ansökan om CE-märkning och rapportering av allvarliga incidenter och överträdelser.
- **Cybersolidaritetsakten:** Initiativet syftar till en genomgripande ökad solidaritet på unionsnivå för att öka resiliensen mot de ökade cyberhoten hos de företag och organisationer som är verksamma i kritiska och högkritiska sektorer. Cybersolidaritetsakten ställer därför övergripande krav på förbättrad säkerhetskultur inom företag och organisationer som bedriver cybersäkerhetstjänster. Anpassningar till skärpta krav kan komma att leda till ökade kostnader för investeringar i kompetens, infrastruktur, verktyg och säkra system för att snabbare upptäcka och hantera cyberhot. EU-kommissionens förslag om en gradvis etablering av en europeisk cyberreserv bestående av betrodda leverantörer och deras tjänster kan leda till en ökad konkurrensställning på den inre marknaden.

Rekommendationer till regeringen

1. **Uppmuntra till genomförande av Cybersäkerhetskollen:** Uppmana organisationer till att genomföra Cybersäkerhetskollen (verktyget består av både Infosäkkollen och It-säkkollen) samt att dess ledning aktivt informerar sig om och följer upp på nivån av informations- och cybersäkerhetsarbetet i organisationen utifrån resultatet och vid behov tillför resurser.

2. **Kartlägg digitala leveranskedjor:** Ge MSB i uppdrag att, tillsammans med sektorsansvariga myndigheter, kartlägga monoberoenden inom de nya beredskapsområdena, samt lämna förslag på hur identifierade monoberoenden ska hanteras.
3. **Sträva efter samordning vid implementering av EU-reglering:** Organisationer kan komma att omfattas av flera av de kommande regleringarna samtidigt. Detta kan innebära stor påfrestning både organisatoriskt och resursmässigt för att möta alla krav, särskilt om de är snarlika och överlappande. Detsamma gäller om liknande uppgifter, exempelvis riskbedömningar, ska utföras på lite olika sätt beroende på vilket regelverk som ska följas. EU-regleringen ger medlemsstaterna tillgång till nya skarpa verktyg för ökad motståndskraft i samhällsviktig verksamhet. Sverige behöver nyttja dessa verktyg effektivt och dra nytta av synergier med beredskapssystemet. Det är också centralt att göra det så enkelt som möjligt för privata och offentliga organisationer att bidra till stärkt motståndskraft. Genom samordning av krav och funktioner ges privata och offentliga organisationer bästa möjliga förutsättningar och statens resurser nyttjas på ett resurseffektivt sätt. Här kan flera åtgärder göra skillnad, exempelvis:

    3.1. Etablera en samlad grundnivå på krav med ett allriskperspektiv: Hur ett systematiskt informationssäkerhetsarbete bedrivs, hur riskbedömningar ska göras och vilka säkerhetsåtgärder som ska vidtas för att upprätthålla en grundläggande nivå av cybersäkerhet i samhällsviktig verksamhet skiljer sig inte mer än marginellt mellan olika sektorer. Ett samlat regelverk enligt NIS2-regleringen med grundläggande krav på cybersäkerhet kan sedan vid behov kompletteras med sektorsspecifika högre krav. De grundläggande kraven kan även kompletteras med motsvarande krav på systematiskt riskhantering- och kontinuitetshantering utifrån CER-direktivet vilket skapar ett baspaket för samhällsviktig verksamhet med krav på säkerhetsåtgärder utifrån ett allriskperspektiv. Ett sådant upplägg gör det enklare och mer transparent för organisationerna att veta vilka krav som gäller och minimerar risken för överlappning samt ett fragmenterat regelverk. Det innebär även en effektiv användning av statens resurser där tillsynsmyndigheterna och MSB bidrar med sin expertis på respektive område samt ger möjlighet till ett betydligt mer samordnat och resurseffektivt arbete med stöd. Ett samlat paket med grundkrav på säkerhetsåtgärder kan också betydligt enklare och snabbare justeras för att ytterligare öka motståndskraften i samhällsviktig verksamhet om det säkerhetspolitiska läget så kräver.

    3.2. Samordnad incidentrapportering för NIS2, CER och DORA: Generellt höjda krav och dyra sanktionsavgifter kommer ställa nya krav på rapporteringspliktiga organisationer. Det kan underlättas genom att de har en och samma kontaktpunkt för all inrapportering. Kontaktpunkten kan sedan vidarebefordra till berörd tillsynsmyndighet. Ett samlat system för incidentrapportering skulle underlätta arbetet med att upprätthålla en kontinuerligt uppdaterad lägesbild, något som både stärker förmågan att upptäcka och hantera större it-incidenter och cyberkriser. Det ger även underlag till arbetet att bedöma förmågan i och utveckla det civila försvaret.

3.3. **Tillsyn över organisationer som omfattas av flera regleringar bör vara samordnad:** Antalet privata och offentliga organisationer som kommer att omfattas av tillsyn från flera olika tillsynsmyndigheter med snarlika krav ökar med NIS2- och CER-direktiven. Utan uttryckliga krav på och stöd för samordning av sådan tillsyn avseende exempelvis tidsplanering, prioritering, metoder, verktyg och liknande kommer tillsynen sannolikt uppfattas betydligt mer belastande för organisationerna. En aktiv samordning gör det dessutom möjligt att nyttja statens tillsynsresurser mer effektivt.

4. **Stimulera forskning, innovation och kompetensförsörjning inom cybersäkerhet:** EU gör en kraftsamling inom området genom inrättandet av ECCC, nätverket av nationella samordningscenter, den europeiska kompetensgemenskapen, forsknings- och innovationsprogrammet Horizon Europe och tillämpningsprogrammet Digital Europe. Det senare programmet kräver nationell samfinansiering, vanligtvis med 50 procent av projektbudgeten. MSB föreslår att regeringen utökar tillgänglig budget för att medfinansiera svenska projekt som kan ta del av EU-finansieringen. MSB föreslår vidare att NCC-SE vid MSB också ges ökade resurser att stödja de cybersäkerhetssatsningar som görs och bör göras inom forskning, innovation och kompetensförsörjning.

Rekommendationer till organisationer

1. **Prioritera det systematiska och riskbaserade informations- och cybersäkerhetsarbetet:** Ledningens engagemang är grundförutsättningen för en god säkerhetskultur och ett systematiskt och riskbaserat informationssäkerhetsarbete utifrån ett allriskperspektiv. Arbetet måste understödjas och nödvändiga resurser ska tilldelas utifrån riskanalysen. Ledningen ska sätta tydliga mål och förväntningar för säkerhet, regelbundet kommunicera vikten av säkerhet, uppmuntra medarbetare att rapportera it-säkerhetshändelser och förbättringsförslag, och föregå med gott exempel. Organisationer bör även bedriva regelbunden uppföljning, exempelvis genom Infosäkkollen[66], för att därigenom öka informationshanteringens robusthet.
2. **Inför och öva arbetssätt för incidenthantering:** Organisationer måste stärka förmågan att genomsöka nätverk och datorer efter vilande skadliga program, och skapa rutiner för att göra detta regelbundet. För att kunna hantera it-incidenter oberoende av orsak för att påverkan på organisationen och dess it-miljö minimeras behövs övade arbetssätt. Några viktiga steg i incidenthanteringen är: 1) Identifiera vad som hänt och vilka system som är påverkade, för att därefter kunna börja vidta skadebegränsande åtgärder. 2) Isolera påverkade enheter, främst vid angrepp. 3) Rapportera händelsen i ett skyndsamt till ansvarig myndighet efter bedömning av incidentens art, enligt NIS-direktivet eller enligt säkerhetsskyddslagen som rör säkerhetskänslig verksamhet. 4) Använd övade arbetssätt för

66. MSB. Infosäkkollen. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/infosakkollen/ (Hämtad 02/2024).

återställning av säkerhetskopior, vid angrepp säkerställ att kopiorna inte blivit kompromitterade[67]. 5) Gör en utredning och säkerställ att incidenten är åtgärdad, vid ett angrepp säkerställ att angriparen inte har fått fotfäste it-miljön genom till exempel behörigheter och/eller skadlig kod.
Ta hjälp av experter på området om rätt kompetens inte finns tillgänglig. Betala aldrig lösensumma då det inte finns garantier att system återställs, att filer dekrypteras eller att angriparen inte återkommer med nya krav och hot.

3. **Inför och öva kontinuitetsplaner:** Organisationer måste säkerställa att de kan fortsätta sin aktivitet och att de skyndsamt kan återhämta sig om en it-incident inträffar till följd av ett cyberangrepp eller annan orsak. För detta behövs övade kontinuitetsplaner. I arbetet ingår att på förhand identifiera och hantera risker, dokumentera och planera för att upprätthålla sin verksamhet på en tolerabel nivå oavsett vilken störning den utsätts för.
4. **Inför arbetssätt för säker ändringshantering:** Till följd av det säkerhetspolitiska läget ökar vikten av att snabbt kunna göra ändringar för att åtgärda sårbarheter. Ändringar i informationssystem måste dock hanteras på ett korrekt och säkert sätt[68] för att inte öka risken för incidenter. Incidenter som i sin tur riskerar att äventyra informationssystems eller informationens konfidentialitet, riktighet och tillgänglighet genom att nya sårbarheter och hot uppstår.
5. **Säkra de digitala leveranskedjorna:** Organisationer ska säkerställa tillgången till särskilt viktiga komponenter och tjänster. Ett så kallat monoberoende riskerar innebära att en verksamhet är avhängig en leverantörs komponent eller tjänst och om det saknas alternativ blir verksamheten sårbar. Därför behöver alla beroenden i viktiga informationssystem granskas och dokumenteras. Planer för alternativa lösningar är viktiga, liksom planer och arbetssätt för hur organisationen ska agera och samordna sig med leverantören om en it-incident inträffar hos dem.[69]
6. **Utbilda medarbetare om den nya kravbilden:** Organisationer bör utbilda medarbetare i de nya EU-regleringarna och riktlinjerna för att säkerställa att kunskap finns om vilka regleringar de omfattas av och dess krav.
7. **Samordna cybersäkerhet och beredskap:** Organisationen bör hantera cybersäkerhets- och beredskapsfrågor på ett sammanhållet och effektivt sätt.
8. **Tillför resurser:** De kommande EU-regleringarna omfattar en mängd olika initiativ med fokus på stärkt informations- och cybersäkerhet.
I det förberedande arbetet behöver resurser tillföras för att:

67. 3-2-1-principen är en strategi för säkerhetskopiering av data som är utformad för att säkerställa att dina data kan återhämtas och snabbt återställas i händelse av en dataförlustincident. Enkelt sammanfattat innebär denna vanliga säkerhetskopieringsstrategi att tre säkerhetskopior lagras på två olika media, varav en av dessa är helt frånskild från nätverket.

68. Rekommendationer för säker ändringhantering finns i MSB:s rapport ”Ändringar som både hotar och skyddar: 20 rekommendationer för säkrare ändringar i våra informationssystem”. https://www.msb.se/sv/publikationer/andringar-som-bade-hotar-och-skyddar-20-rekommendationer-for-sakrare-andringar-i-vara-informationssystem/ (Hämtad 02-2024).

69. Rekommendationer för hur säkerheten kan stärkas finns i MSB:s rapport ”Hoten mot de digitala leveranskedjorna – 50 rekommendationer för att stärka samhällssäkerheten” https://www.msb.se/sv/publikationer/hoten-mot-de-digitala-leveranskedjorna--50-rekommendationer-for-att-starka-samhallssakerheten/ (Hämtad 02-2024).

8.1. Genomföra gap-analyser: Organisationer bör utvärdera sina befintliga säkerhetsåtgärder och jämföra med krav som ställs i de kommande regleringar som organisationen omfattas av. Detta för att avgöra vilka åtgärder som bör prioriteras.

8.2. Arbeta fram arbetssätt utifrån gap-analysen: Säkerställ att prioriterade arbetssätt tas fram, införs och används med hjälp av utbildning och annat stöd.

8.3. Identifiera och hantera informations- och cybersäkerhetsrisker: Organisationer bör utveckla befintligt riskhanteringsarbete till att även omfatta informations- och cybersäkerhetsrisker.

8.4. Säkerställa efterlevnad: Organisationer bör säkerställa att de efterlever de regleringar och riktlinjer de omfattas av för att undvika eventuella påföljder eller sanktioner.

Framåtblick

Framåtblick

I framåtblicken avhandlas olika perspektiv och faktorer som kan komma att påverka svenska organisationers informations- och cybersäkerhet framöver.

Händelserika år är att vänta på informations- och cybersäkerhetsområdet. Redan i år kommer både det svenska Natomedlemskapet och implementeringen av NIS2- och CER-direktiven ställa krav på hur organisationer som berörs arbetar med informations – och cybersäkerhet. Samtidigt skickar den kommande AI-förordningen, Cyberresiliensakten och det samlade Cybersäkerhetsinitiativet viktiga signaler om hur EU kommer att bemöta risker kopplade till den fortgående tekniska utvecklingen och Europas fortsatta digitalisering.

I mars 2024 blev Sverige medlemmar i militäralliansen Nato. Finlands Natointräde följdes av flera cyberangrepp[70], och det svenska medlemskapet kan tänkas påverka angreppsbilden även mot svenska intressen. Samtidigt kommer Natomedlemskapet medföra nya krav på berörda svenska företag och organisationers informations- och cybersäkerhet.

Valet till Europaparlamentet, som infaller den 9 juni 2024, kan också komma att ställa krav på Sveriges, likväl resterande medlemsstaters, cybersäkerhetsarbete.[71] Vid val kan olika sårbarheter i samhället utnyttjas för att försöka påverka valresultatet, exempelvis för att störa röstningsprocessen. Som framkommer i den här rapporten har EU stor betydelse för svensk informations- och cybersäkerhet. Det tillträdande Europaparlament och EU-kommission kommer därmed sannolikt utöva stort inflytande över informations- och cybersäkerhetsområdet.

NIS2- och CER-direktiven håller på att införlivas i svensk lagstiftning. De båda direktiven kommer att innebära en mycket påtaglig förstärkning av möjligheterna att identifiera, kravställa och att upprätthålla en bild av incidenter i samhällsviktig verksamhet. Som tidigare nämnts gör MSB bedömningen att implementeringen av NIS2- och CER-direktiven kommer, åtminstone initialt, få stor påverkan på de organisationer som omfattas. Långsiktigt kommer det dock innebära att informations- och cybersäkerheten inom berörda organisationer stärks. Huruvida det kommer att betunga organisationer beror ytterst på hur direktivet implementeras i svensk lagstiftning och på vilket sätt organisationer som omfattas väljer att utföra arbetet med att anpassa verksamheten för att möta kraven i regleringarna.

70. Yle. *Cyberattacker mot Finland har blivit vanligare – hotnivån har stigit i och med Natomedlemskapet.* https://svenska.yle.fi/a/7-10032967 (Hämtad 02-2024).

71. Valmyndigheten. *Kalender för partier för Europaparlamentsvalet 2024.* https://www.val.se/for-partier/kalender-for-partier-europaparlamentsval-2024.html (Hämtad 02-2024).

Den kommande AI-regleringen och Cyberresiliensakten kommer antagligen få långtgående konsekvenser för hur den europeiska techsektorn kommer att utvecklas framöver. Den snabba teknikutvecklingen och det stora utbudet av olika tjänster ökar komplexiteten i att säkra det digitala ekosystemet. Med ökad digitalisering och användningen av ny teknik inom exempelvis AI, molntjänster och 5G-nätverk kommer även nya säkerhetslösningar att krävas för att skydda samhällsviktiga tjänster. Nya lösningar för artificiell intelligens kan exempelvis komma att få stor inverkan på samhället i stort. AI-utvecklingen väntas innebära stora möjligheter för organisationers cybersäkerhetförmåga, men kan även ge upphov till oförutsägbara risker och integritetsutmaningar. Det öppnar för nya angreppsmetoder och effektivisering av redan existerande tillvägagångssätt. EU-regleringarna kommer förhoppningsvis bidra till att göra EU:s interna marknad säkrare. Huruvida så blir fallet är dock avhängigt av mångfalden och säkerheten i de digitala leveranskedjorna. Risken är att det etableras fler monoberoenden som istället underminerar samhällets förmåga att hantera och återhämta sig från allvarliga incidenter.

Utpressningsangreppet mot TietoEvry[72] i början av 2024 var en av de största leveranskedjeincidenterna som har inträffat i Sverige sett till hur många organisationer som drabbades. Under 2023 och inledningen av 2024 har det inträffat ett stort antal cyberangrepp som väckt stor uppmärksamhet medialt och medfört långtgående konsekvenser både för enskilda organisationer och användare av deras tjänster. Trots att det digitala samhället på många sätt är relativt redundant, visade angreppet mot TietoEvry på hur sårbara svenska organisationer är för störningar i grundläggande digitala tjänster. Om angripare ser en fördel med att angripa sådana typer av tjänster kan förekomsten av liknande angrepp i framtiden förväntas öka.

Ökad digitalisering, en större hotbild och ökade regulatoriska krav innebär ett ökande kompetensförsörjningsbehov både på djupet och på bredden. Detta blir en av de trånga sektorerna som kommer att påverka hur väl Sverige lyckas stärka förmågan inom informations- och cybersäkerhet.

72. BleepingComputer. *Tietoevry ransomware attack causes outages for Swedish firms, cities.* https://www.bleepingcomputer.com/news/security/tietoevry-ransomware-attack-causes-outages-for-swedish-firms-cities/ (Hämtad 02-2024).

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB2341 – mars 2024 ISBN 978-91-7927-494-8