Myndigheten för samhällsskydd och beredskap

Verktyg för ökad motstånds-kraft och stärkt civilt försvar

Årsrapport it-incidentrapportering 2024

Verktyg för ökad motståndskraft och stärkt civilt försvar
– Årsrapport it-incidentrapportering 2024

Enhet: Avdelningen för cybersäkerhet och samhällsviktiga kommunikationer

Foto omslag: Johnér
Foto: Thomas Henriksson sida 3, Johnér sida 8, 60, Johan Eklund sida 12,
Icon Photography sida 16, 56, Magnus Nelson sida 30
Tryck: Åtta45 tryckeri
Produktion: Advant

Publikationsnummer: MSB2563 – mars 2025
ISBN-nummer: 978-91-7927-608-9

Förord

Digitaliseringen inom alla samhällets sektorer fortgår i en rasande takt. Cyberhoten blir alltmer komplexa och sofistikerade. Samtidigt pågår ett fullskaligt krig i Europa. MSB:s lärdomar från cyberkrigföringen i Ukraina poängterar vikten av motståndskraft för att förebygga it-incidenter.[1] Det är därför absolut nödvändigt att organisationer arbetar systematiskt och riskbaserat med cybersäkerhet.

Sammanställningen för 2024 visar att nästan hälften av alla inrapporterade it-incidenter orsakades av misstag eller systemfel. Många av de inträffade i samband med uppdateringar eller konfigureringar och hade kunnat förebyggas med bättre arbetssätt för hantering av ändringar. Under höjd beredskap eller krig kommer misstag och systemfel att fortsätta inträffa. De kommer dessutom förmodligen att öka i antal och bli mer utmanande att hantera på grund av svårare omständigheter och resursbrist.

Jag vill passa på att tacka alla de som uthålligt rapporterar in it-incidenter till myndigheten. Att det ändå förekommer ett större mörkertal i rapporteringen är bekymmersamt. Mörkertalet underminerar myndighetens förmåga att skapa en helhetsbild av nuläget och utvecklingen över tid. Det underminerar även förmågan att ta fram ändamålsenligt stöd. MSB anser att en ökad efterlevnad av rapporteringsplikten är en grundförutsättning för att motståndskraften i det civila försvaret ska kunna öka, vilket lyfts i rapportens slutsatser och rekommendationer.

En större andel it-incidentrapporter har under 2024 inkommit till följd av digitala leveranskedjeincidenter. Dessa incidenter riskerar fortfarande att få störst samhällskonsekvenser på grund av att en mängd organisationer och dess tjänster kan påverkas samtidigt. Därtill saknas ofta information om inträffade it-incidenter när incidenten skett hos en leverantör. Lika viktigt som det är att rapportera in it-incidenter är det även viktigt att organisationer kan informera sig om de bakomliggande orsakerna, både för sig själva och för MSB.

Min förhoppning är att denna rapport inte bara informerar utan också att rapportens temakapitel *Verktyg för ökad motståndskraft och stärkt civilt försvar* även inspirerar till ett proaktivt arbete för ökad motståndskraft att stå emot och bemöta it-incidenter som i sin tur stärker det civila försvaret.

Stockholm, 2024-03-17

Åke Holmgren
Avdelningschef, avdelningen för cybersäkerhet
och samhällsviktiga kommunikationer
Myndigheten för samhällsskydd och beredskap

Not 1. MSB, *När kriget kom nära: årsrapport it-incidentrapportering 2022*. https://msb.se/sv/publikationer/nar-kriget-kom-nara--arsrapport-it-incidentrapportering-2022 (Hämtad 03/2025)

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.

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 (*legalitetsvillkoret*), ii) medför ett utbyte av information som resulterar i en interaktion, konfigurering, installation/sparande, avinstallation/raderande eller överbelastning i något av målets informationssystem (*praktikvillkoret*), iii) resulterar i minst en för målet oönskad konsekvens i termer av konfidentialitet riktighet eller tillgänglighet för målet eller för andra via målet (*incidentvillkoret*) och vi) som angriparen utför i ett antagonistiskt syfte (*uppsåtsvillkoret*).

Cybersäkerhet: MSB nyttjar begreppet som ett samlingsnamn för informations-, it-, ot- och leveranskedjesäkerhet. Informationssäkerhet involverar åtgärder för att skydda informations tillgänglighet, riktighet och konfidentialitet. It- och ot-säkerhet är i sin tur de tekniska åtgärder som vidtas inom digitala miljöer för att säkra informationstillgångar respektive funktioner. Leveranskedjesäkerhet handlar om att säkerställa säkerhet i system och tjänster som en annan organisation tillhandahåller till en organisation.

Cybersäkerhetslagen: Den svenska anpassningen av EU:s NIS2-direktiv (2022/2555). NIS2-direktivet behandlar åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen. Den svenska cybersäkerhetslagen förväntas träda i kraft i Sverige under det närmsta året.

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: European Union Agency for Network and Information Security. Europeiska unionens byrå för nät- och informationssäkerhet.

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 etc.).

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 man 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 korrekt 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, dvs skydd av informationstillgångar avseende konfidentialitet, riktighet och tillgänglighet.

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

Överbelastningsangrepp (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

It-incidentrapporteringen 2024 visar att ungefär hälften av alla it-incidenter orsakades av misstag eller systemfel. Med det rådande säkerhetspolitiska läget måste motståndskraften att stå emot och bemöta it-incidenter öka för att det civila försvaret ska stärkas.

Rapporten är framtagen på uppdrag av regeringen i enlighet med MSB:s instruktion.[1] Rapporten riktar sig i huvudsak till beslutsfattare, cybersäkerhetsansvariga, samt omvärldsbevakande och analyserande funktioner hos samhällsviktiga verksamheter. Syftet är att informera om cybersäkerheten hos svenska organisationer, vilka incidenter som sker, orsakerna till dem och konsekvenserna de medför. Rapporten syftar även till att redogöra för hur organisationer kan och bör gå till väga för att öka sin motståndskraft att stå emot och bemöta cyberangrepp och andra orsaker till it-incidenter för att stärka det civila försvaret.

Under 2024 har totalt 319 it-incidenter rapporterats till MSB från 163 enskilda organisationer. Av dessa har 170 rapporter inkommit från statliga myndigheter och 149 från leverantörer av samhällsviktiga och digitala tjänster. Antalet it-incidentrapporter som inkommit från statliga myndigheter har fortsatt minska under året. Hälso- och sjukvård är, liksom tidigare år, överrepresenterad bland de organisationer som inkommit med en it-incidentrapport i enlighet med NIS-lagstiftningen.

Majoriteten av de rapporterade it-incidenterna har orsakats av misstag eller systemfel. Det ligger i linje med normalbilden, men skiljer sig från 2023 då angrepp var den vanligast rapporterade orsaken. Under våren 2023 observerades en ökad frekvens av rapporterade överbelastningsangrepp.[2] Liksom 2023 var överbelastningsangrepp under 2024 den vanligast rapporterade angreppsmetoden.

Not 1. Sverige Riksdag, *Förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.* https://riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-20081002-med-instruktion-for_sfs-2008-1002 (Hämtad 11/2024)

Not 2. Under våren 2023 rapporterade statliga myndigheter in ett stort antal överbelastningsangrepp i samband med att ett flertal koranbränningar inträffade i Sverige.

Av de it-incidenter som orsakats av systemfel eller misstag har en stor andel inträffat i samband med konfigureringar eller uppdateringar inom it-miljön. Många av dessa hade sannolikt kunnat förebyggas med bättre arbetssätt för att hantera ändringar. Att organisationen har etablerade och inövade rutiner för ändringshantering är centralt för att ändringar ska kunna genomföras på ett säkert sätt.[3] Detta gäller i fredstid såväl som under höjd beredskap och krig, varvid risken för misstag ökar samtidigt som resursbrister kan bli mer påtagliga.

Det som utmärker it-incidentrapporteringen 2024 jämfört med tidigare år är att en större andel rapporter (21 procent) än normalfallet inkommit till följd av digitala leveranskedjeincidenter som påverkat mer än en rapporteringspliktig aktör. MSB har i tidigare rapporter påvisat att störningar i digitala leveranskedjor är de incidenter som riskerar få störst samhällskonsekvenser.[4] Detta eftersom en mängd organisationer och dess tjänster kan påverkas samtidigt.

Vidare noteras i it-incidentrapporteringen att orsaken till incidenten ofta anges som okänd eller övrig när den skett hos en leverantör. Ett problem som har uppmärksammats tidigare[5], men som kvarstår. Detta tyder på att många organisationer saknar rutiner för att få tillbörlig information om it-incidenter som sker hos deras leverantörer. Lika viktigt som det är att organisationer rapporterar it-incidenter är det viktigt att de kan informera sig om bakomliggande orsaker, både för sig själva och för MSB.

MSB:s bedömning är att det fortsatt förekommer ett större mörkertal i rapporteringen, både inom ramen för NIS-lagstiftningens och statliga myndigheters rapporteringskrav. MSB anser att det är allvarligt i en tid då den låga nivån på cybersäkerhetsarbetet[6] i Sverige skyndsamt måste höjas med brådskande åtgärder. Mörkertalet underminerar myndighetens förmåga att skapa en helhetsbild av nuläget och utvecklingen över tid och underminerar förmågan att ta fram ändamålsenligt stöd. MSB bedömer att en ökad efterlevnad av rapporteringsplikten är en grundförutsättning för att motståndskraften i det civila försvaret ska kunna öka.

Not 3. Som MSB informerat om tidigare i rapporten: *Ändringar som både hotar och skyddar: 20 rekommendationer för säkrare ändringar i våra informationssystem.* https://msb.se/sv/publikationer/andringar-som-bade-hotar-och-skyddar-20-rekommendationer-for-sakrare-andringar-i-vara-informationssystem (Hämtad 02/2025)

Not 4. MSB, *Hoten mot de digitala leveranskedjorna – 50 rekommendationer för att stärka samhällssäkerheten*. https://msb.se/sv/publikationer/hoten-mot-de-digitala-leveranskedjorna--50-rekommendationer-for-att-starka-samhallssakerheten (Hämtad 02/2025)

Not 5. MSB, *Cyberangrepp mot samhällsviktiga informationssystem: 25 rekommendationer för stärkt skydd mot cyberangrepp.* https://msb.se/sv/publikationer/cyberangrepp-mot-samhallsviktiga-informationssystem--25-rekommendationer-for-starkt-skydd-mot-cyberangrepp (Hämtad 02/2025)

Not 6. MSB, *Resultatredovisning av Cybersäkerhetskollen 2024: Det systematiska cybersäkerhetsarbetet i den offentliga förvaltningen*. https://msb.se/sv/publikationer/resultatredovisning-av-cybersakerhetskollen-2024--det-systematiska-cybersakerhetsarbetet-i-den-offentliga-forvaltningen (Hämtad 02/2025)

Rapportens temakapitel *Verktyg för ökad motståndskraft och stärkt civilt försvar* redogör för de verktyg som MSB och MSB:s samarbetspartner tillhandahåller. MSB bedömer att ökad kunskap om tillgängliga verktyg kommer att hjälpa organisationer att arbeta med cybersäkerhet på ett systematiskt och riskbaserat sätt. Detta för att både möta kommande krav från EU-regleringar såsom cybersäkerhetslagen och att öka sin motståndskraft att stå emot och bemöta it-incidenter. Vilket i sin tur kommer att stärka det civila försvaret.

MSB har följande rekommendationer till organisationer. De beskrivs närmare i kapitlet *Slutsatser och Rekommendationer*.

Rekommendationer till organisationer:

1. Använd tillgängliga verktyg för att förbättra det systematiska och riskbaserade cybersäkerhetsarbetet (se rapportens temakapitel).
2. Upprätta arbetssätt för rapportering av it-incidenter.
3. Tillsätt resurser och upprätta arbetssätt för säker ändringshantering.
4. Se över kraven på leverantörer för att säkerställa att tillräcklig information lämnas om inträffade it-incidenter.

MSB informerar

MSB informerar

I detta kapitel uppmärksammas några nyheter på cybersäkerhetsområdet som skett under 2024.

Cybersäkerhetskollen 2024

Cybersäkerhetskollen är samlingsnamnet för MSB:s cybersäkerhetsmätningar. I Cybersäkerhetskollen ingår Infosäkkollen, som mäter systematiskt informations- och cybersäkerhetsarbete, samt It-säkkollen, som är motsvarande mätning för it-säkerhet. Båda mätningarna har uppdragits MSB av regeringen.

Cybersäkerhetskollen riktar sig till offentliga förvaltningar och organisationer som omfattas av NIS-regleringen, men alla organisationer som vill följa upp sitt systematiska cybersäkerhetsarbete kan nyttja verktyget.

Mätningarna har två syften. Det ena är att ge organisationer återkoppling om nivån på deras systematiska cybersäkerhetsarbete och förslag på förbättringsområden som kan användas som underlag för att inrikta vidareutvecklingsarbetet. Det andra är att regelbundet redovisa en samlad lägesbild till regeringen av cybersäkerhetsnivån hos Sveriges samhällsviktiga verksamheter. Av samma anledning uppmanas organisationer som nyttjar verktyget att inrapportera sitt svar.

Mellan 3 april och 13 september 2024 genomfördes Cybersäkerhetskollen för tredje gången. Hälften av Sveriges offentliga förvaltningar deltog. I likhet med tidigare mätningar visar resultatet att stora delar av offentlig sektor har allvarliga brister i sitt systematiska cybersäkerhetsarbete. Endast fyra av tio organisationer uppnådde den nivå som motsvarar att man har grundläggande inslag i ett systematiskt cybersäkerhetsarbete på plats. Bland deltagande statliga myndigheter uppnådde enbart åtta av 120 deltagande organisationer den nivå som MSB definierat som en indikation över huruvida en organisation uppfyller föreskriftskraven.

Cybersäkerhetskollen 2024 synliggör också ett bristande engagemang i cybersäkerhetsarbetet hos en majoritet av organisationsledningarna inom Sveriges offentliga förvaltningar. Det övergripande resultatet av Cybersäkerhetskollen 2024 är förvisso en förbättring jämfört med tidigare mätningar, men utvecklingstakten är blygsam sett utifrån den mycket låga grundnivån och de krav på förstärkt säkerhetsarbete som följer av det ansträngda omvärldsläget.

Nästa genomförande av Cybersäkerhetskollen sker under 2025.

Cybersäkerhetsrådgivningen

Hösten 2024 bytte MSB:s rådgivningstjänst för systematiskt informationssäkerhetsarbete namn till Cybersäkerhetsrådgivningen. Det nya namnet speglar det utökade uppdrag som rådgivningen fått under 2024 och den utveckling som ska ske under 2025.

Förutom frågor om systematiskt informationssäkerhetsarbete och NIS2-frågor ska rådgivarna från och med 2025 även stötta i frågor kring hur verksamheter kan arbeta systematiskt och riskbaserat med tekniska säkerhetsåtgärder och cyberfysiska system. Rådgivarna kommer även att kunna ge information avseende stöd till forskning, innovation och kompetensförsörjning inom cybersäkerhet, inom ramen av NCC-SE.

Nytt för 2024 var också att organisationer som genomfört Cybersäkerhetskollen erbjöds en serie rådgivningssamtal som stöd i förbättringsarbetet utifrån deras resultat. Ett viktigt inslag som ger en mer strukturerad och långsiktig rådgivning utifrån ett identifierat behov. Under 2025 kommer denna typ av långsiktig rådgivning utvecklas för fler områden.

CERT-SE

CERT-SE (Sveriges nationella Computer Emergency Response Team) har under året genomfört ett flertal åtgärder inom ramen för regeringsuppdraget till MSB om att stärka funktionen CERT-SE, samt utveckla och förenkla det stöd som lämnas inom cybersäkerhetsområdet.

Det EU-finansierade projektet Datadriven CERT (DDC), som avslutades under 2024, är ett exempel på fortsatt verksamhetsutveckling i syfte att leverera bättre stöd till samhället vid it-incidenter. Projektet har stärkt CERT-SE:s förmåga att hantera cybersäkerhetsrelaterade it-incidenter inom Sverige och förmågan till automatiserad omvärldsbevakning, exempelvis genom funktionen för Automatiska Notifieringar av Tekniska Sårbarheter (ANTS), som förfinats under året.

ANTS uppmärksammar CERT-SE:s målgrupper om tekniska företeelser, exempelvis sårbarheter, som observerats i deras it-miljö och som kan behöva åtgärdas. Alla svenska organisationer kan registrera sig för att få ANTS-notifieringar. Under 2024 skickades cirka 37 500 notifieringar till anslutna organisationer och i slutet av året nådde de automatiska utskicken över 75 procent av Sveriges offentliga sektor. Majoriteten av intressenterna utgörs av den offentliga sektorn.

Under 2024 hanterade CERT-SE nästan 17 500 ärenden, en ökning på nästan 20 procent jämfört med 2023. Ökningen beror bland annat på förekomsten av flera stora sårbarheter i produkter. Ärenden är kopplade till inflödet av information, därför innebär ökningen inte nödvändigtvis en ökning av antalet incidenter. Under året publicerade CERT-SE totalt 198 artiklar på sin webbplats, framför allt om kritiska sårbarheter. Informationen ger organisationer förutsättningar att åtgärda sårbarheter innan någon utnyttjar dem.

Under året har CERT-SE hanterat flera större cybersäkerhetsincidenter i syfte att motverka skadliga effekter på det svenska samhället. Bland dessa återfinns utpressningsvirus- och överbelastningsangrepp mot svenska myndigheter, banker och samhällsaktörer, samt riktade nätfiskekampanjer. Dessa har hanterats i nära samarbete med det nationella cybersäkerhetscentret (NCSC), där tät samverkan gällande incidenthantering och lägesbild sker löpande vid större cybersäkerhetsincidenter. Vid planerade händelser, som EU-valet och Eurovision Song Contest, har it-säkerhetsspecialister från CERT-SE engagerats inom ramen för NCSC för att säkerställa att dessa genomförts utan märkbar påverkan.

Under året har CERT-SE både faciliterat och deltagit i nationella och internationella samverkansforum, med syftet att främja informationsdelning och utvecklingen på området it- och cybersäkerhet. Dessa inkluderar bland annat nationella forum, så som FIDI-forumen och Svenskt CERT-forum, samt CSIRTs Network (EU:s nätverk för nationella Computer Security Incident Response Teams), International Watch and Warning Network (IWWN) och det nordiska samarbetet Nordic CERT Cooperation (NCC). Samverkan sker löpande, dygnet runt, via både digitala kanaler och fysiska möten och konferenser.

De ovan nämnda åtgärderna under 2024 har ökat 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.

Forskning och innovation (NCC-SE)

MSB driver i enlighet med myndighetens instruktion Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE). Uppdraget till MSB att utgöra NCC-SE innebär att bidra till att stärka Sveriges förmåga och konkurrenskraft inom cybersäkerhet inom ramen för den EU-förordning (CCCN-förordningen) som reglerar EU:s kompetenscentrum för cybersäkerhet (ECCC) och nätverket av nationella samordningscenter. NCC-SE ansvarar även för utveckling och inriktning av Sveriges nationella kompetensgemenskap (Cybernode) i samarbete med RISE samt genomför nationella cybersäkerhetsrelaterade utlysningar.

NCC-SE har under 2024 finansierat 37 cybersäkerhetsprojekt med totalt 21 miljoner kronor. Syftet är att stärka Sveriges kapacitet och infrastruktur inom cybersäkerhet genom stöd till små och medelstora företag. Projekten adresserar områden som reglering, AI-baserad detektering, riskhantering samt utbildning och upphandling. Det stora intresset för stödet, med över 180 inkomna ansökningar, visar på den ökade medvetenheten och viljan att stärka cybersäkerhetsområdet, men också på att det i Sverige finns en stark gemenskap på cybersäkerhetsområdet som består av innovatörer inom små- och medelstora företag.

Utlysningen riktade sig till både leverantörer och behovsägare inom cybersäkerhetsområdet och finansieras genom MSB, Vinnova och EU:s program för ett digitalt Europa (DIGITAL). Denna typ av utlysning är ett nytt verktyg som kombinerar EU-finansiering och nationella medel för att möta Sveriges behov av förstärkt cybersäkerhet. Det är första gången MSB finansiellt stödjer det privata näringslivet.

Rapporterade it-incidenter under 2024

Rapporterade it-incidenter under 2024

Statliga myndigheter och leverantörer av samhällsviktiga och digitala tjänster ska enligt lag rapportera in it-incidenter som drabbat dem. Kapitlet redogör för de it-incidenter som rapporterades in under 2024.

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 dessutom krav på sig att rapportera eftersom den verksamhet de bedriver anses särskilt viktig eller kritisk för samhällets funktionalitet. De organisation som har krav på sig att rapportera it-incidenter till MSB är statliga myndigheter[7] och leverantörer av samhällsviktiga och digitala tjänster (NIS-leverantörer)[8, 9].

Under särskilda omständigheter kan en och samma it-incident behöva rapporteras till flera olika myndigheter. Incidenter relaterade till brott bör 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.

Not 7. Sveriges riksdag. *Förordning (2022:524) om statliga myndigheters beredskap.* https://riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-2022524-om-statliga-myndigheters_sfs-2022-524 (Hämtad 01/2025)

Not 8. Sveriges riksdag. *Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.* https://riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174 (Hämtad 01/2025)

Not 9. Sveriges riksdag. *Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.* https://riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-20181175-om-informationssakerhet-for_sfs-2018-1175 (Hämtad 01/2025)

Inkomna it-incidentrapporter

Under 2024 mottog MSB totalt 319 it-incidentrapporter från rapporteringspliktiga organisationer, varav 170 inkom från statliga myndigheter och 149 inkom från NIS-leverantörer. Det utgör en minskning i jämförelse med 2023. Minskningen följer samma trend som de senaste åren då statliga myndigheter inkommit med allt färre it-incidentrapporter.

Tabell 1. Antalet inkomna it-incidentrapporter 2022–2024

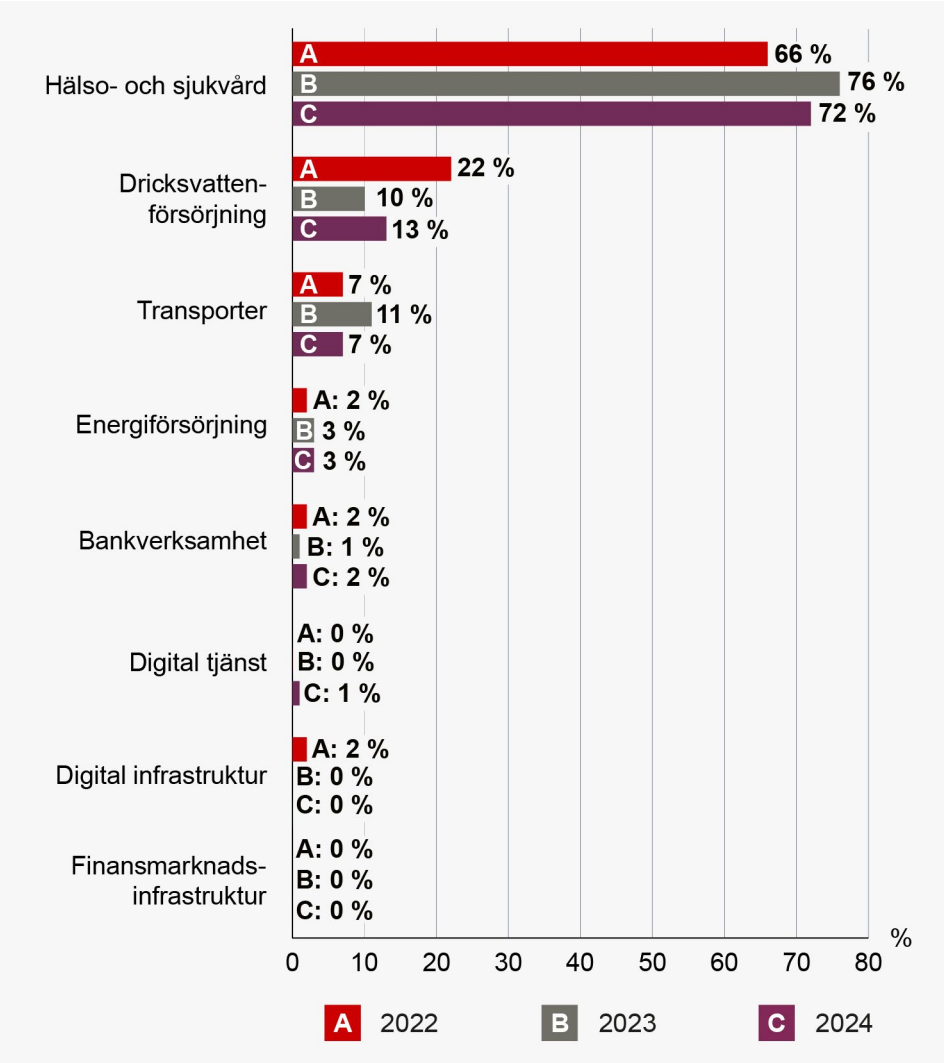
Rapporteringskrav	2024	2023	2022
Statliga myndigheter	170	189	231
Samhällsviktiga och digitala tjänster	149	144	99
Total	**319**	**333**	**330**

Rapporterande organisationer

Sammantaget har 163 rapporteringspliktiga organisationer inkommit med minst en it-incidentrapport. Av dessa har 79 rapporterat i enlighet med NIS-lagstiftningens rapporteringskrav och 84 i enlighet med statliga myndigheters rapporteringskrav. Det utgör en viss ökning i förhållande till förgående år då totalt 136 unika organisationer inkom med minst en it-incidentrapport. Det utgör alltjämt fortsatt en minoritet av rapporteringspliktiga organisationer. År 2024 inkom 24 procent av alla rapporteringspliktiga statliga myndigheter med minst en it-incidentrapport. Motsvarande andel bland NIS-leverantörer estimeras vara cirka 10 procent.

Som *diagram 1* åskådliggör har 72 procent av de it-incidentrapporter som inkommit från NIS-leverantörer rapporterats av organisationer inom hälso- och sjukvårdssektorn. Andelen och antalet är jämförbara med föregående år, men utgör i absoluta termer en ökning i jämförelse med åren 2019–2022. Dricksvatten- och transportsektorn stod för elva respektive nio procent av rapporterade it-incidenter. Resterande sektorer har inkommit med enstaka eller inga it-incidentrapporter under det gångna året.

Diagram 1. Andel it-incidentrapporter per NIS-sektor 2024



Den stora merparten av it-incidentrapporter som inkommit i enlighet med NIS-lagen har rapporterats av organisationer inom offentlig förvaltning. Därtill uppskattas ytterligare åtta procent ha rapporterats av kommunala bolag. Totalt 25 procent av unika rapporterande organisationer utgörs av privata företag. Fördelningen illustreras i *diagram 2*.

Diagram 2. Fördelningen av unika rapporterande organisationer baserat på aktörsgrupp 2024

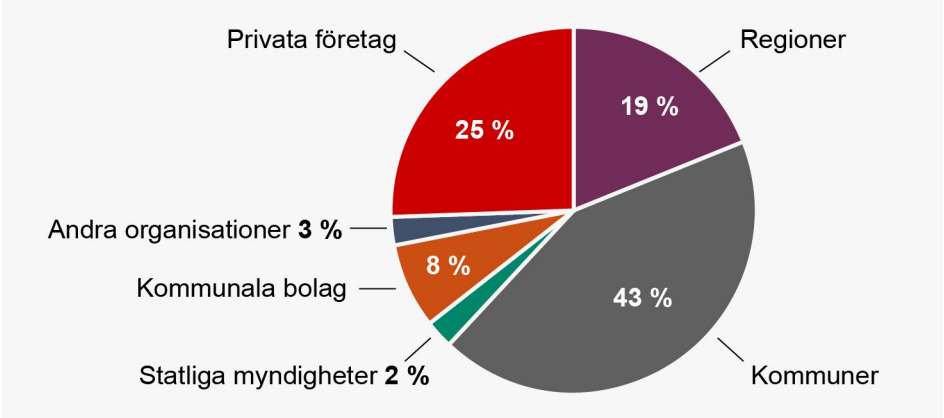
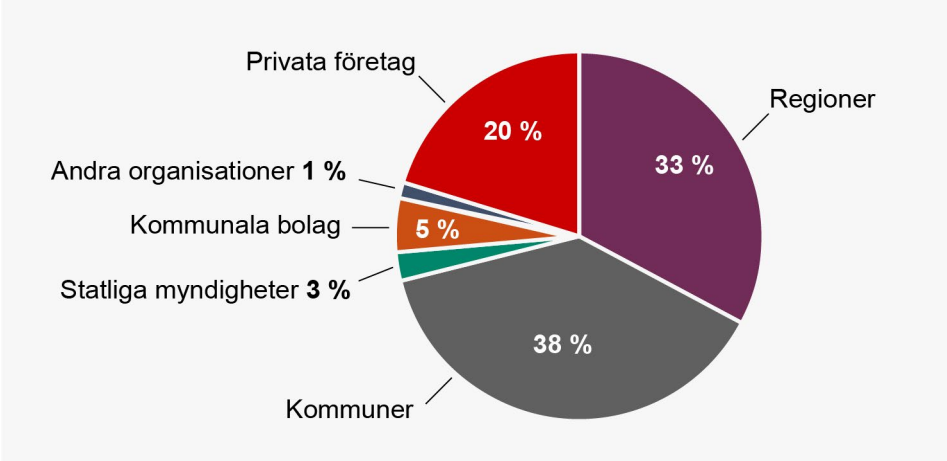


Diagram 3 åskådliggör vidare andelen it-incidentrapporter som inkommit från respektive aktörsgrupp i enlighet med NIS-lagen. Noterbart har cirka 33 procent av det totala antalet inkommit från Sveriges regioner, något som visar på att de är mer benägna att inkomma med fler it-incidentrapporter per år än andra organisationer inom andra aktörsgrupper. Den stora merparten av it-incidentrapporter som inkommer från regioner och kommuner beskriver störningar inom regional eller kommunal hälso- och sjukvård.

Diagram 3. Fördelningen av inkomna it-incidentrapporter per aktörsgrupp 2024



Att den offentliga hälso- och sjukvårdssektorn är överrepresenterad bland NIS-rapportörer bedöms bero på flera faktorer. Utöver att hälso- och sjukvårdssektorns storlek i förhållande till övriga sektorer säkerligen bidrar till att den absoluta frekvensen av rapporteringspliktiga it-incidenter är högre, så kan det indikera att en högre andel av inträffade incidenter blir rapporteringspliktiga i enlighet med existerande krav. Det kan även indikera att det är vanligare att it-incidenter i hälso- och sjukvårdssektorn pågår under en längre tidsperiod.[10]

Bristande rapporteringsbenägenhet

MSB har länge gjort bedömningen att det förekommer ett större mörkertal i it-incidentrapporteringen till myndigheten, både inom ramen för NIS-lagstiftningens och statliga myndigheters rapporteringskrav. Bedömningen är baserad på att i) ett stort antal rapporteringspliktiga organisationer aldrig har inkommit med en it-incidentrapport, ii) MSB får information, via media och andra vägar, om it-incidenter som aldrig rapporteras och att iii) endast vissa organisationer som använder en och samma tjänst, och som drabbats av en it-incident, rapporterar om det.

MSB ser allvarligt på att det förekommer ett mörkertal. Det underminerar myndighetens förmåga att analysera förekomsten och frekvensen av rapporteringspliktiga it-incidenter och däri utvärdera nuläget samt utvecklingen över tid. På sikt påverkar

Not 10. Att it-incidenten varit pågående under vad som uppfattas vara en längre tidsperiod är ett av flera kriterier som gör en it-incident rapporteringspliktig i enlighet med MSB:s föreskrifter om rapportering av incidenter för leverantörer av samhällsviktiga tjänster (MSBFS 2018:9).

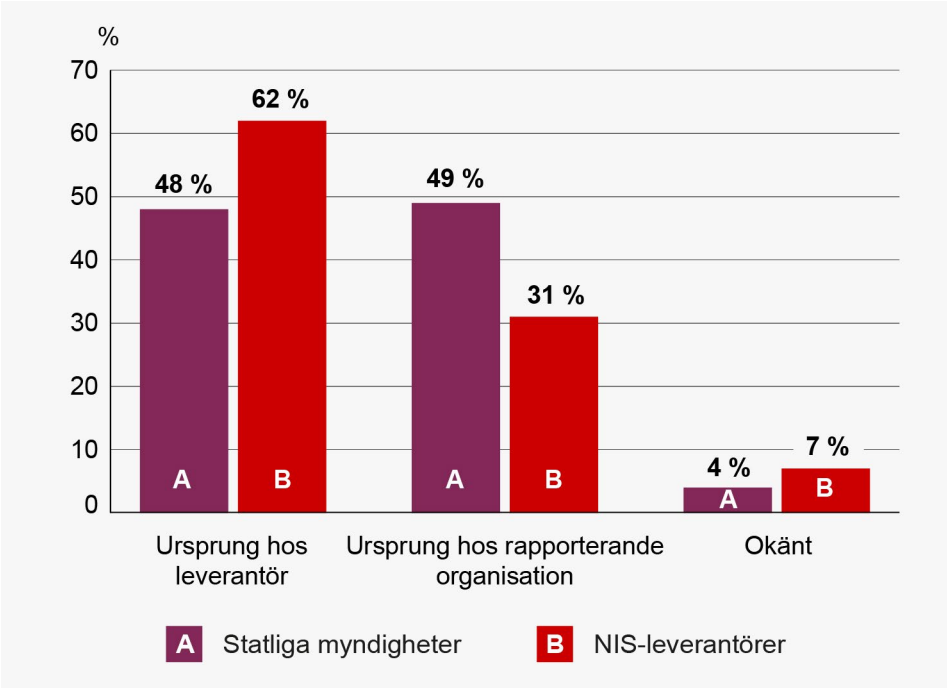
det myndighetens förmåga att ta fram ändamålsenligt och sektorsanpassat stöd till samhällsviktiga organisationer negativt. MSB bedömer att en ökad efterlevnad av rapporteringsplikten är en grundförutsättning för att motståndskraften i det civila försvaret ska kunna öka.

Trots underrapporteringen bedömer MSB att underlaget ger en överblick av fördelningen av rapporterade orsaker och konsekvenser som gör att vissa slutsatser ändå kan dras. Dock med reservation för att slutsatser om it-incidentrapporteringen i enlighet med NIS-lagstiftningen inte är representativa för de sektorer som inkommit med få eller inga it-incidentrapporter under året.

Rapporterade unika it-incidenter

Under 2024 beskrev totalt 51 procent av inkomna it-incidentrapporter att incidenten skett hos en leverantör. Det är en ökning i jämförelse med 2023 och 2022 då 44 procent respektive 35 procent rapporterades ha uppstått hos en leverantör. Ökningen beror på en ökad förekomst av rapporterade leverantörsincidenter bland statliga myndigheter såväl som NIS-leverantörer.

Diagram 4. Andelen leverantörsincidenter 2024

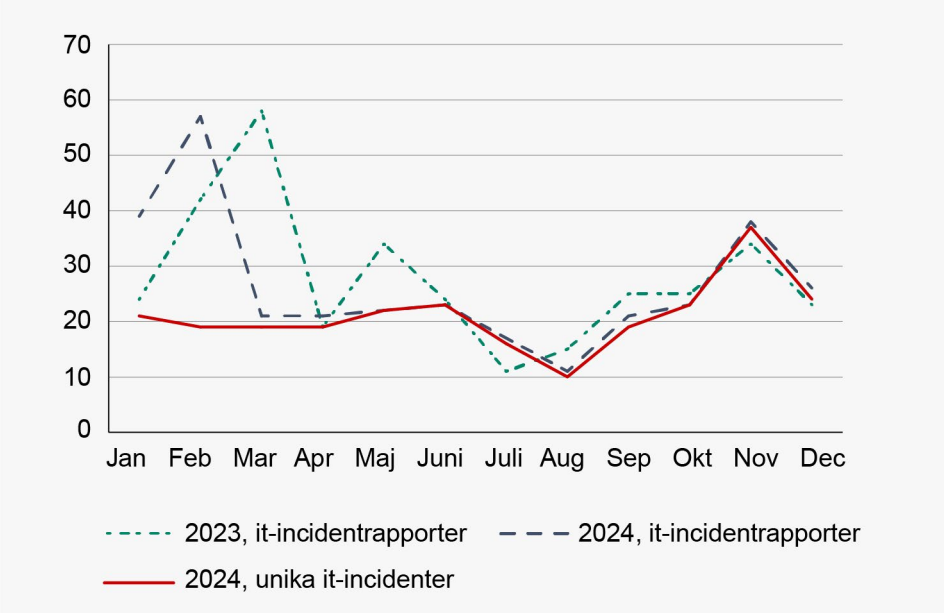


Alla inkomna it-incidentrapporter beskriver inte en unik it-incident. Flera av de it-incidentrapporter som redogör för en incident hos en leverantör är relaterade till en och samma ursprungliga it-incident i en digital leveranskedja. Även om sådana typer av större leveranskedjeincidenter också förekommit i MSB:s incidentrapportering tidigare år, skiljer sig år 2024 på så sätt att det representerar en väsentlig andel av inkomna it-incidentrapporter.

För att dessa inte ska påverka slutsatser om förekomsten av rapporteringspliktiga it-incidenter under begränsade tidsperioder gör MSB en distinktion mellan det

totala antalet inkomna it-incidentrapporter och antalet *unika* it-incidenter som de facto har rapporterats. Under 2024 bedöms 79 procent av de inkomna it-incident-rapporterna beskriva unika it-incidenter. Förhållandet åskådliggörs i *diagram 5* som redogör för hur många it-incidentrapporter som inkommit på en månadsbasis i förhållande till hur många av dessa som beskriver unika it-incidenter.

Diagram 5. Inkomna it-incidentrapporter och rapporterade unika it-incidenter



MSB gör en distinktion mellan rapporterade unika it-incidenter och inkomna it-incidentrapporter. Detta då det kan förekomma större leveranskedjeincidenter som påverkar flertalet rapporteringspliktiga organisationer samtidigt.

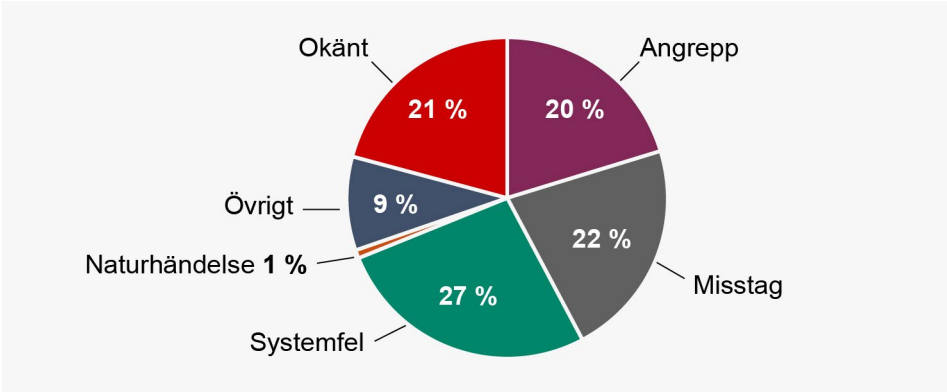
I jämförelse med tidigare går det att koppla ett större antal av inkomna it-incidentrapporter till ett fåtal leveranskedjeincidenter. Dessa är allvarliga på så sätt att risken för samhällskonsekvenser bedöms vara större när flera samhällsviktiga verksamheter påverkas samtidigt.

Diskrepansen mellan inkomna it-incidentrapporter och rapporterade unika it-incidenter är mest påtaglig i början av året. Skillnaden kan härröras till det stora antalet rapporter som inkom till följd av utpressningsangreppet som utfördes mot it-leverantören Tietoevry. Den medialt uppmärksammade incidenten innebar att informationssystem och information som nyttjades av ett stort antal offentliga såväl som privata organisationer blev otillgängliga. It-incidenten innebar därtill viss påverkan på leveransen av samhällsviktiga tjänster inom hälso- och sjukvård.

Systemfel och misstag vanligaste orsakerna

Diagram 6 illustrerar fördelningen av orsaker bakom rapporterade unika it-incidenter, alltså antalet rapporterade it-incidenter exkluderande de rapporter som bedöms beskriva störningar till följd av samma ursprungliga it-incident. Under 2024 utgjorde systemfel och misstag de vanligast rapporterade orsakerna bakom it-incidenter. En större andel av dessa it-incidenter har uppstått till följd av genomförda ändringar inom it-miljön alternativt som en konsekvens av att ändringar inte har genomförts.

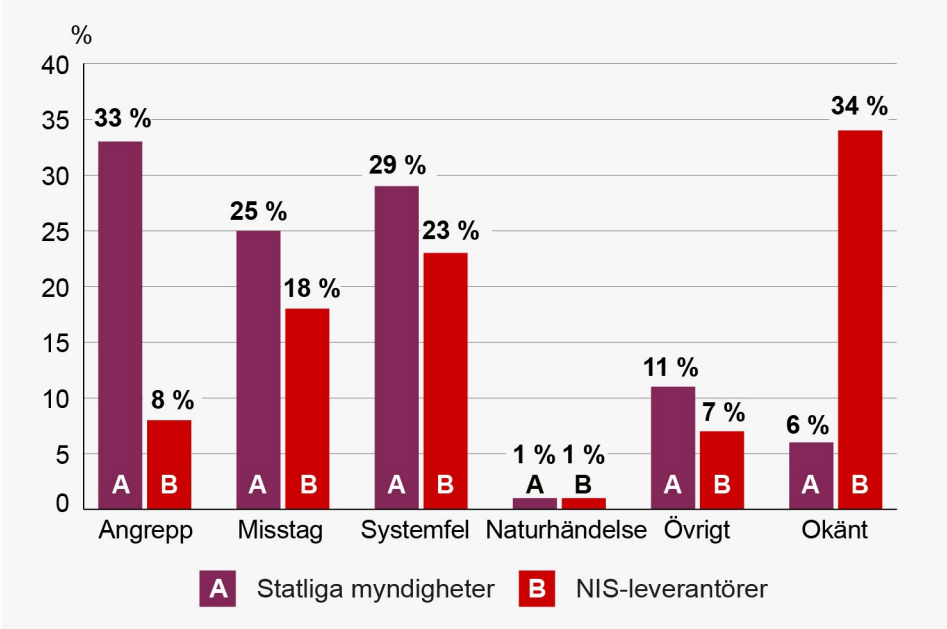
Diagram 6. Fördelning av rapporterade orsaker 2024, unika it-incidenter



Med undantag från 2023 har systemfel och misstag även tidigare år uppgetts vara de vanligaste orsakerna bakom rapporteringspliktiga it-incidenter. 2023 utgjorde angrepp den enskilt största rapporterade orsakskategorin. I perioder, särskilt under våren, rapporterade statliga myndigheter då fler överbelastningsangrepp. Överbelastningsangrepp är också den mest frekvent rapporterade angrepps-metoden under 2024, samtidigt som det i incidentrapporteringen inte går att urskilja samma perioder av intensiv aktivitet som gick att observera under 2023.

Som redogörs i *diagram 7* utgör angrepp fortsatt den mest frekvent rapporterade orsaken för statliga myndigheter, varav en merpart beskriver överbelastningsangrepp. Liksom tidigare år har NIS-leverantörer rapporterat ytterst få angrepp. Det bedöms bero på att konsekvenserna av cyberangreppsförsök, trots att de kan förekomma relativt frekvent, sällan resulterar i störningar som lever upp till MSB:s föreskrifter för rapporteringspliktiga it-incidenter enligt NIS-lagstiftningen. Då en it-incident kan vara rapporteringspliktig för statliga myndigheter oavhängigt om en störning inträffat rapporteras i praktiken fler it-incidenter som inte föranlett några större konsekvenser.

Diagram 7. Fördelning av rapporterade orsaker 2024 statliga myndigheter och NIS-leverantörer, unika it-incidenter



21 procent av rapportörerna har uppgett den bakomliggande orsaken som ”okänd” vid rapporteringstillfället. Andelen ligger i linje med tidigare år och liksom tidigare år står NIS-leverantörer för huvudparten av dessa rapporter. Drygt 80 procent av de it-incidenter som uppges ha en okänd orsak har sitt ursprung hos en leverantör. Det bedöms bero på att orsaken bakom incidenter hos en leverantör inte alltid kommuniceras alls, eller i direkt anslutning till, att en incident inträffat. Förekomsten kan delvis visa på att flera rapporteringspliktiga organisationer av olika anledningar saknar effektiva kontaktvägar för utbyte av information med leverantör vid händelse av en störning i den egna verksamheten.

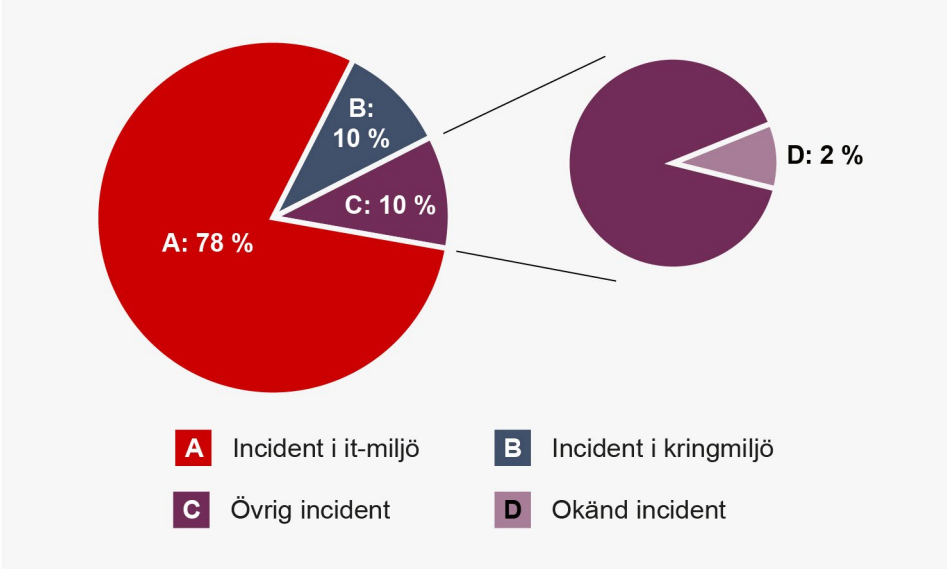
Det är ovanligt att vare sig statliga myndigheter eller NIS-leverantörer inkommer med it-incidentrapporter som redogör för en naturhändelse som bakomliggande orsak. Det beror delvis på en naturhändelse kan vara en orsak till exempelvis systemfel som i sin tur bättre beskriver incidentens rotorsak. De fåtal naturhändelser som förekommit i rapporteringen under de gångna åren utgörs oftast av blixtnedslag som i sin tur resulterat i strömavbrott.

It-incidenters ursprung

Liksom tidigare år uppger de flesta rapportörer att it-incidenten uppstått inom it-miljön, alltså i ett eller flera informationssystem, snarare än kringmiljön. Fördelningen illustreras i *diagram 8*.

Med kringmiljön menas här den infrastruktur som är nödvändig för att upprätthålla en eller flera informationssystem, inkluderande värme- och kylsystem, energiförsörjning eller fysiska förbindelser med komponenter. It-incidenter i kringmiljön orsakas oftast av att en förbindelse upphört. En större andel av dessa har uppstått som konsekvens av att en fiberkabel av misstag skadats vid ett grävarbete. Det är fortsatt ovanligt att det inkommer rapporter som beskriver att infrastruktur skadats till följd av sabotage och ännu mer ovanligt, som tidigare framkommit, att skada har orsakats av en naturhändelse.

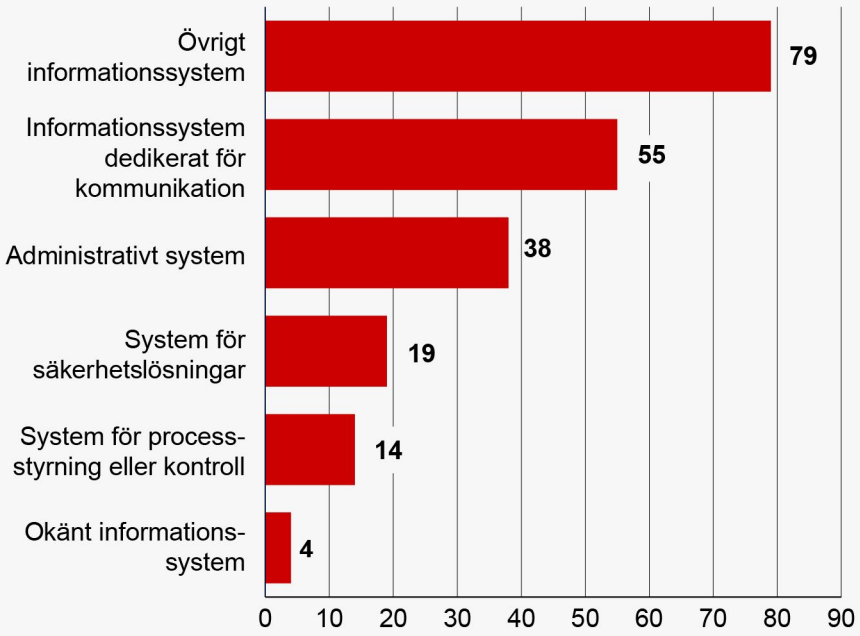
Diagram 8. It-incidentens rapporterade ursprung



Av de it-incidenter som har sitt ursprung i it-miljön så har de allra flesta uppgett att it-incidenten uppstått i ”övrigt informationssystem”, alltså informationssystem som inte specificeras närmare i respektive incidentrapporteringsformulär. Det är vanligt att statliga myndigheter anger detta svarsalternativ. När statliga myndigheter uppgett att it-incidenten påverkat ett ”övrigt” informationssystem har den oftast påverkat externa plattformar och tjänster.

Andra typer av informationssystem som ofta förekommer i rapporteringen är administrativa system samt informationssystem dedikerat för kommunikation, exempelvis e-posttjänster. Då NIS-incidentrapporteringen främst rör incidenter inom hälso- och sjukvården utgörs administrativa system ofta av journalsystem.

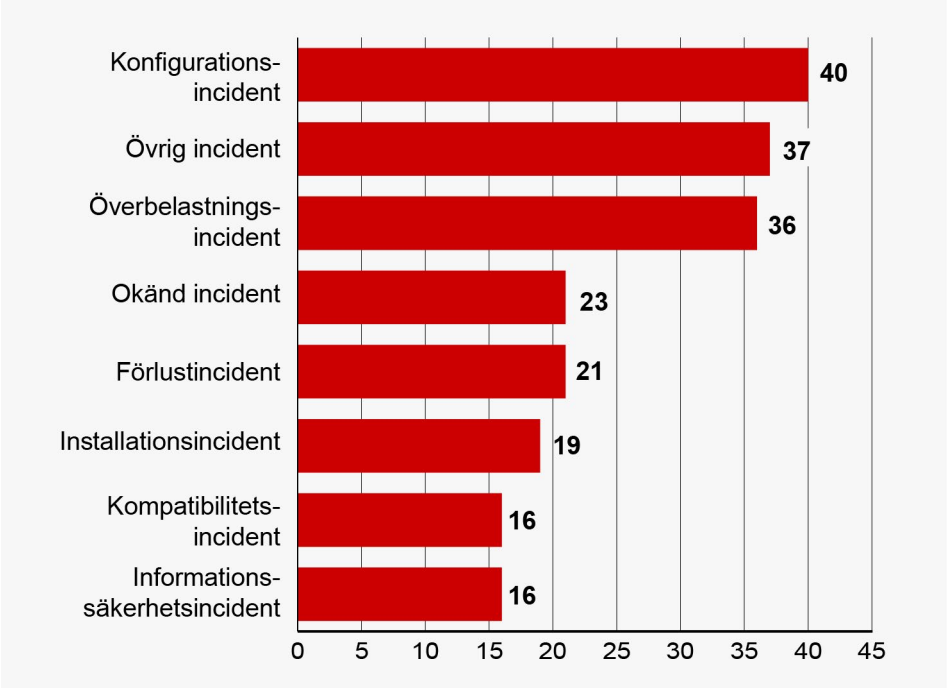
Diagram 9. Påverkad del av it-miljön 2024



Fortsatt stora brister i rutiner för ändringshantering

Som tidigare nämnts är det vanligt förekommande att incidenten har, när den orsakats av systemfel eller misstag, inträffat i samband med en genomförd ändring. I *diagram 11* åskådliggörs att negativ påverkan ofta uppstått som en konsekvens av konfigurations-, installations- och kompatibilitetsincidenter i informationssystem.

Diagram 10. Typer av it-incidenter i it-miljön 2024



Liggande stapeldiagram som redogör för förekomsten av olika typer av it-incidenter i it-miljön under 2024.

I rapporten *Ändringar som både hotar och skyddar: 20 rekommendationer för säkrare ändringar i våra informationssystem*[11] poängterar MSB att en stor andel av de it-incidentrapporter som inkommer till MSB varje år, som beskriver systemfel eller misstag som den bakomliggande orsaken, inträffat i samband en ändring eller till följd av en utebliven ändring. Detta beror på att många rapporteringspliktiga organisationer saknar välfungerande rutiner för att genomföra ändringar i verksamhetskritiska informationssystem och nätverkskomponenter. I flera fall saknar organisationen dessutom nödvändig dokumentation för att kunna genomföra ändringen på ett säkerhet sätt. Utöver att det ökar risken för allvarliga it-incidenter och störningar i samband med ändringar, så kan avsaknaden av rutiner också leda till att organisationen väljer att skjuta på nödvändiga ändringar. Det bidrar i längden till att det uppstår en teknisk skuld som ökar risken för storskaliga incidenter och störningar.

En majoritet av de som uppgett en överbelastningsincident beskriver överbelastningsangrepp som den bakomliggande orsaken. Det förekommer dock enstaka fall som beskriver att en överbelastningsincident uppstod till följd av en intern ändring i ett informationssystem eller en nätverkskomponent.

De som uppgett svarsalternativ ”övrigt” har specificerat olika typer av incidenter. Incidenter som kategoriseras som ”övrigt” eller ”okänt” har i en majoritet av

Not 11. MSB, *Ändringar som både hotar och skyddar: 20 rekommendationer för säkrare ändringar i våra informationssystem.* https://msb.se/sv/publikationer/andringar-som-bade-hotar-och-skyddar-20-rekommendationer-for-sakrare-andringar-i-vara-informationssystem (Hämtad 02/2025)

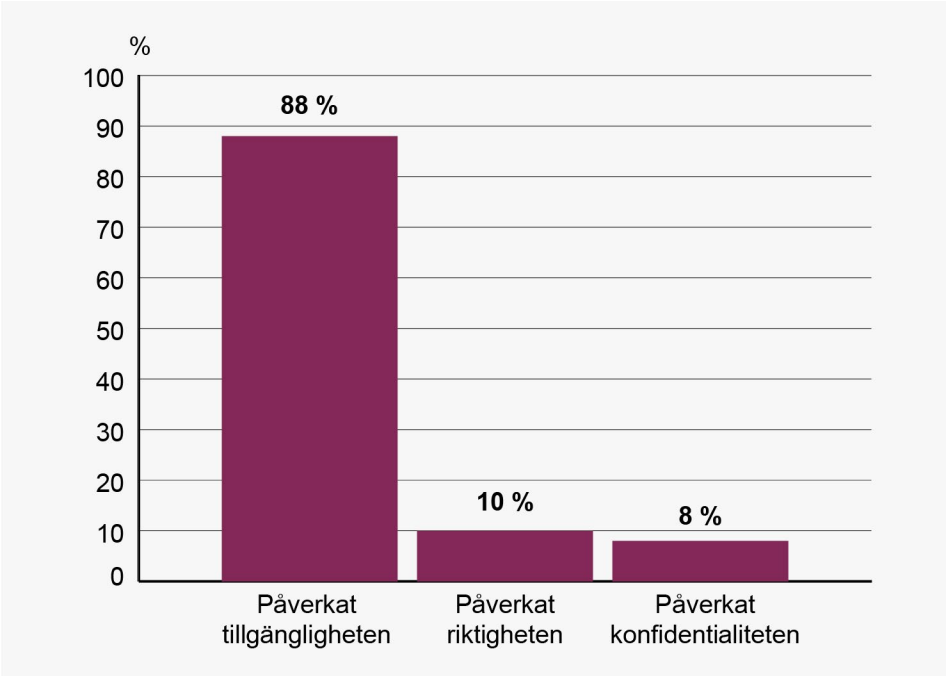
fallen inträffat hos en leverantör till organisationen. Det kan därmed ses som en ytterligare indikation på att många organisationer saknar komplett information från leverantör vid rapporteringstillfället.

It-incidenter påverkar tillgänglighet

I *diagram 12* åskådliggörs, liksom tidigare år, att omkring 90 procent av inkomna it-incidentrapporter har påverkan på tillgängligheten till hela eller delar av ett eller flera informationssystem. Det visar på att rapporteringspliktiga it-incidenter oftast uppstår som en konsekvens av att informationssystem och/eller informationstillgångar blir otillgängliga för användare.[12]

När it-incidenten påverkat riktigheten eller konfidentialiteten har den oftast påverkat ett administrativt system. Flera av dessa it-incidentrapporter beskriver att personuppgifter som lagras i systemen då blivit tillgängliga för obehöriga alternativt att funktioner inte kan administreras på ett korrekt sätt. En knapp majoritet av de it-incidenter som resulterat i att konfidentialiteten eller riktigheten påverkats har inträffat till följd av angrepp.

Diagram 11. Fördelningen av rapporterade it-incidenters påverkan på informationssystem 2024



Rapporterade it-incidenter varierar kraftigt i tidsomfång. De längsta har pågått i flera månader innan de upptäckts och slutligen åtgärdats, medan andra endast resulterat i kortvariga störningar. De fåtal it-incidenter som pågått under längre perioder har ofta upptäckts i ett sent skede. Tvärtom upptäckts de it-incidenter som

Not 12. En del av förklaringen till detta kan vara att rapporteringskrav i enlighet med NIS-lagstiftningen lägger stor vikt vid att förekomsten av, eller en betydande risk för, en störning i leveransen av en samhällsviktig tjänst.

pågått under mycket korta perioder direkt när de inträffar. Så är fallet vid de flesta rapporterade överbelastningsangrepp och andra typ av tillgänglighetsstörningar.

Generellt noteras att majoriteten av rapporterande organisationer specificerar att it-incidenten först upptäcktes av personal. Det kan antas indikera att flera organisationer saknar adekvata tekniska detekteringssystem som skulle kunna ha möjliggjort att en incidenthanteringsprocess kunnat inledas i ett tidigare skede.

De it-incidenter som resulterat i störst konsekvenser för rapporterande organisation är de som orsakat störningar i levererade tjänster under längre perioder. Dessa typer av it-incidenter har ofta resulterat i störningar som gjort det nödvändigt att nyttja alternativa arbetsmetoder under längre perioder, vilket skapar en merkostnad samt underminerar, eller riskerar att underminera, kvalitén i den tjänst eller de tjänster som levereras. Sådana scenarier är vanligt förekommande i incidentrapporterna från hälso- och sjukvårdssektorn samt, i mindre utsträckning, statliga myndigheter.

Att organisationerna applicerar rutiner för kontinuitetshantering är centralt för att störningar ska kunna hanteras utan att det påverkar leveransen av samhällsviktiga tjänster. Av it-incidentrapporteringen framgår det dock att flera organisationer saknar detaljerade och inarbetade sådana. Bland rapporterade leverantörer inom hälso- och sjukvårdssektorn är det exempelvis noterbart att många uttryckligen specificerar behovet av att se över rutiner för alternativa arbetssätt vid utvärdering av hanteringen av störningen.

Få it-incidenter resulterar i samhällspåverkan

It-incidenter kan generellt resultera i negativ samhällspåverkan om den (i) påverkar en samhällsviktig tjänst som levereras till andra och (ii) denna tjänst i sin tur inte kan levereras alls, eller med samma kvalitet, av andra. MSB har tidigare gjort bedömningen att de it-incidenter som resulterat i störst konsekvenser, och således för med sig störst risk att resultera i samhällspåverkan, är de som inträffar inom digitala leveranskedjor som nyttjats av flertalet samhällsviktiga verksamheter. Att it-incidenten resulterar i störningar för flera kan bidra till att incidenten blir mer svårhanterad samt att det kan ta lång tid innan vissa organisationer får den hjälp dem behöver.

Under 2024 har det förekommit ett fåtal större digitala leveranskedjeincidenter som uppmärksammats nationellt såväl som internationellt. De leveranskedje-incidenter som fått störst spridning i Sverige har ofta uppstått som konsekvens av en händelse hos en leverantör av infrastruktur, inkluderande telekommunikationslösningar och it-drift. Det är dock ytterst få av dessa som resulterat i långvariga störningar för ett större antal rapporteringspliktiga organisationer.

Den enskilt största it-incidenten som förekom under året, också sett till mängden it-incidentrapporter som går att härleda till den, är it-incidenten som drabbade it-leverantören Tietoevry i januari 2024. It-incidenten hos Tietoervry illustrerar tydligt risken som uppstår när ett stort antal samhällsviktiga verksamheter är beroende av samma digitala infrastruktur. Samhällskonsekvenserna till följ av it-incidenten hos Tietoevry begränsades samtidigt av det faktum att den generellt påverkade mindre tids- och verksamhetskritiska informationssystem bland samhällsviktiga verksamheter. Bortfallet kunde därmed i de flesta fall kompenseras för på kort sikt.

Leveranskedjeincidenten Tietoevry

Under natten till den 20 januari 2024 drabbades ett datacenter tillhörande företaget Tietoevry för ett utpressningsangrepp som tvingade dem att temporärt isolera och stänga ner delar av datacentret. It-incidenten innebar att informationstillgångar och informationssystem som flera av Tietoevrys kunder nyttjade inom sin dagliga verksamhet blev otillgängliga. Bland påverkade kunder fanns både statliga myndigheter, regioner, kommuner och företag.[13]

Incidenten resulterade i konsekvenser för ett stort antal myndigheter, till stor del på grund av att det av Statens Servicecenters administrerade HR-system Primula blev otillgängligt. Primula nyttjas av 120 myndigheter med sammantaget omkring 60 000 anställda. Under tiden för störningen var det inte möjligt för organisationer som nyttjar tjänsten att exempelvis administrera löner eller medarbetares egenrapportering, exempelvis för sjukfrånvaro eller semester.[14]

Incidenten påverkade även ett stort antal aktörer inom hälso- och sjukvårdssektorn, inklusive flera regioner och kommuner. Detta primärt på grund av att plattformen Prator, som nyttjas för kommunikation mellan vårdorganisationer, blev otillgänglig. Störningen innebar att flera hälso- och sjukvårdsinstanser behövde nyttja alternativa arbetssätt vid exempelvis utskrivning av patienter. Det innebar merarbete för vårdpersonal, och i vissa fall även en fördröjning. Flera regioner såsom Region Blekinge, Sörmland och Uppsala gick upp i stabsläge för att hantera störningen.[15]

I minst två fall kunde krypterad information tillhörande kundorganisationer inte återställas. Tand- och läkemedelsförmånsverket (TLV) förlorade hela sitt digitala diarium.[16] Deras samlade bedömning är att störningen inom deras verksamhet resulterade i logistiska problem för läkemedelsdistributörer och bidrog till ökade samhällskostnader på grund av dess påverkan på läkemedelsmarknaden.[17] I Vellinge kommun betraktades mycket av den information som påverkades, inklusive avslutade patientjournaler från äldreboenden och inom socialtjänsten, som förlorad. Många av de informationssystem som driftades av Tietoevry behövde därutöver återställas från grunden, vilket orsakade omfattande merarbete för kommunen.[18]

Not 13. Tietoevery, *Tietoevry: Slutsatser gällande ransomware-attacken.* https://tietoevry.com/se/nyhetsrum/alla-nyheter-och-pressmeddelanden/pressmeddelande/2024/04/tietoevry-slutsatser-gallande-ransomwarattacken (Hämtad 10/2024)

Not 14. SVT, *120 myndigheter drabbade av it-attack – tiotusentals anställda påverkade.* https://svt.se/nyheter/inrikes/120-myndigheter-drabbade-av-it-attack-tiotusentals-anstallda (Hämtad 10/2024)

Not 15. DagensMedicin, *Regionchefer drar lärdomar efter hackarattacken.* https://dagensmedicin.se/vardens-styrning/digitalisering/regionchefer-drar-lardomar-efter-hackarattacken (Hämtad 10/2024)

Not 16. Läkartidningen, *Stora följder av IT-attacken hos TLV.* https://lakartidningen.se/aktuellt/nyheter/2024/01/stora-foljder-av-it-attacken-hos-tlv (Hämtad 10/2024)

Not 17. TLV, *It-attack ledde till problem för apoteken och omfattande extra samhällskostnader.* https://tlv.se/press/nyheter/arkiv/2024-10-29-it-attack-ledde-till-problem-for-apoteken-och-omfattande-extra-samhallskostnader.html (Hämtad 10/2024)

Not 18. Vellinge Kommun, *IT-attacken som drabbat Vellinge kommun får mycket stora följder*. https://vellinge.se/nyhetsarkiv/2024/01/it-attacken-som-drabbat-vellinge-kommun-far-mycket-stora-foljder (Hämtad 10/2024)

Tema:

Verktyg för ökad motståndskraft och stärkt civilt försvar

Tema: Verktyg för ökad motståndskraft och stärkt civilt försvar

Detta temakapitel ger en översiktsbild över ett urval av de verktyg som MSB och MSB:s samarbetspartner tillhandahåller som stöd till organisationer som vill förbättra sitt cybersäkerhetsarbete. Genom att förbättra cybersäkerheten kan organisationer öka sin motståndskraft att stå emot och bemöta cyberangrepp och andra orsaker till it-incidenter, vilket i sin tur stärker det civila försvaret.

Cybersäkerhet är helt avgörande för Sveriges motståndskraft både i fred, kris och krig. Störningar i digitala tjänster eller informationsflöden kan få allvarliga konsekvenser för samhällsviktiga verksamheter. Utan motståndskraft, det vill säga förmåga att skydda sig mot cyberangrepp och andra hot, blir Sverige sårbart. I ljuset av det säkerhetspolitiska läget är det väsentligt att organisationer arbetar med cybersäkerhets- och beredskapsfrågor på ett sammanhållet och effektivt sätt.

Sverige har ett ”hela samhället”-tillvägagångssätt för att bemöta dessa utmaningar inom ramen för totalförsvaret.[19] Totalförsvaret består av två delar: det militära försvaret och det civila försvaret. Det innebär att alla, inklusive regeringen, myndigheter, privata företag och individer, har en roll i Sveriges försvar. Cybersäkerhet utgör en grundpelare i det moderna civila försvaret.[20] Alla behöver vara kapabla att motstå och bemöta alla typer av hot, inklusive cyberhoten.

För att säkerställa att Sveriges digitala infrastruktur är motståndskraftig behöver organisationer säkerställa att informationssystem och nätverk är robusta, resilienta och har redundans. *Robusthet* uppnås genom att organisationer bedriver ett systematiskt riskförebyggande och riskhanterande säkerhetsarbete. Regelbundet underhåller systemen för att förebygga sårbarheter och säkerställa att systemen är uppdaterade. *Resiliens* uppnås genom att organisationer planerar och övar på såväl incidenthantering som kontinuitetshantering. Resiliens kan förstärkas

Not 19. Regeringskansliet, Totalförsvar. https://regeringen.se/regeringens-politik/totalforsvar (Hämtad 12/2024)

Not 20. Regeringskansliet, *Historisk satsning på cybersäkerhet*. https://regeringen.se/pressmeddelanden/2024/09/historisk-satsning-pa-cybersakerhet (Hämtad 01/2025)

genom samarbete samt tillgång till backuper, reservdelar och komponenter som möjliggör snabb återhämtning efter störningar. *Redundans* kan uppnås genom att undvika så kallade monoberoenden till tjänster och varor från leverantörer. Detta kan exempelvis göras genom avtal med alternativa leverantörer som kan aktiveras vid behov. För vissa kritiska tjänster och varor kan det vara värt att utveckla interna resurser och kapaciteter för att minska beroendet av externa parter.

De senaste åren har flera EU-regleringar tillkommit. Initiativen på cybersäkerhetsområdet förväntas stärka organisationers motståndskraft. Mängden lagar, förordningar och föreskrifter kan dock upplevas som en belastning för många organisationer när de på mycket kort tid måste beakta och implementera flera säkerhetsåtgärder. Samtidigt är organisationers resurser begränsade och kompetens saknas ibland för förbättringsarbetet.[21]

Den snabba tekniska utvecklingen kräver dessutom att organisationer håller sig uppdaterade gällande de senaste verktygen och teknikerna. Det skapar utmaningar kring ständigt lärande, uppdatering av befintliga system och utbildning av medarbetare med mera. En av de största utmaningarna i arbetet med att höja nivån på cybersäkerhetsarbetet är brist på till cybersäkerhetskompetens, vilket bekräftas av flera studier.[22, 23] I frågan om kompetensförsörjning spelar både universitet och tekniska högskolor samt den privata sektorn en central roll. Ett stärkt samarbete mellan privat och offentlig sektor ses därför som nödvändigt för att bemöta avsaknaden av kompetens långsiktigt.[24]

Det här temakapitlet redogör för några av de verktyg som MSB och MSB:s samarbetspartner tillhandahåller. Dessa verktyg, som inkluderar rådgivning, utbildningar, och plattformar för kunskapsutbyte, utgör stöd för organisationer som önskar förbättra sitt systematiska och riskbaserade cybersäkerhetsarbete, men som i vissa hänseenden saknar nödvändig kompetens eller resurser.

Många gånger saknas kunskap om var de tillgängliga verktygen kan hittas och på vilket sätt de kan användas. MSB hoppas göra cybersäkerhetsarbetet enklare för organisationer genom att öka medvetenheten om det stöd som i dagsläget finns att tillgå. Genom implementeringen av gedigna arbetssätt och ökat kunskapsutbyte kan den samlade cybersäkerhetsförmågan och det svenska civila försvaret stärkas.

Not 21. MSB, *Resultatredovisning av Cybersäkerhetskollen 2024: Det systematiska cybersäkerhetsarbetet i den offentliga förvaltningen*. https://msb.se/sv/publikationer/resultatredovisning-av-cybersakerhetskollen-2024--det-systematiska-cybersakerhetsarbetet-i-den-offentliga-forvaltningen (Hämtad 02/2025)

Not 22. ICS, *Cybersecurity Workforce Study 2022*. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf (Hämtad 12/2024)

Not 23. ISSA, *The Life and Times of Cybersecurity Professionals*. https://techtarget.com/esg-global/wp-content/uploads/2023/09/The-Life-and-Times-of-Cybersecurity-Professionals-Volume-VI.pdf (Hämtad 12/2024)

Not 24. Regeringen, *Nationell strategi för samhällets informations- och cybersäkerhet*. https://regeringen.se/regeringens-politik/krisberedskap/nationell-strategi-for-samhallets-informations--och-cybersakerhet (Hämtad 11/2024)

Verktyg översikt

Nationellt cybersäkerhetscenter (NCSC)

MSB arbetar inom NCSC som stärker Sveriges förmåga att förebygga, upptäcka och hantera cyberhot.

Grundläggande verktyg

Grundläggande verktyg för organisationer inom ramen för det egna systematiska och riskbaserade cybersäkerhetsarbetet. Här ingår:

- Cybersäkerhetskollen
- Cybersäkerhetsrådgivning
- Metodstödet
- Föreskrifter
- Vägledningar

Operativt stöd (CERT-SE)

Rådgivning kring hantering av pågående it-incidenter, förebyggande av it-incidenter samt it-incidentrapportering.

Kunskapshöjande verktyg

Verktyg som organisationer kan nyttja för att öka sin kunskap inom cybersäkerhetsområdet. Här ingår:

- Utbildningar
- Rapporter
- Checklistor
- Cybersäkerhet för kommuner
- Informationssäkerhetsmånaden – Tänk säkert
- Termbank

Nätverk och samarbeten

Här presenteras några av de verktyg och nätverk som är öppna för de som samordnar frågor som rör cybersäkerhet.

- Mognadsdialogen
- Nätverk för myndigheter – Snits
- Nätverk för kommuner – KIS
- Nätverk för regioner och andra i ”vården” – HoSIS

Forskning och innovation inom cybersäkerhet (NCC-SE)

Ett sätt att möta framtidens utmaningar är genom forskning och innovation. På det här området ser NCC-SE att Sverige ligger väl till. NCC-SE ansvarar även för utveckling och inriktning av Sveriges nationella kompetensgemenskap:

- Cybernoden

Nationellt cybersäkerhetscenter (NCSC)

- **Målgrupp:** Alla organisationer.
- **Syfte:** Cybersäkerhetscentret syftar till att ge förbättrade möjligheter att höja den nationella förmågan att förebygga, upptäcka och hantera cyberangrepp och andra orsaker till it-incidenter som riskerar att skada Sveriges säkerhet.
- **Länk:** NCSC

MSB arbetar inom NCSC som stärker Sveriges förmåga att förebygga, upptäcka och hantera cyberhot. Här samarbetar myndigheter med kompetens och uppgifter inom svensk cybersäkerhet tillsammans med näringslivet. Centret samverkar med privata och offentliga aktörer för att stärka cybersäkerheten i samhället. NCSC har bland annat tagit fram ett antal rapporter, dessa finns listade i avsnittet *Rapporter* nedan.

NCSC startade 2020 och är sedan 2024 en del av Försvarets radioanstalt, FRA.

Grundläggande verktyg

I detta avsnitt listas de verktyg som MSB bedömer vara grundläggande för organisationer inom ramen för det egna systematiska och riskbaserade cybersäkerhetsarbetet. Ett aktivt nyttjade av dessa verktyg ger organisationen en god översikt av det som behöver göras för att säkerställa att organisationen har vidtagit nödvändiga säkerhetsåtgärder och lever upp till nuvarande eller kommande lagkrav. Verktyg som Cybersäkerhetskollen kan därtill hjälpa organisationen utvärdera de egna insatserna samt jämföra dem med andra jämförbara organisationer.

Många organisationer uppfattar ny lagstiftning på området som svåröversiktlig och resurskrävande. Ett centralt verktyg för att bemöta en stor del av ny lagstiftning är att följa MSB:s föreskrifter om informationssäkerhet samt för statliga myndigheter[25] medföljande vägledning[26].

Not 25. MSB, *MSBFS 2020:6 föreskrifter om informationssäkerhet för statliga myndigheter.* https://msb.se/sv/regler/gallande-regler/krisberedskap-och-informationssakerhet/msbfs-20206 (Hämtad 01/2025)

Not 26. MSB, *Vägledning: säkerhetsåtgärder i informationssystem.* https://msb.se/sv/publikationer/vagledning--sakerhetsatgarder-i-informationssystem (Hämtad 01/2025)

Cybersäkerhetskollen

- **Målgrupp:** Offentlig sektor och samhällsviktiga verksamheter som omfattas av NIS-regleringen. Verktyget kan dock användas av andra organisationer också.
- **Syfte:** Cybersäkerhetskollen är samlingsnamnet för MSB:s cybersäkerhetsmätningar.
- **Länk:** Cybersäkerhetskollen

Cybersäkerhetskollen är samlingsnamnet på MSB:s verktyg för cybersäkerhetsmätningar. Cybersäkerhetskollen består av flera delar, inkluderande:

Infosäkkollen som är en mätning som stödjer uppföljning och förbättring av systematiskt informationssäkerhetsarbete. Med verktyget kan organisationen själv undersöka vilken nivå arbetet befinner sig på och hur det kan utvecklas. Återkopplingen presenteras direkt i verktyget tillsammans med tips med relevant stöd och länkar. Resultatet ger underlag för planering och prioritering, underlag för diskussion i till exempel en ledningsgrupp och med regelbundna uppföljningar kan utvecklingen följas över tid. Infosäkkollen är baserad på MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6), och framtagen och testad tillsammans med offentlig sektor. I samband med utvärderingen av tredje mätningen 2024 uppgav över 80 procent att Infosäkkollen är värdefull för deras organisations cybersäkerhetsarbete, vilket får ses som ett gott betyg för modellens metodik.

It-säkkollen är motsvarande mätning fast för en organisations it-säkerhetsåtgärder. Mätningen har fram tills nu varit en självskattningsundersökning, och har vidareutvecklats för att genomföras i full skala i mätningen 2025. Då kommer It-säkkollens metodik efterlikna Infosäkkollens och även utformas som ett verktyg med direkt återkoppling. Nivå 3 i It-säkkollen är en indikation på att organisationen lever upp till MSB:s föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).

MSB analyserar och sammanställer resultaten och redovisar en nationell lägesbild.[27] När resultaten från en mätning bearbetats tillgängliggör MSB även Infosäkkollen benchmark.[28] Det är ett verktyg som gör det möjligt för inrapporterande organisationer att jämföra sina egna resultat med andra svarande organisationers (på gruppnivå).

Not 27. MSB, *Resultatet från Cybersäkerhetskollen.* https://msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/arbeta-systematiskt-informationssakerhet-och-cybersakerhet/cybersakerhetskollen/resultatet-fran-cybersakerhetskollen (Hämtad 02/2025)

Not 28. MSB, *Infosäkkollen benchmark.* https://msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/arbeta-systematiskt-informationssakerhet-och-cybersakerhet/cybersakerhetskollen/infosakkollen-benchmark (Hämtad 2/2025)

Cybersäkerhetsrådgivning

- **Målgrupp:** Alla organisationer. Prioritet ges främst i ärenden från offentlig sektor, men Cybersäkerhetsrådgivningen tar även emot ärenden från näringsliv, särskilt organisationer inom samhällsviktig verksamhet.
- **Syfte:** att stötta organisationer att anpassa det systematiska och riskbaserade cybersäkerhetsarbetet till deras verksamhetsbehov.
- **Länk:** Cybersäkerhetsrådgivningen

Cybersäkerhetsrådgivningen vänder sig till alla som deltar i, driver eller ansvarar för cybersäkerhetsarbetet i en organisation. Cybersäkerhetsrådgivningen stöttar med:

- Att hitta rätt information och vägledning för det arbete som ska genomföras. MSB har mycket stödmaterial inom cybersäkerhet.
- Att komplettera de vägledningar och stödmaterial som tagits fram för att kunna användas av alla typer av verksamheter. Rådgivningen hjälper till att anpassa arbetet till organisationen.
- Svar på direkta faktafrågor. Det kan till exempel handla om vad ett visst begrepp betyder, standarder som finns på området eller vilket stödmaterial som kan användas.
- Att fungera som bollplank och hjälpa till att komma vidare i arbetet.

Metodstödet

- **Målgrupp:** Alla organisationer.
- **Syfte:** MSB:s metodstöd syftar till att förtydliga hur ett systematiskt och riskbaserat cybersäkerhetsarbete kan utformas utifrån standarder. Metodstödet innehåller vägledningar, verktyg, tips, mallar och annat stöd och råd.
- **Länk:** Metodstödet

Metodstödet består av fyra olika metodsteg som tillsammans bildar helheten av det systematiska och riskbaserade cybersäkerhetsarbetet. Metodstödets delar kan arbetas igenom i tur och ordning eller använda de delar som passar bäst utifrån var organisationer står i sitt informationssäkerhetsarbete. Många arbetar med flera steg parallellt.

Metodstegen är:

- Identifiera och analysera.
- Utforma.
- Använda.
- Följa upp och förbättra.

Metodstödet baseras på standardserien ISO/IEC 27000, som är etablerad i Sverige och internationellt.

Föreskrifter

- **Målgrupp:** Organisationer som omfattas.
- **Syfte:** Gällande regler inom krisberedskap och informationssäkerhet
- **Länkar:**
  - MSBFS 2024:5 föreskrifter om statliga myndigheters redovisning av risk- och sårbarhetsbedömningar
  - MSBFS 2024:4 föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster
  - MSBFS 2020:7 föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter
  - MSBFS 2020:6 föreskrifter om informationssäkerhet för statliga myndigheter
  - MSBFS 2018:11 föreskrifter och allmänna råd om frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet
  - MSBFS 2018:10 föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av digitala tjänster
  - MSBFS 2018:9 föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av samhällsviktiga tjänster
  - MSBFS 2018:8 föreskrifter och allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster
  - MSBFS 2016:7 föreskrifter och allmänna råd om statliga myndigheters risk- och sårbarhetsanalyser *(föreskriften 2016:7 kommer formellt sett att upphöra 2024-07-01. För de redovisningar av risk- och sårbarhetsbedömningar som ska göras 2024-09-30 gäller istället MSBFS 2024:5.)*
  - MSBFS 2015:5 föreskrifter och allmänna råd om kommuners risk- och sårbarhetsanalyser
  - MSBFS 2015:4 föreskrifter och allmänna råd om landstings risk- och sårbarhetsanalyser

MSB:s föreskrifter syftar till att stärka samhällets krisberedskap och informationssäkerhet. Föreskrifterna reglerar hur organisationer och myndigheter ska planera och förbereda sig för att kunna hantera kriser och upprätthålla säker informationshantering. Efterlevnad av MSB:s föreskrifter kan inte ersätta efterlevnad av andra lagkrav som organisationen omfattas av. Däremot kan det i vissa fall vara så att efterlevnad av MSB:s föreskrifter antingen leder till att organisationen klarar andra krav, eller att organisationen har goda förutsättningar att med mindre ansträngningar klara sådana andra krav.

Organisationer som inte regleras av föreskrifterna kan ha dem som grund för sin egen kravställning.

Vägledningar

➜ **Målgrupp:** Alla organisationer.
➜ **Syfte:** Stöd som kan underlätta organisationer i sitt arbete med cybersäkerhet.
➜ **Länkar:**

- Vägledning: säkerhetsåtgärder i informationssystem
- Vägledningar som stöd vid upphandlingar
- Informationssäkerhet för små företag
- CISO:s vänner – samarbeta inom informationssäkerhet
- Vägledning för fysisk informationssäkerhet i it-utrymmen

MSB:s vägledningar finns till för att stödja organisationer i sitt arbete med cybersäkerhet. I nedan stycken beskrivs några av dessa.

Vägledning: säkerhetsåtgärder i informationssystem

Denna vägledning[29] utgör ett stöd vid tillämpningen av Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd (MSBFS 2020:7) om säkerhetsåtgärder i informationssystem för statliga myndigheter, men kan med fördel användas av alla organisationer, till exempel regioner, kommuner eller företag, som stöd i it-säkerhetsarbetet. Vägledningen riktar sig i första hand till de personer som utvecklar, hanterar och förvaltar en organisations it-miljö, till exempel CIO, it-chef, it-säkerhetsansvariga, it-säkerhetsarkitekter samt CISO i sin roll att samordna organisationens informationssäkerhetsarbete. Föreskrifternas krav på säkerhetsåtgärder motsvarar vad MSB bedömer att en statlig myndighet minst behöver göra för att nå en godtagbar nivå av säkerhet i sin it-miljö. Vilka ytterligare säkerhetsåtgärder som behöver vidtas identifierar organisationen genom sitt systematiska och riskbaserade informationssäkerhetsarbete. Annan reglering kan också ställa högre krav på säkerhet, exempelvis dataskyddsförordningen eller säkerhetsskyddslagen.

Informationssäker upphandling

Varje år genomförs tusentals upphandlingar runt om i Sverige. Det är många faktorer att ta hänsyn till när kraven inför upphandling ska formuleras. Som stöd för hur organisation kan upphandla på ett informationssäkert sätt har vägledningar tagits fram. Dessa vägledningar ska ge organisationer stöd i att ställa tydliga informationssäkerhetskrav så att en organisationsinformation hanteras på ett säkert sätt när informationen hanteras av extern part eller det finns andra beroenden till externa parter för att organisationen ska kunna utföra sin verksamhet på ett tillförlitligt sätt.

Not 29. MSB, *Vägledning: säkerhetsåtgärder i informationssystem.* https://msb.se/sv/publikationer/vagledning--sakerhetsatgarder-i-informationssystem (Hämtad 01/2025)

Upphandla informationssäkert

En vägledning som beskriver ett arbetssätt för att identifiera säkerhetskrav vid olika typer av upphandlingar oberoende för vilken organisation eller verksamhet upphandlingen görs.[30]

Upphandling till samhällsviktig verksamhet

En vägledning som fokuserar på stöd till dig som behöver säkerställa att din samhällsviktiga verksamhet fungerar i alla, eller nästan alla situationer.[31]

Säkerhetsskyddad upphandling

När en myndighet (staten, kommun eller region) avser att begära in ett anbud eller träffa avtal om upphandling där det förekommer hemliga uppgifter, ska myndigheten enligt kap. 2 § 6 i säkerhetsskyddslagen (2018:585) träffa ett skriftligt säkerhetsskyddsavtal med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs i det särskilda fallet.

Säkerhetspolisen har publicerat en vägledning[32] som beskriver handläggningen av säkerhetsskyddsarbetet vid en säkerhetsskyddad upphandling. Den vänder sig i första hand till de myndigheter över vilka Säkerhetspolisen har ett tillsynsansvar.

Statliga ramavtal

Webbplatsen avropa.se tjänar som en portal för Statens inköpscentral vid Kammarkollegiet för att ge information om de upphandlingar av statliga ramavtal som genomförs av Statens inköpscentral. Webbplatsen är ett verktyg för upphandlare och inköpare inom offentlig sektor i sitt arbete med att anskaffa varor och tjänster inom de områden som Statens inköpscentral upphandlar statliga ramavtal.

Statliga myndigheter får avropa från de statliga ramavtalen, men kommuner och regioner har efter särskild anmälan möjlighet att utnyttja de ramavtal som Statens inköpscentral tecknar för information och telekommunikation. Hanteringen av fullmakt för kommun och region sker som tidigare via inbjudan inför respektive upphandling.

Exempel på ramavtal med anknytning till informationssäkerhet är:

- E-förvaltningsstödjande tjänster.
- Elektronisk identifiering (eID).
- Systematiskt Informationssäkerhetsarbete i kommuner.
- IT-Driftstjänster.
- IT-konsulttjänster.

Not 30. MSB, *Upphandla informationssäkert: en vägledning.* https://msb.se/sv/publikationer/upphandla-informationssakert--en-vagledning (Hämtad 11/2024)

Not 31. MSB, *Upphandling till samhällsviktig verksamhet: en vägledning.* https://msb.se/sv/publikationer/upphandling-till-samhallsviktig-verksamhet--en-vagledning (Hämtad 11/2024)

Not 32. Säkerhetspolisen, *Säkerhetsskyddsavtal vid upphandlingar och samarbeten.* https://sakerhetspolisen.se/sakerhetsskydd/sakerhetsskyddsavtal-vid-upphandlingar-och-samarbeten.html (Hämtad 11/2024)

Informationssäkerhet för små företag

En vägledning med rekommendationer för organisationer som driver eget företag med upp till 10 anställda. Den innehåller rekommendationer som hjälp för att göra företaget bättre rustat att hantera information säkert genom att möta it- och internetrelaterade risker och använda digitaliseringen till företaget fördel. [33]

CISO:s vänner – samarbeta inom informationssäkerhet

Som CISO finns det sällan andra kollegor i organisationen som arbetar med exakt samma sak. Därför kan det underlätta både för dig som CISO och verksamheten att hitta andra roller i organisationen vars arbete knyter an till informationssäkerhetsområdet. Dessa roller hittas ofta inom informationshantering av olika slag och är de som MSB brukar kalla CISO:s vänner, och samarbete med dem kan ge mervärde på många sätt. Tre områden som har stor nytta av samarbete är säkerhetsskydd, dataskydd och informationssäkerhet.

Våren 2024 samlades representanter från Integritetsskyddsmyndigheten (IMY), Säkerhetspolisen och MSB för att samtala om på vilket sätt som samarbete kan ske och vilka synergier som finns att uppnå. Deras samtal sändes som ett webbinarium som kallades *Tre sidor av samma mynt – att samordna informationssäkerhet, dataskydd och säkerhetsskydd betalar sig* i serien Informationssäkerhet i fokus[34] med en presentation[35].

Vägledning för fysisk informationssäkerhet i it-utrymmen

Informationshantering är ett centralt stöd för alla typer av verksamheter. En viktig faktor för att kunna skydda informationen är det fysiska skydd som omger olika typer av it-utrymmen. Att planera, utveckla och förvalta it-utrymmen innebär ett stort ekonomiskt åtagande där det inte alltid är lätt att avgöra vilka åtgärder som är lämpliga och rimliga för att ge informationen ett tillräckligt bra skydd. För att underlätta för både myndigheter och andra organisationer att utforma it-utrymmen på ett säkert sätt har MSB och Riksarkivet tillsammans tagit fram denna vägledning.[36]

Not 33. MSB, *Informationssäkerhet för små företag: rekommendationer för dig som driver eget företag med upp till 10 anställda.* https://msb.se/sv/publikationer/informationssakerhet-for-sma-foretag--rekommendationer-for-dig-som-driver-eget-foretag-med-upp-till-10-anstallda (Hämtad 11/2024)

Not 34. Youtube, *Informationssäkerhet i fokus – webbinarium 9: Tre sidor av samma mynt – MSB, IMY & Säpo*. https://youtu.be/DjobKaV6qHQ (Hämtad 11/2024)

Not 35. MSB, *Samordnat systematiskt informationssäkerhetsarbete för att skydda information.* https://msb.se/contentassets/d31d69fc42a6478ebcf2d77da3e035d4/tre-sidor-av-samma-mynt-presentation.pdf (Hämtad 11/2024)

Not 36. MSB, *Vägledning för fysisk informationssäkerhet i it-utrymmen.* https://rib.msb.se/filer/pdf/27280.pdf (Hämtad 02/2025)

Operativt stöd (CERT-SE)

➜ **Målgrupp:** Offentlig sektor, privata företag och organisationer.
➜ **Syfte:** Rådgivning kring hantering av pågående it-incidenter, förebyggande av it-incidenter samt it-incidentrapportering.
➜ **Länk:** CERT-SE

CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stötta samhället i arbetet med att hantera och förebygga it-incidenter. CERT-SE arbetar med att:

- Öka it-säkerhetsmedvetandet genom att förmedla kunskap och fakta samt utfärda varningar och råd om sårbarheter i it-system.
- Hantera it-incidenter genom att skyndsamt sprida information och att samordna åtgärder för att avhjälpa eller lindra effekter av det inträffade.
- Vara Sveriges kontaktpunkt gentemot andra länders motsvarande verksamhet.
- Omvärldsbevaka hot och säkerhetsproblem på it-säkerhetsområdet.
- Samarbeta med nationella och internationella funktioner.
- Driva och delta i nationella och internationella it-säkerhetsforum för erfarenhets- och kompetensutbyte.
- Tillhandahåller automatiserade notifierar av tekniska sårbarheter (ANTS).[37]
- Samarbetar med övriga myndigheter inom Nationellt Cybersäkerhets-centrum (NCSC).[38]

Vid en it-incident kan CERT-SE hjälpa till med bland annat rådgivning kring hantering, eventuella kopplingar till pågående eller tidigare händelser samt teknisk analys av angripna system. Vid användning av PGP-kryptering finns CERT-SE:s publika PGP-nyckel[39]. CERT-SE kan nås dygnet runt årets alla dagar.

Gör så här vid pågående it-incident:

- ring CERT-SE på 010-240 40 40, eller
- skicka e-post till cert@cert.se

Not 37. CERT-SE, *Automatiska notifieringar av tekniska sårbarheter (ANTS).* https://cert.se/rad-och-stod/ants (Hämtad 02/2025)
Not 38. NSCS, *Nationellt cybersäkerhetscenter.* https://ncsc.se (Hämtad 02/2025)
Not 39. CERT-SE, *PGP på CERT-SE.* https://cert.se/pgp (Hämtad 11/2024)

Kunskapshöjande verktyg

I detta avsnitt listas flera verktyg som MSB och MSB:s samarbetspartners tillhandahåller och som organisationer kan nyttja för att öka sin kunskap om cybersäkerhetsområdet. Kunskapshöjande verktyg inkluderar utbildningar, checklistor samt fördjupande rapporter om cybersäkerheten i Sverige. Verktygen riktar sig primärt mot CISO:s och organisationsledningar men kan vara användbara för flertalet målgrupper.

Utbildningar

➜ **Målgrupp:** Alla organisationer och privatpersoner.
➜ **Syfte:** Utbildningar som stöd i organisationers cybersäkerhetsarbete.
➜ **Länkar:**
- Kurs för beslutsfattare: Ledningsperspektiv på informations- och cybersäkerhet
- Digital informationssäkerhetsutbildning för alla (Disa)
- Operativ informationssäkerhetskurs
- Taktisk informationssäkerhetskurs
- Filmer om att utbilda andra
- Webbinarier med Informationssäkerhet i fokus
- Signalskydd – en introduktion

Det kan vara svårt att leva upp till de ökade kraven inom cybersäkerhet, särskilt för mindre organisationer. Ofta är det en person som har flera olika roller och lite tid till varje uppdrag som också fått informationssäkerheten på sitt bord. Att utbilda sig kan vara både dyrt och ta tid, särskilt om det krävs resa och övernattningar. Men man kan komma en bra bit på vägen genom digitala utbildningar. MSB har flera intressanta utbildningar – som dessutom är gratis.

Kurs för beslutsfattare: Ledningsperspektiv på informations- och cybersäkerhet

En kurs som vänder sig till personer i ledande befattningar i verksamheter som är viktiga för samhällets funktionalitet, inom statliga myndigheter, regioner och kommuner såväl som näringsliv och frivilligorganisationer.

Kursen är utformad för de som ansvarar för övergripande styrning och ledning i organisationen, som behöver fatta nödvändiga beslut för informations- och cybersäkerheten. Även andra ledare och beslutsfattare kan ha nytta av kursen för att öka sin förståelse och förmåga att stödja arbetet i organisationen.[40]

Not 40. MSB, *Kurs för beslutsfattare: Ledningsperspektiv på informations- och cybersäkerhet.* https://msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/kurser-och-natverk-inom-informationssakerhet/kurs-for-beslutsfattare--ledningsperspektiv-pa-informations--och-cybersakerhet (Hämtad 01/2025)

Digital informationssäkerhetsutbildning för alla (Disa)

En informationssäkerhetsutbildning för användare och erbjuds alla organisationer kostnadsfritt. Utbildningen vänder sig till alla på en arbetsplats och kan användas som introduktion för nyanställda, vikarier, konsulter och annan inhyrd personal.[41]

Operativt informationssäkerhetsarbete

För den som redan har en grundläggande kunskap i informationssäkerhetsarbete finns en kurs som ger metoder för att arbeta systematiskt med informationssäkerhet.[42]

Taktiskt informationssäkerhetsarbete

En kurs om ett riskbaserat och systematiskt informationssäkerhetsarbete. För att kunna ta till sig innehållet i den här kursen behöver man ha grundläggande kunskap i systematiskt informationssäkerhetsarbete.[43]

Att utbilda andra

En del av informationssäkerhetsarbetet består av att utbilda andra i sin egen organisation, både i vikten av informationssäkerhetsarbetet och i hur man faktiskt gör. MSB har tagit fram två filmer som kan användas som en del i utbildningen och en som hjälper till att sätta ihop och hålla utbildning i metodstödet för systematiskt informationssäkerhetsarbete.

- Video: Varför informationssäkerhet är så viktigt.[44]
- Video: Hur du kommer igång med arbetet med informationssäkerhet.[45]
- Vägledning i att utbilda andra i metodstödet.[46]

Webbinarier med Informationssäkerhet i fokus

MSB har en serie webbinarier på temat informationssäkerhet. Syftet är att ge vägledning för informationssäkerhetsarbetet och underlätta tillämpning av det stöd som MSB tillhandahåller. Varje tillfälle omfattar en presentation och en frågestund där deltagarna har möjlighet att ställa frågor till en panel från MSB. Alla webbinarier spelas in och föreläsningsdelen publiceras öppet i efterhand.[47]

Not 41. MSB, *Digital informationssäkerhetsutbildning för alla (Disa)*. https://msb.se/sv/utbildning--ovning/alla-utbildningar/datorstodd-informationssakerhetsutbildning-for-anvandare-disa (Hämtad 11/2024)

Not 42. MSB, *Informationssäkerhet – Operativ informationssäkerhetskurs.* https://msb.se/sv/utbildning--ovning/alla-utbildningar/informationssakerhet---operativ-informationssakerhetskurs-en-introduktionskurs-till-informationssakerhet (Hämtad 11/2024)

Not 43. MSB, *Informationssäkerhet – Taktisk informationssäkerhetskurs.* https://msb.se/sv/utbildning--ovning/alla-utbildningar/informationssakerhet---taktisk-informationssakerhetskurs (Hämtad 11/2024)

Not 44. MSB, *Varför informationssäkerhet är så viktigt.* https://youtube.com/watch?v=2EM-dbwkA2Y (Hämtad 11/2024)

Not 45. MSB, *Hur du kommer igång med arbetet med informationssäkerhet.* https:/youtube.com/watch?v=vMjJj07qKmQ (Hämtad 11/2024)

Not 46. MSB. *Utbilda och kommunicera.* https://metodstod-informationssakerhet.msb.se/sv/anvanda/utbilda-och-kommunicera (Hämtad 11/2024)

Not 47. MSB, *Webbinarieserien Informationssäkerhet i fokus.* https://msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/kurser-och-natverk-inom-informationssakerhet/webbinarier (Hämtad 01/2025)

Signalskydd – en introduktion

En webbkurs som ger grundläggande kunskaper om signalskydd. Kursen är till för organisationer som bedriver säkerhetskänslig verksamhet och vill veta mer om kryptografiska funktioner som har godkänts av Försvarsmakten (signalskyddssystem) och/eller har i säkerhetsskyddsanalysen identifierat ett behov av att dela säkerhetsskyddsklassificerade uppgifter.[48]

Rapporter

- **Målgrupp:** Alla organisationer.
- **Syfte:** Sammanställning av lärdomar om vad som orsakat it-incidenter samt råd och rekommendationer som kan underlätta för organisationer i sitt cybersäkerhetsarbete.
- **Länkar:**

NCSC

- Cybersäkerhet i Sverige 2024.
- Utpressningsangrepp
- Åtgärder för ett säkrare digitalt privatliv
- Cybersäkerhet i Sverige 2022 – Del 1: Hot, metoder, brister och beroenden
- Cybersäkerhet i Sverige 2022 – Del 2: Rekommenderade säkerhetsåtgärder
- Cybersäkerhet i Sverige 2021 – i skuggan av en pandemi

MSB

- Årsrapport it-incidentrapportering 2023: EU förändrar cybersäkerhetsområdet
- Årsrapport it-incidentrapportering 2022: När kriget kom nära
- Årsrapport it-incidentrapportering 2021: En inblick i Sveriges cybersäkerhet
- NIS-leverantörers it-incidentrapportering (2021)
- Temarapport 2023: Cyberangrepp mot samhällsviktiga informationssystem: 25 rekommendationer för stärkt skydd mot cyberangrepp
- Temarapport 2022: Ändringar som både hotar och skyddar: 20 rekommendationer för säkrare ändringar i våra informationssystem
- Temarapport 2021: Hoten mot de digitala leveranskedjorna – 50 rekommendationer för att stärka samhällssäkerheten

Not 48. MSB, *Signalskydd – en introduktion (webbkurs).* https://msb.se/sv/utbildning--ovning/alla-utbildningar/signalskydd--en-introduktion-webbkurs (Hämtad 02/2025)

Inom ramen av det nationella cybersäkerhetscentret (NCSC) har rapporter tagits fram för information och vägledning till organisationer i deras cybersäkerhetsarbete.

MSB sammanställer varje år trender och slutsatser om samhällets cybersäkerhet utifrån inkommen it-incidentrapportering. Underlaget till rapporterna är incidentrapporteringar som MSB får in från statliga myndigheter, leverantörer av samhällsviktiga och digitala tjänster samt organisationers frivilliga rapporteringar. It-incidentrapportering är bra för den egna organisationen, men också en viktig del att skapa kunskap och lärdom om samhällets sårbarheter. I sammanställningarna dras lärdom om vad som orsakar incidenterna, och hur organisationer kan skydda sig. Sammanställningarna om it-incidenter används även i MSB:s strategiska analysarbete och bidrar till att identifiera var det behövs ytterligare säkerhetsarbete.

Cybersäkerhet i Sverige 2024

En rapport för de organisationer som behöver komma igång med cybersäkerhetsarbetet samt de som redan kommit en bit på vägen. På runt 40 sidor får man en grund att stå på. Rapporten går kortfattat igenom hur hotet ser ut, några vanliga metoder för angrepp, saker att observera rörande sina nätverk och till sist tio konkreta råd. Det ersätter inte ett systematiskt cybersäkerhetsarbete, utan ska locka just till att sätta igång med ett sådant, eller aktualisera utvärdering av redan gjorda insatser.[49]

Utpressningsangrepp

En rapport om utpressningsangrepp som har de senaste åren blivit allt mer uppmärksammade, på grund av de konsekvenser som de kan orsaka för organisationer och dess intressenter.[50]

Åtgärder för ett säkrare digitalt privatliv

En rapport med rekommendationerna nedan riktar sig till de som arbetar inom svensk offentlig sektor eller i näringslivet.[51] Är ditt privata digitala liv en språngbräda för hotaktörer som vill påverka din organisation?

Cybersäkerhet i Sverige 2022 – Del 1: Hot, metoder, brister och beroenden

Rapporten ger en samlad lägesbild över cybersäkerhetsrelaterade hot och innehåller exempel från verkligheten under 2022. Rapporten ger även ge stöd till analyser och riskbedömningar vid exempelvis beslut om verksamhetsutveckling, kontrakt eller investeringar.[52]

Not 49. NCSC, *Cybersäkerhet i Sverige 2024.* https://ncsc.se/siteassets/publikationer/cybersakerhet-i-sverige-2024.pdf (Hämtad 01/2025)

Not 50. NCSC, *Utpressningsangrepp.* https://ncsc.se/siteassets/publikationer/utpressningsangrepp---temafordjupning.pdf (Hämtad 01/2025)

Not 51. NCSC, *Åtgärder för ett säkrare digitalt privatliv.* https://ncsc.se/siteassets/publikationer/atgarder-for-ett-sakrare-digitalt-privatliv.pdf (Hämtad 01/2025)

Not 52. NCSC, *Cybersäkerhet i Sverige 2022 – Del 1: Hot, metoder, brister och beroenden.* https://ncsc.se/siteassets/publikationer/ncsc-rappor-1-cybersakerhet-i-sverige-2022-hot-metoder-brister-och-beroenden.pdf (Hämtad 01/2025)

Cybersäkerhet i Sverige 2022 – Del 2: Rekommenderade säkerhetsåtgärder

Rapporten ger rekommendationer om vilka åtgärder som behöver vidtas och hur man rent praktiskt bör gå tillväga för att bygga en säkrare it-miljö. I många fall handlar det om ett ändrat arbetssätt inom organisationen och om att planera, testa, och införa tekniska åtgärder på ett systematiskt sätt.[53]

Cybersäkerhet i Sverige 2021 – i skuggan av en pandemi

Rapporten presenterar myndigheternas bild av hur hotaktörer har agerat under pandemin, och hur svenska verksamheter har agerat. Rapporten redogör även för några lärdomar och rekommenderade åtgärder för att bygga de skydd som kan komma att behövas vid kriser likt pandemin.[54]

Årsrapport it-incidentrapportering 2023: EU förändrar cybersäkerhetsområdet

Rapporten behandlar rapporterade it-incidenter incidenter under 2023 och fördjupar sig 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.[55]

Årsrapport it-incidentrapportering 2022: När kriget kom nära

När kriget kom nära, årsrapport it-incidentrapportering 2022 behandlar it-incidentrapporteringen under 2022, resultatredovisningen från Cybersäkerhetskollen (då kallad Infosäkkollen), ett urval nyheter av särskilt cyberintresse och ett temakapitel om cyberkrigföringen i Ukraina. Årsrapporten sammanställer erfarenheterna i ett kapitel om lärdomar för Sverige och rekommendationer för att stärka den svenska motståndskraften på cybersäkerhetsområdet.[56]

Not 53. NCSC, *Cybersäkerhet i Sverige 2022 – Del 2: Rekommenderade säkerhetsåtgärder.* https://ncsc.se/siteassets/publikationer/ncsc-rapport-2-cybersakerhet-i-sverige-2022-rekommenderade-sakerhetsatgarder.pdf (Hämtad 01/2025)

Not 54. NCSC, *Cybersäkerhet i Sverige 2021 – i skuggan av en pandemi.* https://ncsc.se/siteassets/publikationer/cybersakerhet-i-sverige--i-skuggan-av-en-pandemi-2021.pdf (Hämtad 01/2025)

Not 55. MSB, *EU förändrar cybersäkerhetsområdet: årsrapport it-incidentrapportering 2023*. https://msb.se/sv/publikationer/eu-forandrar-cybersakerhetsomradet--arsrapport-it-incidentrapportering-2023 (Hämtad 02/2025)

Not 56. MSB, *När kriget kom nära: årsrapport it-incidentrapportering 2022.* https://msb.se/sv/publikationer/nar-kriget-kom-nara--arsrapport-it-incidentrapportering-2022 (Hämtad 02/2025)

Årsrapport it-incidentrapportering 2021: En inblick i Sveriges cybersäkerhet

Rapporten innehåller förutom sammanställning av de incidenter som inkommit till MSB under 2021 även lärande exempel, information om incidentrapporteringen och rekommendationer till rapportens målgrupper. Sammanställningen av incidentrapporteringen visar att rapporteringen har minskat och att systemfel och misstag återigen är de mest frekventa orsakerna till incidenterna. Incidenterna inträffar ofta vid misslyckad ändringshantering och påverkar oftast tillgängligheten.[57]

NIS-leverantörers it-incidentrapportering (2021)

Denna rapport behandlar inkomna it-incidentrapporter under 2021 från leverantörer av samhällsviktiga och digitala tjänster, så kallade NIS-leverantörer. NIS-leverantörer är några av de viktigaste organisationerna i Sverige då de tillhandahåller tjänster som är centrala för samhällets funktion. Arbetet med NIS har sitt ursprung i NIS-direktivet som antogs 2016 för att höja den gemensamma nivån på cybersäkerheten i några av den Europeiska unionens viktigaste funktioner. MSB är den myndighet som sedan 2019 tar emot incidentrapporter om incidenter med ursprung i nätverk och informationssystem som orsakat betydande respektive avsevärda störningar från leverantörer av samhällsviktiga och digitala tjänster. Denna rapports målgrupper är främst beslutsfattare, cybersäkerhetsansvariga samt omvärldsbevakande och analyserande roller hos NIS-leverantörer, men de analyser, slutsatser och rekommendationer som presenteras kan vara betydelsefulla även för andra organisationer. Rapporten redogör för incidenterna som inkommit på en övergripande nivå, men presenterar även djupare analys av incidenter inrapporterade av leverantörer inom hälso- och sjukvårds- samt dricksvattensektorn. Utöver detta beskriver rapporten regleringen, hur incidentrapporteringen går till samt ett antal rekommendationer till NIS-leverantörerna som baseras på inkomna incidentrapporter.[58]

Temarapport 2023: Cyberangrepp mot samhällsviktiga informationssystem: 25 rekommendationer för stärkt skydd mot cyberangrepp

Våren 2023 inleddes med ett omfattande antal överbelastningsangrepp. Samtidigt brukar cyberangreppsförsök utgöra mindre än en femtedel av den totala mängden it-incidenter som rapporteras in till MSB. Utifrån identifierade utmaningar har rekommendationer tagits fram för hur en organisation kan stärka sitt skydd mot cyberangreppsförsök, samt minimera skador om en incident ändå inträffar. De organisationer som arbetar systematiskt och riskbaserat utifrån ett allriskperspektiv står bäst rustade. Den här rapporten redogör för

Not 57. MSB, *En inblick i Sveriges cybersäkerhet: årsrapport it-incidentrapportering 2021.* https://msb.se/sv/publikationer/en-inblick-i-sveriges-cybersakerhet--arsrapport-it-incidentrapportering-2021 (Hämtad 02/2025)

Not 58. MSB, *It-incidenter som påverkar samhällsviktiga och digitala tjänster: NIS-leverantörers it-incidentrapportering 2021 årsrapport.* https://msb.se/sv/publikationer/it-incidenter-som-paverkar-samhallsviktiga-och-digitala-tjanster--nis-leverantorers-it-incidentrapportering-2021-arsrapport (Hämtad 02/2025)

angreppsbilden mot statliga myndigheter och leverantörer av samhällsviktiga tjänster baserat på it-incidentrapporter som MSB mottagit från april 2019 till september 2023.[59]

Temarapport 2022: Ändringar som både hotar och skyddar: 20 rekommendationer för säkrare ändringar i våra informationssystem

Ändringar i informationssystem som inte hanteras på ett korrekt och säkert sätt ökar risken för incidenter. Detta kan i sin tur riskera att äventyra informationssystems eller informations konfidentialitet, riktighet och tillgänglighet genom att nya sårbarheter och hot uppstår. Incidentrapporteringen från statliga myndigheter och NIS-leverantörer har under flera år bekräftat detta. Organisationer bör således utveckla och följa arbetssätt där ändringar kan genomföras systematiskt, noggrant och processtyrt.[60]

Temarapport 2021: Hoten mot de digitala leveranskedjorna – 50 rekommendationer för att stärka samhällssäkerheten

Digitala leveranskedjor möjliggör de flesta samhällsviktiga tjänster som används dagligen och är beroende av. Incidenter i leveranskedjorna kan leda till omfattande konsekvenser och kommer sannolikt, i takt med den fortsatta digitaliseringen, att bli allt vanligare. Rapporten visar på att det är mycket vanligt med incidenter i digitala leveranskedjor och att den stora majoriteten av sådana incidenter orsakas av misstag, systemfel och naturhändelser. Analysen har också funnit att informationsdelningen i de digitala leveranskedjorna ofta brister. För att motverka sårbarheterna i och hoten mot de digitala leveranskedjorna presenterar rapporten att antal rekommendationer för att stärka säkerheten.[61]

Not 59. MSB, *Cyberangrepp mot samhällsviktiga informationssystem: 25 rekommendationer för stärkt skydd mot cyberangrepp.* https://msb.se/sv/publikationer/cyberangrepp-mot-samhallsviktiga-informationssystem--25-rekommendationer-for-starkt-skydd-mot-cyberangrepp (Hämtad 02/2025)

Not 60. MSB, *Ändringar som både hotar och skyddar: 20 rekommendationer för säkrare ändringar i våra informationssystem.* https://msb.se/sv/publikationer/andringar-som-bade-hotar-och-skyddar-20-rekommendationer-for-sakrare-andringar-i-vara-informationssystem (Hämtad 02/2025)

Not 61. MSB, *Hoten mot de digitala leveranskedjorna – 50 rekommendation för att stärka samhällsäkerheten.* https://msb.se/sv/publikationer/hoten-mot-de-digitala-leveranskedjorna--50-rekommendationer-for-att-starka-samhallssakerheten (Hämtad 01/2025)

Checklistor

➜ **Målgrupp:** Alla organisationer.

➜ **Syfte:** Checklistor ger tips på hur organisationer med enkla åtgärder kan stärka sin cybersäkerhet för att skydda sin verksamhet.

➜ **Länkar:**

- Skydd av samhällsviktig verksamhet
- Alla kan bidra till Sverige cybersäkerhet. Du också

Om värdefull information hamnar i fel händer kan konsekvenserna bli allvarliga. MSB har tagit fram ett flertal checklistor som ger tips om hur organisationer kan skydda och förhindra att information hamnar i fel händer. Genom enkla åtgärder och rutiner, så förbättras säkerheten avsevärt.

Skydd av samhällsviktig verksamhet

Ökad motståndskraft genom arbete med riskhantering, kontinuitetshantering, informations- och cybersäkerhet och hantera oönskade händelser.

Syftet med detta stödjande dokument är att närmare beskriva med hjälp av checklistor vad aktörer som tillhandahåller samhällsviktig verksamhet behöver arbeta med för att öka motståndskraften och vad som ingår i detta arbete.[62]

Alla kan bidra till Sveriges cybersäkerhet. Du också.

Dessa checklistor ger tips på hur organisationer med enkla åtgärder kan skydda sin verksamhet och förhindra att information hamnar i fel händer. Denna skrift är en del av en informationskampanj som MSB har fått i uppdrag av regeringen att genomföra tillsammans med Polisen. Den syftar till att öka medvetenheten och kunskapen om digitala sårbarheter och hur en enskild person och företagare skyddar sig och sitt företag.[63]

Not 62. MSB, *Skydd av samhällsviktig verksamhet – Ökad motståndskraft genom arbete med riskhantering, kontinuitetshantering, informations- och cybersäkerhet och hantera oönskade händelser.* https://rib.msb.se/filer/pdf/30783.pdf (Hämtad 01/2025)

Not 63. MSB, *Alla kan bidra till Sveriges cybersäkerhet. Du också.* https://msb.se/sv/publikationer/till-foretag.-alla-kan-bidra-till-sveriges-cybersakerhet.-du-ocksa (Hämtad 11/2024)

Cybersäkerhet för kommuner

- **Målgrupp:** Kommuner men kan med fördel användas av andra organisationer.
- **Syfte:** Att förbättra cybersäkerheten hos en kommun.
- **Länk:** Cybersäkerhet för kommuner

Cyberincidenter orsakade av angrepp och andra typer av oönskade händelser fortsätter att drabba Sveriges kommuner. Samtidigt skärps kraven med det nya NIS2-direktivet som införs i hela EU under 2025. Alla behöver bidra till att cybersäkra organisationen.

Färdigt material för arbetsplatsträffar om cybersäkerhet för kommuner och en guide till en cybersäker kommun.

Guide till en cybersäker kommun

En guide till ett 50-tal olika stöd inom informationssäkerhet och cybersäkerhet, utgivna av både MSB och andra. Här ges en snabb överblick över stöd inom sex olika kategorier – på grundläggande nivå, fördjupad nivå och ledningsnivå.[64]

Arbetsplatsträffar

Ett färdigt APT-material som syftar till att bidra till ökad kunskap om informationssäkerhet och cybersäkerhet i kommunen.[65]

Informationssäkerhetsmånaden – Tänk säkert

- **Målgrupp:** Alla organisationer och privatpersoner.
- **Syfte:** Kampanjen är ett långsiktigt arbete med målsättningen att höja medvetenheten och kompetensen hos privatpersoner och organisationer gällande informations- och cybersäkerhet.
- **Länk:** Informationssäkerhetsmånaden – Tänk säkert

Varje år i oktober är informationssäkerhetsmånaden under temat ”Tänk säkert”. Kampanjen är ett långsiktigt arbete med målsättningen att höja medvetenheten och kompetensen hos privatpersoner och företagen för att säkrare hantera exempelvis lösenord, e-legitimation och sin viktigaste information.

Not 64. MSB, *Guide till en cybersäker kommun*. https://msb.se/contentassets/4569eeabc8e64db3952c5c6e0cbc20ae/msb-guide-till-en-cybersaker-kommun-241211.pdf (Hämtad 02/2025)

Not 65. MSB, *Material för arbetsplatsträff*. https://msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/arbeta-systematiskt-informationssakerhet-och-cybersakerhet/cybersakerhet-for-kommuner/apt-material (Hämtad 02/2025)

Digitaliseringen ökar snabbt och påverkar i hög grad enskilda individer och samhället som helhet. Det gör att det är nödvändigt att lägstanivån på samhällets informations- och cybersäkerhet höjs. Kampanjen är ett led i detta.

Kampanjen genomförs av MSB tillsammans med polisen. Därutöver har ett stort antal samarbetspartners från privat, offentlig och ideell verksamhet engagerats för att sprida kampanjens budskap.

Oktober är även EU:s informationssäkerhetsmånad (European Cyber Security Month – ECSM) och arrangeras av EU:s byrå för nät- och informationssäkerhet (Enisa). Syftet är att öka medvetenhet om informations- och cybersäkerhetsfrågor hos allmänheten och hos företag. EU:s informationssäkerhetsmånad har funnits sedan 2012 och Sverige har deltagit genom MSB i ett antal år.

Termbank

- **Målgrupp:** I första hand riktar sig Termbanken för informationssäkerhet till yrkesgrupper som direkt arbetar med informationssäkerhet eller på annat sätt berörs av området. Även journalister, forskare, studenter samt en intresserad allmänhet kan dra nytta av termbankens innehåll.
- **Syfte:** Tjänsten är framtagen för att förbättra möjligheten till samarbeten, genom gemensamma definitioner på centrala begrepp.
- **Länk:** Termbank

Termbanken för informationssäkerhet innehåller den nationella terminologin för informations- och cybersäkerhetsområdet och innehåller svenska och engelska termer, definitioner och förtydligande anmärkningar på svenska med hänvisning till relevanta källor. Terminologiarbetet har utförts inom ramen för nationell (SIS/TK 318) och internationell (ISO/SC 27) standardisering, vilket bidrar till det gemensamma fackspråket.

Termbanken för informationssäkerhet uppdateras kontinuerligt med nya termer och definitioner. Innehållet tas fram av en expertgrupp på MSB som följer nationell och internationell standardisering inom informationssäkerhetsområdet. Genom att göra terminologin lättillgänglig i en termbank vill MSB öka möjligheten att alla som arbetar med informationssäkerhet förstår varandra.

Nätverk och samarbeten

Det finns många olika nätverk för de som arbetar med cybersäkerhet. Här presenteras några av de nätverk som är öppna för de som samordnar frågor som rör cybersäkerhet inom statliga myndigheter, kommuner och regioner. Många som deltar i MSB:s, med flera, cybersäkerhetsnätverk får tillgång till regelbundna lägesbildsuppdateringar och tematiska fördjupningar.

Mognadsdialogen

- ➜ **Målgrupp:** Merparten av organisationer.
- ➜ **Syfte:** En inkörsport till det systematiska och riskbaserade cybersäkerhetsarbetet. Genom dialog skapas en gemensam bild av och förståelse för organisationens nuläge i säkerhetsarbetet.
- ➜ **Länk:** Mognadsdialogen

Mognadsdialogen är en inkörsport till det systematiska och riskbaserade cybersäkerhetsarbetet. Verktyget syftar till att genom dialog skapa en gemensam bild av och förståelse för organisationens nuläge i säkerhetsarbetet som ger en grund till arbete med andra verktyg såsom Cybersäkerhetskollen och Cybersäkerhetsrådgivningen. Det är ett pedagogiskt verktyg för att stödja uppföljning av hur effektivt organisationen arbetar med att skydda sin information utifrån behov, krav och förutsättningar. Genom dialog skapas förståelse och samsyn.

Mognadsdialogen bidrar till att:

- Skapa samsyn och enas om organisationens nuläge.
- Identifiera och prioritera områden för utvecklings- och förbättringsarbetet.
- Öka insikten om vad ett systematiskt arbetssätt innebär.
- Öka förståelsen för vad som ingår i informationssäkerhetsarbetet.
- Öka insikten om vad som krävs för att öka mognaden.
- Öka ledningens engagemang och förmåga att leda och styra.

Nätverk för myndigheter – Snits

Snits är det statliga nätverket för informationssäkerhet.[66] Nätverket är till för dem som innehar en statlig tjänst och har till huvuduppgift att arbeta med informationssäkerhet. Snits ska utgöra ett forum för kontakt- och erfarenhetsutbyte, kompetensutveckling, informationsspridning och diskussioner om systematiskt informationssäkerhetsarbete. Deltagande myndigheter representeras med en person.

Not 66. MSB, *Nätverk om informationssäkerhet för offentliganställda*. https://msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/kurser-och-natverk-inom-informationssakerhet/natverk-om-informationssakerhet-for-offentliganstallda (Hämtad 02/2025)

Snits träffas normalt fyra gånger om året, två gånger på våren och två gånger på hösten. Formerna för sammankomsternas karaktär kan variera, från presentationer till olika typer av gruppdiskussioner. Primärt ska de innehålla aktiviteter som uppmuntrar till deltagande och ger förutsättningar för erfarenhetsutbyten mellan deltagarna.

MSB samordnar och leder nätverkets forum, sammankallar programrådet och förvaltar nätverkets samarbetsyta. Programrådet består av ett antal representanter från myndigheter i nätverket som tillsammans med MSB planerar och tar fram programinnehållet.

Nätverk för kommuner – KIS

Informationssäkerhetsnätverket Sveriges Kommuner, KIS, är ett nätverk för dem som har ett ansvar för arbetet med informationssäkerhet på kommunerna.[67] Syftet med nätverket är att stödja de personer som har det uppdraget på kommunerna med förhoppning om att kommunerna genom att delta i nätverket kan förbättra och effektivisera sitt informations-säkerhetsarbete.

Personer vars arbetsuppgifter handlar om att samordna och utveckla informationssäkerheten i kommunen har behov av att utbyta erfarenheter, kunskap och information med andra kommuner och organisationer.

På Samarbetsrum (länk nedan) finns ett forum för detta. Alla medlemmar får ett eget personligt konto till nätverket. Samarbetsrummet erbjuder ett enklare skydd genom inloggning med lösenord. Där kan man dela med sig av dokument och goda exempel, ställa öppna frågor, ta del av andras erfarenheter, med mera. KIS-nätverket brukar ha två heldagsträffar per år, en på våren och en på hösten. På senare tid har träffarna varit digitala.

Nätverket har idag drygt 360 stycken deltagare fördelat på cirka 180 kommuner, men målet är att alla kommuner i Sverige har minst en person som deltar. Kommunen inbjuds att skicka in namn och e-postadress på den eller de personerna med uppgift att representera kommunen i nätverket.

Nätverk för regioner och andra i ”vården” – HoSIS

Hälso- och sjukvårdens informationssäkerhetsnätverk (HoSIS) är ett nätverk för regionernas och privata vårdgivares informationssäkerhetsansvariga och jurister som arbetar med dessa frågor.[68] Nätverket hette tidigare Nätverket för Informationssäkerhet, (NIS).

Not 67. MSB, *Nätverk om informationssäkerhet för offentliganställda*. https://msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/kurser-och-natverk-inom-informationssakerhet/natverk-om-informationssakerhet-for-offentliganstallda (Hämtad 02/2025)

Not 68. MSB, *Nätverk om informationssäkerhet för offentliganställda*. https://msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/kurser-och-natverk-inom-informationssakerhet/natverk-om-informationssakerhet-for-offentliganstallda (Hämtad 02/2025)

Syftet med nätverket är att stödja personer med ansvar för informationssäkerhetsfrågor i sina respektive organisationer genom erfarenhetsutbyte mellan organisationer.

Medlemmar får ett eget konto i nätverket. Där kan man dela med sig egna, och ta del av andras dokument och goda exempel, erfarenheter etc. Kallelser till möten sker också denna väg. HoSIS brukar ha fyra fysiska möten per år, tre endagarsmöten, oftast i Stockholm, samt ett tvådagarsmöte på någon större ort ute i landet.

HoSIS-nätverket har idag knappt hundra medlemmar fördelade över hela landet.

Deltagande i nätverket är kostnadsfritt men resor och ev. uppehälle i samband med fysiska möten betalas av respektive organisation. HoSIS sponsras av SKR och MSB.

Forskning, innovation och kompetensförsörjning inom cybersäkerhet (NCC-SE)

- **Målgrupp:** Svenska forskningsinstitut, företag och myndigheter.
- **Syfte:** Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE) främjar samarbete mellan för utveckling av cybersäkerhetslösningar.
- **Länk:** NCC-SE

Ett sätt att möta framtidens utmaningar är genom forskning och innovation. På det här området ser NCC-SE att Sverige ligger väl till – men att mycket skulle kunna göras för att stärka Sverige ännu mer, och särskilt vad gäller forskning och innovation inom cybersäkerhet. Inom EU finns en liknande syn – och därför har man antagit den så kallade ECCC-förordningen. Den innebär att man har inrättat ett europeiskt kompetenscenter som, via ett system av nationella samordningscentrum. Pengarna går till satsningar på forskning och utveckling inom cybersäkerhetsområdet. MSB står värd för Sveriges samordningscentrum, kort kallat för NCC-SE, och organiserar tillsammans med RISE den svenska kompetensgemenskapen för forskning, utveckling och innovation på cyberområdet. Sverige har den största kompetensgemenskapen av alla medlemsstater i EU.

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 ansvarar även för utveckling och inriktning av Sveriges nationella kompetensgemenskap (Cybernode) i samarbete med RISE[69] samt genomför nationella cybersäkerhetsrelaterade utlysningar.

Not 69. RISE, *Hållbar omställning och konkurrenskraft på vetenskaplig grund.* https://ri.se/sv (Hämtad 02/2025)

Cybernoden

Cybernoden samverkar med MSB och NCC-SE, där NCC-SE har givit Cybernoden uppdraget att bygga den svenska kompetensgemenskapen inom cybersäkerhet. Denna kompetensgemenskap är en del av EU-projektet ECCC (European Cybersecurity Competence Center).

Nodens operativa arbete styrs av en koordinatorgrupp med deltagare från RISE och NCC-SE. I uppgifterna ingår att löpande bevaka de utlysningar som öppnar, båda inom EU och inom Sverige. Information om detta ges bland annat i deras nyhetsbrev. De genomför teknik-, innovationskonferenser och rundabordssamtal. Noden ska även bidra avseende tolkning av lagar och regler, och därigenom kunna initiera regelförändringar till stöd för innovation.

Nodens webbsidor fortsätter utvecklas och 12 temagrupper finns startade eller är på gång att startas[70].

Not 70. Cybernoden, *Temagrupper.* https://cybernode.se/temagrupper (Hämtad 12/2024)

Slutsatser och rekommendationer

Slutsatser och rekommendationer

Nivån på cybersäkerhetsarbetet i Sverige är låg. Sett i ljuset av det säkerhetspolitiska läget krävs en skyndsam förbättring.

Digitaliseringen inom alla samhällets sektorer fortgår i snabb takt. Cyberhoten blir alltmer komplexa och sofistikerade.[71] Samtidigt pågår ett fullskaligt krig i Europa. Utan motståndskraft, det vill säga förmåga att skydda sig mot cyberangrepp och andra hot, blir Sverige sårbart. Cybersäkerheten är inte bara en teknisk fråga, utan en fråga om nationell säkerhet, ekonomisk stabilitet och allmänhetens förtroende.

Liksom tidigare år visar it-incidentrapporteringen 2024 att organisationers sätt att genomföra ändringar i sina informationssystem är en vanligt återkommande orsak till incidenter. Det tyder på att många organisationer saknar etablerade och inövade arbetssätt för ändringshantering. Avsaknaden av gedigna arbetssätt för ändringshantering ökar risken för allvarliga incidenter och störningar, inte minst under höjd beredskap eller krig då arbetsförhållandena kan tänkas påverkas negativt. Avsaknaden gör det dessutom mer sannolikt att organisationer ackumulerar en teknisk skuld över tid, med utdaterade system och mjukvarulösningar. Det kan leda till att organisationer blir mer sårbara för såväl cyberangrepp som misstag.

På grund av det oroliga omvärldsläget betraktar MSB det stora mörkertalet[72] i it-incidentrapporteringen som allvarligt. Det underminerar myndighetens förmåga att skapa en helhetsbild av nuläget och utvecklingen över tid. På sikt påverkar det även myndighetens förmåga att ta fram ändamålsenligt och sektorsanpassat stöd till samhällsviktiga verksamheter. MSB bedömer att en ökad efterlevnad av rapporteringsplikten är en grundförutsättning för att motståndskraften i det civila försvaret ska kunna öka.

Not 71. Regeringskansliet, *Historisk satsning på cybersäkerhet.* https://regeringen.se/pressmeddelanden/2024/09/historisk-satsning-pa-cybersakerhet (Hämtad 01/2025)

Not 72. En bedömning som är baserad på att i) ett stort antal rapporteringspliktiga verksamheter aldrig har inkommit med någon it-incidentrapport, ii) myndigheten får information, via media och andra källor, om it-incidenter som sedan aldrig inrapporteras och att iii) det i regel endast är vissa som rapporterar om en incident till följd av leveranskedjeincidenter som påverkar fler rapporteringspliktiga organisationer.

Många it-incidentrapporter beskriver att incidenten har inträffat hos en leverantör till den rapporterande organisationen. MSB bedömer att större leveranskedje-incidenter fortsatt utgör den största utmaningen. Dessa incidenter riskerar att få störst samhällskonsekvenser på grund av att en mängd organisationer och dess tjänster kan påverkas samtidigt. Vidare noteras att orsaken till incidenten ofta anges som okänd eller övrig när den skett hos en leverantör. Detta tyder på att många organisationer saknar rutiner eller kontaktvägar för att få tillbörlig information om it-incidenter som sker hos deras leverantörer. Lika viktigt som det är att organisationer rapporterar it-incidenter är det viktigt att de kan informera sig om bakomliggande orsaker. Detta för att de själva ska kunna analysera och hantera konsekvenserna, samt för att MSB ska kunna analysera nuläget och ta fram ändamålsenligt och anpassat stöd.

Den snabba tekniska utvecklingen kräver att organisationer håller sig uppdaterade gällande de senaste verktygen och teknikerna. Det skapar utmaningar kring ständigt lärande, uppdatering av befintliga system och vidareutbildning av medarbetare. Organisationer behöver tillföra tillbörliga resurser till förbättringsarbetet. Förutom ökade resurser kan också takten på säkerhetsarbetet ökas genom att arbeta effektivare, genom att exempelvis dra nytta av befintliga stöd som listas rapportens temakapitel *Verktyg för ökad motståndskraft och stärkt civilt försvar*. Ett verktyg för att bemöta de många kommande EU-regleringarna är att följa MSB:s föreskrifter och tillhörande vägledningar. En organisation som klarar MSB:s föreskriftkrav bedöms vara på god väg i arbetet med att möta kraven på säkerhetsåtgärder i den kommande cybersäkerhetslagen.

Med anledning av det oroliga säkerhetspolitiska omvärldsläget måste den låga nivån på cybersäkerarbetet i Sverige[73] skyndsamt höjas. När samhällets motståndskraft att stå emot cyberangreppsförsök och andra orsaker till it-incidenter ökar stärks även det civila försvaret. Mot bakgrund av detta har följande rekommendationer tagits fram till organisationer.

Not 73. MSB, *Resultatredovisning av Cybersäkerhetskollen 2024: Det systematiska cybersäkerhetsarbetet i den offentliga förvaltningen.* https://msb.se/sv/publikationer/resultatredovisning-av-cybersakerhetskollen-2024--det-systematiska-cybersakerhetsarbetet-i-den-offentliga-forvaltningen (Hämtad 02/2025)

Rekommendationer till organisationer

1. **Använd tillgängliga verktyg för att förbättra det systematiska och riskbaserade cybersäkerhetsarbetet (se rapportens temakapitel)**
   Genom att förbättra cybersäkerheten ökar motståndskraften att stå emot och bemöta cyberangrepp och andra orsaker till it-incidenter, vilket i sin tur stärker det civila försvaret. MSB tillhandahåller verktyg som stöd för organisationer i sitt cybersäkerhetsarbete såsom Cybersäkerhetskollen för att mäta nivån på sitt systematiska cybersäkerhetsarbete, föreskrifter och vägledningar för att förbereda för kommande krav från EU-regleringar såsom cybersäkerhetslagen. Cybersäkerhetsrådgivningen kan hjälpa organisationer att hitta information och vägledning bland de verktyg som redogörs för i rapportens temakapitel *Verktyg för ökad motståndskraft och stärkt civilt försvar*.
2. **Upprätta arbetssätt för rapportering av it-incidenter**
   Förutom att det för många organisationer kommer att vara ett krav att rapportera it-incidenter så är det ur ett samhälls- och verksamhetsperspektiv viktigt att it-incidenter rapporteras. Ju fler it-incidenter som rapporteras desto bättre kan det förebyggande arbetet utvecklas och struktureras. Incidentdata bidrar även till nulägesbilder och till den långsiktiga strategiska analysen, som i sin tur ligger till grund för investeringar i forskning, utveckling och kompetensförsörjning – inte minst inom ramen för NCC-SE. I det långa loppet hjälper det till att öka motståndskraften och höja cybersäkerhetsnivån i landet.
3. **Tillsätt resurser och upprätta arbetssätt för säker ändringshantering**
   Ändringar i informationssystem är en vanligt återkommande orsak till att it-incidenter uppstår. Många av dessa incidenter hade kunnat förebyggas med fler resurser och bättre arbetssätt för ändringshantering. Här ingår även rutiner för återställning och kontinuitetshantering om en ändring trots allt skulle gå fel. Till följd av det säkerhetspolitiska läget ökar vikten av att snabbt kunna genomföra ändringar för att åtgärda sårbarheter som riskerar att äventyra informationssystems eller informationens konfidentialitet, riktighet och tillgänglighet. Exempelvis kritiska sårbarheter som lyfts upp av CERT-SE.[74]
4. **Se över kraven på leverantörer för att säkerställa att tillräcklig information lämnas om inträffade it-incidenter**
   It-incidenter som inträffat hos en leverantör rapporteras ofta med bakomliggande orsak som okänd då organisationen saknar denna information. Denna information är ofta nödvändig för att organisationen ska kunna analysera och hantera konsekvenserna av incidenten. Nya EU- regleringar såsom den kommande cybersäkerhetslagen kommer även att ställa krav på att organisationer vidtar åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem exempelvis gällande driftskontinuitet och säkerhet i leveranskedjorna.

Not 74. CERT-SE utfärdar regelbundet varningar och råd om kritiska sårbarheter i it-system på deras webbplats: https://cert.se

Framåtblick

Framåtblick

Det säkerhetspolitiska läget kräver att motståndskraften inom Sveriges digitala infrastruktur ökar för att bemöta framtidens hot. Den nya cybersäkerhetslagen kommer också ställa högre krav på cybersäkerhet inom ett stort antal samhällssektorer.

Det säkerhetspolitiska läget och dess betydelse för den fortsatta utvecklingen av Sveriges samlade cybersäkerhetsförmåga har löpt som en röd tråd genom den här rapporten. Sammantaget har det konstaterats att den samlade förmågan i dagsläget inte lever upp till dagens krav. En majoritet av de samhällsviktiga organisationerna saknar grunderna i sitt systematiska och riskbaserade cybersäkerhetsarbete.

Samtidigt kommer risken för större störningar fortsätta öka i takt med digitaliseringen och den teknologiska utvecklingen. Hoten mot de digitala leveranskedjorna kommer med stor sannolikhet att bli fler i takt med att digitaliseringen fortgår. De storskaliga, sektorsöverskridande it-incidenterna hos Tietoevry och cybersäkerhetsföretaget Crowdstrike är två aktuella exempel som visar på hur bräckliga de stora digitala leveranskedjorna kan vara vid avsaknaden av tillräckliga säkerhetsåtgärder. Den teknologiska utvecklingen har därtill bidragit till att tiden mellan det att en sårbarhet upptäcks och att den utnyttjas krymper. Det innebär att organisationer framöver kommer att behöva bli allt snabbare på att införa nya åtgärder för att inte stå oskyddad.

Under de senare åren har EU introducerat ett stort antal regleringar på cybersäkerhetsområdet som syftar till att öka motståndskraften inom den inre marknaden. Den nya svenska cybersäkerhetslagen förväntas träda i kraft relativt snart. Cybersäkerhetslagen kommer vara central för arbetet med att säkerställa att samhällsviktiga organisationer, inom såväl offentlig som privat sektor, uppnår önskad grundnivå. Fler samhällssektorer kommer att omfattas av krav och kommer behöva implementera säkerhetshöjande åtgärder. Samtidigt har det i denna rapport, samt i andra kanaler konstaterats att detta kommer utgöra en utmaning för många svenska organisationer, speciellt de som inte omfattats av lagkrav sedan tidigare. Den fortgående digitaliseringen, den föränderliga hotbilden och en avsaknad av cybersäkerhetskompetens utgör alla utmaningar som kommer ställas på sin spets under kommande år.

För att cybersäkerhetslagen ska få önskad effekt behöver samarbetet mellan offentlig och privat sektor inom cybersäkerhetsområdet fortsätta att öka. Förbättrade förutsättningar för samverkan inom områden såsom informationsdelning och incidentkoordinering förväntas kunna minska bördan för enskilda organisationer och samtidigt lägga grunden för en gemensam lägesbild. För detta syfte är det centralt att organisationer som förväntas rapportera it-incidenter i enlighet med cybersäkerhetslagen samt annan lagstiftning vidtar nödvändiga åtgärder för att säkerställa efterlevnad. Ytterst krävs även ett ännu närmare samarbete mellan EU:s medlemsstater vid hanteringen av gränsöverskridande hot, sårbarheter, it-incidenter och störningar.

Bedömningen är att stora satsningar på cybersäkerhet, både inom offentlig och privat sektor, kommer behöva vidtas för att önskad nivå ska kunna uppnås. Under det gångna året har flera beslut fattats på politisk nivå för att allokera resurser för detta ändamål. Genom att förstå cyberhoten, anta effektiva skyddsåtgärder, utbilda för att öka cyberkompetens och medvetenhet, samt genom att främja forskning och innovation kommer samhällets motståndskraft att stärkas. När Sveriges samlade förmåga att stå emot och bemöta cyberangrepp och andra orsaker till it-incidenter ökar stärks samtidigt det civila försvaret.

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publikationsnummer: MSB2563 – mars 2025 ISBN-nummer: 978-91-7927-608-9