Policy för stärkt informationsdelning på cybersäkerhetsområdet

Nulägesbeskrivning och analys sammanställdes i oktober 2025. Dessa kommer att uppdateras till slutversionen av policyn.

Nulägesbild för policyområdet

I Sverige sker mycket frivillig informationsdelning på cybersäkerhetsområdet i både nationella och internationella sammanhang, bland offentliga, privata och idéburna aktörer och inom akademin. Det saknas en samlande plattform på nationell nivå, men det finns en pluralism av olika initiativ med olika fokus, syfte och deltagare. Organisationer har stor möjlighet att välja bland tjänsterna.

Nationell sektorsövergripande många till många-delning

Det finns inte någon dedikerad, sektorsövergripande tjänst med tillhörande infrastruktur för att möjliggöra cybersäkerhetsrelaterad informationsdelning mellan ett stort antal verksamhetsutövare i Sverige idag.

En nationell portal där information både kan delas ut till många, samlas in från många och delas mellan aktörer och där rapportering och begäran om stöd kan ske är under uppbyggnad. Portalen kommer initialt att möjliggöra anmälan och rapportering av incidenter i enlighet med kraven i Cybersäkerhetslagen (CSL, som implementerar NIS2-direktivet i Sverige) respektive kraven i Lagen om motståndskraft hos kritiska verksamhetsutövare (som implementerar CER-direktivet i Sverige), men är tänkt att över tid också kunna inkludera rapportering i enlighet med andra regelverk.

Syftet med portalen och dess funktioner är att det ska vara lätt för verksamhetsutövare att utöva sitt arbete enligt de krav som finns och få tillgång till den information och de tjänster som de har rätt till. En del av det stöd som verksamhetsutövare har rätt till enligt CSL är att ta del av information ifrån CSIRT-enheten och andra behöriga myndigheter. En annan del av stödet består i att verksamhetsutövare ska kunna utbyta information sinsemellan. Det ska också vara möjligt att begära sådant stöd av CSIRT-enheten som verksamhetsutövare har rätt till. Ett ytterligare syfte med portalen är att den över tid ska bli den naturliga mötesplatsen för allmän informationsdelning i cybersäkerhetsfrågor för

organisationer i Sverige, oavsett om organisationen omfattas av Cybersäkerhetslagen eller inte.

Många till många-delning

Genom många till många-delning delar flera aktörer kontinuerligt information med varandra genom exempelvis nätverk eller partnerskap. Svenska aktörer delar information om cybersäkerhet i många olika forum, nätverk och sammanhang, både på internationell och nationell nivå. Ett urval av dessa är:

EU-relaterade forum och nätverk för offentliga aktörer

- Horisontella rådsarbetsgruppen för cyberfrågor i Europeiska rådet som samordnar medlemsstaternas ståndpunkter i cyberrelaterade frågor. Nationella representanter från medlemsstaterna deltar.
- NIS Samarbetsgrupp med syfte att samordna arbetet med att genomföra och tillämpa NIS2. Nationella myndigheter från medlemsländer, EU-kommissionen och ENISA deltar.
- Europeiska gruppen för cybersäkerhetscertifiering, en expertgrupp som samordnar EU:s ramverk för cybersäkerhetscertifiering enligt Cybersecurity Act. Nationella certifieringsmyndigheter, EU-kommissionen och ENISA deltar.
- CSIRT-nätverket (Computer Security Incident Response Teaams Network), är ett operativt samarbetsnätverk där nationella CSIRT:er, CERT-EU och ENISA deltar
- EU-CyCLONe (European Cyber Crisis Liaison Organisation Network), är ett EU-nätverk för cyberkrishantering på strategisk nivå där nationella myndigheter för cyberkrishantering, EU-kommissionen, ENISA och CSIRT-nätverket deltar.

På övrig internationell nivå ingår exempelvis MSB/CERT-SE i Forum of Incident Response and Security Teams (FIRST), Task Force CSIRT (TF-CSIRT) och European Government CERTs group (EGC). Informationen som delas i forumen och nätverken används för informationsdelning nationellt, för förmågeutveckling, i utveckling av nya tjänster, tillhandahållandet av stöd och mycket annat.

På nationell nivå finns också många initiativ, både för offentliga aktörer, privat-offentlig samverkan (POS) och exklusivt för privata aktörer eller branschrepresentanter. Några är:

- SNITS, det statliga nätverket för informationssäkerhet, är till för statsanställda med informationssäkerhet som huvuduppgift. MSB samordnar och leder nätverket.
- KIS (Kommunernas Informationssäkerhetsnätverk), ett nätverk för personer som ansvarar för arbetet med informationssäkerhet i Sveriges kommuner. Nätverket drivs ideellt av engagerade kommunrepresentanter.
- HoSIS (Hälso- och sjukvårdens informationssäkerhetsnätverk), ett nätverk för regionernas och privata vårdgivares informationssäkerhetsansvariga.

- Cybernoden, landets största POS. Cybernoden finns hos RISE men inriktas av NCC-SE och realiserar därigenom kraven på Sverige enligt EU:s ECCC-förordning om att ha en nationell kompetensgemenskap för forskning, innovation och kompetensförsörjning inom cybersäkerhet. Cybernoden är den största av EU:s kompetensgemenskaper och hade 2025 över 400 medlemmar.
- FSPOS, Finansiella Sektorns Privat-Offentliga Samverkan, är ett frivilligt samverkansforum med deltagare från det privata näringslivet och de offentliga institutionerna i finanssektorn.
- NTSG, Nationella Telesamverkansgruppen, privat-offentlig samverkan vid allvarliga störningar i elektronisk kommunikation.
- Säkerhets- och försvarsföretagens, SOFF, cyberförsvarsgrupp med syfte att sprida kunskap, bidra till offentlig-privat samverkan och dela hotinformation. Gruppen driver också SOFF MISP.
- Forum för informationsdelning, FIDI, är sektorsspecifika POS inom många branscher, bland andra FIDI-Drift och FIDI-SCADA kring säkerhet i industriella informations- och styrsystem. Forumen är mycket aktiva och har god representation samt tätt informationsutbyte

För offentliga aktörer finns bland andra eSams expert- samt sakområdesgrupp Säkerhet och plattformen Dela digitalt där anställda kan dela med sig av både frågor och information. Inom akademin finns bland andra SWITS (Swedish IT Security Network for PhD Students) och Forum for Cyber Security and Cyber Operations.

Det finns också många exempel på nätverk, communitys och liknande om cybersäkerhet som samlar branschkollegor, yrkespersoner och andra, vissa av dem belagda med medlemsavgifter. Några exempel är Altingets Cybersäkerhetsnätverk utbildningsföretaget JUC:s Nätverk i Cybersäkerhet och Svenska Försäkringsföreningens Nätverk Informationssäkerhet i försäkringsbranschen.

Tekniska tjänster för många till många-delning

MISP-SE är en nationell hotdelningsplattform där svenska verksamhetsutövare kan dela med sig av och konsumera andras hotinformation. Delningen sker via verktyget MISP (Malware Information Sharing Platform) som används för att samla in, lagra, analysera och dela information om cyberhot och incidenter. Den möjliggör strukturerad och standardiserad delning av hotindikatorer (IOC), såsom IP-adresser, domäner och skadlig kod. MISP stödjer både manuell och automatiserad hantering av information, vilket gör det lättare att snabbt reagera på nya hot. MSB förvaltar MISP-SE.

WIS är en portal för Sveriges civila beredskap där aktörer delar information före, under och efter samhällsstörningar. I WIS finns funktioner som underlättar samverkan och samordning. WIS har också funktioner för att begära in och analysera information till den samlade lägesbilden. Dokument, bilder, kartor eller annan information kan också delas mellan aktörer eller inom den egna organisationen. Myndigheter, kommuner, regioner,

frivilligorganisationer och privata aktörer med en roll i Sveriges civila beredskap får använda WIS. 2025 var 900 aktörer registrerade i WIS, med över 10 000 användare.

Rakel (RadioKommunikation för Effektiv Ledning) är Sveriges nationella kommunikationssystem för samverkan och ledning för organisationer med ansvar inom allmän ordning, säkerhet, hälsa och försvar där lägesinformation delas. Rakelsystemet används också av ett stort antal andra myndigheter, energibolag, kollektivtrafikmyndigheter och verksamheter som hanterar farliga ämnen. Alla landets länsstyrelser, kommuner och regioner är anslutna till Rakel. Rakel används inte bara som huvudsamband i sekund- och minutoperativ verksamhet, det används även som ett robust och pålitligt reservsystem vid händelser då andra system, som mobiltelefoni och internet är överbelastade eller har drabbats av elavbrott eller andra störningar.

En till många-delning

En till många-delning betyder att en aktör samlar in och delar relevant information till flera mottagare. Det finns ett antal olika sådana förfaranden som alla organisationer i Sverige i dagsläget kan ansluta sig till, där både offentliga och privata aktörer delar cybersäkerhetsinformation. MSB:s lägesbildssändningar över videolänk varannan vecka, blixtmeddelanden samt veckobrev från CERT-SE samt information som delas av Stöldskyddsföreningen inom ramen för Säkerhetskollen och Digitala varningsgruppen är några exempel. Det finns även informationstjänster som tillhandahålls av privata bolag.

ANTS (Automatiska Notifieringar av Tekniska Sårbarheter) är en en till många-informationsdelningstjänst som varnar anslutna organisationer då information upptäcks om tekniska företeelser som kan behöva åtgärdas, exempelvis om enheter anslutit till övertagna botnät, om servrar har sårbara mjukvaror eller om tjänster har sårbara konfigurationer. ANTS är kostnadsfritt och tillgängligt för alla svenska organisationer (både i offentlig och privat sektor) som vill ha hjälp med övervakning av sina angreppsytor på internet. Tjänster som liknar ANTS tillhandahålls av många cybersäkerhetsbolag. Den svenska staten har full rådighet över vilka organisationer som ansluts till ANTS och vilka datakällor som väljs in i ANTS.

Analys av nuläget

Den svenska samverkanskulturen syns tydligt inom informationsdelningsfrågorna. Det är positivt att det finns många forum och nätverk, att de finns på många olika nivåer, att information delas enligt olika modeller för olika syften och att det finns olika sätt att ta del av information utifrån den egna organisationens förutsättningar. Genom frivillig informationsdelning kan samhällets motståndskraft stärkas genom att incidenter, hot och sårbarheter både upptäcks och kan hanteras snabbare, även utanför formella rapporteringskrav. Med sådan framförhållning skapas möjligheter för att proaktivt hantera risker och att hantera incidenter innan kritiska funktioner påverkas.

De tydligaste bristerna inom området består i:

- Att tjänster och infrastrukturer ännu saknar behövd funktionalitet som kan möjliggöra och effektivisera informationsdelning. Utökad funktionalitet behövs för att möjliggöra delning i större konstellationer av organisationer, i synnerhet avseende många till många-delning. Bristande bakomliggande orsaker handlar om en komplex blandning av legala utmaningar, höga kostnader och behov av prioritering av begränsade resurser hos organisationer som spelar nyckelroller i tillhandahållandet och utvecklingen av sådana tjänster.
- Att inte tillräckligt många verksamhetsutövare är ansluta till de tjänster och infrastrukturer som finns. Bristande bakomliggande orsaker handlar om okunskap om vilka tjänster och infrastrukturer som finns samt begränsningar i dem, resursbrist och omedvetenhet om varför det är viktigt.
- Att mikro-, små- och medelstora företag samt idéburna aktörer endast i begränsad utsträckning kan försörjas med viktig cybersäkerhetsinformation. Bristande bakomliggande orsaker handlar dels om att det (med några undantag) saknas tjänster som är utformade efter sådana organisationers förutsättningar i termer av kunskapsnivå, resurser och tid, och dels om de förutsättningar som sådana organisationer har att begagna sig av de tjänster som erbjuds.
- Att informationsdelning på cybersäkerhetsområdet framförallt berör tekniska förhållanden av betydelse för cybersäkerhetsspecialister. Det bidrar till att cybersäkerhetsområdet avskärmas ifrån den bredare krisberedskapen och det civila försvaret – och det innebär att det inte byggs förmåga att samverka mellan cybersäkerhetsprofessionen och andra professioner som också har incident- eller krishanterande roller i det civila försvaret.

REFERENSLISTA

- https://www.fhs.se/forskning/natverk-och-samarbeten/forum-for-cyber-security-and-cyber-operations.html
- https://www.altinget.se/natverk/cybersakerhet
- https://juc.se/produkter/natverk-i-cybersakerhet
- https://forsakringsforeningen.se/utbildning/20250514/natverk-informationssakerhet-i-forsakringsbranschen