Enhet

Policy för att främja ett aktivt cyberskydd

Nulägesbeskrivning och analys sammanställdes i oktober 2025. Dessa kommer att uppdateras i det vidare arbetet med policyn.

Nulägesbild för policyområdet

MSB:s mätning Cybersäkerhetskollen visade 2024 att många organisationer inom offentlig förvaltning i Sverige brister i det förebyggande arbetet med cybersäkerhet och saknar de mest grundläggande delarna i det systematiska cybersäkerhetsarbetet. Cybersäkerhetskollen visade även att organisationerna menar att de saknar den budget som krävs för att förbättra cybersäkerhetsarbetet.

Staten erbjuder ett antal grundläggande tjänster inom aktivt cybersskydd, både kostnadsfria och avgiftsbelagda. Därutöver bedöms näringslivet och akademi inneha en mycket viktig roll i att kunna erbjuda kompletterande tjänster inom aktivt cybersskydd, även dessa tjänster kan vara kostnadsfria respektive avgiftsbelagda. Den svenska cybersäkerhetsmarknaden är snart värd över 16 miljarder kronor[1] och är en innovativ och konkurrenskraftig bransch som gärna vill och kan erbjuda kvalificerade och relevanta säkerhetstjänster[2].

Tjänsteerbjudanden inom aktivt cyberskydd idag

Idag erbjuds en rad tjänster inom ett aktivt cyberskydd både av svenska myndigheter och näringsliv.

Myndigheten för samhällsskydd och beredskap erbjuder exempelvis följande tjänster inom ett aktivt cybersskydd idag:

- **Automatiska Notifieringar av Tekniska Sårbarheter (ANTS).** ANTS-SE är CERT-SE:s verktyg för att hjälpa svenska verksamheter med övervakning av sina angreppsytor på internet. ANTS riktar sig i första hand till de verksamhetsutövare som faller under NIS2, men är tillgängligt för alla svenska verksamheter. ANTS är en kostnadsfri tjänst.[3]

[1] https://techsverige.se/2025/09/syna-regeringens-cybermiljard/
[2] https://techsverige.se/samverkan-med-techbranschen-avgorande-for-ett-digitalt-starkt-sverige/
[3] https://cert.se/rad-och-stod/ants/

- **Blixtmeddelanden** är CERT-SE:s varningsutskick när det finns kritiska cyberhot att informera om generellt som kräver omedelbar eller skyndsam åtgärd. Blixtmeddelanden skickas ut per mejl till den prenumerationslista som är knuten till tjänsten och blixtmeddelandet kommer även kommuniceras genom publicerad artikel på www.cert.se.[4]
- **SOC-SE** är beställningsbara tjänster för monitorering och realtidsövervakning som tillhandahålls på uppdrag av CERT-SE. Tjänsterna kommer att erbjudas för både IT- och OT-miljöer och kommer att drivas genom privat-offentlig samverkan. SOC-SE kommer preliminärt att erbjudas som tjänst under 2026 och är kostnadsbelagd.
- **MISP-SE** är Sveriges nationella Malware Information Sharing Platform-tjänst. MISP-SE en tjänst som ska användas för att sammanställa, lagra och dela information om hotunderrättelser genom att dela angreppsindikatorer. Enskilda organisationer kan registrera ett s.k. event över hotunderrättelsen inklusive angreppsindikatorer. MISP-SE kommer att finnas tillgängligt under 2026.
- **MSB Lägesuppfattning cybersäkerhet** som är MSB:s lägesuppfattning inom området som delas i två veckors intervaller med cirka 500 aktörer inom både privat och offentlig sektor.
- **Forum för informationsdelning**, där MSB deltar eller driver sektorsspecifika forum och nätverk för informationsdelning kring hot- och sårbarhetsinformation. (till exempel FIDI Scada, FIDI Telekom, SNITS, HOSIS).
- **Cybersäkerhetskollen** som är samlingsnamnet för MSB:s cybersäkerhetsmätningar inom informationssäkerhet, it-säkerhet, ot-säkerhet och leveranskedjor. Cybersäkerhetskollen mäter nivån på verksamhetens systematiska cybersäkerhetsarbete, samt ger stöd för förbättringsarbete.[5]

Utöver dessa tjänster utvecklar Myndigheten för samhällsskydd och beredskap även en ny tjänst:

- **DNS-SE** är en DNS-resolver som ska erbjudas av CERT-SE. DNS-SE kan användas av verksamheter för att filtrera bort skadligt innehåll genom att stoppa användares åtkomst till skadliga webbplatser. Tjänsten kommer att erbjudas under 2026.

Försvarets radioanstalt tillhandahåller exempelvis följande tjänst inom aktivt cyberskydd:

- **TDV** som är ett tekniskt detekterings- och varningssystem till de mest skyddsvärda verksamheterna bland statliga myndigheter och enskilda verksamhetsutövare som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende.

[4] https://cert.se/prenumerera/
[5] https://www.msb.se/cybers%C3%A4kerhetskollen

Även näringslivet erbjuder många tjänster inom ramen för ett aktivt cyberskydd. Leverantörer av hanterade säkerhetstjänster erbjuder tjänster inom exempelvis incidenthantering, penetrationstester, säkerhetsrevisioner och konsulttjänster som proaktiva åtgärder inom ramen för ett aktivt cyberskydd. Dessa innehar en särskilt viktig roll när det gäller att bistå organisationer i deras arbete med att förebygga, upptäcka, reagera på eller återhämta sig från incidenter.

Exempel på självbetjäningstjänster som erbjuds av näringslivet och stiftelser idag är:

- **Webbtjänsten Securitytxt.se:** en tjänst som syftar till att bidra till att fler organisationer (webbplatsinnehavare) har publicerat information på sin webbplats i en security.txt-fil om vart upptäckare av sårbarhetsinformation som berör organisationen ifråga kan skicka sådan information.[6]
- **Webbtjänsten Zonemaster:** en kostnadsfri tjänst från Internetstiftelsen som hjälper domännamnsinnehavare att bedöma hur organisationens domännamn fungerar och kvaliteten i uppsättningen av organisationens DNS-tjänst och om det finns behov av att vidta säkerhetsåtgärder.[7]
- **Webbtjänsten Säkerhetskollen** från Stöldskyddsföreningen är en samlingsplats för digital säkerhet som även gör varningsutskick om digitala brott.[8]

Näringslivet erbjuder även säkerhetstjänster med t.ex. övervakning av it-system, incidenthantering, analyser och kontroller. Det finns till exempel företag som erbjuder säkerhetstjänster vid leveranskedjeincidenter. Några av de tjänster som erbjuds i Sverige är Managed Detection and Response (MDR) och Security Operations Center (SOC) som innebär att företagen stöttar i incidenthanteringen genom övervakning för att upptäcka, analysera och agera på säkerhetshot i it-system. Vid nyttjande av MDR sker även aktiv respons och hotjakt.

Det upprättas även sektorsspecifika CERT som aktivt hjälper och stöttar organisationer i att hantera och förebygga cybersäkerhetsincidenter.

Analys av nuläget

Sverige har i dagsläget en grundläggande nivå vad gäller erbjudande och tillhandahållande av tjänster inom aktivt cybersskydd. Många viktiga proaktiva tjänster inom aktivt cyberskydd finns och tillhandahålls – av svenska myndigheter, näringsliv och akademi. Samtidigt saknas det kännedom om nyttjandet av det aktiva cyberskyddet och till vilket stöd det varit för organisationerna. Det finns utmaningar inom det aktiva cyberskyddet och de tydligaste är:

- Det saknas statistik på hur nyttjade tjänster inom ett aktivt cyberskydd är. Detta innebär att det saknas förutsättningar för att bedöma utbudet och efterfrågan samt vilka satsningar som bör göras inom ramen för ett aktivt cyberskydd. Till exempel

[6] https://www.securitytxt.se/
[7] https://zonemaster.se/sv/run-test
[8] https://sakerhetskollen.se/privat

är många av de tjänsterna som Myndigheten för samhällsskydd och beredskap erbjuder nya tjänster där utvärderingar inväntas. Konsekvensen av detta är att det utveckling av aktivt cyberskydd potentiellt inte ligger i linje med efterfrågan och behovet.

- Utvecklingen av det aktiva cyberskyddet saknar idag en formaliserad och närmare samverkan och process mellan myndigheter, akademi och näringsliv som tar sikte på styrning, samordning och dialog om framtidssäkra lösningar för att åstadkomma ett aktivt cybersskydd. Detta leder till att lösningar utformas utan sikte på en sammanhållen målbild för Sveriges aktiva cyberskydd.
- Kännedomen hos organisationer om vilka tjänster som finns och erbjuds idag bedöms vara låg. Det finns etablerade tjänster som eventuellt inte nyttjas i den utsträckningen som de skulle kunna för att upprätta ett aktivt cyberskydd för organisationer. En förklaring till detta kan vara att det saknas formaliserad samverkan kring tjänsteutbudet eller att ytterligare främjande- och kommunikationsinsatser krävs om vilka tjänster som tillhandahålls av vilka organisationer. Nuläget leder till att organisationer inte nyttjar det tjänsteutbude som finns idag.
- Förmågan hos enskilda organisationer att agera proaktivt bedöms behöva öka och Cybersäkerhetskollens resultat från 2024 visar att organisationer inte avsätter tillräckligt med personella och monetära resurser för ett förebyggande cybersäkerhetsarbete. Detta bedöms behöva tillföras för att de effekter som krävs ska uppnås. Med Cybersäkerhetslagen kommer det risker för att organisationer tilldelas sanktionsavgifter på grund av ett bristande systematiskt cybersäkerhetsarbete och uteblivet arbete med ett aktivt cyberskydd. Om resurser inte tillsätts i organisationerna kan de inte nyttja hela tjänsteutbudet inom det aktiva cyberskyddet och få ett bra cyberskydd.

Sammanfattningsvis visar nuläget att det finns ett utbud av tjänster för ett aktivt cyberskydd, men att det finns flera utmaningar för området. Tjänsternas nyttjande och utvecklingen av dem kräver en vidareutvecklad och förfinad samverkan mellan organisationer inom privat sektor, offentlig förvaltning och akademi. Det saknas en strategisk samverkan som behöver komma på plats för att kunna leverera ett utbud av aktivt cyberskydd som motsvarar cyberhotlandskapet vid var tid. Samverkan krävs för att kunna erbjuda ett utbud som motsvarar efterfrågan, men också för att ge information om utbudet.

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240 Fax: 010-240 56 00
registrator@msb.se www.msb.se
Org.nr: 202100-5984