Bilaga 2: Organisationer med roller och ansvarsområden inom cybersäkerhet

Nationell strategi för cybersäkerhet 2025–2029

Regeringskansliet
Försvarsdepartementet

Organisationer med roller och ansvarsområden inom cybersäkerhet

Cybersäkerhet är en horisontell fråga och medför ett sektoröverskridande ansvar inom regeringen och Regeringskansliet.

Denna bilaga kommer uppdateras när NIS 2-direktivet implementerats nationellt och ansvarsförhållanden har definierats samt när uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (dir. 2024:111) redovisats och omhändertagits.

Nationellt cybersäkerhetscenter (NCSC)

Nationellt cybersäkerhetscenter har i uppdrag att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter.

Från och med den 1 november 2024 finns centret inom FRA som har ansvaret för att leda NCSC.

Gemensam kontaktpunkt

Den roll som enligt NIS 2-direktivet benämns gemensam kontaktpunkt (på engelska SPOC, Single Point Of Contact) kommer att utses och närmare definieras i kommande reglering som implementerar NIS 2-direktivet i Sverige. Den gemensamma kontaktpunkten ska enligt NIS 2-direktivet utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete mellan medlemsstatens myndigheter och relevanta myndigheter i andra medlemsstater och, när det är lämpligt, kommissionen och Enisa samt ett sektorsövergripande samarbete med andra behöriga myndigheter i medlemsstaten.

För NIS-direktivet har MSB uppgiften att vara nationell gemensam kontaktpunkt[1].

1 Uppgiften inkluderar bland annat att tillhandahålla vägledning och utbyta praxis i fråga om NIS-direktivets genomförande, samverkan med regulatoriska policyfrågor, tillsynssamordning, stödja samordning mellan NIS 2- och CER-direktiven, säkerställa samarbete mellan brottsbekämpande myndigheter och dataskyddsmyndigheter, förvalta och utveckla föreskrifter om informations- och cybersäkerhet för aktörer som omfattas av NIS-regleringent.

Nationell CSIRT-enhet

CERT-SE är nationell CSIRT-enhet enligt NIS-direktivet, vilket regleras i förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Varje medlemsstat ska i enlighet med NIS 2-direktivet utse eller inrätta en eller flera CSIRT-enheter (på engelska Computer Security Incident Response Team). CSIRT-enheten ska enligt NIS 2-direktivet bland annat övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå samt tillhandahålla varningar och sprida information om dessa. Sveriges nationella CSIRT-funktion kommer att pekas ut i kommande reglering som implementerar NIS 2-direktivet i Sverige.

Cyberkrishanteringsmyndighet

Varje medlemsstat ska i enlighet med NIS 2-direktivet utse eller inrätta en eller flera cyberkrishanteringsmyndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser.[1]

Ansvarig cyberkrishanteringsmyndighet kommer att utses av regeringen

Statliga myndigheter som tar emot incidentrapporter[2]

Vid en cybersäkerhetsincident finns ett antal aktörer som, beroende på typ av incident, ska ta emot rapporter om incidenter utifrån olika regleringar. Några av dessa är:

- CERT-SE är mottagare av it-incidentrapporter, vilket följer av ett flertal regleringar.
- Säkerhetspolisen tar emot anmälningar om säkerhetshotande händelser och verksamhet enligt säkerhetsskyddsförordningen (2021:955). Om verksamhetsutövaren tillhör Försvarsmaktens tillsynsområde ska anmälan också göras till Försvarsmakten.
- Integritetsskyddsmyndigheten hanterar personuppgiftsincidenter.
- Polismyndigheten tar emot anmälningar om misstänkta brott[3].

1 Varje medlemsstat ska anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Planen ska bland annat innehålla cyberkrishanteringsmyndighetens uppgifter och ansvarsområden. Utformningen av den nationella planen ingår inte i utredningens uppdrag.

2 Detta avsnitt berör inte statliga myndigheter som mottar sektorspecifik incidentrapportering såsom för elektroniska kommunikationer eller inom exempelvis finanssektorn.

3 Incidenter som rapporteras under olika regelverk bör alltid polisanmälas av organisationer om incidenterna misstänks bero på brott. Myndigheter som tar emot incidentrapportering har också rutiner för att vid behov notifiera Polismyndigheten.

Tillsynsmyndigheter under NIS-regleringen

Sex tillsynsmyndigheter ansvarar för tillsynen inom de sektorer som träffas av NIS-direktivet. MSB driver ett nationellt samarbetsforum gällande NIS-frågor där de sex tillsynsmyndigheterna och Socialstyrelsen ingår. Forumets syfte är att underlätta den nationella samordningen och att åstadkomma en effektiv och likvärdig tillsyn. De sex NIS-tillsynsmyndigheterna är följande.

Tillsynsmyndighet	Sektor
Statens energimyndighet	Energi
Transportstyrelsen	Transport
Finansinspektionen	Bankverksamhet Finansmarknadsinfrastruktur
Inspektionen för vård och omsorg	Hälso- och sjukvård
Livsmedelsverket	Leverans och distribution av dricksvatten
Post- och telestyrelsen	Digital infrastruktur

NIS 2-direktivet omfattar 18 sektorer. Tillsynsansvaret, som föreslås fördelas över flera myndigheter, kommer att framgå i kommande nationell författning som implementerar NIS 2-direktivet i Sverige.

Utöver NIS-regleringen finns flera andra relevanta regelverk med cybersäkerhetskrav och som omfattas av tillsyn. Dessa berörs inte närmare i denna strategi.

Cybersäkerhet i det civila försvaret

Beredskapsmyndigheterna ansvarar, enligt förordningen (2022:524) om statliga myndigheters beredskap, för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt.

Myndigheter med särskilt ansvar för säkerhetsskydd

Säkerhetspolisen och Försvarsmakten har enligt säkerhetsskyddsförordningen till uppgift att samordna övriga tillsynsmyndigheter inom säkerhetsskyddsområdet och utövar även tillsyn över de allra mest skyddsvärda verksamheterna.

Försvarsmakten leder och samordnar totalförsvarets signalskyddstjänst. Myndigheten ansvarar bland annat även för att godkänna kryptografiska funktioner för skydd av säkerhetsskyddsklassificerade uppgifter samt för att meddela föreskrifter inom dessa områden.

Enligt säkerhetsskyddslagen (2018:585) ska informationssäkerhet förebygga att säkerhetsskyddsklassificerade uppgifter röjs, ändras, görs otillgängliga eller förstörs av obehöriga. Utöver det ska

informationssäkerhet också förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet. Med ”säkerhetsskyddsklassificerade uppgifter” avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), eller som skulle ha omfattats av lagen om den varit tillämplig i den aktuella verksamheten.

Nationell myndighet för cybersäkerhetscertifiering

Försvarets materielverks (FMV) är nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt. FMV bedriver tillsyn och samverkan över det europeiska ramverket för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt.

Kommuner och regioner

Av 14 kap. 2 § regeringsformen framgår att kommunerna sköter lokala och regionala angelägenheter av allmänt intresse på den kommunala självstyrelsens grund. Närmare bestämmelser om detta finns i lag. På samma grund sköter kommunerna även de övriga angelägenheter som bestäms i lag. Kommuner och regioner ansvarar för sin egen cybersäkerhet och har en central roll för Sveriges cybersäkerhet.

Andra nationella cybersäkerhetsaktörer

Centrum för cyberförsvar och informationssäkerhet (CDIS)

CDIS initierades genom ett nära samarbete mellan Kungl. Tekniska högskolan (KTH) och Försvarsmakten. Totalförsvarets forskningsinstitut (FOI), MSB, FRA och Försvarshögskolan ingår också i CDIS. CDIS är en del av Skolan för elektroteknik och datavetenskap vid KTH.

En styrgrupp med partnerrepresentanter leder centrets arbete.

Cyber Range and Training Environment (Crate)

FOI, Försvarsmakten och MSB har i samverkan utvecklat Sveriges nationella cyberanläggning för totalförsvaret, Crate. FOI använder sedan 2009 Crate för att tillhandahålla träning i cybersäkerhet till relevanta aktörer inom totalförsvaret.

RISE Cyber Range

RISE Cyber Range är en testbädd som drivs av RISE (Research Institutes of Sweden). Genom testbädden kan företag och organisationer testa tekniska system, identifiera sårbarheter och säkerställa adekvata rutiner och organisation. Målgruppen är både näringsliv som offentlig sektor.

Cybercampus Sverige

Cybercampus Sverige inrättades 2024 och har fokus på forskning, innovationer och utbildningar. Det är en satsning och ett samarbete mellan universitet, institut, myndigheter och företag i hela Sverige. KTH är huvudman för uppdraget att etablera och utveckla Cybercampus Sverige.

Cybernoden

Cybernodens primära syfte är att skapa en samverkansplattform. Cybernoden utgör den nationella kompetensgemenskapen för forskning och innovation inom cybersäkerhet och drivs av RISE på uppdrag av NCC-SE, inom ramen för EU:s kompetenscentrum för cybersäkerhet.

Nationellt it-brottscentrum

Nationellt it-brottscentrum, utgör Polismyndighetens expertfunktion för utredning av komplexa cyberbrott, internetrelaterade sexualbrott mot barn och andra brott där internet är en bärande del. Sektionen biträder även den övriga brottsbekämpande verksamheten med insamling och hantering av digital bevisning och digitala spår.

NCC-SE

NCC-SE är Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet. NCC-SE främjar samarbete mellan svenska och europeiska forskare, företag och myndigheter för utveckling av cybersäkerhetslösningar.

NCC-SE bidrar i framtagande av arbetsprogram på EU-nivå, marknadsför de europeiska cybersäkerhetsutlysningarna samt ger vägledning till svenska aktörer som söker EU-medel för projekt inom arbetsprogrammen. NCC-SE stödjer, tillsammans med övriga medlemsländers nationella samordningscenter, EU:s kompetenscentrum för cybersäkerhet (ECCC) i uppdraget för ökad cybersäkerhet inom EU.