ERICSSON

Public:
Date: 2024-05-27

Your Reference: Diarienummer Fö2024/00496
Your Date: 2024-03-06

Försvarsdepartementet
Rättssekretariatet

Svar på remiss med diarienummer Fö2024/00496 – Nya regler om cybersäkerhet (SOU 2024:18)

Ericsson intar en positiv inställning till SOU 2024:18 och önskar att kommentera utredningens arbete gällande incidentrapportering samt certifiering.

1 Kort beskrivning om Ericsson

I nästan 150 år har Ericsson varit en drivande faktor i både Sveriges och Europas innovationsklimat och spelat en avgörande roll i samhällets digitalisering. Vi samarbetar med relevanta intressenter för att uppnå Sveriges och Europas digitala och gröna ambitioner, genom att utnyttja teknologier som 5G, Artificiell Intelligens, API:er och molntjänster samt att stärka cybersäkerheten i omnämnda teknologier.[1]

De senaste tre åren (2021, 2022 och 2023) har Ericsson blivit erkänd som ledare inom 5G-teknologi av två oberoende branschkonsultföretag.[2] Detta teknologiska ledarskap är en av de grundläggande anledningarna till Ericssons ledande position på marknaden. Ericsson var även först med att implementera 5G på fyra kontinenter, inklusive Europa, och i Q1 2024, hade Ericsson 160 kommersiella avtal om 5G-nät i 68 länder. Totalt har Ericsson 60 000+ patent och kunder i 180 länder.

Gällande Ericssons cybersäkerhetsarbete, har Ericsson utvecklat ett holistiskt policyramverk[3] baserat på Ericsson Trust Stack[4]. Denna ansats har även uppmärksammats inom OECDs[5] arbete gällande: "Enhancing the security of communication infrastructure". Ericsson rekommenderar att denna ansats fortsatt beaktas i relevanta cybersäkerhets regelverk på EU samt nationell nivå,

[1] https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security

[2] https://www.ericsson.com/en/news/2023/5/ericsson-tops-frost-radar-global-5g-network-infrastructure-market-ranking-for-third-year-in-a-row samt https://www.ericsson.com/en/press-releases/2023/3/ericsson-named-a-leader-in-the-2023-gartner-magic-quadrant-for-5g-network-infrastructure-for-csps-report

[3] https://www.ericsson.com/en/public-policy-and-government-affairs/cyber-network-security?video-dialog=1_kw4tjgm6

[4] https://www.ericsson.com/en/security

[5] https://www.oecd-ilibrary.org/docserver/bb608fe5-en.pdf?expires=1715952137&id=id&accname=guest&checksum=2C88FFF5722365937B04743C6903242F sid. 38-40.

vilket bla redan återspeglas väl i NIS 2 Direktivet samt CRA och relationen mellan dessa två regelverk.

2 Incidentrapportering

Ericsson rekommenderar:

- När det gäller definitionen av "betydande incident" rekommenderar Ericsson att det ska finnas en möjlighet för företag att definiera "betydande" utifrån sin storlek och verksamhet.
- Gällande rapportering av cybersäkerhetsincidenter som sträcker sig över EU, rekommenderar Ericsson att utredningen säkerställer möjligheten att rapportera sådana incidenter till den nationella CSIRT, dvs CERT-SE eller till EU CSIRT. Vi stödjer inte ett införande av ett nytt förfarande som avviker från denna rekommendation gällande cybersäkerhetsincidenter som sträcker sig över EU.

3 Certifiering

Gällande certifiering av IKT-produkter önskar vi påtala kommande EU Cyber Resillience Act (EU CRA) och dess effekt att höja nivån på IT-säkerhet i IKT-produkter.

Enligt remissen kommer medlemsstaterna att uppmuntras att främja användningen av europeiska och internationella standarder och tekniska specifikationer som är relevanta för säkerheten i nätverks- och informationssystem. Ericsson välkomnar detta och ser positivt på hänvisningen till standarder, speciellt med tanke på Ericssons långa arbete inom standardisering, tex inom mobilnätsstandardisering genom 3GPP och speciellt inom området för IT-säkerhet.

Vidare nämns att medlemsstaterna kan kräva väsentliga och viktiga verksamhetsutövare att använda certifierade IKT-produkter, -tjänster och -processer enligt europeiska cybersäkerhetscertifieringar. Det är i denna kontext vi vill poängtera den ökade IT-säkerhetsnivån som kommer åläggas alla produkter med digitalt element, inklusive fristående mjukvaror, genom införandet av EU CRA.

Kraven inom EU CRA kan delas upp i processkrav och funktionella krav, vilket motsvarar uppdelningen i assurans- och funktionella krav enligt Försvarsmaktens KSF, om än att KSF kraven är mer uttömmande och avser nationell säkerhet. Uppfyllande av EU CRA kraven bekräftas genom en så kallad Declaration of Conformity som företagsrepresentant skriver under. Företag med certifierat kvalitetssystem, såsom Ericsson, kan med hjälp av harmoniserade Europeiska Normer (hEN) bekräfta att de uppfyller tillämpliga lagkrav under eget ansvar. Detta tillvägagångssätt gäller inte enbart för kommande EU CRA utan även för andra existerande applicerbara lagkrav såsom radioemission och systemsäkerhet, och är ett etablerat förfarande inom EU som del av CE-märkning av produkter. Tillverkaren måste fortfarande upprätta detaljerade tekniska dokument som beskriver hur lagkraven uppfylls och på begäran från

marknadsövervakningsmyndigheter göra dessa tillgängliga. Det krävs dock ingen tredje part för att certifiera varje version av en produkt, vilket är fördelaktigt för 5G-system som består av många ingående produkter, samtidigt som EU CRA kommer vidmakthålla en god IT-säkerhetsnivå på IKT-produkter.

Det etablerade konceptet med Declaration of Conformity inom EU är kostnadseffektivare än certifiering, men det finns vissa skillnader i assuransnivå. Genom att undersöka närmare kraven inom EU CRA ser man att de är relativt högt satta och i princip motsvarar assuransnivån substantial för processdelen av EU CRA. Det första EU CSA-certifieringsschemat, EUCC, har lanserats och baseras på Common Criteria (CC) och assuransnivå hög, vilket lämpar sig väl för IKT-produkter som SmartCards. För Operational Technology (OT) som används inom kritisk infrastruktur som energi och vatten finns inga planer på ett EU CSA-certifieringsschema. Istället strävar man efter att EU CRA ska vara grunden för OT IKT-produkter, och för dessa OT IKT-produkter skapa en harmoniserad Europeisk Norm (hEN) baserad på en internationell standard.

Ett EU CSA-certifieringsschema som är under utveckling är EU5G, vilket har en assuransnivå substantial. Det är intressant att jämföra vad man får med EU5G-certifiering jämfört med kommande EU CRA-krav och tillhörande hEN. EU5G:s koppling till de omfattande 3GPP-standarderna är mer än motsvarande EU CRAs funktionella krav, men det bör beaktas att 3GPP-kraven ingår i kommersiella avtal mellan mobiloperatörer och dess leverantörer. När det gäller processdelen av EU5G, som avser säker utveckling, bygger den på etablerade standarder som också förbereds för att kunna bli harmoniserade Europeiska Normer(hEN) kopplade till EU CRA. Processkraven i EU CSA-certifieringsschemat EU5G kommer därmed att motsvara vad EU CRA kommer att erbjuda, men genom det mer kostnadseffektiva förfarandet med [Self] Declaration of Conformity. Dessutom förstärker avsaknaden av ett EU CSA-certifieringsschema för OT argumentet att certifiering av IKT-produkter bör begränsas till mycket specifika IKT-produkter, lämpligtvis på assuransnivå hög.

Ericsson rekommenderar:

- Uppmuntra användningen av europeiska och internationella standarder och tekniska specifikationer av relevans för säkerheten i nätverks- och informationssystem där 3GPP standarden är ett bra exempel.
- Dra fördel av kommande EU CRA för att kostnadseffektivt säkerställa en god IT-säkerhet på IKT-produkter för väsentliga och viktiga verksamhetsutövare.
- Applicera EU CSA certifierings på mycket begränsat område av IKT produkter, tex Smartcards, för vilka assurans nivå hög krävs.
- Att berörda SoU gällande Certifiering gör en adekvat avvägning som bör beaktas oförändrat i fortsatta arbetet i att implementera NIS 2 i svensk lagstiftning.

Patrik Forslund
Senior Director and Head of Government and Policy Advocacy Sweden