Remissvar

2021-12-21
Diarienummer: Fö2021/00796

Remissvar avseende ”Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem” (SOU 2021:63).

Saken

Teknikföretagen delar utredningens slutsats att det behövs kraftfulla och omfattande åtgärder på många olika områden för att stärka informations-och cybersäkerheten i Sverige. Teknikföretagen ser det därför som angeläget och prioriterat att stärka det nationella cybersäkerhetscentret och använda detta som plattform för gemensamma hot- och sårbarhetsanalyser. Mandat och resurser till det nationella cybercentret bedöms som mer ändamålsenligt än att införa en, för Sverige, särskilt anpassad certifieringsordning för IKT-produkter, -tjänster och -processer som används i nätverks-och informationssystem i säkerhetskänslig verksamhet.

I övrigt stödjer Teknikföretagen de slutsatser och förslag som Säkerhets- och Försvarsföretagen (SOFF) lämnat i sitt remissvar till utredningen.

Huvudsaklig grund för ställningstagande

Teknikföretag driver Sveriges digitalisering

Teknikföretagen vill börja med att tacka för möjligheten att lämna synpunkter på utredningen ”Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)” och lämnar i detta remissvar organisationens samlade bedömning i frågan.

Teknikföretagen är en bransch- och arbetsgivarorganisation för teknikindustrin i Sverige, det vill säga företag som producerar och utvecklar industriella varor och tjänster. Organisationens 4 200 medlemmar är huvudsakligen små och medelstora företag men inkluderar också världsledande aktörer som exempelvis ABB, Ericsson, Saab, Volvo och Scania. Gemensamt för Teknikföretagens medlemmar är att de genom stora investeringar i forskning, utveckling och demonstration leder och driver digitaliseringen. Skydd av nätverks- och informationssystem är därför helt centralt.

Digitalisering kräver att säkerhet prioriteras

Ur Teknikföretagens perspektiv är digitalisering ett generiskt teknologiområde som påverkar hela samhället. Genom att alla samhällssektorer och områden påverkas kräver en ökad digitalisering oundvikligen att säkerhet beaktas och prioriteras. På samma sätt som digitaliseringen av samhällets olika verksamheter kontinuerligt medför fördelar genererar den också i ökad utsträckning hot, sårbarheter och risker. Hoten mot Teknikföretagens medlemmar kommer främst från statliga aktörer som genomför cyberangrepp med syfte att utföra

företagsspionage och sabotera verksamhet.[1] Volymen och sofistikeringsgraden på dessa attacker har nått en sådan omfattning att de hotar företagens konkurrenskraft och därmed exportintäkter och jobbskapande i Sverige. Situationen är bekymmersam. Allvarliga brister i informations- och cybersäkerheten på många olika områden innebär uppenbara risker för cyberangrepp.[2]

Undvik att införa nationell certifiering

Medan situationen är allvarsam är det dock uppenbart att det inte bara är Sverige och svenska företag som drabbas.[3] Utvecklingen är snarlik i många av EU:s medlemsländer och det är också skälet till att Europeiska kommissionen vidtagit åtgärder för att öka skyddet via EU:s cybersäkerhetsakt. Vad den föreliggande utredningen därför primärt avser svara på är om kommissionens arbete behöver kompletteras med nationella särskilda krav (certifiering) på digitala produkter, -tjänster och -processer för säkerhetskänslig verksamhet? Teknikföretagens svar på den frågan är nej.

För närvarande föreligger inte tillräckliga skäl för en nationell särskilt anpassad certifieringsordning för IKT-produkter, -tjänster och -processer som används i nätverks- och informationssystem i säkerhetskänslig verksamhet. Enskilda åtgärder av detta slag riskerar att skapa administrativa bördor för företagen utan att i realiteten bidra till ökad säkerhet. Specifikt är Teknikföretagen oroade över att en nationell certifiering blir kostnadsdrivande och leder till att företag väljer att helt *avstå* från certifiering. Detta är också en farhåga som utredningen påtalar.

Prioritera stärkt styrning och samordningen

Istället för nationell särlagstiftning ser Teknikföretagen i nuläget behov av att prioritera stärkt styrning och samordningen av digitaliseringen, särskilt när det gäller utbyggnad av infrastruktur och samordning av arbete med informations- och cybersäkerhet. Att myndigheter gemensamt tar fram hot-, sårbarhets- och riskbedömningar är exempelvis mycket angeläget. I detta sammanhang vore det särskilt välkommet med en tydligare roll och klarare mandat för det nationella cybersäkerhetscentret. Centret behöver kunna ta ledarskap. För att axla en sådan roll och ansvar krävs givetvis erforderliga resurser. Teknikföretagen ser det därför som prioriterat att centret ges resursförstärkning och tillerkänns handlingsmandat. Det är synnerligen bekymmersamt att tillsyn över såväl statliga

---

[1] Teknikföretagen, ”Cyberhoten”, https://www.teknikforetagen.se/nyhetscenter/rapporter/2020/cyberhoten---sa-ser-hotbilden-och-attackerna-ut-mot-svenska-teknikforetag/

[2] Säkerhetspolisen, ”Årsbok 2020”, https://www.sakerhetspolisen.se/download/18.4ffee9b31787cb4eddc36f/1622105064669/sakerhetspolisens_arsbok_2020.pdf

[3] ENISA, ”ENISA Threat Landscape”, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

myndigheters som regioners och kommuners verksamhet avseende nätverks-och informationssystem är i det närmaste obefintlig.

Övrigt

Till sist vill Teknikföretagen påtala att organisationen till fullo stödjer och ställer sig bakom de slutsatser och förslag som branschorganisationen Säkerhets- och Försvarsföretagen (SOFF) lämnat i sitt remissvar till utredningen.

För Teknikföretagen

Maria Rosendahl

Näringspolitisk chef