Talousvaliokunta
TaV@eduskunta.fi

Viite
Talousvaliokunnan
asiantuntijapyyntö asiassa VNS 6/2025 vp

Kyberturvallisuuskeskuksen asiantuntijalausunto valtioneuvoston selonteosta sisäisestä turvallisuudesta VNS 6/2025 vp

Talousvaliokunta on pyytänyt Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen asiantuntijalausuntoa valtioneuvoston selonteosta sisäisestä turvallisuudesta (VNS 6/2025 vp). Tässä lausunnossa selontekoa tarkastellaan yksinomaan Kyberturvallisuuskeskuksen tehtävien kannalta keskittyen talousvaliokunnan pyynnössään ilmoittamaan selonteon osuuteen, joka koskee kriittisen infrastruktuurin suojaamista (luku 3.7). Liikenne- ja viestintäviraston Kyberturvallisuuskeskus muun ohella tukee, ohjaa ja valvoo tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä. Se ylläpitää kansallisen kyberturvallisuuden tilannekuvaa. Lisäksi Kyberturvallisuuskeskus huolehtii viestintätoimialan varautumisesta normaaliolojen häiriötilanteisiin ja poikkeusoloihin, edistää ja valvoo sähköisen viestinnän toimintavarmuutta sekä tukee toimialallaan yhteiskunnan yleistä varautumista normaaliolojen häiriötilanteisiin ja poikkeusoloihin (Laki Liikenne- ja viestintävirastosta 3 §).

Kyberturvallisuuskeskus kiittää mahdollisuudesta lausua asiassa ja esittää lausuntonaan kunnioittavasti seuraavaa:

Suomelle kriittisen infrastruktuurin suojaaminen

Selonteossa todetaan, että Suomenlahdella viime vuosina tapahtuneet kriittisen infrastruktuurin vauriot voivat vaikuttaa yhteiskunnan elintärkeiden toimintojen toimivuuteen (s. 16). Viestintäverkkojen- ja palvelujen toimivuus on välttämätöntä yhteiskunnan elintärkeille toiminnoille. Niin viranomaiset, kriittiset yksityisen sektorin toimijat kuin myös tavalliset kansalaiset hyödyntävät jokapäiväisessä toiminnassaan digitaalisia palveluita, joiden jatkuvuus on kyettävä mahdollisimman hyvin varmistamaan normaaliolojen häiriötilanteissa sekä valmiuslain mukaisissa poikkeusoloissa. Yleisten viestintäverkkojen ja -palvelujen eli teletoiminnan toimintavarmuudesta ja varautumisesta huolehtiminen on ollut osa toimijoita koskevaa lainsäädäntöä ja viranomaisohjausta ja -valvontaa jo 1990-luvulta lähtien. Tällä ja Kyberturvallisuuskeskuksen jatkuvasti tekemällä teleyritysyhteistyöllä on ollut merkittävä vaikutus siihen, että mm. merikaapelikatkoksista on ollut tuskin lainkaan näkyviä vaikutuksia teleyritysten asiakkaille. Vaikka viestintäverkkojen

toimintavarmuus Suomessa on korkealla tasolla, voidaan vastaavanlaisten vaurioiden mahdollisia vaikutuksia vähentää kehittämällä edelleen kansainvälisten yhteyksien varmistuksia, eli esimerkiksi lisäämällä maantieteellisesti hajautettuja maa- ja merikaapeliyhteyksiä.

Kuten selonteossa todetaan, kriittisen infrastruktuurin suojaaminen edellyttää ajantasaista lainsäädäntöä (s. 17). Selonteossa mainitun CER-direktiivin tavoitteena on yhteiskunnan kriittisten palvelujen häiriönsietokyvyn parantaminen ja direktiivin kansallisella toimeenpanolla pyritään muun ohella kriittisten palvelujen häiriönsietokyvyn parantamiseen. Lisäksi NIS 2 -direktiivin tavoitteena on vahvistaa sekä EU:n yhteistä että jäsenvaltioiden kansallista kyberturvallisuuden tasoa useiden yhteiskunnan toiminnan kannalta kriittisten toimialojen osalta. Kansallisesti NIS 2 -direktiivi on pantu täytäntöön 8.4.2025 voimaan tulleella Kyberturvallisuuslailla, jossa mm. osoitetaan yhteiskunnan kriittisille toimialoille kyberturvallisuutta vahvistavia riskienhallintavelvoitteita ja raportointivelvoite merkittävistä poikkeamista.

Yleiseen teletoimintaan käytettävien merikaapelien suojaamista koskevista vaatimuksista säädetään sähköisen viestinnän palveluista annetussa laissa, jonka mukaan yleiset viestintäverkot ja -palvelut on suunniteltava, rakennettava ja ylläpidettävä mm. siten, että ne kestävät normaalit odotettavissa olevat ilmastolliset, mekaaniset ja sähkömagneettiset ja muut ulkoiset häiriöt ja niiden toimivuutta merkittävästi häiritsevät viat ja häiriöt voidaan havaita. Lisäksi Liikenne- ja viestintävirasto on antanut useita määräyksiä teletoiminnan tietoturvaan ja varmistamiseen liittyen sekä teleyrityksille suosituksen varautumisesta.

Kyberturvallisuuskeskus pitää kannatettavana panostusta kriittisen infrastruktuurin kohteiden suojaamiseen CER-direktiivin toimeenpanon edellyttämällä tasolla ja sitä, että arvioidaan merialueilla olevan kriittisen infrastruktuurin ylläpidon ja suojaamisen haasteet sekä näiden edellyttämä lainsäädännöllinen, valvonnallinen ja teknologinen vaste (s. 22). Merikaapeleiden valvonnallisen ja teknologisen vasteen osalta kansallinen ja kansainvälinen yhteystyö sekä yhteistyö yksityisen sektorin toimijoiden kanssa on tärkeää. On myös keskeistä, että kansallisten viranomaisten vastuut ovat selkeät. Lisäksi olisi tärkeää kiinnittää huomiota myös kyvykkyyteen korjata kriittisen infrastruktuurin vauriot ja korjaamiseen tarvittaviin resursseihin.

Kyberturvallisuuden tilannekuva ja viranomaisten roolit

Kyberturvallisuuskeskuksen yksi keskeisimpiä tehtäviä on tuottaa kansallista kyberturvallisuuden tilannekuvaa. Tilannekuvaa muodostetaan niin kansallisista kuin kansainvälisistä verkostoista tulevalla tiedolla. Tieto voi olla yksittäinen tekninen uhkatieto tai muu ei-tekninen tieto, joka on oleellinen tilannekuvan muodostamiselle. Kybermaailman poikkeamat tapahtuvat harvoin omassa tyhjiössä vaan ne linkittyvät yhä enenevissä määrin reaalimaailman tapahtumiin ja trendeihin. Tästä esimerkkinä on valtiollisten toimijoiden ja rikollisten toimijoiden rajapinnan hämärtyminen, sillä molemmat toimijat käyttävät samoja menetelmiä, mutta niiden tavoitteet voivat erota toisistaan.

Kyberturvallisuuskeskus on rakentanut yli 20 vuoden ajan luottamuksellisia suhteita yksityiseen sektoriin ja huoltovarmuuskriittisiin organisaatioihin, jotka omistavat vähintään 90% Suomen verkkoinfrastruktuurista. Suomen kriittisen infrastruktuurin organisaatiot ovat se eturintama, johon uhkat kohdistuvat. Kyberturvallisuuskeskuksen rooli kansallisen tilannekuvan muodostamisessa on erittäin tärkeä, koska Kyberturvallisuuskeskuksella on muihin turvallisuusviranomaisiin verrattuna suorempi ja välittömämpi yhteys näihin toimijoihin.

Kyberturvallisuuskeskus on kansallinen tietoturvaviranomainen, jolla on laaja kansallinen ja kansainvälinen verkosto. Nämä verkostot jakavat tilannekuvatietoa tietoturvapoikkeamista ja siten Kyberturvallisuuskeskus saa usein ensitiedon myös vakavammista tietoturvapoikkeamista, joiden taustalla on todennäköisesti valtiollista toimintaa. Tätä tietoa jaetaan muille turvallisuusviranomaisille, joilla on toimivalta asian selvittämisessä. Kyberturvallisuuskeskuksen rooli ensitiedon vastaanottajana ja avun tarjoajana on keskeinen, kun puhutaan kyberturvallisuudesta ja sen tilannekuvasta. Kyberturvallisuuskeskuksen rooli yhtenä kansallisena turvallisuusviranomaisena olisi syytä tunnistaa, kun kyse on kyberuhkien havaitsemisesta ja torjunnasta.

Osana toimenpiteitä ja linjauksia olisi tärkeää myös varmistaa resurssit toiminnalle, jotta työhön osallistuvat viranomaiset voivat torjua vakavaa rikollisuutta ja hybridivaikuttamista sekä kehittää tiedustelua vastaamaan muuttuneen turvallisuus- ja kyberympäristön vaatimuksia.

Jutta Sarvilinna
lakimies

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus