Kirjallinen kysymys KK 801/2020 vp

Mia Laiho kok

Kirjallinen kysymys sosiaali- ja terveydenhuollon tietoturvallisuudesta ja kyberturvallisuudesta

Eduskunnan puhemiehelle

Psykoterapiakeskus Vastaamo kertoi 21.10.2020 joutuneensa tietomurron ja kiristyksen kohteeksi. Tuhannet ihmiset ovat saaneet henkilökohtaisia kiristysviestejä tietomurtoon liittyen. Tapaus on laajuudeltaan sekä Suomessa että kansainvälisesti ainutlaatuinen ja poikkeuksellinen. Vastaamon tietoturvamurto ja kiristys ei koske vain uhreja, vaan myös ihmisten luottamusta potilastietojen tietoturvaan kaikkialla sosiaali- ja terveyspalveluissa. Yleisessä GDPR tietosuoja-asetuksessa (EU 2016/679), asetetaan yrityksille ja organisaatioille henkilötietojen keräämistä, säilytystä ja hallinnointia koskevat tarkat vaatimukset. Asiakastietolaissa (159/2007) käytössä olevat tietojärjestelmät jaetaan kahteen luokkaan A ja B. A-luokan saa liittää Kanta-palveluihin.

Suomessa on noin 260 sosiaali- ja terveydenhuollon alan yritystä, joiden tietojärjestelmiä valvoo sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira. Tietoturvakäytännöt ovat kuitenkin hyvin vaihtelevat ja Valviran mahdollisuudet valvoa kaikkia yrityksiä ovat resurssien takia heikot. Käytännössä yrityksien tietoturvataso on niiden oman valveutuneisuuden ja huolellisuuden varassa. Näiden lisäksi Suomessa on käytössä Kanta-palvelu ja kaikkien julkisten sairaaloiden ja terveyskeskusten potilastietojärjestelmät ja ajanvarausjärjestelmät sekä lukuisat etämittaus ja -valvontalaitteistot.

Teknologian nopea kehitys ja globalisaatio ovat tuoneet henkilötietojen suojeluun uusia haasteita. Hallitus on arvioinut, että digitalisaatiota voidaan käyttää lisääntyvästi ja että sote-uudistuksessa on myös ajateltu saatavan säästöjä digitalisaation avulla. On kuitenkin huomioitava, että kaikessa digitalisaatiossa on oltava korkeat laatuvaatimukset tietoturvan osalta. Sama pätee myös potilaskontakteihin, sekä etäyhteyksien että valvontajärjestelmien tietoturvaan ja erilaisiin hälytys-ja valvontalaitteisiin liittyen. Yksityisyyden suojan lisäksi myös asiakkaan tietosuojan on oltava korkealla tasolla ja on voitava luottaa siihen, ettei tiedot pääse ulkopuolisten käsiin.

Sähköisen asioinnin käyttö lisääntyy sosiaali- ja terveyspalveluissa jatkuvasti. Sähköisten palveluiden käyttöön ottaminen vaatii tarkkaa suunnittelua ja määrittelyä palvelun toimittajan, henkilökunnan ja asiakkaan välillä, jotta tietoturvamurtoja voidaan välttää. Tietomurto on yksi keskeisimmistä uhkatilanteista. Motiivina murrolle voi olla taloudellinen hyöty, joka toteutuu myymällä henkilötietoja tai kiristämällä asianomaista, tai tietovuoto, jossa salaisia tietoja päätyy esimerkiksi mainonnan kohdentamiseen. Palvelunesto on kolmas keskeinen uhkatilanne, jossa hyökkääjä voi häiritä tai estää sähköisen asioinnin käytön esimerkiksi häiritäkseen viranomaisten toimintaa.

Valmis
5.0

Kirjallinen kysymys KK 801/2020 vp

Sosiaali- ja terveydenhuollon organisaatiot voivat kärsiä näistä murroista ja se näkyy selvästi esimerkiksi sairaalojen taloudessa, maineessa ja sekä potilaiden että henkilökunnan turvallisuudessa ja yksityistiedoissa. Suurimmat kyberuhat liittyvät lääketieteellisiin laitteisiin; ohjelmistojen haavoittuvuudet, mobiililaitteet, etähallittavat laitteet ja järjestelmien käyttötavat sekä salasanakäytänteet. Nämä vaativat korkeatasoisia tietoturvajärjestelmiä, jotteivät ulkopuoliset tahot pääse näihin luottamuksellisiin toimintoihin.

Sähköiset palvelut, digitalisaatio ja robotiikka ovat jo tätä päivää ja niiden määrä on kasvussa. Ihmisten oikeusturvan suojaamisen lisäks yhteiskunnan kriittiset toiminnot, kuten sairaanhoito, energiantuotanto, rahaliikenne ja lennonjohto, ovat riippuvaisia tietojärjestelmien ja verkkojen toimivuudesta sekä suojauksesta.

Kyberturvallisuutta ei voi ajatella erillisenä tietoteknisenä kysymyksenä, vaan se on potilasturvallisuutta. Kyse on myös kansallisesta turvallisuudesta.

Edellä olevan perusteella ja eduskunnan työjärjestyksen 27 §:ään viitaten esitän asianomaisen ministerin vastattavaksi seuraavan kysymyksen:

Miten valvotaan Kanta-palveluiden ulkopuolella olevien yritysten tietohallintopalveluita, niiden asiakastiedon ja tietoturvan hallintaa ja tasoa,

miten hallitus varmistaa, ettei laajoissa kansalaisten tietoja sisältävissä järjestelmissä kuten Kanta-palveluissa ole tietoturvariskejä,

onko hallitus tehnyt riskinarviota ja riskinhallintasuunnitelmaa sote-maakuntaratkaisuun liittyen tietojärjestelmien osalta,

miten hallitus on huomioinut sote-lakivalmistelussa tietojärjestelmien tietoturva-asiat,

kuinka hallitus on arvioinut riittävän tietoturvan sote-palveluissa käytettäviin digitaalisiin palveluihin, potilastietojärjestelmiin ja henkilöstöhallintoon,

miten asiakastietojen luottamuksellisuuden lisäksi huomioidaan henkilökunnan tietoturva,

miten henkilöstöhallinnon tietoturva on huomioitu sote-valmistelussa,

milloin hallitus on tuomassa eduskuntaan tietojen käsittelyä koskevan kokonaislainsäädännön uudistuksen,

miten hallitus on huomioinut sote-lain valmistelussa asiakastyössä käytettävän digitalisaation korkeatasoisen tietoturvan niin, että kaikki tiedot pysyvät luottamuksellisina ja

kuinka hallitus varmistaa, että robotiikan ja terveydenhuollon digitalisaation kyberuhat ja hyökkäykset esim. lääkinnällisten laitteisiin, ohjelmistojen haavoittuvuuteen, mobiililaitteisiin, etähallittaviin laitteisiin ja järjestelmien käyttötapoihin sekä salasanakäytänteisiin huomioidaan nykytilanteessa ja suunnitellussa sote-uudistuksessa?

Kirjallinen kysymys KK 801/2020 vp

Helsingissä 26.10.2020

Mia Laiho kok