JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Hallituksen esitys eduskunnalle laiksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä sekä eräiksi siihen liittyviksi laeiksi

Professori, ST Martti Lehto

4.12.2020

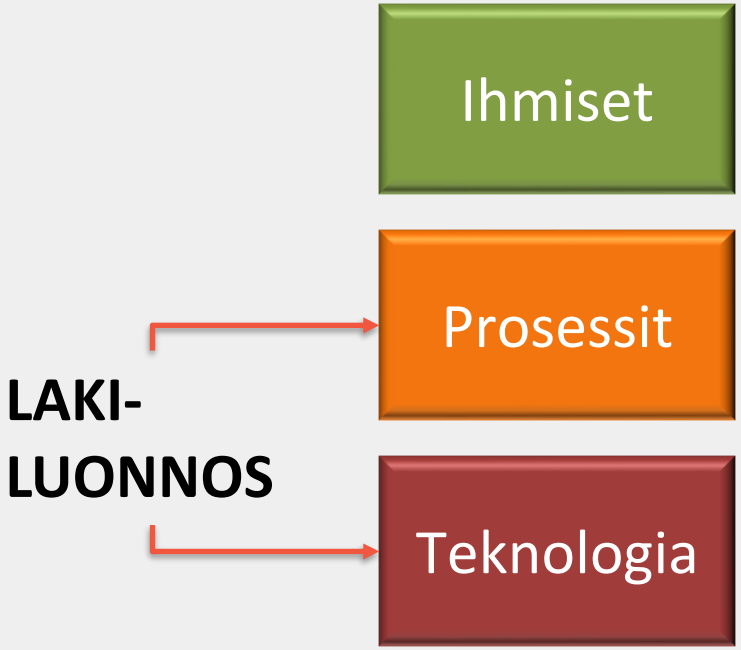
SOTE-järjestelmä – osa yhteiskunnan kriittistä infrastruktuuria

Tarvitaan älykkäitä ICT-ratkaisuja, joilla asiakkaiden tietoja voidaan käyttää organisaatio- ja aluerajoista riippumattomasti sekä ensisijaiseen että toissijaiseen käyttöön.

Menetykset kyberrikollisuudesta ovat noin 0,5–2,5 % BKT:stä.

Menetykset 6 biljoonaa dollaria.

Kyberhaavoittuvuudet

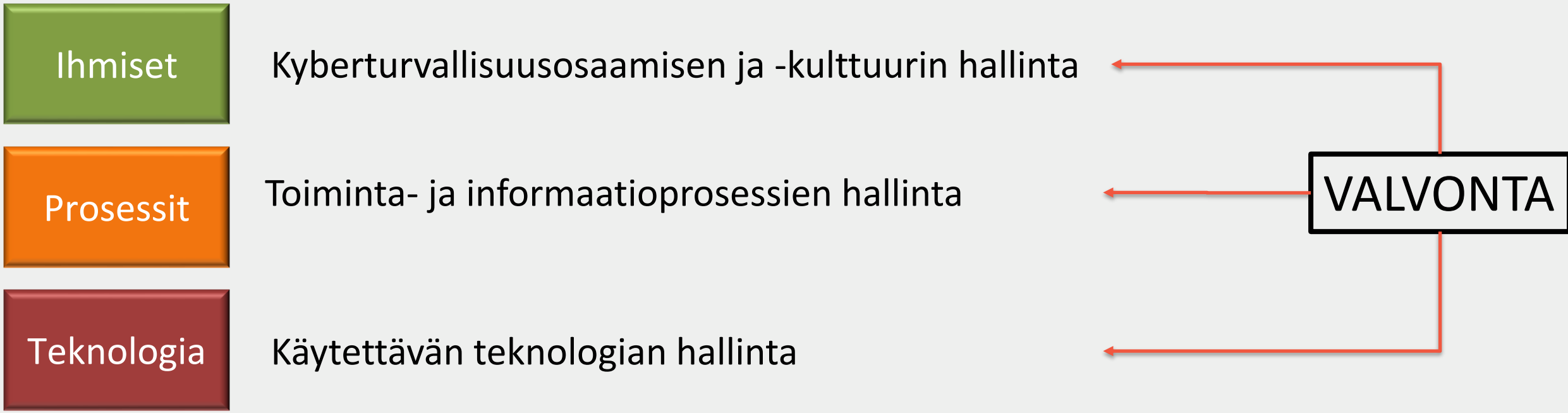


Sosiaalinen manipulointi (tietojen kalastelu, korruptoidut yrityssähköpostit, yms.).

Kyberriskien hallinnan puutteet, salasanakäytänteet, pääsynhallinta, epäselvät toimintaprosessit, kyberturvallisuusratkaisut.

Puutteet teknologiassa (ohjelmistovirheet (SW), laitteistovirheet (HW), algoritmi- ja konfigurointi heikkoudet .

Kyberturvallisuus



Kybertilannekuvan puute

- 8 % yrityksistä kykenee erittäin nopeaan kyberhyökkäysten havainnointiin
- 11 % yrityksistä kykenee nopeaan kyberhyökkäysten havainnointiin
- 21 % yrityksistä on yksi yhteinen näkymä ICT-varantoihin

Päivittäin tuotetaan 350 000–400 000 uutta haittaohjelmaa ja vanhojen variantit ml. lähes kolme miljoonaa

Source: RSA Research, March 2016

Singaporen pääministerin terveystiedot vietiin valtavassa kyberhyökkäyksessä – Asiantuntijat: Hyökkääjä oli toinen valtio

Singaporen terveysministerin mukaan hyökkäys oli tarkoin harkittu, kohdistettu ja hyvin suunniteltu.

Jussi Salmela HS

Julkaistu: 21.7. 2018 18:13

SINGAPOREEN iski suuren mittaluokan kyberhyökkäys kesäkuun lopussa. Hakkerit iskivät valtion tietokantoihin ja varastivat 1,5 miljoonan singaporelaisen terveystiedot, kertoo uutistoimisto AFP.

Valtio tiedotti asiasta perjantaina.

Myös maan pääministerin Lee Hsien Loongin terveystiedot vietiin hyökkäyksessä. Valtion mukaan juuri pääministeri oli erityisesti hyökkäyksen kohteena.

Kyberhyökkäyksen jälkeinen toipuminen ja korjaaminen

Recovery / repair costs due to a cyber attack increased by 52% - an average of $ 1.1 million per company between 2017 and 2018.

In healthcare, recovery / repair costs are even higher: $ 1.4 million.

In 2018, 93% of companies surveyed were attacked and ransomware was the most common - 51% of attacks.

Kyberturvallisuusinvestoinnit ovat vapaavalintaisia – kyberhyökkäysten korjauskustannukset pakollisia

Lakiluonnos: näkökohtia 1

Järjestelmätason näkökulma

1. Kyberturvallisuus on otettava huomioon laitteiden ja järjestelmien suunnitteluvaiheesta alkaen (Cyber Security by Design).
2. Kirjautuminen tulee tehdä vahvan kaksivaiheisen tunnistautumisen kautta.
3. Hyvinvointisovelluksille kattava sertifiointimenettely (suhteellisuusperiaate: riski).

Valvonnan näkökulma

1. Omavalvonta tuottaa perustason kyberturvallisuuden.
2. Tarvitaan ulkopuolisen toimijan tekemä tietoturva-auditointi kyberturvallisuuden vahvistamiseksi.
3. Laitteiden, järjestelmien ja prosessien sertifiointi
4. Valvontavastuiden ja -kyvykkyyksien vahvistaminen

Lakiluonnos: näkökohtia 2

Tilannekuvan näkökulma

1. Tarvitaan kyberturvallisuustoimijoiden luottamusverkoston vahvistamista.
2. Kaikkien kyberturvallisuustapahtumien raportointi.
3. SOTE-toimijoiden välistä vapaaehtoispohjalta tapahtuvaa kyberuhkia koskevaa tietojenvaihtoa tulee edistää.
4. Havainnointikyky luo perustaa oikeinmitoitetuille kyberturvallisuustoimenpiteille ja varautumiselle.

Osaamisen ja tutkimuksen näkökulma

1. Kyberosaamisenhallinnan varaan rakentuu organisaation kyberturvallisuuden rakentaminen
2. Tarvitaan laaja SOTE-alaa käsittävä tutkimus: nykytila ja tarvittavat implementoinnin toimenpiteet

Lain toimeenpano vaatii resursseja

Ehdotuksessa lueteltuihin keskeisin rahoitustarvetta edellyttäviin kehittämiskohteisiin tulee lisätä kyberturvallisuuden vahvistamisesta aiheutuvat kustannukset.

Tarvitaan investointeja laitteisiin ja tietojärjestelmiin, kybertilannekuvan luomiseen eri organisaatioissa, auditointi- ja sertifiointiprosessien vahvistamiseen, kyberosaamisen tehostamiseen sekä SOTE-alan kyberturvallisuuden tutkimukseen.

Kaikkien toimijoiden tulisi nähdä kyberturvallisuus toiminnan varmistajana ja toimintaedellytysten luojana, eikä kustannuseränä.

Lakiluonnos

Kokonaisuutena hallituksen esitys eduskunnalle laiksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä vahvistaa Suomen digitalisaatiokehitystä.

Laissa ja sen toimeenpanossa tulee kiinnittää erityistä huomiota SOTE-järjestelmän kyberturvallisuuteen holistisesta järjestelmänäkökulmasta = yksittäisitä ratkaisuista kokonaisvaltaiseen systeemiseen ratkaisuun.

Liiketoiminnalle aiheutuvat kustannukset

Petya/Non-Petya hyökkäyksen Ukrainaan kesäkuussa 2017 aiheuttamat kustannukset liiketoiminnan palauttamiselle:

Farmasiayhtiö Merck: $870,000,000
JakeluyhtiöFedEx: $400,000,000
Rakennusyhtiö Saint-Gobain: $384,000,000
Laivakuljetusyhtiö Maersk: $300,000,000
Elintarvikeyhtiö Mondelēz: $188,000,000
Terveys- ja hygieniatuoteyhtiö Reckitt Benckiser: $129,000,000

Yhteensä vahingot $10 miljardia

Kesäkuussa 2019 American Medical Collection Agency (AMCA) menetti hakkereille lähes 20 miljoonan potilaan henkilökohtaiset tiedot: nimi, syntymäaika, osoite, puhelinnumero, palvelupäivä, palveluntarjoaja, saldotiedot, luottokorttitiedot, pankkitili.

AMCA hakeutui konkurssiin.

Kyberhyökkäyksiä SOTE-tietojärjestelmiä vastaan 2019–2020, USA

Organisaatio<	Tapahtuma	Syy
American Medical Collection Agency	25 miljoonaa asiakastietoa	Hakkerointi
Dominion National	2,96 miljoonaa; henkilötietoja, osittaisia potilastietoja	Hakkerointi
Inmediata Health Group	1,57 miljoonaa; henkilö- ja potilastietoja	Tietokannan saastuttaminen
University of Washington Medicine	974,000; henkilötietoja, potilastietoja	Palvelimen väärä konfigurointi
Magellan Health	654,000; henkilötietoja	Kannettavan tietokoneen varkaus
Florida Orthopaedic Institute	640,00; potilastietoja	Lunnashaittaohjelma ja mahdollinen tietomurto
Wolverine Solutions Group	600,000; henkilötietoja	Lunnashaittaohjelma ja tietomurto
Oregon Department of Human Services	625,000; henkilötietoja, potilastietoja	Tietojen kalastelu
Elite Emergency Physicians	550,000; potilastietoja	3.osapuolen huonosti hoitama tietojenkäsittely
Magellan Health	365,000; henkilöstö- ja potilastietoja	Tietojen kalastelu ja haittaohjelma
UConn Health	330,000; henkilötietoja, osittaisia potilastietoja	Tietojen kalastelu
BJC Healthcare + 19 muuta samassa verkostossa	290,000; henkilötietoja, potilastietoja	Tietojen kalastelu
Navicent Health	280,000; henkilötietoja, osittaisia potilastietoja	3.osapuolen kautta
ZOLL Services	280,000; henkilötietoja, osittaisia potilastietoja	Virhe siirrettäessä tietoja palvelimelta
Benefit Recovery Specialists	275,000; henkilötietoja, osittaisia potilastietoja	Hakkeroituminen käyttäen työntekijän oikeuksia
Ambry Genetics	232,000; henkilötietoja, osittaisia potilastietoja	Työntekijän emailin hakkerointi
PIH Health	200,000; henkilötietoja, osittaisia potilastietoja	Usean työntekijän emailin hakkerointi
BST & CO. CPAs	170,000; henkilötietoja	Lunnashaittaohjelma

Kiitos

www.jyu.fi/it