



Kuntamarkkinat



11. - 12.9.2019

Digiturvallisuus

12.9.2019 klo 12-12.45 tila A 3.6

Tietoturva tiedonhallintalaissa, johtava asiantuntija Kirsi Janhunen,
väestörekisterikeskus

Tietoturvaloukkaukset ja niistä ilmoittaminen, tilannekuva- ja
yhteistyöverkostot -ryhmän päällikkö Jarna Hartikainen,
Kyberturvallisuuskeskus



Tietoturva tiedonhallinta-alaissa

Kirsi Janhunen, VRK

Kuntamarkkinat 12.9.2019



Väestörekisterikeskus

Sisältö

- Tiedonhallintalaki pähkinänkuoressa
- Täytäntöönpanon tuki
- Mitä ovat tietoturvasäännösten toimeenpanon suositukset?
- Muutamia käytännön vinkkejä toteuttajille



Tiedonhallintalaki pähkinänkuoressa

- Laki julkisen hallinnon tiedonhallinnasta (906/2019)
<https://www.finlex.fi/fi/laki/alkup/2019/20190906>
- Laissa säädetään julkisuusperiaatteen ja hyvän hallinnon vaatimusten toteuttamisesta viranomaisten tiedonhallinnassa.
- Laissa säädetään myös tietojärjestelmien yhteentoimivuuden toteuttamisesta.
- Laki sisältää koko julkista hallintoa koskevat säännökset tiedonhallinnan järjestämisestä ja kuvaamisesta, tietovarantojen yhteentoimivuudesta, teknisten rajapintojen ja katseluyhteyksien toteuttamisesta sekä tietoturvallisuuden toteuttamisesta.
- Lakia tarkennetaan asetuksilla, jotka koskevat turvallisuusluokiteltavia asiakirjoja, tiedonhallintalautakunnan toimintaa sekä valtion viranomaisia koskevaa tiedonhallinnan muutosten lausuntomenettelyä.

Laki astuu voimaan 1.1.2020



Digipalveluissa huomioitavat tietoturvallisuusvaatimukset

Toimintaympäristön tietoturvallisuustilan seuranta
Tietoturvallisuuden varmistaminen tiedon elinkaaren ajan
Tietoriskien hallinnan järjestäminen ja siihen perustuvat tietoturvatoimet
Vikasietoisuuden ja toiminnallisen käytettävyyden varmistaminen
Hyvän julkisuus ja salassapitorakenteen huomioiminen tietovarantojen tietorakenteissa
Salassa pidettävien tietojen suojaaminen yleisessä tietoverkossa tietoja siirrettäessä
Tietoaineistojen turvallisuuden varmistaminen
Käyttöoikeuksien määrittely ja hallinta tietojärjestelmiin
Tarpeellisten lokitietojen kerääminen
Turvallisuusluokiteltavat asiakirjat + niiden käsittely (asetus)

Lähde: VM



Väestötietokeskus

Täytäntöönpanon tuki

- Tiedonhallintalain täytäntöönpanoa johtaa valtiovarainministeriö. Vuodenvaihteen jälkeen tiedonhallintalautakunnalla tulee olemaan keskeinen rooli täytäntöönpanon varmistamisessa.
- Yksittäisen kunnan kannalta täytäntöönpanoa tukeva informaatio on keskeistä
- Erilaisten verkostojen merkitys kasvaa. Kunnan oma aktiivisuus on tärkeää.
- Tietoturvan osalta kannattaa seurata VRK:n JUDO-hanketta ja VM:n tiedonhallintalain tietoturvallisuuden alatyöryhmää



Tietoa ja tukea toimeenpanoon

- JUDO-hanke toimeenpanee valtiovarainministeriö digitaalisen turvallisuuden kehittämisohjelmaa 2018-2021 www.vrk.fi/judo
- JUDO-työpajojen tilaisuudet on katsottavissa tallenteilta <http://www.mediaserver.fi/live/judo>
- Digiturvapalveluiden postituslista <https://response.questback.com/vestrekisterikeskus/digiturva>
- Twitterissä #digiturva
- digiturva@vrk.fi
- Tiedonhallintalain täytäntöönpanosta viestitään VM:n verkkosivuilla: <http://vm.fi/tiedonhallintalain-taytantonpano>
- Twitterissä #tiedonhallintalaki



Tietoturvasäännösten toimeenpanon suositukset

- Tiedonhallintalain tietoturvasäännökset kuvaavat keskeiset vaatimukset tietoturvallisuudelle.
- Laissa toimenpiteet on kuvattu sellaiselle tasolle, että tiedonhallintayksikkö voi suunnitella varsinaisen toteutuksen tarkoituksenmukaisesti.
- Organisaatiot tarvitsevat kuitenkin tukea toimeenpanoon.
- Suositusten valmistelu on käynnistetty etupainotteisesti osana valtiovarainministeriön digitaalisen turvallisuuden kehittämisohjelmaa. (JUDO-hanke)



Suosituksen valmistelu

- Tiedonhallintalain 4 luvun säännöksiä avaavia ”soveltamiskortteja” on valmisteltu julkisen hallinnon digitaalisen turvallisuuden toimeenpanohankkeen (JUDO) koordinoimana. Työhön on osallistunut erityisesti VAHTI:n asiantuntijajaokset.
- Myös tiedonhallintalain nojalla annettavan turvallisuusluokitusta käsittelevän asetuksen tueksi laaditaan soveltamiskortteja. Työhön osallistuvat erityisesti turvallisuusviranomaiset.



Suosituksien käsittely

- Suositukset luovutetaan valmistumisjärjestyksessä VM:n Tietoturvallisuus -alatyöryhmälle jatkokäsittelyyn.
- Suositustyön organisointi tarkentuu osana tiedonhallintalautakunnan tehtävien toteuttamista viimeistään tiedonhallintalautakunnan aloitettua toimintansa.
- Luonnosten valmisteluun voi osallistua kommentoimalla soveltamiskortteja. Lisätietoja digiturva@vrk.fi



Syksyn 2019 aikana valmistuvat suositukset ja liitemateriaalit

- 13.2 § riskienhallinta
- 17 § lokitietojen kerääminen,
- 15.1 §, 2 kohta: vahingoilta suojaaminen
- 13.1 § elinkaaren huomioiminen tietojärjestelmissä, tietojenkäsittelyssä
- 13.4 § tietoturvallisuus hankinnoissa
- Turvallisuusluokitteluasetus
 - Tarkentuu kun työryhmä käynnistää toiminnan



Miten ottaa tiedonhallintalain tietoturvaa haltuun?

Yhdessä opittua 





1. Tutustu tiedonhallintalakiin

- Lue laki läpi. Tutustu tarvittaessa lain perustelumuiistioon.
<https://www.finlex.fi/fi/laki/alkup/2019/20190906>
- Tutustu koulutusmateriaaleihin ja aiemmin kerrottuihin lähteisiin
- Verkostoidu muiden kanssa
- Osallistu aihetta käsitteleviin seminaareihin ym.





2. Paloittele lain vaatimukset

13 §

Tietoaineistojen ja tietojärjestelmien tietoturvallisuus

Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan.

Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvaluustoimenpiteet riskiarvioinnin mukaisesti.

13.1 § Elinkaari

13.2 § Riskienhallinta

Viranomaisen tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava riittävällä testauksella säännöllisesti.

Viranomaisen on suunniteltava tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvä tietojenkäsittely siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa.

Viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvaluustoimenpiteet.

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista säädetään erikseen.





3. Listaa laissa olevat vaatimukset ja tee karkea soveltamissuunnitelma

Vaatus	Vaatusen tila	Toteutustapa	Vastuu
13.1 § Elinkaari			
13.2 § Riskienhallinta			
13.3 §			
13.4 §			



4. Listaa laissa olevat vaatimukset ja tee karkea soveltamissuunnitelma

Vaatus	Vaatus	Toteutustapa	Vastuu
	Arvioi työmäärä. Mitä luontevammin tehtävät sisältyvät organisaation toimintaan, sen parempi.		
13.1 § Elinkaari	Projektoi tarvittaessa. Projektointi voi auttaa laajempien kehityskohteiden resursoinnissa ja budjetoinnissa.		
13.2 § Riskienhallinta	Huomioi työssä, että dokumentit usein vanhentuvat pian. Panosta enemmän toimiviin ratkaisuihin kuin dokumentaation tuottamiseen. Huolehdi siitä, että organisaation johto saa tarvittavasti tietoa. Sitouta, motivoi, innosta.		
13.3 §			
13.4 §			



5. Dokumentoi järkevästi

- Panosta enemmän laatuun kuin määrään
- Huolehdi siitä, että dokumentaatiota on mahdollista pitää kohtuullisella työllä ajan tasalla
- Monet tietoturvapääalliköt tukeutuvat tietoturvakäsikirjaan. Käsikirjassa kuvataan keskeisimmät tietoturvakäytännöt. Käsikirjan pohjalta voidaan tehdä vaatimustenmukaisuutta kuvaavia listauksia. (Seuraa vinkkejä JUDO-hankkeessa)





Lopuksi

- Hyödynnä organisaatiossa tehtyä työtä
- Tee yhteistyötä muiden kanssa
- Hyödynnä hyviä käytänteitä
- Kannusta hyvään turvallisuuskulttuuriin



Kiitos mielenkiinnosta!

Lisätietoja: digiturva@vrk.fi



Västöräkisterikeskus

Kyberturvallisuuskeskus

Ilmoita tietoturvaloukkaudesta!

Kuntapäivät 12.9.2019

Jarna Hartikainen @JarnaHnen

Tilannekuva-yksikön päällikkö

Osaava edelläkävijä – maailman toimivin ja turvallisin yhteiskunta



Huolehdimme elintärkeästä ympäristöstämme, annamme mahdollisuuden innovatiivisille palveluille sekä varmistamme toimivat ja turvalliset yhteydet.

TRAFICOM
Liikenne- ja viestintävirasto

Toimintamme perustuu luottamukseen ja vuorovaikutukseen. Olemme arvostettuja asiantuntijoita ja pidämme huolta hyvinvoinnista.

Kyberturvallisuuskeskus

Kansallinen tietoturvaviranomainen, jonka tehtävinä mm.

- **Kerätä tietoa** tietoturvaloukkauksista ja niiden uhkista
Tiedottaa tietoturva-asioista sekä viestintäverkkojen ja viestintäpalvelujen toimivuudesta;
- **Selvittää** verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia.
- Teleyritysten **tietoturvallisuuden ja varautumisen** valvonta ja ohjaus
- **Järjestelmien ja verkkojen tarkastus ja hyväksyntä**
- **Sähköisen viestinnän yksityisyydensuojaan** liittyvien velvoitteiden valvominen





Koordinointi ja avunanto tietoturvaloukkauksissa

Tarjoamme tarvittaessa **luottamuksellista** apua tietoturvaloukkauksen selvittämiseksi sekä koordinoimme tarvittavia toimenpiteitä.

- ▶ **Toimenpiteet voivat pitää sisällään muun muassa:**
 - ▶ Tiedon jakamista
 - ▶ Yhteistyökumppanien ja -verkostojen kontaktointia
 - ▶ Teknistä analyysiä
 - ▶ Lainopillista neuvontaa



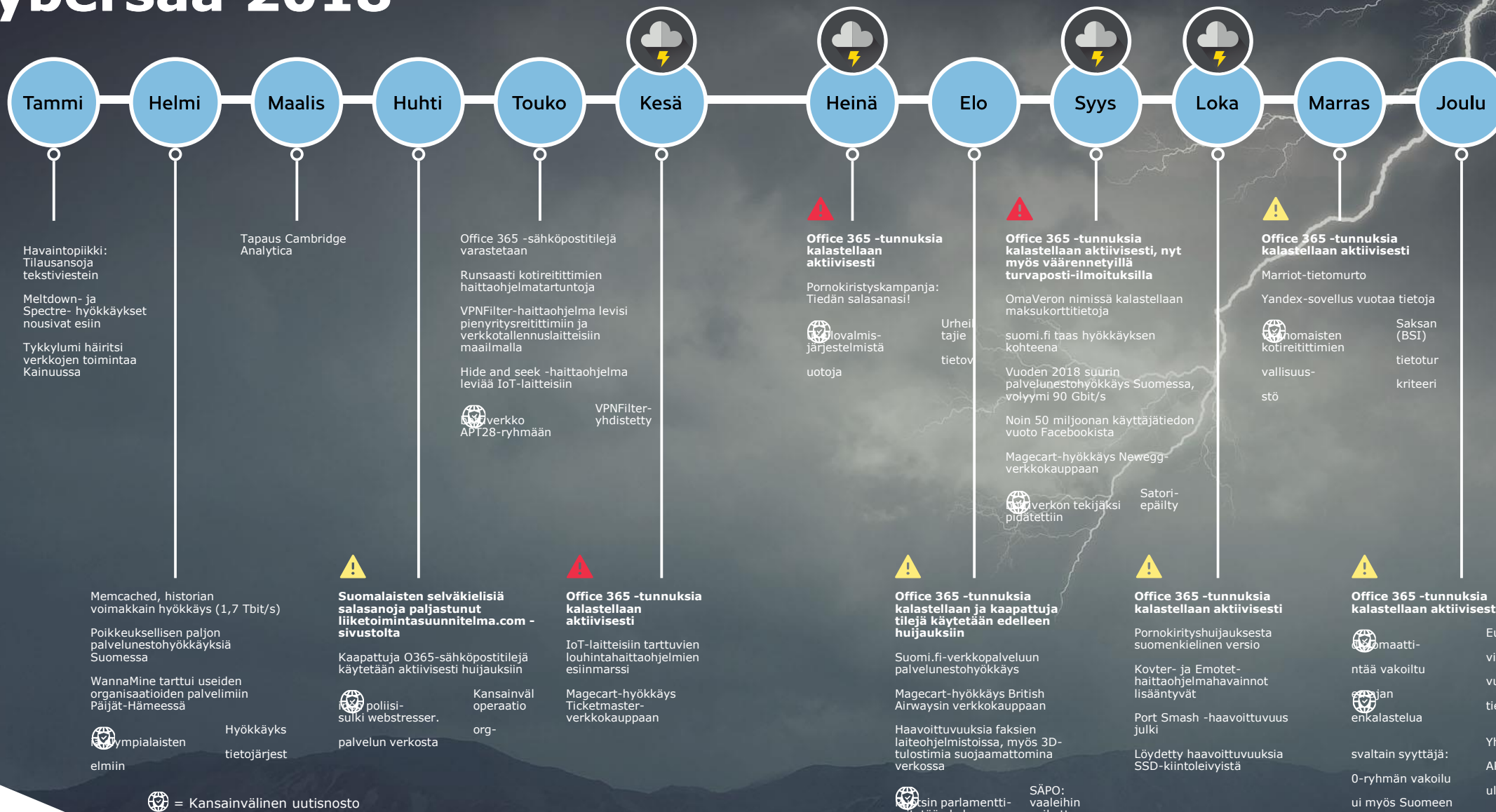


TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Kybersää 2018



= Kansainvälinen uutisnosto

Kybersää heinäkuu 2019



Verkkojen toimivuus

- ▶ Kolme merkittävää toimivuushäiriötä, mikä on keskimääräistä vähemmän
- ▶ Paikannusjärjestelmä Galileo ei toiminut viikkoon
- ▶ Palvelunestohyökkäyksien vaikutukset onnistutaan torjumaan aiempaa paremmin.



Vakoilu

- ▶ Pohjois-Korean väitetään anastaneen yhteensä 2 miljardia US dollaria kyberhyökkäyksiin ydinaseohjelman rahoittamiseksi
- ▶ Kiinalaisryhmittymä Winnti on vakoillut vuosien ajan useita saksalaisia korkean teknologian yrityksiä



Haittaohjelmat ja haavoittuvuudet

- ▶ Applen iMessage-sovelluksessa useita vakavia haavoittuvuuksia.
- ▶ VxWorks-käyttöjärjestelmästä löydetty useita vakavia haavoittuvuuksia, jotka vaikuttavat kriittisiin sovelluksiin
- ▶ BlueKeep-haavoittuvuus voi johtaa haittaohjelmaepidemiaan.



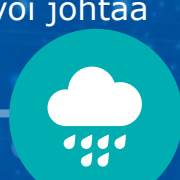
Tietomurrot ja -vuodot

- ▶ Kokemäen kaupungin järjestelmiin kohdistui tietomurto ja kiristyshaittaohjelma.
- ▶ Tietomurto Capital One –pankkiin.
- ▶ Tietomurtojen kohteeksi joutuneet organisaatiot määrättiin maksamaan satoja miljoonia euroja uhreille.



Huijaukset ja kalastelut

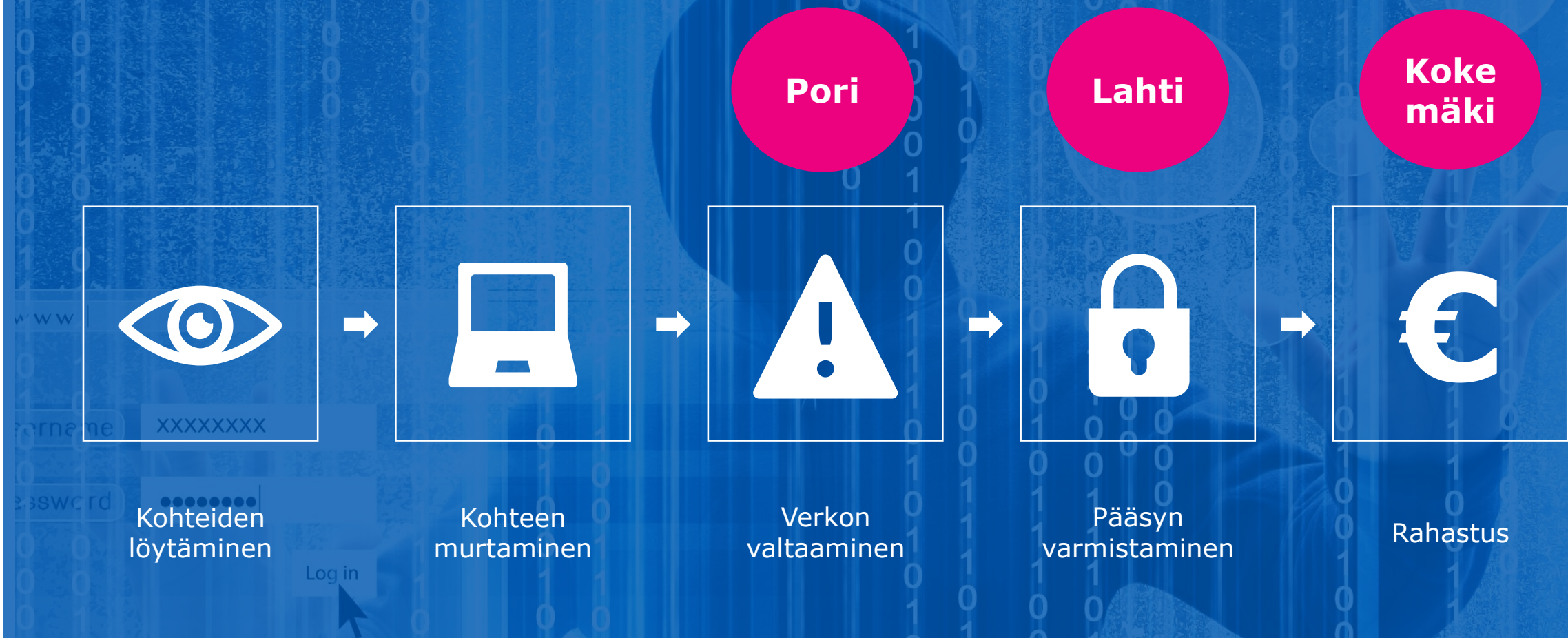
- ▶ Lomakausi sijaisuuksineen on näkynyt jälleen lisääntyneinä toimitusjohtajahuijauksina
- ▶ O365-aiheinen kalastelu jatkuu edelleen runsaana ja johtaa onnistuneisiin tietomurtoihin.



IoT ja automaatio

- ▶ Sääntelyyn herätty Euroopan tasolla
- ▶ IoT-laitteiden hyväksikäyttö kohdentuu organisaatioihin, hyödyntäen organisaatioiden kasvaa varjo-IT:tä.

Tietomurrot osana rikollisten rahantekoa



Kyberhyökkäys vaarantaa kuntapalvelut

Lahti - kaupungin koko tietoverkko - vaikutukset

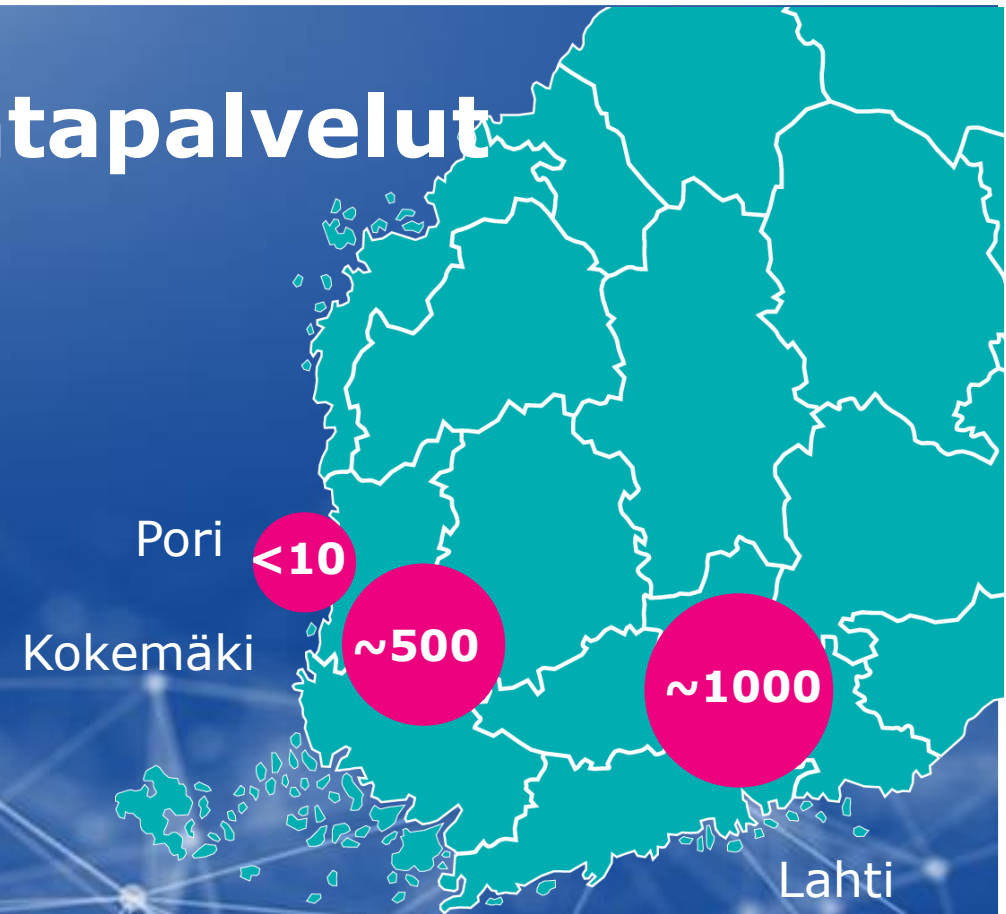
- Terveys- ja sosiaalihuollon pääsy potilas- ja ajanvaraustietoon
- Laajat vaikutukset kriittisiin palveluihin onnistuttiin estämään
- Korjauskustannukset elokuussa 690 000 €

Kokemäki - kaupungin hallinnon tietoverkko - vaikutukset

- Tietoverkon käyttökeltvottomuus esti kunnan päätöksenteon
- Sosiaalihuollon käyttämät sähköiset palvelut pois käytöstä
- Kaupungin maksuliikenne pois käytöstä

Pori - koulujen tietoverkko - vaikutukset

- Käyttäjätilien kautta pääsy oppilaiden tietoihin ja tiedostoihin
- Laajentumisen riski kriittisempiin verkkopalveluihin, identiteettivarkaudet



Lahti
6/2019 ->

Kokemäki
7/2019

Kesäkuu

Heinäkuu

Pori
Elokuu
8/2019

Yhteenvetoa ja analyysiä

- ▶ **Kokonaiskuva** – Kuntien kyberturvallisuuden tilanteesta ei ole kokonaiskuvaa, koska ilmoitusvelvollisuutta poikkeamista ei ole.
- ▶ **Ympäristö** - Porin etuna, että kohteena pieni ja erillinen ympäristö, jolloin mahdollisuus tehdä torjuntatoimet rauhassa oikein.
- ▶ **Valvonta** - Lahdessa ja Porissa tietoturvan tekninen valvonta onnistui.
- ▶ **Eriytys** - Kokemäellä ja Porissa eri verkot oli eristetty hyvin toisistaan. Se rajoitti automaattisesti vahinkojen suuruutta ja helpotti palautumista.



Pintaraapaisu Manner-Suomen kuntien tilanteeseen

- ▶ 10/10 isoimman kunnan julkisesta palvelupinta-alasta sisältää ongelmia
- ▶ 9/10 pienimmän kunnan julkisesta palvelupinta-alasta sisältää ongelmia

Esimerkkejä aukoista:

- ▶ Palomuurin hallinta
- ▶ Tietokanta
- ▶ Intranet
- ▶ Vanhentuneet käyttöjärjestelmät ja ohjelmistot
- ▶ Vanhentuneet palvelimet jne.



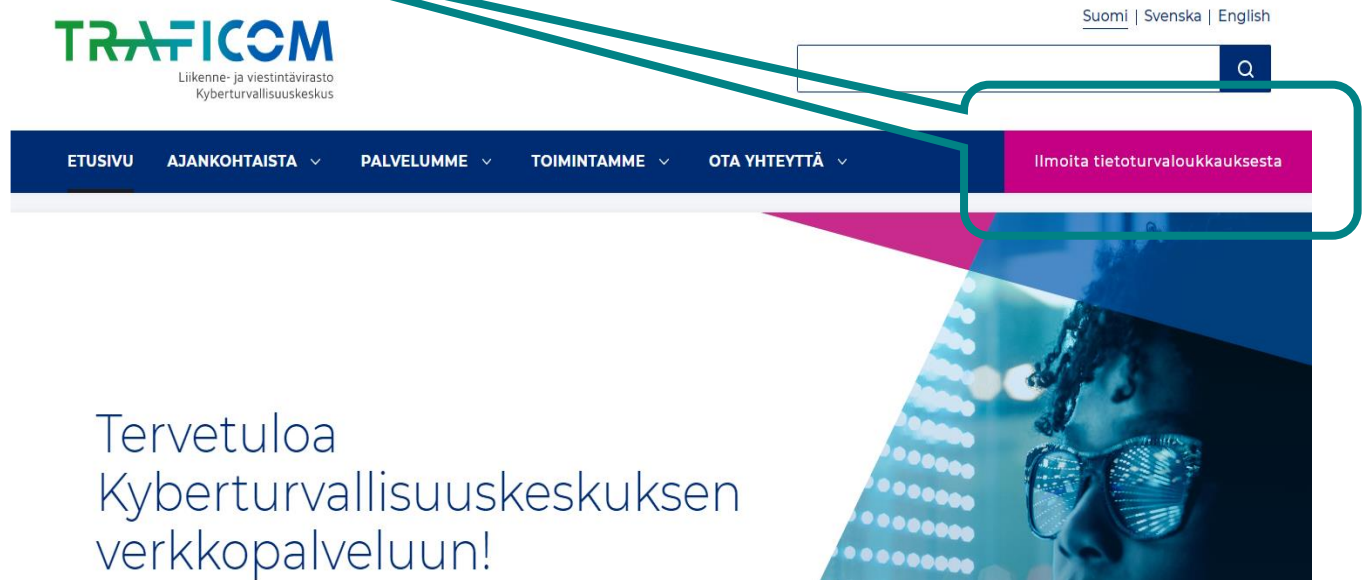
Tärkeimmät opit

- ▶ Tiedä mitä omistat ja mistä olet vastuussa.
 - ▶ Olet vastuussa myös ulkoistamiesi palveluiden toiminnasta.
 - ▶ Ymmärrä vastuittesi ja järjestelmien väliset riippuvuudet
- ▶ Laadi jatkuvuus- ja palautussuunnitelmat kunnan eri tehtäville ja harjoittele niitä käytännössä.
- ▶ Investoi aktiiviseen tietoturvatyöhön.
- ▶ Ilmoita tietoturvaloukkauksista Kyberturvallisuuskeskukselle.



Palvelumme

- ▶ Tietoturvapalvelumme ovat pääsääntöisesti maksuttomia ja kuuluvat kaikille.
- ▶ Lisätietoa palveluistamme osoitteesta ja tietoturvaloukkauseilmoituksen tekeminen:
 - ▶ **www.kyberturvallisuuskeskus.fi**
 - ▶ sähköpostitse **cert@traficom.fi**



Kiitos!

jarna.hartikainen@traficom.fi
@JarnaHnen

TRAFFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus