Mihin varautua, kun sairaala varautuu kyberuhkiin?

Perttu Halonen

Sosiaali- ja terveydenhuollon ATK-päivät, 24.5.2017

Sisällys

- Keskeisimpiä kyberuhkia
- Liian paljon huomiota kiinnitetään...
- Liian vähän huomiota kiinnitetään...
- Ratkaisuita

Keskeisimpiä kyberuhkia

Lääkinnälliset laitteet

- Ehkä suojaamattomina internetissä?
- Mahdollisia seurauksia:
  - hoitovirheet
  - yksityisyyden loukkaukset
- Todennäköisyys kohtalainen ja kasvaa
- Seuraus vakava
- Syitä uhkalle:
  - päivitysten puuttuminen
  - kyvyttömyys asentaa päivitykset ajallaan
  - huono tietoverkkojen suunnittelu
  - tiedonkulun puutteet sairaalan organisaatiossa

Potilastiedot: saatavuus

- Pääsy tietoihin estyy yllättäen
- Mahdollisia seurauksia:
  - hoito hidastuu
  - hoitovirheet
- Todennäköisyys kohtalainen ja kasvaa
- Seuraus kohtalainen
- Syitä uhkalle:
  - työntekijä käynnistää kiristyshaittaohjelman vahingossa
  - tietoliikennehäiriö
  - tietojärjestelmien virhe tai epäyhteensopivuus

Potilastiedot: satunnainen paljastuminen

- Yksittäisten potilaiden tietoja paljastuu sivullisille
- Mahdollisia seurauksia:
  - yksityisyyden loukkaus
  - identiteettivarkaus
  - potilaan kiristäminen
- Todennäköisyys kohtalainen
- Seuraus kohtalainen
- Syitä uhkalle:
  - hoitohenkilökunnan olan yli kurkkiminen
  - tietoja varastava haittaohjelma yksittäisellä hoitohenkilökunnan tietokoneella

Potilastiedot: massiivinen paljastuminen

- Tietomurto potilastietokantaan ja tietojen varastaminen
- Mahdollisia seurauksia:
  - yksityisyyden loukkaus
  - identiteettivarkaus
  - potilaiden ja sairaalan kiristäminen
- Todennäköisyys pieni
- Seuraus vakava
- Syitä uhkalle:
  - päivitysten puuttuminen
  - kyvyttömyys asentaa päivitykset nopeasti
  - huono tehtävien eriyttäminen
  - huono verkonvalvonta

Liikaa huomiota kiinnitetään...

"Rautaa rajalle"

- Tunkeutumisenhavaitsemisjärjestelmä, palomuuri, tietoturvatiedon- ja lokienhallintajärjestelmä, tietoturvamittaristo, anti-viruskaranteeni, ...
- Tietoturvatekniikka ei ratkaise mitään, jos sitä ei käytetä oikein
- Käyttö vaatii ihmisresursseja

Erillisratkaisut

- Tässä sairaalassa X:n ja Y:n palomuuri, tuolla Z:n toimittama. Yhdellä osastolla historiallisista syistä erillinen käyttöoikeuksien hallinta. Jne.
- Tietojärjestelmistä ja niiden turvajärjestelmistä tulee monimutkaisia ja hankalia hallita.
- Tarvitaan tietoturvastrategiaa ja -arkkitehtuuria!

Jokapäiväiset häiriöt

- Päivittäisten tapausten lapioiminen vie kaiken huomion
- Mitä jos harvinainen häiriö haittaakin sairaalan toimintaa laajasti eikä siitä selvitä normaaleilla voimavaroilla?
- Miten eskaloidaan joulupäivänä kello 2.40?
- Mitkä korjaustoimenpiteet priorisoidaan?
- Mistä lisää resursseja?

Liian vähän huomiota kiinnitetään...

Kyberturvallisuushenkilöstön riittävyys

- Hallittavia yksityiskohtia on väistämättä paljon
- Uhkakenttä muuttuu jatkuvasti
- Organisaatiosiiloissa piilevät resurssit eivät ole riittävän tehokkaassa käytössä

Ohjelmistojen päivittäminen

- Ajantasaiset ohjelmistot ovat paras turva haittaohjelmia vastaan!
- Jokainen ohjelmisto on oltava päivitetty
  - » Tai tietokone kunnolla eristetty verkosta
- Inventaario laitteista, ohjelmistoista, versioista, ylläpitäjistä!

Tietoturvalliset työskentelytavat

- Tietoturvahygienia
- Vaatii koko henkilöstön pitämistä mukana tietoturvallisuuden suunnittelussa ja jalkauttamisessa
  - » Työ ja välineet on suunniteltava siten, että ne ohjaavat toimimaan tietoturvallisesti joka päivä
  - » Koulutus

Käyttöoikeuksien rajaaminen

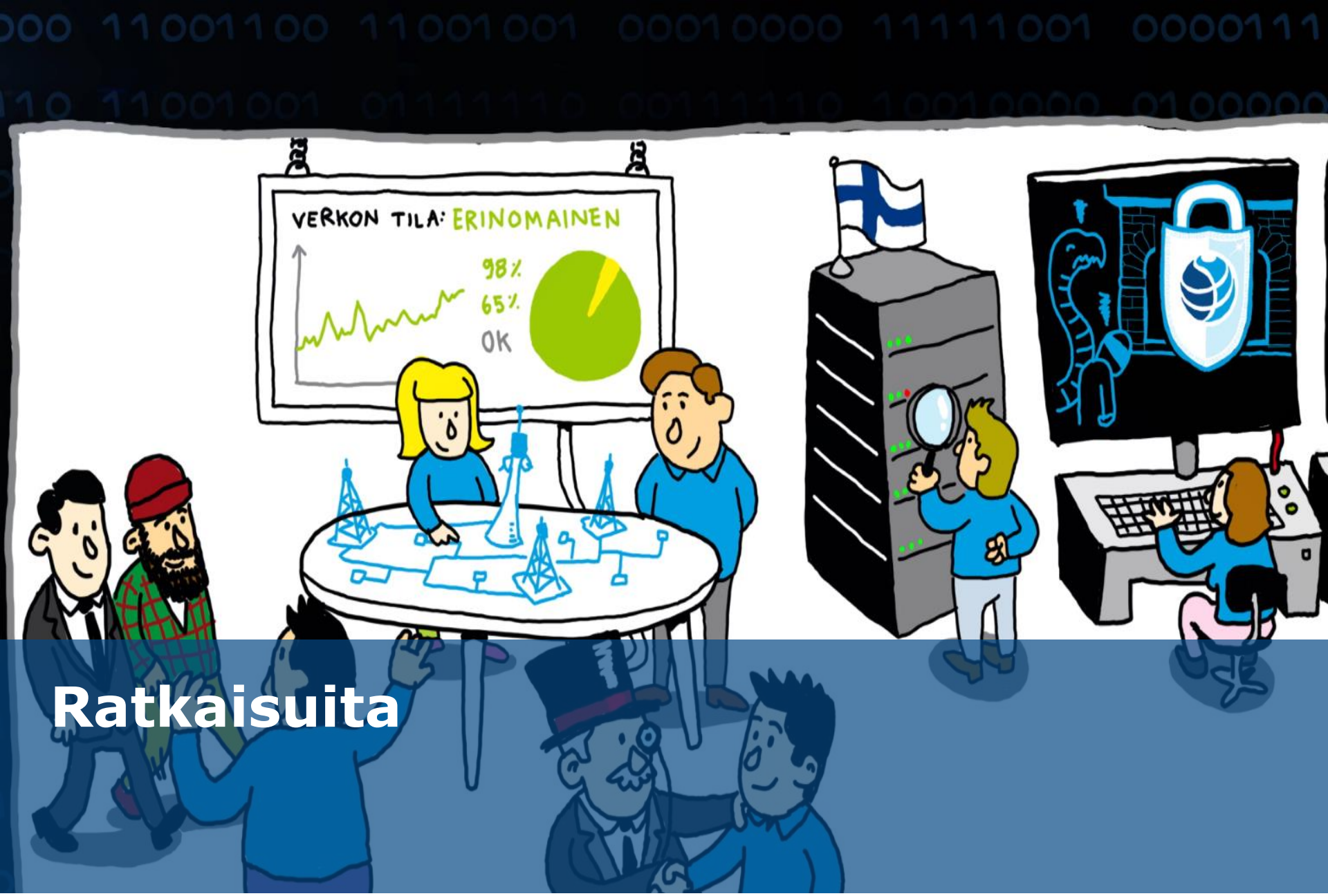
- Oikeuksia vain todellisen tarpeen mukaan
- Tarpeet muuttuvat
  - » Tasapainoilu ylläpidon työkuorman ja vahinkojen korjaamisen välillä

Tietoturvan valvonta

- Tietoturvapoikkeamat on kyettävä havaitsemaan
  - » Myös silloin, kun joku ulkopuolinen tulee sanomaan, että teillä on jossakin tietoturvaongelma
- Lokien keräys, säilytys ja analysointikyky
- Matala ilmoituskynnys, selkeä eskalointi

Tietojen vaihto

- Kollegat toisissa terveydenhuollon organisaatioissa
- Yhteiset tuotteet ja ratkaisut
- Tietoturvan hallinta, tietoturvaloukkausten ehkäisy, loukkauksiin reagoiminen



Ratkaisuita

Asennekasvatus

- Kyberturvallisuus ei ole vain ATK-nörttien työtä
- Jokaisen tulee pitää huoli, että potilaat saavat hyvää hoitoa huomennakin

Rahaa kyberturvallisuuden hallintaan

- Riittävästi osaamista omassa talossa, jotta tiedetään, mitä tarvitaan ja halutaan
- Yhteistyökumppaneita suuritöisten tilanteiden hallintaan
- Tarpeelliset työkalut ammattilaisille

Asiantuntijatiimit

- Sairaalan toimialoja yhdistäviä kyberturvallisuuden asiantuntijatiimejä
  - » Yhteinen tilannekuva
  - » Organisaation siilojen ylittäminen

TOP 5 UHAT: Organisaatiot

Päivitysten laiminlyönti
Muutostenhallinta on monista syistä hankalaa. Päivittämättömät laitteet kaapataan resursseiksi haittakäyttöön.

Kiristyshaittaohjelmat
Työasemat ja verkkopalvelimet lukitaan lunnaita varten. Jälkien korjaaminen aiheuttaa pitkiä katkoksia toiminnassa.

Huijausviestit ja tietojen kalastelu
Laskutus- ja toimitusjohtajahuijaukset aiheuttavat suuria taloudellisia menetyksiä. Urkittuja tietoja käytetään uusiin rikoksiin.

Ulkoistusten ja laitehankintojen hallinta
Laitteet, ohjelmistot ja palvelut ostetaan eri paikoista. Vastuut, sopimukset ja tietoturva koetaan toisarvoisiksi hankintahetkellä. Kokonaisuuden riskejä on vaikea hallita.

Palvelunestohyökkäykset ovat internetin arkipäivää. Se on huomioitava organisaation riskiarvioissa joko hyökkäysten sietämisen tai varautumisen ja suojautumisen kannalta.

TOP 5 RATKAISUT: Organisaatiot

Järjestelmien rutiininomainen päivitys
Ota päivittäminen kiinteäksi osaksi tietohallinnon prosesseja, niin pysyt järjestelmiesi kanssa ajan tasalla.

Koulutettu henkilöstö
Tarkkaavaiseksi koulutettu henkilökunta on paras suoja uhkia vastaan. Myös verkkoympäristön segmentointi auttaa pitämään syntyneet vahingot pieninä.

Varmuuskopiot
Tee varmuuskopioinnista säännöllistä ja harjoittele niiden palauttamista.

Lokien hallinta
Tapahtuneen selvittely, vahinkojen korjaaminen ja haavoittuvuuksien paikkaaminen onnistuvat vain, jos lokeista selviää, mitä on tapahtunut.

Tietoturvan hallittu johtaminen
Sovi etukäteen vastuut sekä oman väen että yhteistyökumppaneiden kanssa. Silloin akuutissa tilanteessa tiedetään, miten tulee toimia.

TOP 5 UHAT: Yksityishenkilöt

Huijaukset ja tilausansat
Uskottava ulkoasu ja kieli saavat yhä useamman haksahtamaan huijauksiin.

Kiristyshaittaohjelmat leviävät älylaitteisiin
Lunnastroijalaiset lukitsevat tietokoneiden lisäksi muitakin laitteita, kuten televisioita ja tabletteja.

IoT tuli joka kotiin,
mutta tietoisuus sen riskeistä ei tullut samassa paketissa.

Yksityisyys somemaailmassa
Kaikki jakamasi ja tekemäsi siirtyy markkinoijan käyttöön, halusit sitä tai et.

Salasanojen kierrätys
Koska moni käyttää samoja vanhoja salasanoja eri palveluissa, yhteen palveluun murtautuminen vaarantaa muidenkin palveluiden käytön.

TOP 5 RATKAISUT: Yksityishenkilöt

Mieti ennen kuin klikkaat
Varmista, että linkki tai tiedosto, jota olet avaamassa, on sitä mitä väittää olevansa. Älä aukaise, jos epäilet huijausta.

Salasanojen hallinta
Käytä vahvoja salasanoja, vaihda ne säännöllisesti äläkä käytä samoja salasanoja eri palveluissa.

Päivitä verkossa olevat laitteet ja käyttämäsi ohjelmistot säännöllisesti
Ajan tasalle päivitetyt ohjelmistot ja käyttöjärjestelmä ovat paras turva tietoturvauhkia vastaan.

Varmuuskopiot tärkeistä tiedoista
Ota tavaksi säännöllinen varmuuskopiointi.

Käytä tietoturvaohjelmistoja
Pidä tietoturvaohjelmistosi ajan tasalla ja ota selaimen varoitukset vakavasti.

Viestintävirasto
Kyberturvallisuuskeskus

perttu.halonen@viestintavirasto.fi

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi