Ajankohtaiset kyberuhat terveydenhuollossa

Esitelmän sisältö

- Tällä hetkellä pinnalla olevat kyberuhkat
- Onko terveydenhuollon järjestelmät rakennettu kestämään kyberhyökkäyksiä?
- Kiristyshaittaohjelmat
- Terveydenhuoltoalan kyberuhkia -raportin uudistaminen

Tällä hetkellä pinnalla olevia kyberuhkia

Suomessa jatkuvasti näkyvää

1. Laskutushuijaukset (CEO-fraud)
2. Kiristyshaittaohjelmat
3. Palvelunestohyökkäykset (ja niillä uhkailu)
4. Arkaluontoisen tiedon varastaminen (kohdistetut hyökkäykset)
5. Haittaohjelmien jakelualustat (EK) jylläävät HAVARO-havainnoissa
6. Palvelimen tai muun laitteen käyttäminen väliresurssina (esim. murrettu Wordpress-sivusto)
7. Tietojenkalastelu (luottokorttitiedot, käyttäjätunnukset ja salasanat)

Maailmalla näkyy, mutta ei (vielä) Suomessa

- Pankkihaittaohjelma asiakkaan tietokoneessa (ei aktiivisesti kohdistettu Suomeen)
- Suuret tietomurtojen avulla tehdyt petokset (esim. SWIFT)
- Massiiviset palvelunestohyökkäykset (>>100 gbps)
- Kohdistetut hyökkäykset teollisuusjärjestelmiä (ICS) vastaan, esim. sähkönjakelun sabotaasi

Terveydenhuollon tietojärjestelmät

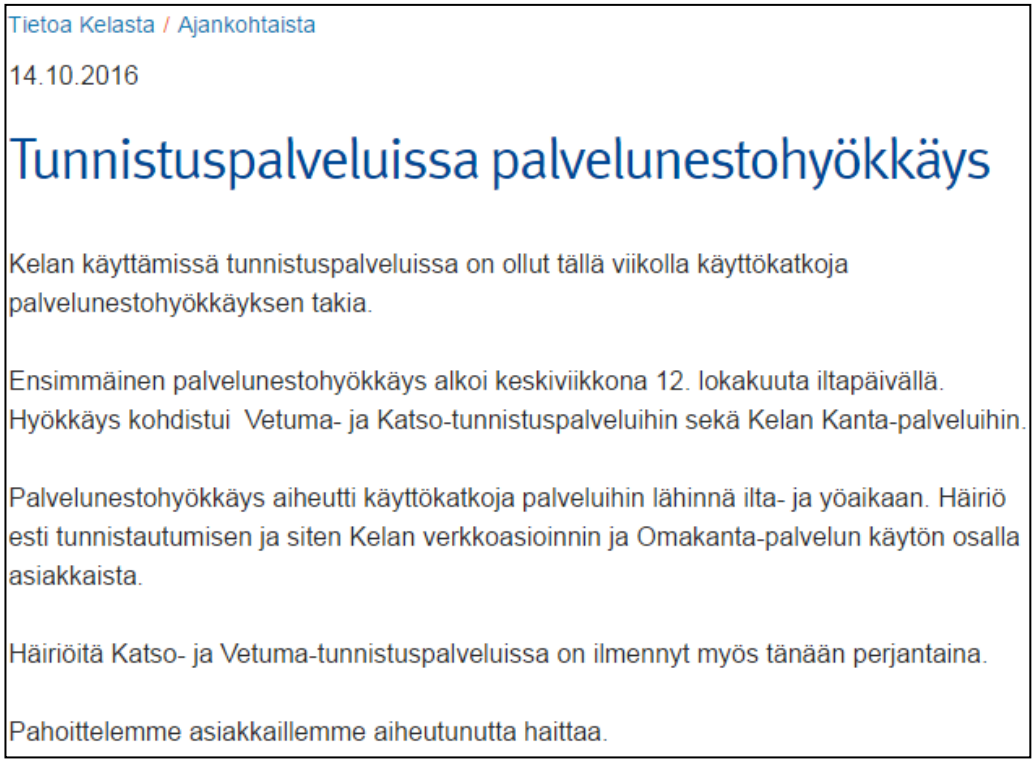
Olemmeko varautuneet hyökkäykseen? Oikeasti?

#OpSafePharma 3.0: tietomurtoja Italian terveydenhuoltoon

- Hakkerit tyytymättömiä terveydenhuollon hoitosuosituksiin ja rahankäyttöön.
- Neljään terveydenhuollon organisaatioon tietomurto elokuussa 2016; niistä kahdesta vuodettiin tietoja nettiin, kaikkien sivuja töhrittiin.
- Hyökkäysvektorina yhteisen sisällönhallintajär-jestelmän haavoittuvuus

Palvelunestohyökkäykset Kanta-palveluun

- Useita hyökkäyksiä 12.10. alkaen
- Kohteina myös tunnistuspalvelut:
  - » yrityksille suunnattu Katso (omistajat TEM ja Verohallinto)
  - » kansalaisille suunnattu Vetuma (omistaja Valtori)
- Seurauksia: apteekista ei saa ostettua reseptilääkkeitä



Tietoa Kelasta / Ajankohtaista

14.10.2016

Tunnistuspalveluissa palvelunestohyökkäys

Kelan käyttämissä tunnistuspalveluissa on ollut tällä viikolla käyttökatkoja palvelunestohyökkäyksen takia.

Ensimmäinen palvelunestohyökkäys alkoi keskiviikkona 12. lokakuuta iltapäivällä. Hyökkäys kohdistui Vetuma- ja Katso-tunnistuspalveluihin sekä Kelan Kanta-palveluihin.

Palvelunestohyökkäys aiheutti käyttökatkoja palveluihin lähinnä ilta- ja yöaikaan. Häiriö esti tunnistautumisen ja siten Kelan verkkoasioinnin ja Omakanta-palvelun käytön osalla asiakkaista.

Häiriöitä Katso- ja Vetuma-tunnistuspalveluissa on ilmennyt myös tänään perjantaina.

Pahoittelemme asiakkaillemme aiheutunutta haittaa.

Miksi joku hyökkäisi terveydenhuollon tietojärjestelmään?

- "Koska se on mahdollista"
- Maineen hankkiminen mustahattujen piireissä
- Kohteen maineen pilaaminen
- Kosto organisaatiolle tai yksittäiselle henkilölle
- Painostaminen toiminnan muuttamiseksi
- Rahan kiristäminen
- Henkilötietojen varastaminen ja myynti
- Käyttö muun hyökkäyksen välikappaleena
- Tietojen väärentäminen kovien lääkkeiden saamiseksi
- ...

Hyökkäysvektoreita

- **Fyysinen:** Kävellään sisään sairaalaan ja pannaan verkkopistoke seinään tai hyödynnetään langatonta lähiverkkoa.
- **Työasemat:** Lähetetään etähallinnan antava haittaohjelma sähköpostilla sairaalan työntekijälle. Murrettua työntekijän tietokonetta käytetään jalansijana lateraalileviämisessä.
- **Työntekijät:** Huijataan työntekijältä käyttäjätunnus ja salasana ja toimitaan sitten työntekijän identiteetillä.
- **Infrastruktuuri:** Skannataan avoimia palveluita ja pyritään hyödyntämään niiden haavoittuvuuksia jalansijan saamiseksi.

Kyberturvallinen järjestelmä

- Suunnittelu
- Toteutus
- **Testaus hyökkääjien silmin**
- Tuotantoon vienti
- Ylläpito ja korjaukset
- Käytöstä poisto

NIS-direktiivin tilanne

- NIS-direktiivin osalta Liikenne- ja viestintäministeriö on käynnistänyt terveydenhuoltoalaa koskevan työryhmän, jossa ovat mukana STM ja Valvira.
  - 1) tietoturvan vähimmäistaso
  - 2) poikkeamista ilmoittaminen
  - 3) keskeisten yritysten/toimijoiden määrittely
- Direktiivi koskee seuraavia sektoreita:
  - 1) Energia, 2) Liikenne, 3) Pankkiala, 4) Finanssimarkkinoiden infrastruktuurit, 5) Terveydenhuoltoala (mukaan lukien sairaalat ja yksityisklinikat), 6) Juomaveden toimittaminen ja jakelu, 7) Digitaalinen infrastruktuuri
- Direktiivi tuli voimaan elokuussa 2016. EU:n jäsenvaltioiden on saatettava säännökset osaksi kansallista lainsäädäntöä 9. toukokuuta 2018 mennessä.

Kiristyshaittaohjelmat

Medbit Oy:n kokemuksia

Medbitin havaintoja

- Vuosina 2015 ja 2016 useita tartuntoja tiedostoja salaavista kiristyshaittaohjelmista
- Toistaiseksi ei todella merkittäviä vaikutuksia tuotantoon
  - » Yksittäisiin järjestelmiin/toimintoihin on tullut käyttökatkoja
  - » Hukattu työaika
- Kiristyshaittaohjelmat ovat toistaiseksi melko yksinkertaisia.

Medbitin tyypillinen vaste tartuntaan

- Havainnointi: havainto käyttäjältä tai virustorjunnasta
- Eristäminen: saastunut käyttäjätunnus ja konetili suljetaan
- Palautuminen: salakirjoitetut kohteet paikannetaan ja palautetaan varmuuskopioista
- Tutkinta: tunnistaako virustorjunta; jos ei, niin miksi?
- Hallinnolliset toimenpiteet: tiedottamista, tilastointia, rikosilmoitus

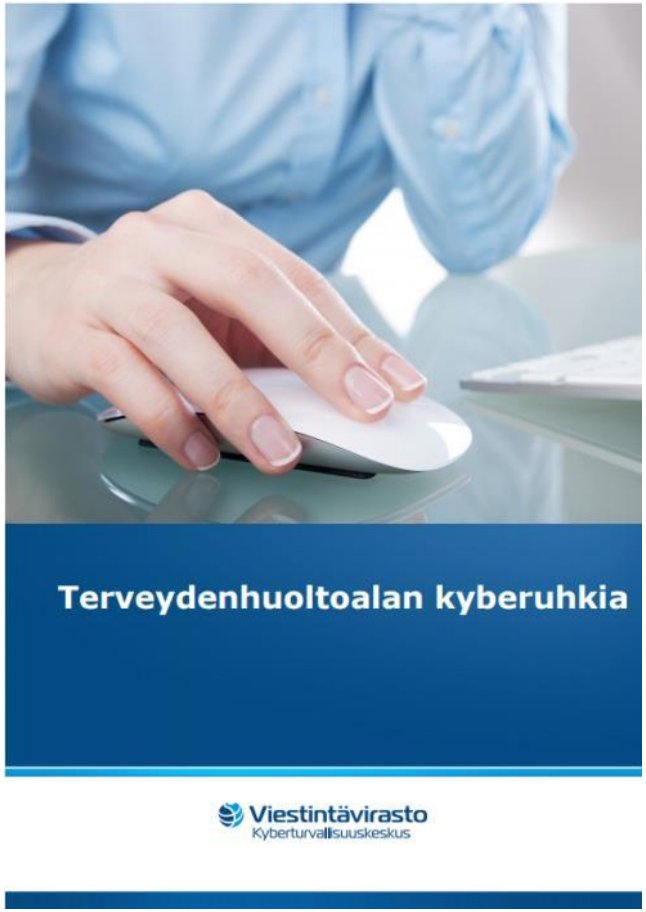
Medbitin kehitystoimet

- Uusi sisäinen ohjeistus erityisesti kiristyshaittaohjelmatartuntojen selvittämiseksi
- Tietoturvapoikkeamaprosessin parantaminen
- Käyttövaltuushallinto ja verkkolevyjen käyttöoikeudet
- Varmuuskopiointi- ja palautusrutiinien parantaminen
- IPS:n käyttöönotto internetliikenteessä
  - » Yhdessä virustorjunnan kanssa toistaiseksi täydellinen tartuntojen torjunta.
- Tiedottaminen käyttäjille
- Tulevaisuudessa: suorituksenaikainen haittaohjelmien käyttäytymisen analysointi, eri lokilähteiden automaattinen analysointi, ohjelmistojen valkolistaus, operoinnin resurssit

Terveydenhuollon kyberuhkia -raportin uudistaminen

Terveydenhuoltoalan kyberuhkia -raportti

- Katsaus organisaatioiden johdolle ja kyberturvallisuudesta vastaaville henkilöille
- Julkaistiin vuodenvaihteessa 2015-2016
- Raportti tullaan päivittämään loppuvuonna. Kehitysehdotukset ja syötteet ovat tervetulleita!



Viestintäviraston Kyberturvallisuuskeskus

Tietoturvapalvelut huoltovarmuuskriittisille yrityksille

- Tietoturvaloukkausten ilmoituspiste ja tilannekuva
  - Neuvonta, opastus
  - Vahinkojen rajoittaminen
  - Luottamuksellinen käsittely
  - Yleinen ja toimialakohtainen tilannekuva
- Tietoturvaloukkausten havainnointi (HAVARO)
  - Haitallisen ja/tai normaalista poikkeavan liikenteen havainnointi
  - Asiakkaiden varoittaminen
  - Raportointi
- Yhteistyöverkostot
  - Luottamuksellinen tietoturva-asioiden tiedonvaihto
  - Kaksi tasoa: 1) Toimialakohtainen sähköpostijakelu 2) Tiedonvaihtoryhmät
- Haavoittuvuuskoordinointi
  - Yhteistyö haavoittuvuuden tai vakavan ohjelmistovirheen löytäjän ja ohjelmistovalmistajien kanssa
  - Tieto haavoittuvuudesta loppukäyttäjille
- Järjestelmäturvallisuus
  - Turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvät turvallisuusasiat
  - Salaustuotteiden ja tietojärjestelmien hyväksyntä
  - Kansallisen ja kansainvälisten turvaluokitellun tietoaineiston käsittelyn ohjeistus

Viestintävirasto
Kyberturvallisuuskeskus

cert@viestintavirasto.fi

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi