Kyberturvallisuutta sosiaali- ja terveysalan ammattilaisille 3 op

Tietosuoja sosiaali- ja terveysalalla

Johanna Niskakangas

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

jamk

Luentomateriaalin jakaminen

Tämä ohjedia poistettava varsinaisesta luentomateriaalista!

- Tämän materiaalin voi käsitellä yhtenä luentona (n. 20 min) tai pilkkoa kolmeksi pienemmäksi luennoksi (5-10 min) seuraavasti
  - Luento 1 (diat 3 & 4)
    - Tietosuoja ja Tietosuojaan liittyviä käsitteitä
  - Luento 2 (diat 5-8)
    - GDPR, Henkilötietojen käsittelyä koskevat periaatteet GDPR:n mukaisesti & GDBR:ssä myös henkilötietojen turvallisuudesta
  - Luento 3 (dia 9)
    - Arjen tietosuojatekoja!

jamk

Tietosuoja

Asiakkaan kiinnostusta omien henkilötietojensa käsittelyä kohtaan ei pidä koskaan aliarvioida!

- Tietosuojalla tarkoitetaan järjestelyjä, joilla pyritään varmistamaan henkilötietojen asianmukainen käsittely ja niiden yksityisyyden säilyminen (Kyberturvallisuuden sanasto 2018)
- **Tietosuoja**
  - Rekisteröidyn oikeuksien ja vapauksien toteutumisen turvaaminen henkilötietojen käsittelyssä
  - Henkilötietojen käsittelyn edellytysten osoittaminen (milloin ja millä edellytyksillä)
- **Tietosuojan hallitsemisen hyödyt sote-ammattilaisen näkökulmasta**
  - Työntekijän oman oikeusturvan parantaminen
  - Asiakkaan luottamuksen kasvattaminen toimintaa ja sen lainmukaisuutta kohtaan
  - Joustavuus lisääntyy, kun tietosuoja on mitoitettu oikein

jamk

Tietosuojaan liittyviä käsitteitä

- **Henkilötiedot**
  - Kaikki tunnistettuun tai tunnistettavissa olevaan henkilöön (= rekisteröity) liittyvät tiedot. Muun muassa nimi, henkilötunnus, osoite, sähköpostiosoite, verkkotunnistetiedot (esim. IP-osoite), pankkitiedot, terveystiedot
- **Rekisterinpitäjä**
  - Ihminen tai organisaatio, joka yksin tai yhdessä toisten kanssa määrittelee, mihin tarkoitukseen ja millä tavalla henkilötietoja käsitellään
- **Henkilötietojen käsittelijä**
  - Ihminen tai organisaatio, joka käsittelee henkilötietoja rekisterinpitäjän puolesta

(mukaillen GDPR 4 artikla; tietosuoja.fi)

jamk

GDPR (General Data Protection Regulation)

EU:n yleinen tietosuoja-asetus

- EU:n lainsäädäntö on lakihierarkiassa kansallisen lainsäädännön yläpuolella
- Siirtymäajan jälkeen velvoittava Suomessa 25.5.2018 (astui voimaan 24.5.2016)
- Mitä GDPR:n myötä?
  - Rekisteröidyille (henkilöille) enemmän oikeuksia
  - Rekisterinpitäjille ja henkilötietojen käsittelijöille uusia velvoitteita
  - Täsmennyksiä voimassa olevaan sääntelyyn sekä merkittäviä uusia velvoitteita ja sanktioita
    - Velvollisuuksien laiminlyönnistä voidaan langettaa merkittäviä seuraamuksia, kuten korjaavia toimenpiteitä ja hallinnollisia seuraamusmaksuja
- Muun muassa tietosuojalaki (1050/2018) täsmentämässä ja täydentämässä EU:n yleistä tietosuoja-asetusta sekä sen kansallista soveltamista

jamk

Henkilötietojen käsittelyä koskevat periaatteet GDPR:n mukaisesti

Henkilötietoja on

- Käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- Kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten
- Kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden (”tietojen minimointi”)
- Päivitettävä aina tarvittaessa; epätarkat ja virheelliset tiedot on poistettava tai oikaistava viipymättä
- Säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten
- Käsiteltävä luottamuksellisesti ja turvallisesti (huomioiden asianmukaiset tekniset ja organisatoriset toimet)

(Tietosuoja.fi/tietosuojaperiaatteet; mukaillen GDPR:n artikla 5)

Rekisterinpitäjän on pystyttävä osoittamaan, että tietosuojaperiaatteet toteutuvat tehokkaasti henkilötietojen käsittelyssä (osoitusvelvollisuus)

jamk

GDPR:ssä myös henkilötietojen turvallisuudesta

Nostoja liittyen läheisesti myös kyberturvallisuuteen (mm. tekniset ja organisatoriset toimenpiteet)

- **Lähetätkö potilaiden/asiakkaiden henkilötietoja suojaamattomalla sähköpostilla tai Whatsappissa?**
  - Asianmukaisen turvallisuustason arvioimisessa on kiinnitettävä erityistä huomiota käsittelyn sisältämiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi (mukaillen artikla 32)
- **Tunnetko ja noudatatko organisaatiosi tietoturvaohjeita ja käytäntöjä sekä asiakas- ja potilastietojen käsittelyohjeita?**
  - Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti, ellei unionin oikeudessa tai lainsäädännössä toisin vaadita (mukaillen artikla 32)

jamk

GDPR:ssä myös henkilötietojen turvallisuudesta

Nostoja liittyen läheisesti myös kyberturvallisuuteen (mm. tekniset ja organisatoriset toimenpiteet)

- **Kerrothan esihenkilöllesi tai tietosuojavastaavalle havaitsemistasi tietoturva- tai tietosuojarikkomuksista!**
  - Henkilötietojen tietoturvaloukkauksista ilmoittaminen ilman aiheetonta viivästystä ja mahdollisuuksien mukaan 72 tunnin kuluessa tapahtuman ilmitulosta (paitsi, jos tapahtumasta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä). Jos ilmoitusta ei anneta, rekisterinpitäjän on toimitettava valvontaviranomaiselle perusteltu selitys (mukaillen artikla 33)
  - Rekisterinpitäjän on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivästystä silloin, kun se todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille (mukaillen artikla 34)

jamk

Arjen tietosuojatekoja!

- Selvitä ja noudata oman organisaatiosi tietoturvaohjeita ja -käytäntöjä sekä asiakas- ja potilastietojen käsittelyohjeita
- Käytä vain henkilökohtaisia käyttäjätunnuksia
- Ilmoita vääränlaisista käyttöoikeuksista käyttäjäoikeuksien ylläpitäjälle
- Säilytä salasanat ja muut kirjautumisessa käytettävät tunnisteet huolellisesti
- Huolehdi hyvin papereiden, puhelinten, salasanojen, avainten, toimikorttien yms. asianmukaisesta käsittelystä ja säilyttämisestä
- Lukitse tietokoneesi ja ohjelmat sekä puhelimesi, kun ne eivät ole valvonnassa
- Varo paljastamasta luottamuksellisia tietoja sivullisille esimerkiksi tehdessäsi etätöitä
- Käytä viestimisessä järjestelmiä, joissa on riittävän vahva salaus ja joissa osapuolet voidaan tunnistaa luotettavasti (esim. ei suojaamattomia sähköposteja)
- Kerro esihenkilölle tai tietosuojavastaavalle havaitsemistasi tietoturva- tai tietosuojarikkomuksista

Lähteet

- Andreasson, A. 2020. Tietosuoja terveydenhuollossa. Oppiportin verkkokurssi. Kustannus Oy Duodecim.
- EU:n yleinen tietosuoja-asetus (GDPR) 2016/679 https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504
- Tietosuojavaltuutetun toimisto (n.d.) https://tietosuoja.fi/ Viitattu 8.2.2023.
- Lue lisää: Tietosuojalaki (1050/2018)

Kiitos!

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

jamk

Sosiaali- ja terveysalaan kohdistuvat kyberturvallisuusuhat

Tiina Blek

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Luentomateriaalin jakaminen

Tämä dia poistetaan varsinaisesta opetusmateriaalista

- Tämän materiaalin voi käsitellä yhtenä luentona (noin 30 minuuttia) tai pilkkoa kahteen erilliseen luentoon
- Luento 1
  - Sosiaali- ja terveysalaan kohdistuvien kyberuhkien yleisyys ja syyt miksi ala kiinnostaa kyberrikollisia (diat 2-7)
- Luento 2
  - Sosiaali- ja terveysalaan kohdistuvat yleisimmät kyberuhat (dia 8)

jamk

Tapahtumakuvaus Yhdysvalloista

Marraskuu 2023

- Kyberhyökkäys vaikutti neljän osavaltion alueella toimiviin sairaaloihin
- Potilaita jouduttiin käännyttämään pois ensiavusta
- Suunniteltuja toimenpiteitä peruttiin
- Tietojärjestelmät pois käytöstä

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

jamk

Uutinen

Hakkerit iskivät jouluaattona kolmeen sairaalaan – kiristyshaittaohjelma teki ensiavun antamisesta mahdotonta

Marja Tienari 29.12.2023 13:45 | päivitetty 29.12.2023 13:45 KYBER KIRISTYSHAITTAOHJELMAT PALVELUNESTOHYÖKKÄYKSET TIETOTURVA HAITTAOHJELMAT HAKKERIT ENSIHOITO TERVEYSTEKNOLOGIA

Ransomware attack spreads chaos at a major hospital in Barcelona

Updated on: November 15, 2023 12:53 PM

Ulkomaat | **Yhdysvallat**

Kyberhyökkäys seisautti kiireellistä hoitoa neljän osavaltion alueella Yhdysvalloissa

Yhteensä 16:ta sairaalaa operoiva yritys kärsii tietoturvaan liittyvästä ongelmasta.

STT–AFP
5.8.2023 2:31

Hyvinvointialueet

Tietomurto Tena-tuotteita kuljettavaan yritykseen – tuhansien asiakkaiden henkilötietoja vaarassa

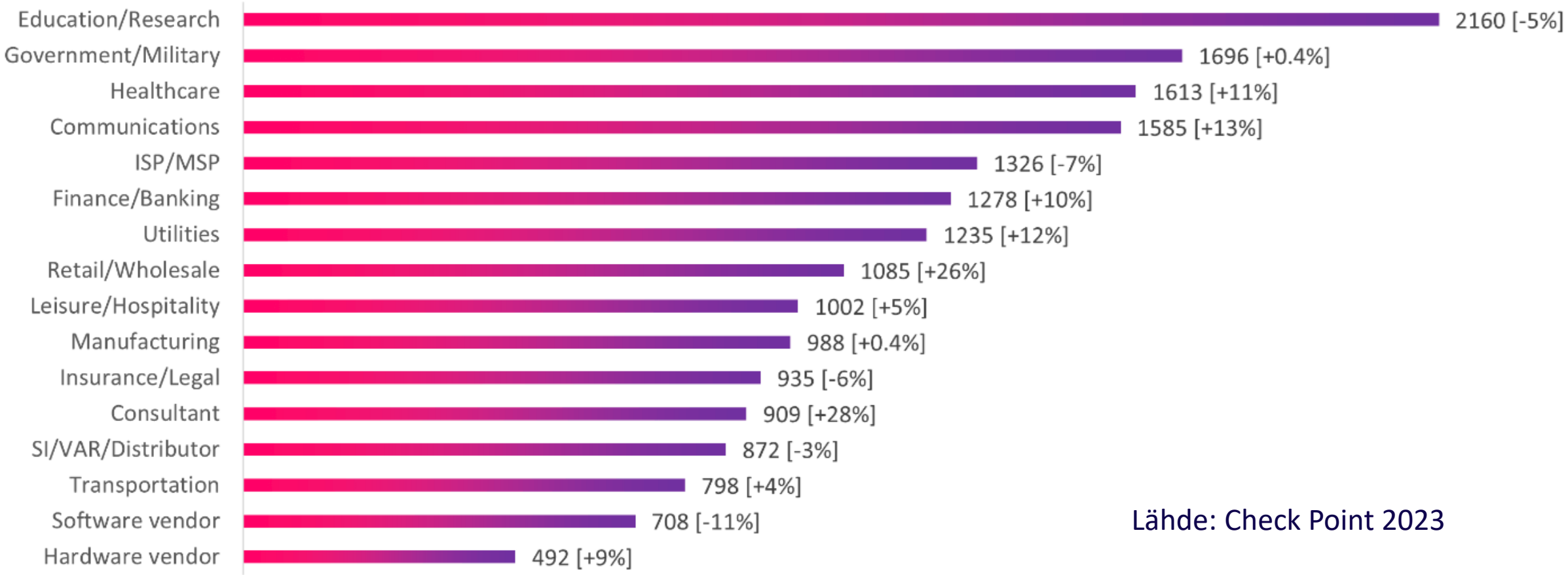
https://yle.fi/

Uhkien yleisyys

- *Vuonna 2023 terveydenhuollon järjestelmiin kohdistui maailmanlaajuisesti keskimäärin 1613 kyberhyökkäystä viikossa.
  - Hyökkäysten määrässä noin 11 prosentin kasvu edellisvuoteen verrattuna.
  - Kiristyshaittaohjelman (ransomware) kohteeksi joutui keskimäärin noin joka 34. organisaatio (kaikki alat mukaan luettuna)
  - Terveydenhuoltoala oli toiseksi eniten alttiina näille hyökkäyksille. Joka 25. terveysalan organisaatio joutui kiristyshaittaohjelmahyökkäyksen kohteeksi.
    - Eniten kiristyshaittaohjelmahyökkäyksiä kohdistui hallinnon / armeijan järjestelmiin (joka 24. organisaatio)
- Hyökkäyksiä esiintyy kaikkialla maailmassa ja määrä lisääntyy vuosittain.

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU
jamk

Global Average Weekly Cyber Attacks per Industy
(2023 vs. 2022)



Lähde: Check Point 2023

Miksi sote-järjestelmät houkuttavat verkkorikollisia?

- Terveysalan tietojärjestelmiä pidetään ”pehmeinä kohteina”
- Potilastietojärjestelmät ovat potilaiden hoidon kannalta elintärkeitä
- Potilastietojärjestelmien tiedot ovat sensitiivisiä ja salassa pidettäviä
- Potilastietojärjestelmän sisältämät tiedot ovat pimeillä markkinoilla arvokkaampaa kauppatavaraa, kuin esimerkiksi luottokorttitieto (tiedot eivät ole helposti muutettavia)
- Käytössä olevien laitteiden suuri määrä ja vanhentunut tekniikka
- Lääkinnälliset laitteet, joihin verkkorikolliset pääsevät helposti sisään
- Henkilökunta, jolla ei aina ole riittävää osaamista verkkoriskeistä
- Alalla vallitseva jatkuva kiire ja resurssipula
- Terveysalalla työskentelevien ominaispiirteet (luottamus, auttamisen halu)

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

jamk

Yleisimmät kyberuhat

- Terveydenhuollon järjestelmiin kohdistuvat yleisimmät kyberuhkat muodostuvat
  - tietomurroista (data breach)
  - tietojenkalastelusta (phishing, vhishing, smishing, spoofing)
  - kiristyshaittaohjelmista (ransomware) sekä
  - palvelunestohyökkäyksistä (denial of service, DoS)
  - lääkinnällisiin laitteisiin ja niiden kautta tapahtuvista hyökkäyksistä

- Tutustu näihin uhkiin myös Kyberhäiriöiden hallinta –käsikirjan avulla.

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

jamk

Lähteet

Check Point. 2023. Viitattu 4.1.2024. A Continuing Cyber-Storm with Increasing Ransomware Threats - Check Point Blog.

Kyberhäiriöiden hallinta. Käsikirja terveydenhuollon toimijoille. Viitattu 5.1.2024. kyberhairioiden-hallinta-kasikirja-terveydenhuollon-toimijoille.pdf (jyvsectec.fi)

Kyberturvallisuus. Ohje sosiaali- ja terveydenhuollon toimijoille. Viitattu 5.1.2024. Kyberturvallisuus Ohje sosiaali- ja terveydenhuollon toimijoille (valtioneuvosto.fi)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Lääkinnällisten laitteiden kyberuhat

Tiina Blek

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

jamk

Luentomateriaalin jakaminen

Poista tämä dia varsinaisesta esitysmateriaalista

- Voit käsitellä tämän materiaalin yhdellä luennolla (noin 30 minuuttia) tai voit jakaa sen osiin seuraavasti:
- Luento 1
  - Lääkinnällisen laitteen määritelmät ja niihin kohdistuvat kyberuhat (diat 1-6)
- Luento 2
  - Lääkinnällisistä laitteista löydetyt haavoittuvuudet, tapausesimerkit, ohjeet kuinka lisätä laitteiden käyttöön liittyvää kyberturvallisuutta (diat 7-10)

jamk

Mitä lääkinnälliset laitteet ovat?

- Yleisesti lääkintälaitteiksi miellettyjen (ekg, MRI, infuusiopumppu, hengityskone jne.) laitteiden lisäksi esimerkiksi:
  - kuulolaite, kondomi, laastari ja verenpainemittari
  - Myös ohjelmisto, kun sitä käytetään yksin tai yhdessä muiden lääkinnällisten laitteiden kanssa hankkimaan tietoja fysiologisten tilojen, terveydentilan, sairauksien tai synnynnäisten epämuodostumien havaitsemiseksi, diagnosoimiseksi, valvomiseksi, ennakoimiseksi tai hoitamiseksi.
- Lääkinnällisiä laitteita taas eivät ole esimerkiksi:
  - sykemittarit, hengityssuojaimet tai terveyssiteet

Lähde: Fimea

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

Lääkintälaitteiden kyberriskeistä

- Kaikki laitteet, jotka toimivat verkossa, WiFi tai Bluetooth –yhteydellä ovat mahdollisia kyberhyökkäysportteja
  - glukoosisensorit / -monitorit, infuusiopumput, insuliinipumput, ventilaattorit, sydämentahdistimet, kamerat ja elintoimintojen mittaamiseen käytetyt laitteet (ekg, potilasmonitorit)

- Laitteista jopa 74 % on kytketty sairaalaverkkoon
- Monissa laitteissa on käytössä vanhentunutta teknologiaa / käyttöjärjestelmiä
- Lääkintälaitteiden suojaus on usein puutteellista (eivät ole tietohallinnon hallinnassa)
- Laitteiden päivitykset voivat puuttua / olla vanhentuneita (vastuut?)
- Voi olla epätietoisuutta siitä, mitä laitteita, kuinka paljon ja missä niitä on käytössä (vastuut epäselviä?)

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

jamk

Lääkintälaitteisiin kohdistuvat hyökkäykset

Neljä erilaista skenaariota

Lääkinnällisiin laitteisiin kohdistuvia uhkia ovat muun muassa

- Palvelunestohyökkäys
- Hoidon manipulointi
- Tietomurto
- Omaisuuden (laitteen) vahingoittaminen

Kaikki neljä ovat potentiaalisia riskejä potilaalle ja organisaatiolle.

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

jamk

Terveydenhuollon toimintaympäristöstä raportoituja hyökkäyksiä

- Lääkintälaitteisiin kohdistuneita ja niiden kautta tapahtuneita hyökkäyksiä on toteutettu muun muassa verikaasuanalysaattoreiden sekä röntgen ja MRI-laitteiden kautta
- Potilaan itsensä hakkeroima PCA-(kipu)pumppu, jolla lisäsi itselleen määrättyä opioidiannosta → johti yliannostukseen (Itävalta)
- Potilasmonitorien sulkeminen (Etelä-Amerikka)
- Lääkepumppujen toiminnan estäminen (USA)

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

jamk

Tutkijoiden / valkohattuhakkereiden löytämiä haavoittuvuuksia

- Kohtalokkaita puutteita lääkeinfuusiopumpuissa
- Kirurgisen robotin haltuunotto
- Sydämen tahdistimien haavoittuvuus

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

jamk

Tutkijoiden ja valkohattuhakkereiden löytämiä haavoittuvuuksia

- CT–kuviin lisätyt / poistetut syöpälöydökset. 2018. Malicious Tampering of 3D Medical Imagery using Deep Learning
  - Tutkimuksessa 99 % radiologeista ei pystynyt erottamaan lisättyä syöpälöydöstä → diagnosoi terveelle potilaalle keuhkosyövän
  - Radiologeista 94 % ei havainnut CT-kuvasta poistettua syöpälöydöstä → diagnosoi syöpäpotilaan terveeksi
- Lisää tapauksesta: Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists - The Washington Post

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

jamk

Arjessa muistettavat asiat

- Oletussalasanojen vaihtaminen!
- Käytä vahvoja salasanoja ja noudata työnantajasi antamia tietoturvaohjeita
- Käytä / kytke lääkintälaitetta/sovellusta/ohjelmaa vain suojatussa verkossa
- Huomioi laitteen/sovelluksen/ohjelman poikkeava käytös (esim. sammuminen/uudelleen käynnistyminen, näytön ”pysähtyminen” jne.)
- Ole selvillä, kenelle häiriöstä ilmoitetaan.
- Opettele / tiedä mistä löydät toimintaohjeet lääkintälaitteisiin kohdistuvan hyökkäyksen tapahtuessa.
- Ole tietoinen, kuinka ilmoitat potilaille, jos heidän lääkinnälliset laitteensa ovat vaarantuneet
- Kerro potilaalle, kenelle hän ilmoittaa lääkintälaitteen poikkeavasta toiminnasta

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

Laitteessa olevan kyberhäiriön havaitseminen - tutkimuksessa ja harjoituksessa

Simulaatiotutkimus esimerkki (Willing ym. 2021)

Sairaalajärjestelmiin kohdistuvan kyberhyökkäyksen harjoitus (JYVSECTEC)

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

jamk

Lähteet

- Fimea, Lääkealan turvallisuus ja kehittämiskeskus. Viitattu 6.1.2023. https://www.fimea.fi/laakinnalliset_laitteet/mita-ovat-laakinnalliset-laitteet-.
- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. Healthcare and Public Health sector coordinating Councils. N.d. Viitattu 12.5.2022. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (phe.gov)
- JYVSECTEC. Viitattu 6.1.2023. https://jyvsectec.fi/fin/terveydenhuolto/
- Sherman, C. & Schiano, S. 2019. Best Practices: Medical Device Security Control Your Hospital's Expanding Device Risk Exposure. For Security & Risk Professionals. Forrester.

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU
jamk

Sote-henkilöstön rooli kyberturvallisuuden varmistamisessa

Tiina Blek

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

jamk

Luennon jakaminen

Poista tämä dia esitysmateriaalista

- Voit käyttää tätä materiaali joko kokonaisuutena (noin 30 minuuttia) tai jakaa sen osiin seuraavasti:
- Luento 1
  - Henkilöstön rooli ja vastuut kyberturvallisuuden edistämisessä (diat 1- 5)
- Luento 2
  - Esihenkilöiden ja organisaation vastuut kyberturvallisuuden edistämisessä (dia 6)

Henkilöstön merkitys kyberuhkien torjumisessa

- Henkilöstön rooli on kriittinen kyberturvallisuuden varmistamisessa terveydenhuollon alalla
- Henkilöstö on ensimmäinen puolustuslinja kyberuhkia vastaan.
- Asianmukaisella koulutuksella ja tietoisuudella voidaan merkittävästi vähentää riskejä ja suojella potilaiden ja organisaation tietoja

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

jamk

Henkilöstön (tietoturva)käyttäytymiseen vaikuttavia syitä

- Yleisiä syitä ovat
  - tietoisuus omaan toimintaan liittyvien riskien laajuudesta vähäistä
  - virheiden havaitsemiseen ja korjaamiseen liittyvä ajan puute
  - toistuvien tehtävien suorittaminen
  - ei tiedetä keinoa, kuinka peruuttaa tahaton, virheellinen toiminta
  - asenteet tietoturvaohjeita kohtaan
  - ulkoiset tekijät (esim. sosiaalinen paine)
  - halu järkevöittää toimintaa ja säästää aikaa
  - tieto- ja kyberturvallisuutta koskevan tiedon ja koulutuksen puute

- Työtapojen äkilliset muutokset ja pitkäaikainen stressi vaikuttavat siihen, että työntekijät ovat alttiimpia huijattaviksi ja tekemään virheitä.

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU
jamk

Mitä henkilöstön tulisi osata / tunnistaa?

- *Tiedostaa oma rooli ja käyttäytymisen/toiminnan merkitys* tietoturvan varmistamisessa
- *Tunnistaa reitit*, joita kautta kyberhyökkäys voi levitä järjestelmiin
  - Kriittisiä portteja ovat esimerkiksi työasemat, kopiokoneet, viivakoodilukijat, mobiililaitteet (älypuhelimet, kannettavat tietokoneet, tabletit), pilvipohjaiset sovellukset, etäkirjautuminen, työntekijöiden omat laitteet, kolmansien osapuolien (esim. potilaat, vierailijat, opiskelijat) laitteet sekä suojaamattomat Wi-Fi yhteydet.
  - Myös lääkinnälliset- ja etäseurantalaitteet voivat toimia porttina haittaohjelmien leviämiseen.
- *Tunnistaa tietojenkalastelun* eri muodot
- *Havaita* tietojärjestelmään, lääkintälaitteeseen tai sovellukseen liittyvä poikkeava toiminta
- *Tietää kuinka* poikkeustilanteeseen *reagoidaan* ja kuinka siinä *toimitaan*
- *Ohjata potilaita* lääkintä- ja etäseurantalaitteiden tietoturvalliseen käyttöön

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU

jamk

Työnantajan / esihenkilöiden vastuu ja varautumistoimet

- Osaamisen / tietoisuuden kehittäminen ja jatkuva ylläpitäminen
- Poikkeustilanteiden toimintamallien suunnittelu ja varmistus, että malli on henkilöstöllä tiedossa / helposti löydettävissä
- Riskienhallinta (järjestelmiin, laitteisiin, hankintoihin, henkilöihin, toimittajiin liittyvät riskit)
- Jatkuvuussuunnitelmat (liittyy toimintamalleihin kuinka toiminnan jatkuvuus turvataan esim. jos potilastietojärjestelmä ei toimi)
- Vastuiden määrittely
- Viestintäsuunnitelma ajan tasalle

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU
jamk

Lähteet

- Argaw ST, Bempong N-E, Eshaya-Chauvin B, Flahault A. The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. BMC Medical Informatics and Decision Making. 2019 Dec 11;19(1).
- Cost of a Data Breach Report 2021. Ponemon Institute and IBM Security.
- Dobran, B. 2019. 31 Must-Know Healthcare Cybersecurity Statistics 2020. Viitattu 6.4.2022. 31 Healthcare Cybersecurity Statistics For 2020 (phoenixnap.com).
- Martin G., Martin P., Hankin C., Darzi A. & Kinross J. Cybersecurity and healthcare: how safe are we? British Medical Journal (BMJ). 2017 Jul 6;358.
- Willing M., Dresen C., Gerlitz E., Haering M., Smith M. & Binnewies C, et al. Behavioral responses to a cyber-attack in a hospital environment. Scientific Reports. 2021 Dec 29;11(1):19352.

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus
Euroopan unionin rahoittama – NextGenerationEU
jamk