Terveys- ja hyvinvointialojen opintokokonaisuus

Kyberturvallisuuskoulutuksen ja siihen liittyvän yhteistyön kehittäminen korkeakouluissa

OPETUS- JA KULTTUURIMINISTERIÖ
UNDERVISNINGS- OCH KULTURMINISTERIET

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

04A – Kyberhygienia

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Kyberhygienia

Terminologia

- **Monivaiheinen tunnistautuminen**: Käyttäjän tunnistaminen useamman menetelmän avulla, kuten matkapuhelin, biometriset tunnisteet tai kulkukortti.
- **Säännölliset päivitykset**: Käyttöjärjestelmän, ohjelmistojen ja laitteiden ajan tasalla pitäminen.
- **Tietojen varmuuskopiointi**: Tietojen säännöllinen kopiointi ja säilytys turvallisessa paikassa.
- **Virustorjuntaohjelmisto**: Ohjelmisto, joka suojaa tietokonetta haittaohjelmilta.
- **IoT (Internet of Things)**: Verkkoon liitettyjen laitteiden ja järjestelmien kokonaisuus, joka mahdollistaa tiedon keräämisen ja vaihtamisen.
    - **IoMT (Internet of Medical Things)**: IoT-teknologioiden alaryhmä, joka koostuu verkotetuista laitteista ja sovelluksista lääketieteellisissä ja terveydenhuollon IT-sovelluksissa.

jamk

Kyberhygienia

Yleisesti

Mikä	Työntekijäminä	Yksityisminä
Vahvat salasanat	Uniikki monipuolinen vaikeasti arvattava	Eri kuin työtekijätilillä
Monivaiheinen tunnistautuminen	Matkapuhelin, biometriset, kulkukortti	Pääsähköposti, matkapuhelin, biometriset
Säännölliset päivitykset	Käyttöjärjestelmä (Windows), ohjelmistot (selain), muut osaston laitteet, matkapuhelin, lääkinnälliset älylaitteet	Käyttöjärjestelmä, ohjelmistot, laitteet
Tietojen varmuuskopiointi	Huomioi salassa pidettävät, säilytysmääräykset ja turvaluokitukset	3-2-1 Järjestelmä, tärkeille tiedoille
Tietojenkalastelun välttäminen	Tietoisuus, älä jaa yrityssähköpostiasi tarpeettomiin palveluihin	Tietoisuus, luo roskapostiosoite
Virustorjuntaohjelmisto	Keskitetyt järjestelmät loppukäyttäjien koneille	Anti-virus (Windowsissa vakiona)
Turvalliset verkkoyhteydet	Ei liitetä työntekijäkoneita julkisiin verkkoihin	Oman kännykän Wifi on turvallisempi, kuin julkinen wifi

jamk

Kyberhygienia

Tietokoneen turvallinen käyttäminen

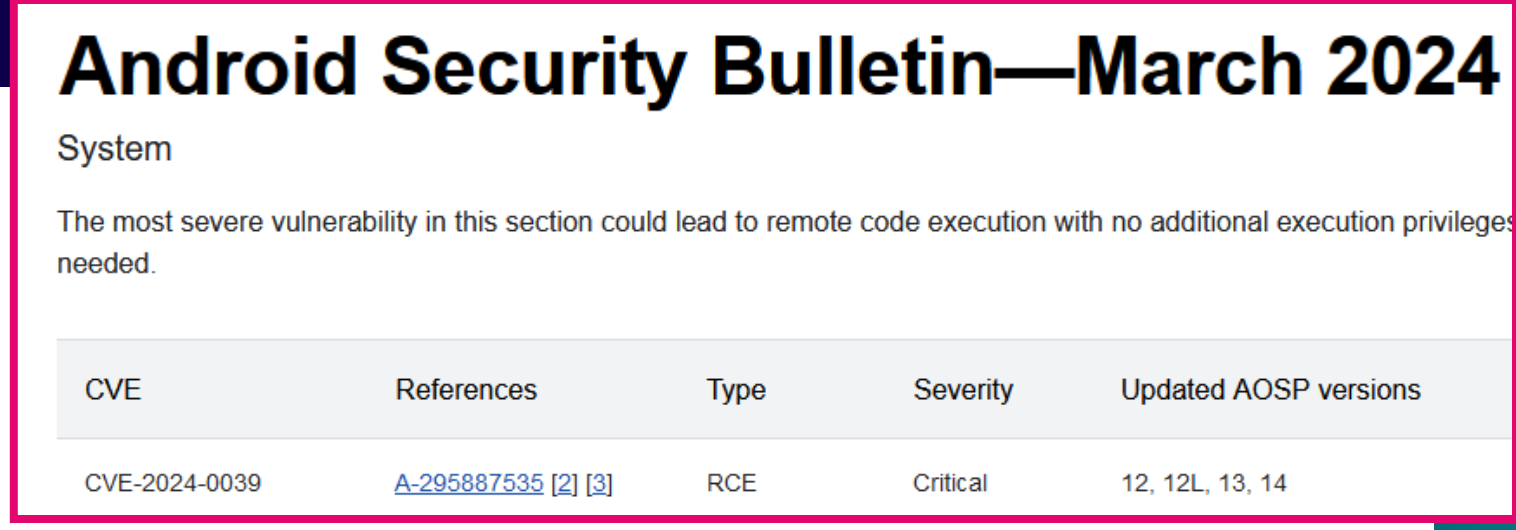
- Tietokone ja sen ohjelmat tulee aina olla päivitettyinä. Jos käyttöjärjestelmä pyytää päivitystä, muttei sitä pysty vaikkapa potilasturvallisuuden nimissä välittömästi ajamaan, siirrä päivitys esim. seuraavalle kahvi- tai ruokatunnille.

- Kun poistut tietokoneen tai työpisteen äärestä varmista tai tee seuraavat
  1. Tallenna työsi
  2. Sulje ohjelmat
  3. Poista ulkoiset laitteet ja mahdollinen kirjautumiskortti
  4. Älä jätä luottamuksellisia tietoja näkyville (Myös post-it laput)
  5. Varmista fyysinen turvallisuus (Lukitse ovi)
  6. Kirjaudu ulos (Lyhyen poissaolon ajaksi, lukitse tietokone ⊞WIN + L)

jamk

Kyberhygienia

Päivitysten tärkeys



Android Security Bulletin—March 2024

System

The most severe vulnerability in this section could lead to remote code execution with no additional execution privileges needed.

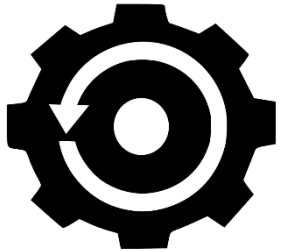
CVE	References	Type	Severity	Updated AOSP versions
CVE-2024-0039	A-295887535 [2] [3]	RCE	Critical	12, 12L, 13, 14

1. **Turvallisuus**: Päivitykset korjaavat tietoturva-aukkoja, joita hakkerit voivat hyödyntää. Ilman päivityksiä laitteesi ovat alttiimpia viruksille ja hyökkäyksille.
    - Myös päivitystiedot ovat usein julkista tietoa, kun päivitys on korjattu siitä ilmoitetaan päivitystiedoissa (patch notes), jolloin myös rikolliset saavat tietoon, millainen ongelma päivittämättömässä laitteessa on.
        - Esimerkki Android käyttöjärjestelmässä keväältä 2024 CVE-2024-0039, patch notes kuvankaappaus kalvon oikeassa yläreunassa.
2. **Uudet ominaisuudet**: Päivitykset tuovat usein mukanaan uusia toimintoja ja parannuksia, jotka tekevät laitteiden käytöstä helpompaa ja mukavampaa.
3. **Parannettu suorituskyky**: Päivitykset voivat tehdä laitteista nopeampia ja vakaampia, mikä parantaa käyttökokemusta.
4. **Yhteensopivuus**: Uudet sovellukset ja ohjelmistot vaativat usein uusimpia päivityksiä toimiakseen kunnolla. Päivittämällä varmistat, että kaikki toimii yhteen saumattomasti.

Voit ajatella päivityksiä kuin auton huoltoa – ne pitävät laitteesi turvallisina, toimivina ja ajan tasalla.

jamk

Kyberhygienia



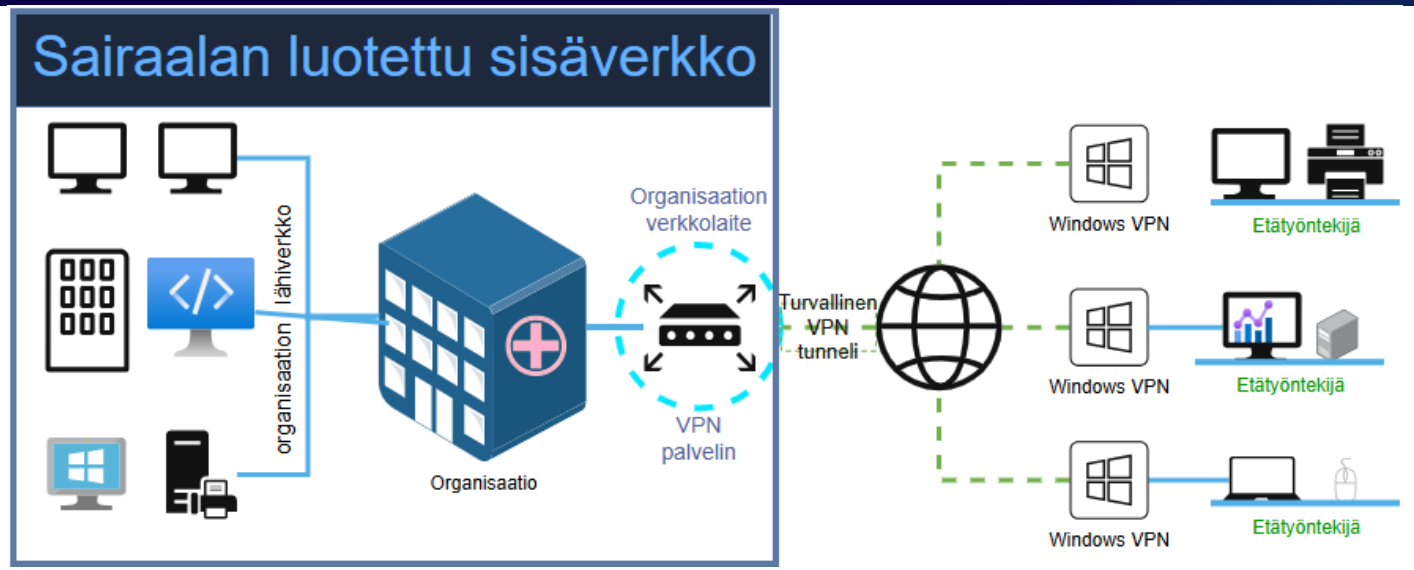
Laitteiden turvallinen konfigurointi – Parhaita käytänteitä

- Estä automaattinen kirjautuminen -> Kirjautumisen tulisi pyytää salasanaa tai muuta tunnistetta.
- Salli automaattiset päivitykset.
- Varmista tiedostojen tai tietojen varmuuskopiointi, mikäli se on tärkeää.
- Säädä ohjelmien pääsyluvat minimaalisiksi (esim. kamera, mikrofoni, paikannus, kontaktitiedot).
- Monivaiheinen tunnistautuminen lisää turvallisuutta.
- Vaihda oletussalasana -> Laitteiden oletussalasanat ovat usein julkista tietoa (myös SIM).
- Poista käytöstä tarpeettomat ominaisuudet, kuten tulostaminen laitteilta joilta ei tulosteta.
- Laitteesta riippuen harkitse virusturvan tai palomuurin asentamista tai päälle kytkemistä.

jamk

Kyberhygienia

Henkilökohtaiset laitteet ja työympäristö



- Työverkko on tarkoitettu pelkästään laitteille, jotka ovat työnantajan hallinnoimia laitteita. Työverkkoon ei tule yhdistää henkilökohtaisia laitteita.
  - Henkilökohtaisissa laitteissa voi potentiaalisesti olla haittaohjelma, joka laukeaa vasta ympäristössä, josta löytyy tietyt asiat, kuten vaikkapa kohteeksi tarkoitettu potilastietojärjestelmä.

Kuvalähde: https://wiki.teltonika-networks.com/images/9/97/Networking_RUTX_VPN_between_HQ_topology_v4.png, viitattu 12.11.2024

jamk

Kyberhygienia

Pohdi hetki

- Mitä sinulle tulee mieleen kyberhygieniasta?

    - Mitä hyviä tapoja jo käytät?
    - Mitä olet miettinyt käyttäväsi tulevaisuudessa?
    - Onko tietojärjestelmien käytössäsi eroja koti laitteiden kanssa verrattuna työpaikan tietojärjestelmiin?

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

04B – Poikkeamat ja poikkeamien hallinta

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Kyberpoikkeamat, käsittely ja reagointi

Terminologia

- **Kyberpoikkeama**: Odottamaton tapahtuma, joka vaikuttaa tietojärjestelmien turvallisuuteen.
- **Reagointi**: Toimenpiteet, joilla vastataan kyberpoikkeamaan.
- **Ilmoitusvelvollisuus**: Velvollisuus ilmoittaa tietoturvapoikkeamista valvovalle viranomaiselle.
- **Sisäinen uhka**: Organisaation sisällä oleva henkilö, joka tahattomasti tai tahallisesti aiheuttaa tietoturvariskin.

jamk

Kyberpoikkeamat, käsittely ja reagointi

Reagointi

- **Velvoitteet**: Kyberhäiriöiden hallinta, analysointi, dokumentointi ja raportointi ovat tärkeitä velvoitteita.
- **Poikkeamien käsittely**: Poikkeamat tulee käsitellä turvallisuuden ja toimintavarmuuden palauttamiseksi.
- **Dokumentointi**: On oltava menettelyt toiminnan jatkuvuuden ja häiriötilanteista palautumisen osalta.
- **Haitallisen liikenteen estäminen**: Haitallinen tekninen liikenne viestintäverkossa tulee kyetä havaitsemaan ja estämään.
- **Varmuuskopiointi**: Toimijan on määritettävä varmuuskopioinnin käytänteet.
- **Ilmoitusvelvollisuus**: Toimijan on toimitettava valvovalle viranomaiselle ilmoitukset tietoturvapoikkeamista.

* Tämä velvoittaa organisaatiota kokonaisuutena, ei ainoastaan rivityöntekijää

Lähde: https://www.fisc.fi/sites/fisc/files/inline-files/KYBERALA_NIS2_OPAS_0.9_BETA.pdf, viitattu 11.11.2024

jamk

Kyberpoikkeamat, käsittely ja reagointi

Tietoturvapoikkeamia – Microsoftin esimerkit

1. **Tietojenkalastelu:** Sosiaalisen manipuloinnin hyökkäys, jossa hyökkääjä tekeytyy luotettavaksi tahoksi saadakseen uhrin lataamaan haittaohjelman tai antamaan salasanansa.
2. **Haittaohjelma:** Haittaohjelma, joka on suunniteltu vahingoittamaan tietojärjestelmää tai varastamaan tietoja.
3. **Kiristyshaittaohjelma:** Hyökkäys, jossa haittaohjelma salaa kriittiset tiedot ja vaatii lunnaita niiden palauttamiseksi.
4. **Palvelunestohyökkäys - Denial of Service (DDoS):** Hyökkäys, jossa verkkoa tai järjestelmää kuormitetaan liikenteellä, kunnes se hidastuu tai kaatuu.
5. **Viestinnän manipulointi - Man in the Middle:** Hyökkääjä asettuu kahden osapuolen väliseen viestintään varastaakseen tai muokatakseen tietoja.
6. **Sisäinen uhka:** Sisäpiirin uhka, jossa organisaation sisällä oleva henkilö vuotaa tietoja tahattomasti tai tahallisesti.
7. **Luvaton pääsy:** Tietomurto, joka alkaa varastetuilla käyttäjätunnuksilla ja johtaa haittaohjelmien asentamiseen tai tietojen varastamiseen.

Lähde: https://www.microsoft.com/en-us/security/business/security-101/what-is-incident-response, viitattu 11.11.2024

jamk

Kyberpoikkeamat, käsittely ja reagointi

Roolit ja vastuut

- Tässä on esimerkki rooleista ja vastuutaulukosta poikkeamia varten.
- Joissain yrityksissä saattaa olla eri tiimejä jonne ilmoitetaan tapahtumia.
- Useimmiten tietoturvavalvomo (SOC).
- Kybertiimille, on usein saatavilla puhelinnumero, sähköpostiosoite, ja/tai jokin portaali esim. tiketöinti järjestelmä.

Nimi	Vastuu
Koko työvoima	Raportoida kaikki epäilyttävä toiminta kybertiimille
Kybertiimi	Käydä läpi kaikki aktiviteetti raportit ja vaste hälytykset tunnistaakseen potentiaalisia uhkia. Eskaloida tapahtumat vuorovastaavalle, tietoturvapäällikölle tai vastaavalle
Kybertiimin vuorovastaava tms.	Käydä läpi tarkenteet kyberpoikkeamasta päätöskriteeristöä vastaan ja suositella koordinoitua vastetta.
Tietoturvapäällikkö ja varapäällikkö	Valtuuttaa aktivoitu koordinoitu vaste ja tiedottaa sairaalaa poikkeustoiminnasta.

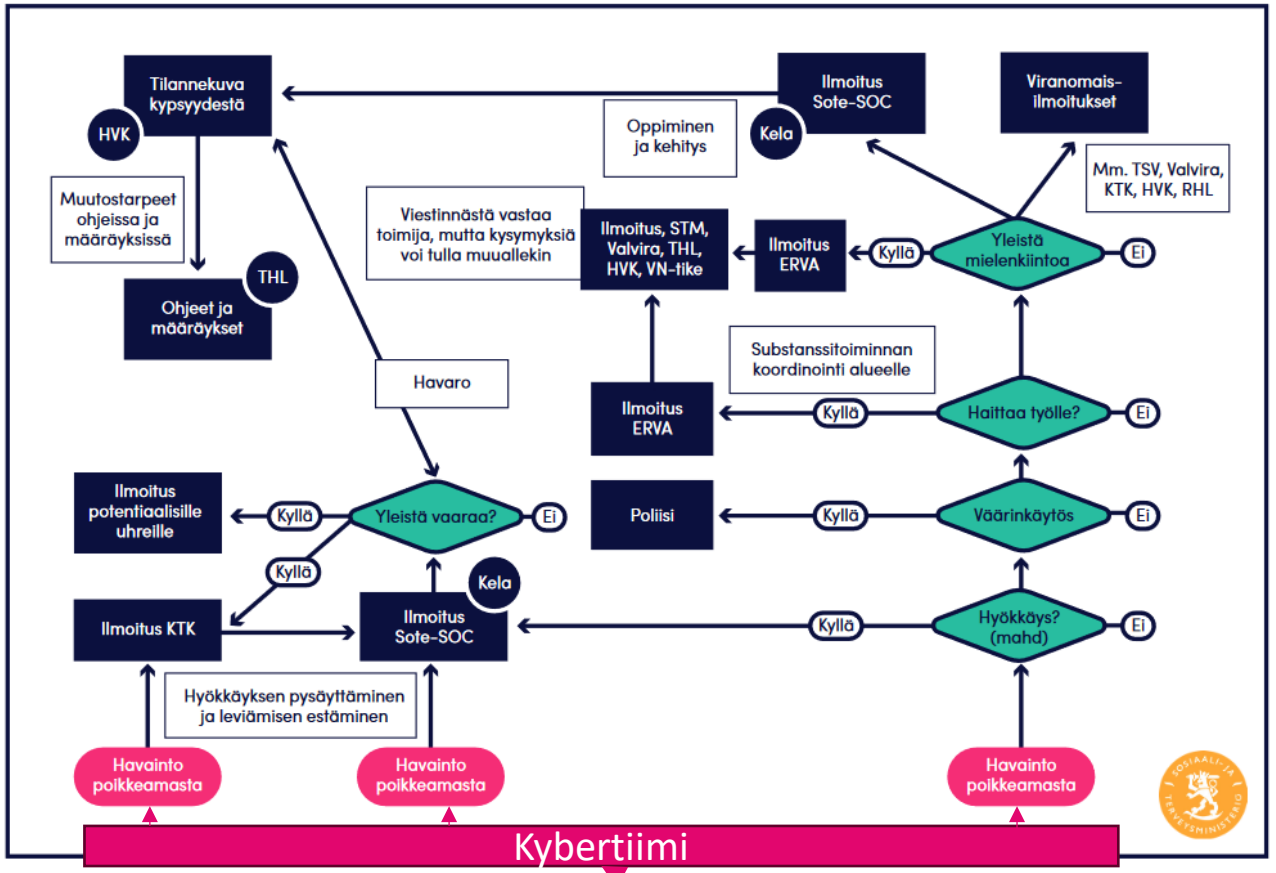
Lähde: https://healthsectorcouncil.org/wp-content/uploads/2023/07/HIC-CHIRP-FINAL_1.pdf, viitattu 11.11.2024

jamk

Kyberpoikkeamat, käsittely ja reagointi

Tiedonkulku

- Ohessa on sosiaali- ja terveysministeriön Teemupekka Virtasen tekemä kuva, jossa on havainnollistettu sosiaali- ja terveysalan kyberpoikkeaman/-häiriön osalta tiedonkulkua ja toimintaa. Oheinen kuva on luonnos, joten sen sisältämät tiedot voivat päivittyä.
- Kuvaan lisätty rivityöntekijän ja kybertiimin välinen osio



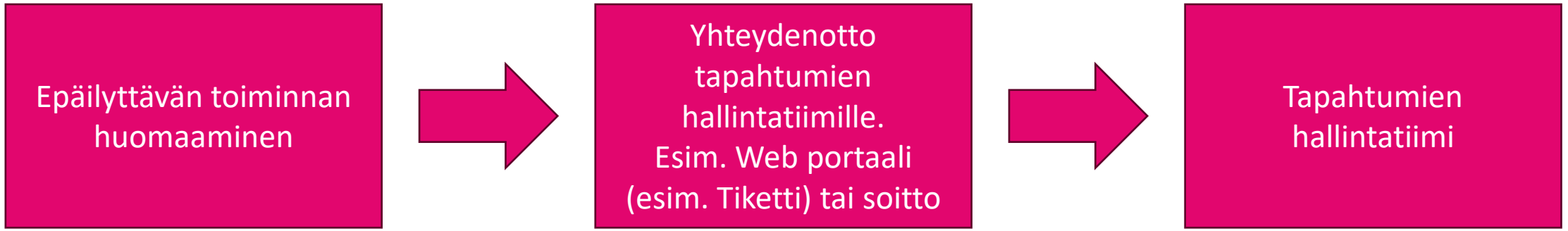
KYS ERVA Kyber Road Show, STM:n Teemupekka Virtasen esitys "SoTe-sektorin kyberturvallisuuden tilannekuva", Teemupekka, 2020 (alkuperäisen kuvan visuaalista ilmettä on muokattu tekijän luvalla)

Lähde: https://jyvsectec.fi/wp-content/uploads/2020/12/kyberhairioiden-hallinta-kasikirja-terveydenhuollon-toimijoille.pdf, viitattu 11.11.2024

Kyberpoikkeamat, käsittely ja reagointi

Tiedonkulku

- Sama yksinkertaistettuna työntekijän näkökulmasta
  - Tapahtumien hallintatiimi hoitaa tapauksen eteenpäin tai/ja neuvoo kuinka toimia

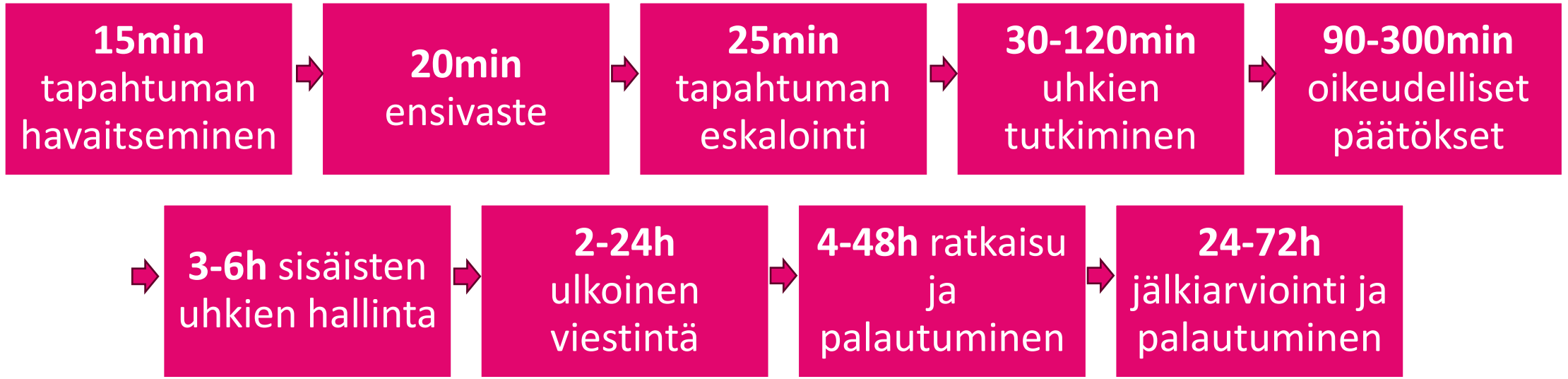


- **HUOM!** Tässä voi olla työpaikoilla erilaisia käytänteitä ja yhteydenottokanavia

jamk

Kyberpoikkeamat, käsittely ja reagointi

Kuvitteellinen **esimerkki** – **Virka-aikana**



jamk

Kyberpoikkeamat, käsittely ja reagointi

Kyberturvallisuusharjoitukset

- **Pilottiharjoitus ja osallistujien kokemuksia harjoituksesta**
- Terveydenhuoltoalan kyberturvallisuuden pilottiharjoituksessa harjoiteltiin terveydenhuollon toimijoiden kykyä vastata kyberhäiriöihin. Harjoitukseen osallistuneet kokivat harjoituksen erittäin hyödylliseksi toiminnan kehittämisen näkökulmasta.
- Videolla kerrotaan myös yleisesti mistä harjoittelussa on kyse
  - https://jyvsectec.fi/wp-content/uploads/2021/12/HCCR_Pilotti_final_fi_1.3.mp4
- Kaikki harjoitukset eivät ole teknillistoiminnallisia, kuten tässä videossa. Pöytälaatikkoharjoituksissa harjoitellaan reagointia tapahtumakorttien avulla.

Lähde: https://jyvsectec.fi/fin/terveydenhuolto/terveydenhuollon-harjoitukset/, viitattu 12.11.2024

jamk

Kyberpoikkeamat, käsittely ja reagointi

Ota selvää

- Miten tehdään poikkeusilmoitus organisaatiossanne?
- Miten toimitaan, kun havaitaan jotain tavallisesta poikkeavaa?
- Miten toimitaan, kun tietoliikenne ei toimi?
  - Minne ja miten kirjataan potilastapahtumat?
  - Miten palautumisen jälkeen toimitaan?
- Miten ja kenelle ilmoitetaan tietoliikenteen toimimattomuudesta?
- Mistä tämä tieto löytyy?

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

04C – Kyberhyökkäyksen vaiheet

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Kyberhyökkäyksen vaiheet

Hyökkääjän eteneminen

- Kyberhyökkäyksien etenemisen kuvaamiseen voidaan hyödyntää monia erilaisia malleja. Alalla useimmiten käytetyt kokonaisen hyökkäysketjun kuvaavat viitekehykset ovat:
  - **Lockheed Martin: Cyber Kill Chain**
    - Lockheed Martinin kehittämä malli, joka kuvaa hyökkäyksen vaiheet.
  - **Mitre Att&ck framework**
    - Viitekehys, joka kuvaa hyökkääjien käyttämiä taktiikoita ja tekniikoita.
  - Ja näitä molempia yhdistelevä ja lisäävä: **The Unified Kill Chain**

jamk

Kyberhyökkäyksen vaiheet

Mitre Att&ck - Viitekehys

- MITRE ATT&CK - Kehys on laajasti käytetty tietoturvaviitekehys, joka kuvaa eri taktiikoita ja tekniikoita, joita hyökkääjät käyttävät saavuttaakseen tavoitteensa.
- Mitren-viitekehys jakaa hyökkäysketjun neljääntoista (14) eri vaiheeseen. Jokaisessa hyökkäyksessä ei täyty aina kaikki 14 kohtaa, vaan osan kohdista tietyt hyökkäykset jättävät välistä.
- Viitekehys tukee erilaisia käyttöjärjestelmiä ja monia alitekniikoita. Keskitymme tässä ketjussa vain yleisentason yrityksille kohdistettuun malliin.

Lähde: MITRE ATT&CK® sekä generatiivisen tekoälyn luomat käännökset (joita on muokattu ja tulkittu uudestaan).

jamk

Kyberhyökkäyksen vaiheet

Mitre Att&ck – Viitekehys - Vaiheet

1. Taustatyö: Hyökkääjä kerää tietoa kohteesta valmistellakseen hyökkäystä.

2. Hyökkäyksen valmistelu: Hyökkääjä hankkii esim. työkaluja ja tietoa, jotka tukevat hyökkäystä.

3. Ensimmäinen sisäänpääsy kohdejärjestelmään: Hyökkääjä saa ensimmäisen jalansijan kohdejärjestelmässä, esimerkiksi tietojenkalastelun tai haittaohjelman avulla.

4. Haitallisen ohjelmistokoodin suorittaminen: Hyökkääjä suorittaa koodia kohdejärjestelmässä saavuttaakseen päämääränsä.

Lähde: MITRE ATT&CK® sekä generatiivisen tekoälyn luomat käännökset (joita on muokattu ja tulkittu uudestaan).

jamk

Kyberhyökkäyksen vaiheet

Mitre Att&ck – Viitekehys - Vaiheet

5. Jatkuvuuden ylläpitäminen järjestelmään: Hyökkääjä varmistaa, että hänellä on jatkuva pääsy kohdejärjestelmään myös järjestelmän uudelleenkäynnistysten jälkeen.

6. Järjestelmän käyttöoikeuksien korottaminen: Hyökkääjä pyrkii nostamaan käyttöoikeustasojaan järjestelmävalvojaksi tavallisen käyttäjän tasolta.

7. Suojausten väistäminen: Hyökkääjä yrittää väistää havainto- ja suojautumismekanismit, kuten virustorjunnan.

Lähde: MITRE ATT&CK® sekä generatiivisen tekoälyn luomat käännökset (joita on muokattu ja tulkittu uudestaan).

jamk

Kyberhyökkäyksen vaiheet

Mitre Att&ck – Viitekehys - Vaiheet

- **8. Kirjautumistietojen kaappaaminen**: Hyökkääjä pyrkii saamaan haltuunsa käyttäjän kirjautumistiedot, kuten käyttäjätunnuksen ja salasanan, esim. järjestelmien tai tietoliikenneverkkojen kautta.
- **9. Tiedonhakua kohdeverkosta**: Hyökkääjä tutkii ja tarkkailee yrityksen sisäistä verkkoinfrastruktuuria ja pyrkii löytämään uusia kohteita.
- **10. Tunkeutumisen laajentaminen kohdeverkossa**: Hyökkääjä pyrkii laajentamaan jalansijaansa toisiin verkossa oleviin kohteisiin tyypillisesti hyödyntämällä varastettuja tunnuksia tai järjestelmän haavoittuvuuksia.

Lähde: MITRE ATT&CK® sekä generatiivisen tekoälyn luomat käännökset (joita on muokattu ja tulkittu uudestaan).

jamk

Kyberhyökkäyksen vaiheet

Mitre Att&ck – Viitekehys - Vaiheet

- **11. Tietojen kerääminen**: Hyökkääjä kerää kohdejärjestelmistä hänelle hyödyllistä tietoa, kuten potilastietoja.
- **12. Ohjaus ja hallinta**: Hyökkääjä pyrkii muodostamaan yhteyden saastuneista kohdejärjestelmistä omalle palvelimelleen hallitakseen keskitetysti kohdejärjestelmiä.
- **13. Tietojen vieminen tai poistaminen**: Hyökkääjä siirtää kohdejärjestelmästä keräämänsä tiedot ulkopuolisille palvelimille tai poistaa ne.
- **14. Vaikutus**: Hyökkääjä pyrkii vaikuttamaan kohdejärjestelmän toimintaan, esimerkiksi manipuloimalla, häiritsemällä tai tuhoamalla järjestelmää tai tietoja.

Lähde: MITRE ATT&CK® sekä generatiivisen tekoälyn luomat käännökset (joita on muokattu ja tulkittu uudestaan).

jamk

Kyberhyökkäyksen vaiheet

Mitre Att&ck – Viitekehys - Vaiheet

- Hyökkäysketjut eivät aina toteudu lineaarisesti, eivätkä niissä aina toteudu kaikki kohdat.
- Seuraavan kalvon esimerkissä toteutuu vain muutama kohta, joka on tyypillistä myös oikean maailman hyökkäyksille.
- Numerointi esimerkissä viittaa Mitren-hyökkäysketjun numeroituun vaiheeseen.

jamk

Kyberhyökkäyksen vaiheet

Fysioterapeutin työtehtäviin kohdistunut kyberkampanja esimerkki

2. Hyökkäyksen valmistelu: Hyökkääjät lähettävät fysioterapeutille sähköpostin, joka näyttää tulevan potilaalta. Sähköpostissa on liitteenä muka potilaan lääkärinlausunto.

4. Haitallisen ohjelmistokoodin suorittaminen: Fysioterapeutti avaa liitteen, joka sisältää haittaohjelman. Haittaohjelma asentuu tietokoneelle ja antaa hyökkääjille pääsyn järjestelmään.

11. Tietojen kerääminen: Hyökkääjät keräävät tietoja potilaista ja fysioterapeutin työtehtävistä. He voivat myös seurata terapeutin viestintää ja aikatauluja.

12. Ohjaus ja hallinta: Hyökkääjät käyttävät haittaohjelmaa lähettääkseen fysioterapeutin nimissä sähköposteja kollegoille ja potilaille, yrittäen saada lisää tietoja tai levittää haittaohjelmia.

13. Tietojen vieminen tai poistaminen: Hyökkääjät varastavat arkaluonteisia potilastietoja ja fysioterapeutin henkilökohtaisia tietoja, joita voidaan käyttää myöhemmin esimerkiksi kiristykseen.

7. Suojausten väistäminen: Hyökkääjät poistavat jälkensä järjestelmästä, jotta heidän toimintansa ei huomattaisi heti.

Lähde: Kampanja esimerkki toteutettu hyödyntäen generatiivista AI:ta

jamk

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences