Terveys- ja hyvinvointialojen opintokokonaisuus

Kyberturvallisuuskoulutuksen ja siihen liittyvän yhteistyön kehittäminen korkeakouluissa

OPETUS- JA KULTTUURIMINISTERIÖ
UNDERVISNINGS- OCH KULTURMINISTERIET

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

01A-Johdatus aiheeseen

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Johdatus aiheeseen

Tilanne

- Tietovuodot ovat tulleet jäädäkseen.
- Ihmiset lankeavat jatkuvasti huijauksiin.
- Huijarit myös kehittyvät päivä päivältä paremmiksi.

jamk

Johdatus aiheeseen

Kuinka ongelmia voidaan vähentää

- Levittämällä tietoisuutta
- Varautumalla
  - Jos jokin menee pieleen, niin vahinko/vahingot on minimoitu (varmuuskopiot ja muut suunnitelmat).
- **Muuttamalla työskentelykulttuuria**
  - jos joku tekee virheen, hän ei vain yritä piilottaa sitä, vaan tiedottaa asiasta välittömästi eteenpäin.
  - Mitä pidempi aika menee tapauksen ilmoittamiseen, sitä enemmän aikaa pahalle tekijälle jää aikaa tunkeutua järjestelmiin.

jamk

Johdatus aiheeseen

Tässä koulutuspaketissa

- Tullaan tutuiksi kyberturvallisuuden kanssa sosiaali- ja terveysalan työntekijän näkökulmasta:
  - **Terminologia**: Mitä erilaisilla termeillä tarkoitetaan?
  - **Lainsäädäntö**: Miten toimia lainpuitteissa oikein ja millaisia lakeja tulee ymmärtää?
  - **Haittaohjelmat**: Millaisia haittaohjelmia tyypillisesti näkee? Millaisia tietojärjestelmiä on? Millaisia älylaitteita on olemassa ja miten ne liittyvät kyberturvallisuuteen?
  - **Kyberhygienia**: Miten toimia (tieto)turvallisesti niin kotona kuin työpaikalla?
  - **Poikkeamat**: Miten toimia tilanteessa, jossa epäillään tietoturvaloukkausta ja miten toiminta etenee ilmoituksen jälkeen?
  - **Pääsynhallinta**: Miten pääsynhallinta liittyy tietoturvallisuuteen? Miksi vain IT-henkilöstöllä voi hallita asennettuja ohjelmistoja?
  - **Salasanat**: Mistä koostuu hyvä salasana? Miksi salasanan pitää olla niin monimutkainen vai pitääkö sen olla?
  - **Fyysinen tietoturva ja tilaturvallisuus**: Miten "pahantekijän" toimia voi hankaloittaa työarjessa?
  - **Tietojenkalastelu**: Miten kalastaminen liittyy tietokoneisiin ja mitkä ihmeen tiedot sieltä pyritään onkimaan?
  - **Uhat:** Millaisia uhkia on olemassa, jotta meidän on helpompi ymmärtää millaisia suojauksia käytetään?
  - **Uhkatekijä**: Millaisia uhkatekijöitä on olemassa ja mitä "pahantekijöiden" motiivit voivat olla? Miten heidän toimintamallit eroavat toisistansa?
  - **IT:n näkökulma, johtaminen ja riskienhallinta**: Mikä/Mitkä tekijät loppujenlopuksi ohjaa/ohjaavat työntekijäkenttää? Miksi jatkuvasti tulee uusia ohjeistuksia? Mitä kaikkea jo tehdään ja mitä kaikkea jo nähdään?

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

01B-Terminologia

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Terminologia

- **Kyberturvallisuus (Cybersecurity / Cyber Security)**: Toimenpiteet ja teknologiat, joilla suojataan tietojärjestelmiä, verkkoja ja dataa kyberhyökkäyksiltä ja luvattomalta käytöltä. Kyberturvallisuus kattaa laajan alueen, mukaan lukien tietoturvan ja tietosuojan.
  - **Tietoturva (Information Security)**: Toimenpiteet ja käytännöt, joilla suojataan tietoa luvattomalta käytöltä, muutoksilta ja tuhoutumiselta. Tietoturva keskittyy erityisesti tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistamiseen.
  - **Tietosuoja (Data Protection)**: Toimenpiteet ja lainsäädäntö, joilla suojataan henkilötietoja ja varmistetaan, että niitä käsitellään lainmukaisesti ja yksityisyyttä kunnioittaen. Tietosuoja keskittyy erityisesti yksilöiden oikeuksiin ja heidän henkilötietojensa suojaamiseen.

jamk

Terminologia

- **Kriittisellä infrastruktuurilla** tarkoitetaan kaikkia niitä palveluita, järjestelmiä ja rakenteita, jotka ovat elintärkeitä yhteiskuntamme toiminnalle. Esimerkkejä kriittisen infrastruktuurin osista ovat mm. maksujärjestelmät, liikenteenohjausjärjestelmät tai esimerkiksi sähköverkko tai **terveydenhuolto**.
- **Kyberuhalla** tarkoitetaan sellaisen kybermaailmaan vaikuttavan teon tai tapahtuman mahdollisuutta, joka toteutuessaan vaarantaa kybermaailman oikean ja virheettömän toiminnan.
- **Uhkatoimija** on henkilö tai ryhmä, joka pyrkii aiheuttamaan vahinkoa tai häiriötä tietojärjestelmiin, verkkoihin tai tietoihin. He voivat käyttää erilaisia menetelmiä ja tekniikoita saavuttaakseen tavoitteensa.
- **Kyber(toiminta)ympäristö** on ympäristö, joka koostuu toisiinsa kytketyistä tietokoneista ja muista laitteista sekä tietoverkoista, jotka on tarkoitettu digitaalisen tiedon käsittelyyn.

jamk

Terminologia

- **Haittaohjelma**: Ohjelmisto, joka on suunniteltu vahingoittamaan tai häiritsemään tietokonejärjestelmiä.
- **Tietojenkalastelu**: Huijausyritys, jossa hyökkääjä yrittää saada luottamuksellisia tietoja esittämällä luotettavaa tahoa.
  - **Kohdistettu tietojenkalastelu**: On kohdistettu tiettyä kohderyhmää vastaan.
- **Palomuuri**: Turvajärjestelmä, joka valvoo ja hallitsee saapuvaa ja lähtevää verkkoliikennettä tietoturvan parantamiseksi.
- **Salaus**: Prosessi, jossa tieto muutetaan sellaiseen muotoon, että vain valtuutetut osapuolet voivat lukea sen.
- **Tietomurto**: Tilanne, jossa luottamuksellista tietoa päätyy luvattomien henkilöiden haltuun.
- **Kyberhyökkäys**: Tahallinen yritys vahingoittaa tietojärjestelmää tai varastaa tietoa.

jamk

Terminologia

- **Haavoittuvuus**: Heikkous tietojärjestelmässä, jota hyökkääjä voi käyttää hyväkseen.
- **Palvelunestohyökkäys (Denial of Service, DoS):** Hyökkäys, jossa hyökkääjä pyrkii estämään palvelun tai verkkosivuston normaalin toiminnan.
- **Kaksivaiheinen tunnistautuminen**: Turvamenetelmä, joka vaatii käyttäjältä kahta erillistä todennusmuotoa kirjautumisen yhteydessä, kuten salasanan ja tekstiviestikoodin.
    - **Monivaiheinen tunnistautuminen**: Turvamenetelmä, joka vaatii käyttäjältä useita erillisiä todennusmuotoja.

jamk

Johdatus aiheeseen

- Terveydenhuollon organisaatiot ovat erityisen houkuttelevia kohteita kyberrikollisille, koska ne käsittelevät suuria määriä arkaluonteista tietoa, kuten potilastietoja. Kyberuhat voivat vaarantaa potilasturvallisuuden ja hoidon laadun, joten tietojen saatavuus ja lääketieteellisten laitteiden turvallisuus ovat kriittisiä.
- Kyberuhat ja niiden vaikutukset:
  - **Kiristysohjelmahyökkäykset**: Näissä hyökkäyksissä hyökkääjät salaavat potilastiedot ja vaativat lunnaita niiden palauttamiseksi. Tämä voi johtaa tietojen vuotamiseen julkisuuteen ja lisätä riskejä entisestään.
  - **Tietomurrot**: Potilastiedot ovat arvokkaita identiteettivarkauksissa ja petoksissa. Haavoittuvuudet digitaalisissa terveysalustoissa tai lääkinnällisissä laitteissa voivat paljastaa suuria määriä arkaluonteista tietoa.
  - **Palvelunestohyökkäykset (DoS)**: Nämä hyökkäykset voivat häiritä kriittisiä terveydenhuollon palveluita, mikä vaarantaa potilasturvallisuuden.

Lähde: https://www2.deloitte.com/fi/fi/pages/life-sciences-and-healthcare/articles/terveydenhuollon-kyberturvallisuus.html, viitattu 20.1.2025

jamk

Johdatus aiheeseen

- Ratkaisut ja suositukset:
  - **Tietoturvapäivitykset**: On tärkeää pitää lääketieteellisten laitteiden ja järjestelmien tietoturvapäivitykset ajan tasalla.
  - **GDPR**: EU:n yleinen tietosuoja-asetus asettaa vaatimuksia ja rajoituksia henkilötietojen suojaamiselle. Tämä on erityisen tärkeää terveydenhuollossa, jossa käsitellään arkaluonteisia henkilötietoja.
  - **Viranomaisten tuki**: Kansallisella tasolla viranomaiset tukevat kyberturvallisuutta harjoittelemalla ja varautumalla tunnistettuihin uhkiin sekä laatimalla säännöllisiä riskiarvioita.

Lähde: https://www2.deloitte.com/fi/fi/pages/life-sciences-and-healthcare/articles/terveydenhuollon-kyberturvallisuus.html, viitattu 20.1.2025

jamk

OPETUS- JA KULTTUURIMINISTERIÖ
UNDERVISNINGS- OCH KULTURMINISTERIET

jamk