OULUN AMMATTIKORKEAKOULU

TIETOTURVAKOULUTUS SOSIAALI- JA TERVEYSALALLE

Heli Rajamäki
Opinnäytetyö
Kevät 2025
Tietojenkäsittelyn tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittelyn tutkinto-ohjelma

Tekijä(t): Heli Rajamäki
Opinnäytetyön otsikko: Tietoturvakoulutus sosiaali- ja terveysalalle
Työn ohjaaja(t): Teppo Räisänen
Työn valmistumislukukausi ja -vuosi: Kevät 2025
Sivumäärä: 56

Opinnäytetyön tarkoituksena oli kerätä tietoperustaa tietoturvakoulutuspohjan taustalle sekä luoda helposti muunneltavissa oleva koulutuspohja. Aiheita, joita työssä käytiin läpi, ovat yleisesti tietoturva, psykologiaa tietoturvakoulutusten taustalla, teoriaa tietoturvakoulutuksen luomisen taustalla sekä sosiaali- ja terveysalan tietoturvateoriaa, johon tietoturvakoulutuspohjakin perustuu.

Tietoturva ja tietoturvakoulutukset ovat välttämättömiä jokaisessa organisaatiossa sekä jokaisen henkilön arjen digikäyttäytymisessä. Erityisesti sosiaali- ja terveysalalla ollaan jatkuvasti tekemisissä arkaluonteisten tietojen kanssa, jonka takia tietoturva on erityisen tärkeää.

Aineistoa opinnäytetyöhön kerättiin erilaisten artikkelien ja kirjojen avulla. Osaksi aineistoa yritettiin myös saada haastattelu liittyen sosiaali- ja terveysalan tietoturvakoulutukseen korkeakoulututkinnossa, mutta valitettavasti vastaukset eivät ehtineet tähän versioon. Opinnäytetyön toiminnallista osuutta ei julkaista osana opinnäytetyötä.

Opinnäytetyön johtopäätöksenä todettiin, että tietoturvakouluttaminen tulee olla suunnitelmallista ja säännöllistä. Koulutuksissa tulisi ottaa huomioon käytännön esimerkit arjesta sekä sitä, miten koulutuksen kohderyhmä huomioidaan.

Tuloksia voidaan hyödyntää tietoturvakoulutuksen suunnitteluun sekä henkilöstön tai opiskelijoiden tietoturvaosaamisen tukemiseen.

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Business Information

Author(s): Heli Rajamäki
Title of thesis: Information security training for the health and wellness sector
Supervisor(s): Teppo Räisänen
Term and year when the thesis was submitted: Spring 2025
Number of pages: 56

The purpose of this thesis was to gather a theoretical foundation to support the development of a cybersecurity training template and to create a training base that is easily adaptable. The topics covered in the thesis include general cybersecurity, psychological aspects behind cybersecurity training, theoretical frameworks for designing training, and specific cybersecurity theory related to the social and healthcare sector, which forms the basis for the created training template.

Cybersecurity and cybersecurity training are essential in every organization as well as in the digital behavior of individuals in everyday life. This is particularly true in the social and healthcare sector, where professionals handle sensitive data on a daily basis, making data security especially critical.

The material for the thesis was collected through various articles and books. An interview related to cybersecurity training in higher education degree within the social and healthcare field was also attempted as part of the data collection, but unfortunately, the responses were not received in time for this version of the thesis. The functional part of the thesis will not be published.

The main conclusion of the thesis was that cybersecurity training must be systematic and continuous. The training should include practical everyday examples and take into account the specific characteristics and needs of the target audience.

The results can be used in the planning of cybersecurity training and in supporting the cybersecurity skills of employees or students.

SISÄLLYS

SANASTO

käsite	selite
kyberuhka	haittaohjelma, järjestelmähaavoittuvuudet, tietovuodot,
kryptologia	tiedon käyttämistä ja varastoimista turvallisin ja matemaattisin salausmenetelmin
enkryptaus	tiedon salaaminen matemaattisesti, tiedon turvaaminen,
tietoturvaresilienssi	organisaation kyky toimia ja palautua tietoturvauhkia kohdatessaan

1 JOHDANTO

Tämä opinnäytetyö käsittelee tietoturvaa ja tietoturvakoulutuksen luomista sosiaali- ja terveysalalle. Tietoturva on yksi tärkeimmistä asioista, jota myös sosiaali- ja terveysalalla tulisi kehittää, jotta tietoturvan taso vastaisi nykypäivän tarpeita ja vaatimuksia. Opinnäytetyön tavoitteena on perehtyä syvällisesti sosiaali- ja terveysalalla tarpeelliseen tietoturvaan sekä luoda tietoturvakoulutuspohja alan työntekijöille ja alalle kouluttautuville. Opinnäytetyön toimeksiantajana on Breathe Mobile Solutions.

Tietoperusta käsittelee yleisesti tietoturvaa, mitä ihmisaivoissa tapahtuu tietoturva-asioita käsitellessä, yleisiä tietoturvamalleja sekä tietoturvakoulutuksen luomista. Tietoperustaan hyödynnetään kirjoja ja artikkeleita aiheisiin liittyen.

Opinnäytetyön luvussa kaksi käsitellään tietoturvan pääkäsitteitä kuten tieto- ja kyberturva, katsaus tietoturvauhkiin, CIA-luokittelu ja Zero Trust -periaate. Tietoturva itsessään saattaa olla näkymättömänä elementtinä, vaikka nykypäivänä tietoturvan tulisi olla osana jokaisen työntekijän arkea ja siihen tulisi jokaisen kiinnittää huomiota. Näiden lisäksi luvussa käydään läpi yleisesti tietoturvakoulutuksen luomisesta sekä psykologiasta kouluttamisen taustalla.

Kolmannessa luvussa syvennytään sosiaali- ja terveysalan tietoturvaan. Sosiaali- ja terveysalalla käsitellään päivittäin erittäin arkaluonteista tietoa potilas- ja asiakastietoja käsitellessä, joten tietoturvan merkitys alalla on merkittävän suuri. Tämän lisäksi kasvavat tietoturvariskit korostavat työntekijöiden tietoturvaosaamista. Aiheina ovat muun muassa tosielämän esimerkit tietoturvauhkista, kalasteluviestit, lainsäädäntö ja työntekijän merkityksestä tietoturvaprosessissa.

Neljännessä luvussa saa katsauksen tietoturvakoulutuksen kehittämiseen. Koulutuksen toiminnallisessa osuudessa käytettyjä materiaaleja ja tekniikoita ei julkisesti jaeta osaksi opinnäytetyötä.

Opinnäytetyön tuloksena laadittiin koulutuspohja kerätyn tietoperustan perusteella. Tietoperusta nosti esiin sosiaali- ja terveysalan keskeisiä

tietoturvatarpeita. Koulutuspohjan luomisessa korostui sen helppo soveltaminen. Työ antaa suuntaviivat tietoturvakoulutuksen sisällön ja rakenteen jatkokehittämiseen.

Opinnäytetyössä ei käsitellä potilasturvallisuutta, vaan tietoturvallisuutta ja siihen liittyviä koulutuksia, säännöksiä ja käytänteitä.

2 TIETOTURVA

2.1 Tieto- ja kyberturva

Tietoturvasta puhutaan käsitellessä tietojen suojaamista. Tietojen suojaaminen pitää sisällään erilaisia toimenpiteitä ja sääntöjä, joiden tavoitteena on estää arkaluonteisten tietojen päätyminen vääriin käsiin sekä suojata tietoja ja tietojärjestelmiä. Tietosuojasäännösten avulla pyritään suojaamaan niin fyysinen, digitaalinen kuin suullinenkin tieto. Käytäntöjen ja sääntöjen avulla huolehditaan myös, että tarvittava tieto on saatavilla ja tieto pysyy muuttumattomana.

Yksittäisen käyttäjän tietoturvakäytöksellä on paljon merkitystä tietoturvakentällä, mutta kehittämällä lähtökohtaisestikin turvallisempia sovelluksia ja järjestelmiä pystyy suojautumaan myös käyttäjiltä, jotka joko tahallisesti tai tahattomasti löytää tietoturva-aukkoja organisaation järjestelmistä. Teknisen tietoturvan merkitys käytännön työssä on suuri ja oikeiden työkalujen avulla yksittäinen työntekijä, joka ei suoranaisesti työskentele tietoturvan parissa, voi keskittyä enemmän omiin työtehtäviinsä. (Luo & Zhdanov 2016, 1.)

Vastuullisesti kehityt sovellukset ja järjestelmät vaativat kumminkin aina rinnalleen myös tietoturvan kannalta vastuullista loppukäyttäjää eli loppukäyttäjällä tulisi olla vähintään arjen tietoturvataidot hallussa. Valitettavasti tämä ei aina päde ja loppukäyttäjät nähdäänkin tietoturvaketjun heikoimpana lenkkinä aiheuttamiensa uhkien takia. Tietoturvauhkat organisaatioiden sisällä johtuu 72–95 % loppukäyttäjien puutteellisista tietoturvataidoista. (Carlton, Levy & Ramim 2019.)

Loppukäyttäjän puutteellisia tietoturvataitoja ovat vajavaiset salasanakäytännöt, kalasteluyritysten tunnistamattomuus, osaamattomuus tietoturvaohjelmien käytössä, sosiaalinen hakkerointi tunnistamattomuus, julkisen Wi-Fin käyttäminen, arkaluonteisen tiedon lähetys/antaminen suojaamatonta väylää pitkin (esimerkiksi sähköpostiviesti ilman turvasähköposti ominaisuutta) tai laitteiden

jättäminen suojaamatta julkisella paikalla, jolloin kuka vain voi päästä laitteeseen käsiksi edes lyhytaikaisesti.

Tietoturva aiheenaan nousee usein esiin tietoturvauhkien kautta, koska oikeaoppiset tietoturvakäytännöt ovat lähtökohtaisesti huomaamattomia. Niin kauan, kun kaikki menee tietoturvakentällä hyvin, niin mitään ei kuulu. Kun kuuluu, niin vahinko on jo ehtinyt suurimmassa osassa tapauksia tapahtua. Tietoturvauhkat ovat tärkeitä nostaa esiin ja niiden kautta oppii, mutta tärkeää olisi myös kehittää organisaation tietoturvaresilienssiä, lanseerata se osaksi organisaation tietoturvakäytänteitä ja tuoda sitä aiheena esiin arjen työssäkin. Tietoturvaresilienssin kehittäminen pitää sisällään myös varautumisen uhkiin ja oikeaoppisia tietoturvakäytänteitä. Sen lisäksi tietoturvaresilienssin avulla mitataan organisaation kykyä taistella mahdollisia uhkia vastaan ja mahdollisuuksia palautua niistä. (IBM s.a.)

Tietoturvaresilienssin kehittäminen organisaatiossa nousee yleensä esiin siinä kohtaa, kun ymmärretään sosiaalisteknisten järjestelmien olevan suunniteltu suurimmassa osaa tapauksista vain tasaisen turvalliseen ympäristöön (Araujo, Machado & Passos 2024). Kehittämällä tietoturvaresilienssiä ja ottamalla sen osaksi suunnitelmaa organisaatio pystyy minimoimaan vahingot, joita syntyy tietoturvauhkia kohdatessaan. World Economic Forumin ja Oxfordin tietoturvakeskuksen yhteistyössä tekemässä raportissa annettiin viisi vinkkiä tietoturvaresilienssin kehittämiseen: 1. Täytyy tunnistaa, että 100 % aukoton tietoturva ei ole mahdollista. 2. Täytyy olla suunnitelma uhkakuvien varalle. 3. Tietoturvaresilienssi osaksi organisaation eri liiketoimintaprosesseja. 4. Varjele luottamuksellista tietoa. 5. Ota opiksi aiemmista (tietoturva)tapahtumista. (Beato & Saunders 2024.)

2.1.1 Yleiskatsaus tietoturvauhkiin

Tietoturvauhkia on monia erityyppisiä, joista suurin osa voi kohdistua niin organisaatioon kuin yksityishenkilöönkin. Kiristyshaittaohjelmat, virukset ja tietojenkalastelut pystyy vahingoittamaan yksittäisen henkilön lisäksi myös kokonaista organisaatiota tai ihmisjoukkoa. Palvelunestohyökkäykset kohdistuvat

lähtökohtaisesti organisaatioiden verkkopalveluihin haitaten samalla myös yksityishenkilönä palvelun käyttöä. Vuonna 2024 tietovuodot maksoivat maailmanlaajuisesti 4,88 miljoonaa Yhdysvaltojen dollaria. (IBM 2024, 4.)

Työntekijöiden ja organisaatioiden tulisi huolehtia myös fyysisestä tietoturvasta estääkseen tietoturvauhkia, joita voi ilmaantua niissä tilanteissa, joissa laitteisto päätyy vääriin käsiin edes lyhytaikaisesti tai fyysinen laitteisto varastetaan. Tällaisissa tilanteissa hyökkääjä saa mahdollisuuden varastaa tietoja tai asentaa haittaohjelman organisaation laitteistoon, joka päätyy saastuneen laitteen kautta organisaation verkkoon. Laitteisto, joka on ollut varastettuna, kadoksissa tai laitteeseen on yhdistetty esimerkiksi muistitikku, jonka alkuperästä ei ole varmaa tietoa, ei tulisi yhdistää organisaation tai oman kodin sisäverkkoon. Saastunutta laitetta ei välttämättä saa enää käyttökelpoiseksi myöskään tehdasasetuksia palauttamalla.

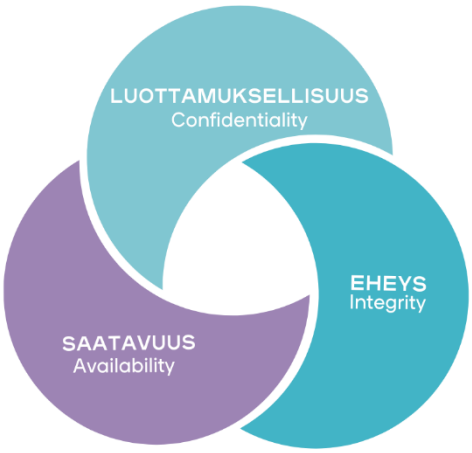
Sosiaaliset tietoturvauhkat pitää sisällään muun muassa sosiaalista manipulointia. Sosiaalisesta hakkeroinnista tunnetun edesmenneen Kevin Mitnickin oppien mukaan vastapuoli yrittää luoda tunneyhteyden hakkeroinnin kohteeseen kerryttääkseen luottamusta heidän välilleen. Luottamuksen kartuttua hakkeroija pystyy manipuloimaan kohdettaan paljastamaan tietoja, joita ei saisi paljastaa. (Mitnick & Simon 2002, s. 41)

Pew Research Centerin tutkimuksissa on käynyt ilmi, että 64 % amerikkalaisen tiedot ovat eri tavoin olleet osana tietovuotoja. Tutkittavilla oli kokemusta muun muassa yllättävistä luottokorttiveloituksista, arkaluonteisen tiedon vuotamisesta, tilien hakkeroitavana olemisesta, henkilötunnuksen vuotamisesta, yrityksistä ottaa luottoa tai lainaa heidän nimiinsä tai joku on esiintynyt heinä vilpillisesti veroilmoitusta tehdessään. (Olmstead & Smith 2017, 1.)

2.1.2 CIA-luokittelu

CIA-luokittelu vastaa sanoja confidentiality (luottamuksellisuus), integrity (eheys) ja availability (saatavuus). Nämä arvot ovat tietoturvallisuuden keskiössä. Luottamuksellisuuden avulla taataan, että tiettyihin tietoihin pääsee käsiksi vain sellaiset ihmiset, joille on tarpeellista esimerkiksi työtehtäviensä puitteissa käsitellä

tietoja ja vain silloin, kun se on oikeasti tarpeellista (Cochran 2024, 2). Esimerkkinä CIA-luokittelun luottamuksellisuuden tärkeydestä ja rikkomisesta voi pitää vuonna 2023 ilmi käynyttä tapausta Helsingin ja Uudenmaan sairaanhoitopiiristä, jossa kolme sairaanhoitopiirin työntekijää oli hyväksikäyttänyt oikeuttaan tutkia potilastietoja ilman työtehtävän edellyttämää tarvetta. (Raita-aho 2023.)



Kuva 1. CIA-mallin osa-alueet (Sallanmaa 2023.)

Luottamuksellisuutta ylläpidetään usein eri toimenpitein, joista käyttöoikeuksien hallinnan lisäksi tärkeänä osana on kryptologiasta tunnettu enkryptaus eli datan salaus (Cochran 2024, 2). Enkryptatun tiedon näkevät vain osapuolet, joilla on käyttöoikeudet tiedon katseluun.

Enkryptauksen lisäksi luottamuksellisuutta ylläpidetään myös datan luokittelun avulla. Data luokitellaan tiedon turvallisuustarpeiden mukaan (Cochran 2024, 2). Datan luokittelun avulla organisaatio suojaa arkaluonteisen tiedon oikeaoppisesti. Jos kaikkea dataa kohtelee samalla tavalla ja arkaluonteinenkin data on saatavilla ilman tarvittavia suojaustoimenpiteitä, on organisaatiolla käsillä ainekset vahingollisiin seurauksiin. Myöskään kaiken datan suojaaminen arkaluonteisena ei ole järkevää, sillä se kuluttaa enemmän resursseja ja tekee arkaluonteisen datan vuotamisen seuraamisesta hankalampaa. (Brook 2023.)

Data luokitellaan julkiseen, yksityiseen, luottamukselliseen ja rajoitettuun tietoon. Julkinen data ei lähtökohtaisesti ole arkaluonteista ja organisaatio pystyy jakamaan tiedon julkisesti ilman seurauksia, jotka vahingoittaisivat organisaatiota. Julkista tietoa voi olla esimerkiksi työntekijöiden nimet sekä tiedot, joita

organisaatio jakaa verkkosivuillaan ja sosiaalisen median tileillään. Yksityinen data on tietoa, joka on saatavilla vain organisaation työntekijöille, kuten esimerkiksi työkavereiden puhelinnumerot tai sähköpostit, jotka eivät kumminkaan ole välttämättä julkisesti saatavilla organisaation ulkopuolisille henkilöille. (Brook 2023.)

Luottamukselliseen dataan pääsee käsiksi vain nimetyt henkilöt organisaation sisällä, jotka tarvitsevat kyseistä dataa suorittaakseen työtehtävänsä. Esimerkiksi palkanlaskennassa saatetaan tarvita tiettyjä henkilötietoja, jotka ovat tarpeellisia työtehtävien ja toimintaprosessien kannalta, mutta ei saa olla julkisesti tai yksityisesti saatavilla isommalle yleisölle. Rajoitettu data on erittäin arkaluonteista ja siitä voi koitua suuret vahingot organisaatiolle, jos se päätyy vääriin käsiin tai tieto vuodetaan tahallisesti tai tahattomasti eteenpäin. Tällaista tietoa voi olla esimerkiksi erilaiset sopimukset. Rajoitettua dataa pyritäänkin turvaamaan yleensä kaikista eniten ja sen suojaamiseen on tiukimmat lakisäätelytkin. (Brook 2023.)

CIA-mallin arvo eheys pitää huolen datan luotettavuudesta. Arvon mukaan pitäisi olla todennettavissa, että saatavilla olevaa tietoa ei ole muutettu luvatta ja että dokumentin kirjoittajaan voi luottaa. (Cochran 2024, 2.)

Eheyden tunnustamiseen käytetään erinäisiä tapoja, kuten hajautus- tai tiivistefunktiot (hash functions), allekirjoitukset ja versionhallinnan tiedot (Cochran 2024, 2). Tiivistefunktioiden avulla data muutetaan uniikiksi bittijonoksi toimien toiselta nimeltään myös kryptografisena tiivisteenä (Hakatemia s.a.).

Yksisuuntaisuus, törmäysresistanssi, lumivyöryefekti ja nopeus ovat neljä perusperiaatetta, joihin kryptografiset tiivisteet perustuvat. Yksisuuntaisella tiivisteellä tarkoitetaan tiivistettä, jonka alkuperäistä syötettä ei pystytä enää palauttamaan, koska se veisi paljon aikaa. Yksisuuntaista tiivistettä käytetään esimerkiksi salasanojen suojaukseen tämän takia. (Hakatemia s.a.) Salasanoista helpoimmat voi kumminkin salauksesta huolimatta silti olla ratkaistavissa esimerkiksi sanakirjahyökkäyksen avulla, mutta tiedon salaus yksisuuntaisella tiivisteellä auttaa siinä, että arkaluonteista tietoa ei anneta tarjottimella hyökkääjälle.

Törmäysresistanssin avulla voidaan parhaimmassa tapauksessa taata, että syötteistä luodut tiivisteet olisivat uniikkeja. Tiivistefunktion avulla tiedon eheyttä

tarkistaessa tämä tarkoittaisi esimerkiksi sitä, että jos samat tiivisteet toistuisivat, niin siinä olisi suurempia tietoturvariskejä tiedon eheyden puolesta, jolloin mahdollinen hyökkääjä pystyisi luomaan väärennettyjä tietoja toistuvien tiivisteiden avulla ja manipuloimaan tietoa. (Hakatemia s.a.)

Lumivyöryefekti on tärkeä törmäysresistanssin kannalta. Lumivyöryefektillä tarkoitetaan sitä, kun syötteestä muutetaan vain yksi merkki, niin sen tiiviste muuttuu kokonaan. Ilman lumivyöryefektiä hyökkääjät pystyisivät helposti päättelemään tiivisteet muuttamalla syötteitä ja tarkastelemalla mitkä osat tiivisteestä muuttui syötteen muutoksen myötä. (European Information Technologies Certification Academy, 2023.)

Kryptografisten tiivisteiden kokoja on erilaisia, mutta yleisimmät käytössä olevat koot ovat 256, 384 ja 512 bittiä. Tiivistefunktioperheitä on olemassa SHA-1, SHA-2 ja SHA-3, joista SHA-3 on kaikista uusin. Kaikissa näissä perheissä on käytössä ainakin yleiset tiivistekoot. (Aalto yliopisto 2022a.) SHA-1 tiivistefunktioperheen edeltäjä oli SHA-0, joka todettiin vain muutaman vuoden käytön jälkeen hyödyttömäksi tietoturvakentällä juuri törmäysresistanssin puuttumisen takia (Faria 2020).

Kyberturvallisuuskeskus uutisoi vuonna 2020, että SHA-1-tiivistefunktio on lopullisesti murrettu eikä sitä tulisi enää käyttää tiedon eheyden varmistamiseksi. Tutkijat Gaëtan Leurent ja Thomas Peyrin olivat löytäneet keinon, jolla he pystyivät todentamaan, että SHA-1 ei ole enää törmäysresistanssi ja täten sen käyttö on tietoturvauhka. Kyberturvallisuuskeskus ohjeistikin viimeistään tuolloin siirtymään SHA-2- tai jopa SHA-3-tiivistefunktioiden käyttöön. (Kyberturvallisuuskeskus 2020.)

Dokumenttien versionhallinnalla pystytään pitämään kirjaa dokumentissa tapahtuneista muutoksista ajan mittaan. Versionhallinnalla todennetaan, että milloin dokumenttiin on tehty muutoksia ja kuka ne on tehnyt. Näin ylläpidetään dokumentin eheyttä. (Cochran 2024, 2.)

CIA-mallin arvolla saatavuus tarkoitetaan sitä, että tiedon tulisi olla jatkuvasti ja helposti saatavilla. CIA-mallin mukaan tiedon tulisi siis olla saatavilla myös poikkeusoloista huolimatta jokaisessa tilanteessa. (Irwin 2023.) Saatavuuden tärkeys

korostuu esimerkiksi pankkien verkkopalveluissa sekä sairaalassa potilastietojen kanssa, joihin sairaalahenkilökunta aina tarvittaessa tarvitsee pääsyn.

Tietojen tai järjestelmän saatavuutta voi CIA-mallissa mitata usealla eri tapaa. Yksi tavoista on ottaa selvää kuinka paljon katkoksia järjestelmän käytössä tai tietojen saatavuudessa tulee määrätyllä aikavälillä. Katkoksella tarkoitetaan tämän yhteydessä sitä, että tietoihin tai järjestelmään ei ole lainkaan pääsyä. (Cochran 2024, 2.)

Saatavuutta saadaan ylläpidettyä myös varmuuskopioiden sekä varajärjestelmien avulla. Ne ovat yleensä varatoimenpiteitä, jotka otetaan käyttöön, kun tietoon tai järjestelmään ei alkuperäisellä tavalla pääse käsiksi. (Cochran 2024, 2.)

2.1.3 Zero trust-malli

Zero trust-mallin avulla taataan turvallinen verkkoympäristö organisaatioissa, joissa on monimutkainen digitaalinen ekosysteemi. Digitaalisella ekosysteemillä tarkoitetaan tässä yhteydessä kokonaisuutta, jossa organisaatiot toimivat yhteistyöorganisaatioidensa kanssa jakaen keskenään dataa tai mahdollisesti jopa kokonaisia järjestelmiä. Myös työntekijöiden etänä työskentely tuo uuden ulottuvuuden organisaation digitaaliseen ekosysteemiin. (Yrityksen digitalous 2022.)

Mallille ominaista on se, että kehenkään tai mihinkään ei luoteta ja siitä tuleekin zero trust-mallin yhteydessä käytettävä lausahdus ’Never trust, always verify’. Zero trustin kolme perusperiaatetta ovat 1. Oleta tietomurtoa. 2. Aina varmenna, älä koskaan luota. 3. Käyttäjällä tulisi olla vain minimioikeudet niin, että pystyy suoriutumaan kumminkin työtehtävistään (Yacono 2024). Malliin kuuluu myös viisi pilaria, jotka eroavat perusperiaatteista. Pilarit ovat identiteetti, laite, tietoverkko, sovellukset ja työkuormat sekä data. (Trevino, Cutler & Guccione 2024.)

Zero trust-malliin yhdistetään myös ZTNA eli Zero Trust Network Access. ZTNA:sta puhuttaessa kyseessä on useita eri teknologioita, joiden avulla esimerkiksi etäkäyttäjät pääsevät turvallisesti käsiksi sisäisiin järjestelmiin. (Zscaler s.a. a.)

Käytännössä zero trust tarkoittaa usein sitä, että esimerkiksi työntekijöiden on jatkuvasti todennettava henkilöllisyytensä ja käyttöoikeutensa usealla eri tavalla. Enää ainoastaan salasana ei riitä, sillä pelkästään salasanan avulla suojautuminen nykypäivänä on vain ajan kysymys, milloin joku pääsee kyseisiin käyttäjätileihin kiinni ja miten huomattavaa vahinkoa jo pelkän salasanan päätyminen vääriin käsiin voisi saada aikaan ilman monivaiheista tunnistautumista. Loppukäyttäjät valitsevat mieluummin helposti muistettavan salasanan kuin esimerkiksi salasanamanagerin avukseen luodakseen monimutkaisempia salasanoja, jonka takia kaksi- tai monivaiheinen tunnistus astuu kuvioihin tässä kohtaa. (Das 2023, 1.)

Vuoden 2021 IBM:n Cost of Data Breach -raportin mukaan zero trust-malli on ollut tärkeänä osana madaltamassa yritysten tietovuotojen kustannuksia. Raportin mukaan organisaatioille, joilla oli käytössä zero trust-käytäntö, maksoi tietovuodot 1,76 miljoonaa dollaria vähemmän kuin organisaatioille, jotka eivät hyödyntäneet zero trustia. Jopa 65 % vastaajista ei ollut implementoinut zero trust-lähestymistapaa osaksi organisaationsa tietoturvakäytänteitä ja 43 % organisaatioista ei ollut aikomustakaan ottaa sitä käyttöön. (IBM 2021.)

Zero trust-mallin yhtenä keskeisenä elementtinä oleva vahva salaus oli yksi merkittävimmistä keinoista vähentää tietomurroista koituvia kustannuksia. Vahva salaus sijoittui kolmanneksi vertailussa, kun sitä ennen kustannuksia vähentämässä oli myös edistynyt tekoälyn sekä analytiikan hyödyntäminen. (IBM 2021.)

Kaksivaiheinen tunnistus sisältää aina kaksi saman identiteetin tunnistustapaa ennen kuin loppukäyttäjä pääsee haluamaansa palveluun sisälle. Monimutkaisen salasanan tapaan myös kaksivaiheinen tunnistus estää tietoturvarikollisia pääsemästä käsiksi käyttäjän tai organisaation tietoihin. Kaksivaiheinen tunnistus on myös käyttäjäystävällinen. Usein autentikointiin käytetään muun muassa tekstiviestiä tai mobiilisovellusta, jolloin ei ole tarvetta erilliselle tunnuslukulaitteelle, vaikka sellaisiakin saattaa olla joillain organisaatioilla käytössä. Tekstiviesti tai mobiilisovellus toimii hyvin yksityishenkilölläkin kaksivaiheiseen tunnistukseen, jolloin ei tarvitse mitään lisälaitteita turvatakseen omat käyttäjätilinsä. Tekstiviesti- tai sovellusgenerointi autentikointitunnukselle on myös sen puolesta turvallinen,

että sama luku ei tulisi toistua uudelleen identiteetin todennuksen yhteydessä. (Microsoft s.a.)

Kaksivaiheisen tunnistuksen tehtävänä tietoturvan kannalta on toimia pesäpallohanskana salasanan jälkeen. Jos hyökkääjä saa ratkaistua salasanan, on hyökkääjän vielä pystyttävä autentikoimaan itsensä toistamiseen kertaluontoisella tunnusluvulla, joka on vaikeampaa hakkeroida. Senkään hakkerointi ei ole kuminkaan mahdotonta, jolloin tilalle saattaa haluta monivaiheisen tunnistuksen. (Das 2023, 1.)

Monivaiheinen tunnistus käyttää kahta useampaa autentikoitumistapaa ennen kuin loppukäyttäjä pääsee sisälle haluamaansa palveluun. Monivaiheinen tunnistus luo entistäkin turvallisemman kirjautumistavan ja minimoi hyökkäyksiä. Eri autentikoitumistapoja ovat salasanan lisäksi kännykällä tunnistautuminen tai joku muu vastaava tapa, esimerkiksi kulkutunniste. Monivaiheisessa tunnistuksessa saatetaan käyttää myös loppukäyttäjän biometrisiä tunnisteita tai lokaatiota vahvistukseen. (Cyberark s.a.)

Zero trust-mallin peruspilareista identiteetti näkyy arjessa muun muassa niin, että käyttäjään eikä laitteeseen tulisi luottaa, vaan jokainen pyyntö päästä käsiksi dataan käsitellään erikseen ja yhtä vahvasti minimoiden tietoturvariskejä. Työntekijälle se voi näyttäytyä turhauttavana, mutta tietoturvakentällä siitä on hyötyä. Osana identiteetin vahvistusta tulisi olla monivaiheinen tunnistus. (Silverfort s.a.)

Laiteturvallisuus zero trust-mallissa toimii samaan tapaan. Laite on tunnistettava turvalliseksi ennen kuin sille voi antaa pääsyä organisaation dataan. Käytännössä se tarkoittaa sitä, että laitteella, jonka organisaatiossa vaaditut palomuuri tai tietoturvaohjelmisto ei ole ajan tasalla, ei välttämättä pääse organisaation dataan käsiksi. (Beyond Identity s.a.)

Peruspilarina verkkoturvallisuus toteutuu aiemmin mainitun Zero Trust Network Accessin eli ZTNA:n avulla. ZTNA myöntää tunnistetuille käyttäjille pääsyn tiettyihin sovelluksiin erottaen verkon käytön esimerkiksi etänä työskennellessä. Tämä vähentää organisaation verkkoon kohdistuvia tietoturvariskejä. (Zscaler s.a. a.)

ZTNA-palveluita välittävän palveluntarjoajan avulla organisaatio pystyy tekemään sisäverkostaan myös ulospäin suuntautuvan, jolloin verkosta tulee näkymätön ulkopuolisille. Liikenne voi palveluntarjoajan kautta olla myös vain tietyille henkilöille valtuutettu. Sen avulla voi siis minimoida ulospäin näkyvää hyökkäyspinta-alaa organisaation verkossa. (Zscaler s.a. a.)

Zero Trust Network Accessissa organisaation tietoturvallisuuden tärkeänä tekijänä on myös verkon segmentointi. Verkon segmentointia on kahta erilaista, mikrosegmentointia ja segmentointia. Eroa näillä kahdella segmentointitavalla on verkon segmentointiosien suuruudessa. Mikrosegmentoinnissa puhutaan, kun verkko yritetään jakaa mahdollisimman pieniin osiin, jopa osastokohtaisesti organisaation sisällä. Normaalista segmentoinnista puhutaan, kun verkko jaetaan osiin suurpiirteisemmin, karkeasti jaoteltuna esimerkkinä vierasverkkoon ja organisaation sisäverkkoon. (Zscaler s.a. b.)

Verkon segmentointi on yksi yleisimpiä tietoturvatoimenpiteitä, joilla organisaatio voi pienentää verkon hyökkäyspinta-alaa. Segmentoinnin avulla liikennettä eri segmenttien välillä on rajoitettu tai liikenne on kokonaan estetty verkon osien välillä. (Zscaler s.a. b.)

Segmentoidussa verkossa tietomurto yhdellä verkkoalueella saattaa eristää tietomurron parhaimmassa tapauksessa vain sille alueelle ja estää sen leviämisen muille verkkoalueille. Tämän lisäksi verkkoalueita on helpompi seurata pienempinä kokonaisuuksina kuin yhtenä isona verkkoliikennekokonaisuutena. Verkon segmentointi minimoi riskiä sisäisistä tietoturvauhista, jos jokainen osasto on jaoteltu omiin verkon osiinsa ja heille on määritelty kyseisissä verkon osissa sallittavat järjestelmät käytettäväkseen, jolloin kaikki järjestelmät ei ole jokaiselle työntekijälle saatavilla verkkorajojen yli, jos he eivät niitä työtehtäviensä puolesta tarvitse. Näiden hyötyjen takia kannustetaan myös jaottelemaan vierasverkko erikseen organisaation sisäverkosta. (Zscaler s.a. b.)

Verkon segmentoinnin tyylisesti ZTNA:n yhtenä peruspilarina on myös järjestelmä- sekä työkuormaturva, joka varmistaa sen, että organisaation työntekijät pääsevät vain heille välttämättömiin järjestelmiin. (Zscaler s.a. a.)

2.2 Tietoturvakoulutuksen luominen

Tieto- ja kyberturvan koulutukseen alan tekijöille, joilla syvällisempää tuntemusta ei välttämättä vielä ole, on monia eri toteutustapoja. Usein tietoturvakoulutuksissa lähestymistapana on kertoa mahdollisimman vähän, joka tarkoittaa sitä, että syvällisempää ymmärrystä ei edes onnistuta luomaan ja tietoturva pysyy edelleenkin sellaisena abstraktina asiana, josta joku muu huolehtii tai jota ei käyttäjän mielestä tarvitse olla olemassa. (Nielson 2023, 1.)

Tärkeänä osana vaikuttavan tietoturvakoulutuksen luomista, on ymmärtää miksi ihmiset ovat erehtyväisiä tietyissä tietoturvatoimenpiteissä (Nielson 2023, 2). Miksi käyttäjä päätyy siihen tilanteeseen, että hän syöttää tietonsa huijaussivulle? Tietoturvakoulutuksessa pitää käydä läpi vinkkejä, joilla käyttäjä pystyy itse kriittisesti tarkastelemaan sivun tai auktoriteetin oikeellisuutta. Miksi käyttäjä päätyy käyttämään samaa salasanaa jokaisessa eri palvelussa? Perehdytys siihen miksi olisi tärkeää käyttää eri salasanoja eri palveluissa. Miksi käyttäjä lataa epämääräisen tiedoston tai yhdistää tuntemattoman muistitikun laitteeseensa? Vinkkejä tunnistaa vaaralliset tiedostot ja mitä tehdä, jos on vahingossa ladannut tiedoston, jossa epäilee olevan haittaohjelma tai mitä tehdä, jos kohtaa tuntemattomia tiedonsiirtovälineitä, joiden alkuperästä ei tiedä. Miksi käyttäjä yhdistää julkiseen Wi-Fi-verkkoon? Koulutusta siihen, miksi julkista Wi-Fi-verkkoa ei lähtökohtaisesti kannattaisi käyttää tai mitä toimenpiteitä tulee ottaa huomioon, jotta saa pienennettyä julkisen verkon tietoturvariskejä.

Pew Research Centerin tekemässä tutkimuksessa selvisi, että tutkittavat eivät luota siihen, että viralliset tahot pitäisivät heidän tietonsa turvassa. Samaan aikaan tutkimukseen osallistuneista suurin osa myönsi, että he eivät myöskään yksilöinä omaa parhaimpia kyberturvataitoja. Tutkimukseen osallistuneista aikuisista 41 % myönsi jakaneensa jonkin tilinsä salasanan ystävän tai perheenjäsenen kanssa, 39 % osallistujista kertoi käyttävänsä samaa tai lähes samaa salasanaa eri palveluissa ja 25 % myönsi käyttävänsä ennemmin helposti muistettavaa salasanaa kuin turvallista salasanaa. (Kennison & Chan-Tin 2020.)

Pew Research Centerin tutkimus osoittaa ihmisen välinpitämättömyyttä oman toiminnan merkityksestä tietoturvaa kohtaan. Usein tietoturvakäytännöt niin organisaatioissa kuin yksilöidenkin arjessa huomataan vasta sitten, kun jotain on mennyt vikaan. Kukaan ei valitettavasti tule kiittelemään oikeaoppisista tietoturvakäytännöistä, koska tietoturva tulisi lähtökohtaisesti olla huomaamatonta ja itsestään selvää – myös nykypäivänä yksilön digikäyttäytymisessä. Sen takia sen tärkeys helposti unohtuukin. (Reeves, Calic & Delfabbro 2021.)

Välillä tietoturvakoulutuksilla voi olla jopa ajateltua päinvastainen vaikutus. Koulutettavat saattavat uupua ja hämmentyä tietojen monimutkaisuudesta tai se voi olla liian vaikeasti ymmärrettävässä muodossa. Tietoturvakoulutusta suunnitellessa tulisikin ymmärtää myös koulutettavan näkemystä ja pohjatietämystä aiheesta. Koulutuksia suunnittelevilla kyberturva-ammattilaisilla ja koulutettavilla saattaa olla eri käsitykset koulutettavan kyvykkyydestä suoriutua tietoturvaa vaativista tehtävistä tietoturvakoulutuksen jälkeen. Kyberturva-ammattilaiset eivät pysty ottamaan koulutuksessa huomioon kaikkia ulkoisia tekijöitä, joita koulutettava saattaa kohdata päivittäisessä työssään. (Reeves ym. 2021.)

Koulutuksen luomisessa tulee myös huomioida selkeys ja johdonmukaisuus, nimittäin epäselkeät koulutusmateriaalit tekevät tietoturvasta hankalan käsittää hänelle, jolla ei siitä aiempaa kokemusta ole. Myös koulutusten yksitoikkoisuus vaikuttaa siihen, miten koulutettavat suhtautuvat tietoturvakoulutukseen. (Reeves ym. 2021.)

Kyberturvallisuuskeskuksen mukaan organisaation henkilöstössä jokaisen tulisi osata tunnistaa ja suojautua huijauksilta, sekä tietää toimintatavat, jos on tullut huijatuksi. Haittaohjelmien suhteen tärkeää olisi kouluttaa henkilöstölle se, miten haittaohjelmat voivat tarttua, mitä tehdä organisaation ulkopuoliselta taholta tulleille laitteeseen kiinnitettäville välineille kuten esimerkiksi muistitikulle, mistä voi tunnistaa haittaohjelmatartunnan sekä mitä tehdä, jos epäilee haittaohjelmatartuntaa. (Kyberturvallisuuskeskus 2023.)

Henkilöstölle olisi myös hyvä kouluttaa mitä välineitä he voivat käyttää työntekoon, mitä laitteita voivat kytkeä työvälineisiin, mitä ohjelmistoja saa asentaa

työvälineisiin ja mihin työvälineitä voi käyttää, salasanakäytännöt sekä mitä tehdä, jos työväline ei toimi, se katoaa tai se varastetaan. (Kyberturvallisuuskeskus 2023.)

Kyberturvallisuuskeskuksen mukaan henkilöstölle olisi hyvä tehdä selväksi myös turvallinen nettiin yhdistäminen etätöissä ja työmatkoilla, mitä työvälineitä matkalle saa ottaa mukaan, miten suojata työvälineet ja työasiat ulkopuolisilta sekä mitä tehdä, jos työväline katoaa tai varastetaan työmatkalla. Tietojenkäsittelyyn liittyvistä asioista työntekijöille tulisi kouluttaa mitä tietoa työpaikalla käsitellään, miten työntekijän tulee käsitellä arkaluonteista tietoa ja mitä asioita saa jakaa työpaikan ulkopuolelle. (Kyberturvallisuuskeskus 2023.)

2.3 Psykologiaa tietoturvan taustalla

Ihmiset usein ajattelevat nykypäivänä, että oma kriittinen ajattelu on korvattavissa kännykkäsovelluksella tai tietokoneohjelmalla. Parhaimmatkin tietoturvasovellukset ja -ohjelmistot tarvitsevat kriittistä ihmisajattelua ja perustason tietoturvatietämystä toimiakseen odotetulla tavalla. Nykyajan yhteiskunnassa useammat asiat ovat helppoa ja suotavaakin ulkoistaa oman psyykkisen taakan minimoimiseksi, joten moderni ihminen jo luonnostaankin etsii tapoja ulkoistaa asioita, joihin ei koe jaksavansa itse perehtyä tai kokee oman henkisen taakkansa olevan jo tarpeeksi. Tilanne tietoturvan kanssa on tämän hetken maailmassa se, että ulkoistettavia ratkaisuja ei ole siinä mittakaavassa, joissa niitä kaivattaisiin ja kiinnostus tietoturvaan tulee lähteä yleensä ihmisestä itsestä, jotta ihminen osaa tehdä arjessa oikeanlaisia tietoturvaratkaisuja tai tarkastella tietoturvaan liittyviä tilanteita kriittisesti. (Nielson 2023, 2.)

Nykyisten tietoturvajärjestelmien akilleen kantapäänä on se, että ajatellaan ihmisten olevan loogisia ja tähän myös eri tietoturvajärjestelmät sekä -koulutukset nojautuvat. Tietoturvakoulutukset ja -järjestelmät ei koskaan ole itsenäisiä ihmisen omasta kriittisestä ajattelusta. Lähtökohtaisesti niissä ajatellaan, että ihmisen ajattelutapa pitää korjata, kun todellisuudessa tulisi luoda joko vaikuttavia

koulutuksia tai järjestelmiä, jotka ottavat huomioon sen, että ihminen on useimmissa tapauksissa tunteella reagoiva olento. (Nielson 2023, 2.)

Ihmiset elää usein myös siinä illuusiossa, että esimerkiksi oma tietoturvakäyttäytyminen on kunnossa, koska mitään kriittistä ei ole vielä tapahtunut (Nielson 2023, 2). Tähän pätee edelleen myös se, että tietoturva huomataan yleensä vasta siinä kohtaa, kun jotakin menee vikaan. Niin kauan, kun kaikki on kunnossa, ei normaali ihminen välttämättä kiinnitä suurempaa huomiota omaan tietoturvakäyttäytymiseensä tai organisaatio ei huomaa isompaa puutetta tietoturvatoimissaan.

Myös tietoturvarikolliset käyttävät hyödyksi ihmisten erehtyväisyyttä tietoturvan parissa. Rikolliset löytävät haavoittuvaiset järjestelmän osat, joiden kautta he saavat esimerkiksi varastettua arkaluontoista tietoa tai saavat käyttäjän lataamaan haittaohjelman. (Kyberturvallisuuskeskus 2024.)

Tietoturvatietämyksen psykologian kannalta organisaatioiden tietoturva-asiantuntijat pitävät omaa tietämystään lähtökohtana tietoturvatietämykselle eivätkä välttämättä osaa suhteuttaa tai ymmärrä, että kaikilla organisaation työntekijöillä ei ole samaa pohjatietämystä. Ajatellaan siis, että organisaatiossa kaikki näkevät ja ymmärtävät tietoturvan samalla tavoin kuin organisaation tietoturva-asiantuntija. (Ashenden s.a.)

Eräässä tutkimuksessa tutkittavat nostivat esiin, että myös sillä on merkitystä omaankin tietoturvakäyttäytymiseen, miten työkaverit hoitavat tietoturva-asiat. Kollegoiden tapa hoitaa osaltaan tietoturvaa saattoi toimia joko motivaationa toimia itse oikein tai sitten vastaavasti joukkopaineen alla vetää mukaan huonoihin tietoturvavalintoihin. (Reeves ym. 2021.)

3 TIETOTURVA SOSIAALI- JA TERVEYSALALLA

3.1 Tietoturvauhkat

Terveydenhuolto on alana kiinnostava kyberrikollisille. Se tarjoaa paljon arkaluonteista dataa hyökkääjille, jota voi myydä tuottoisasti eteenpäin. Terveystietojen varastamisella ja haittaohjelmahyökkäyksillä sairaaloihin hyökkääjä saa paljon vahinkoa aikaan. Potilaiden luottamus terveydenhuollon turvallisuuteen hupenee, romuttaa terveydenhuollon toimijoita sekä pahimmassa tapauksessa uhkaa ihmishenkiä. (Coventry & Branley 2018.)

IoT-laitteiden hyödyntäminen sairaalaolosuhteissa tuo helpotusta sairaalahenkilökunnalle sekä myös potilaille, mutta samalla lisää uudenlaisia uhkia tietoturvallisuuden osalta. Muiden alojen tapaan sosiaali- ja terveysalalla tietoturvatoimet eivät ole nykyisiä uhkia vastaavalla tasolla. Palaten digitaalista aikaa edeltävään aikaan, jolloin potilaiden tiedot olivat saatavilla vain fyysisesti, puhuttiin tietovuodoista, jotka koskettivat vain satoja tai tuhansia potilaita. Datan ollessa yhdistettynä nyt eri järjestelmiin ja verkkoihin, tietovuotojen yhteydessä puhutaan miljoonien potilaiden henkilö- ja terveystiedoista. Toisaalta nyt on myös helpompi pitää kirjaa työntekijöistä, jotka luvatta katselevat potilaiden terveystietoja. (Coventry & Branley 2018.)

Hyökkääjät kohdistavat iskunsa terveydenhuollon toimijoihin erilaisista rahallisista, poliittisista tai sodankäynnin syistä. Useimmissa tapauksissa syynä on raha, sillä potilastiedot ovat myös rahallisesti arvokkaita. (Coventry & Branley 2018.)

Vuoden 2021 IBM:n Cost of Data Breach -raportin mukaan terveydenhuollon tietovuotojen keskiarvo oli noussut noin 9,23 miljoonaan Yhdysvaltain dollariin ja jo vuonna 2023 IBM:n sen vuotisen raportin mukaan kulut olivat nousseet jopa 10,93 miljoonaan dollariin, nostaen terveydenhuollon tietovuotojen kulut eri alojen vertailussa selkeästi korkeimmaksi. (Chin 2024.)

Tietoturvauhkia sosiaali- ja terveysalalla tietomurtojen ja kyberhyökkäysten lisäksi ovat sisäiset uhat kuten henkilökunnan huolimattomuus sekä tietojen tai käyttöoikeuksien tahallinen väärinkäyttö. Tähän liittyy tietojen kalasteluyrityksiä useimmiten verkossa. Myös terveydenhuollon järjestelmiin voidaan kohdistaa palvelunestohyökkäyksiä, jotka voivat pahimmassa tapauksessa viivästyttää potilaiden hoitoa johtaen erinäisiin henkeäkin uhkaaviin tilanteisiin. (Coventry & Branley, 2018.)

HIPAA Journalin mukaan 90 % sosiaali- ja terveysalan tietoturvahyökkäyksistä on kalasteluyritysten muodossa (Murray-Watson s.a.).

3.1.1 WannaCry

WannaCry on kiristyshaittaohjelma, joka salaa saastuneen koneen tiedostot ja lupasi palauttaa ne Bitcoin-lunnaita vastaan (Kaspersky s.a. b.). WannaCry-haittaohjelmasta on kolmea eri versiota, joista ensimmäinen oli beta-versio, toinen WannaCry 1.0 ja kolmas WannaCry 2.0 (Yang 2017).

WannaCryn beta-versio salasi saastuneelta koneelta tiedostot AES-128 salausmenetelmän avulla, mutta beta-versiolla ei ollut vielä onnistunutta leviämistapaa (Yang 2017). Kirjaimet AES ovat lyhenne sanoista Advanced Encryption Standard. Sitä käytetään muun muassa korkean tason suojaukseen luottamuksellisten asiakirjojen kanssa. Niille, joilla ei ole asianmukaista käyttöoikeutta asiakirjoihin, AES-algoritmin avulla tiedostot saa enkryptattua hyödyttömään muotoon. AES-menetelmää käytetään myös muun muassa VPN-yhteyksissä, salasanamanagereissa, selaimissa sekä sitä pystyy käyttämään myös tietokannoissa salaamaan luottamukselliset tiedot. (Pandasecurity 2024.)

WannaCryn beta-version AES-menetelmässä käytettiin juuri 128 bitin avainkokoa, josta tulee käytetty salausmenetelmä AES-128. Käytettäviä avainkokoja on tuon lisäksi 192 ja 256 bittiä. Mitä korkeampi bittisempi avainkoko, sitä monimutkaisemmasti salatumpaa tieto on. (Pandasecurity 2024.)

WannaCry 1.0:ssa oli parannuksia beta-versioon verrattuna, kuten pakattujen, salasanalla suojattujen kansioiden hyödyntäminen salauksessa, mikä yleensä

vaikeuttaa myös haittaohjelman tutkimista. 1.0-versiossa päivittyi myös salattujen tiedostojen muoto, mikä voi tarkottaa esimerkiksi sitä, että salausavaimien käsittelytapa muuttui verrattuna beta-versioon. (Yang 2017.)

WannaCryn 1.0-versio yritti levittäytyä eri verkkoympäristöihin sanakirjahyökkäyksen avulla (Yang, 2017). Sanakirjahyökkäyksellä tarkoitetaan testattavia sanoja, jotka ohjelmisto käy läpi yrittäen murtautua haluamaansa kohteeseen, WannaCryn tapauksessa organisaatioiden verkkoihin (Laakso 2011).

WannaCry 1.0 teki tietoturva-asiantuntijoiden työn monimutkaisemmaksi käyttämällä RSA-avainta AES-salausmenetelmän suojauksessa (Yang 2017). Jokaista saastunutta laitetta kohden haittaohjelma loi uuden RSA-avaimen (Counter Threat Unit 2017). Nykypäivän RSA-avaimia on jo lähtökohtaisesti vaikeampi murtaa, mutta tekemällä RSA-avaimesta tämän lisäksi muuttuvan jokaiseen eri laitteeseen, tekee tietoturva-asiantuntijoiden haittaohjelman tutkimisesta vaikeampaa. RSA-avaimet perustuvat alkulukuihin, jonka tulon tekijät on yleensä vaikea selvittää, jos on kyseessä tarpeeksi suuren luvun tekijät (Aalto Yliopisto 2022b).

WannaCry 2.0 oli edeltäjiinsä verrattuna laajimmin leviävä versio WannaCrysta hyödyntäen EternalBlue-työkalua (Yang 2017). EternalBluen avulla hyökkääjät pystyivät käyttämään Windowsin haavoittuvuuksia levittääkseen haittaohjelmaa (Malwarebytes s.a.).

WannaCry-haittaohjelmahyökkäys vaikutti organisaatioihin ympäri maailman saastuttamalla yli 230 000 tietokonetta. Suurin vaikutus hyökkäyksellä oli etenkin terveydenhuollon toimijoihin, joilla oli käytössä vanhentunut Windowsin käyttöjärjestelmäversio. Hyökkäys lamautti tai jätti pois käytöstä hengelle välttämättömiä terveydenhuollon laitteita sekä sulki ensiapujen ovia. (Fortinet s.a. a.)

3.1.2 Ruyk-haittaohjelma Benešovin sairaalassa Tsekissä

Vuoden 2019 joulukuussa Benešovin sairaalaan hyökättiin Emotet-Trickbot-Ryuk-haittaohjelmayhdistelmällä (Filipec & Plasil 2021). Hyökkäystä kutsutaan

kolmoisuhaksi, koska siinä käytetään erillisiä Emotet- ja Trickbot-troijalaisia porttina Ruyk-haittaohjelmalle (Roy 2019).

Haittaohjelmayhdistelmä pääsi leviämään tietojenkalastelusähköpostin välityksellä. Sähköposti sisälsi haittaohjelmalla saastuneen Microsoft Office -dokumentin ja vastaanottajan ottaessa dokumentin sisällön käyttöönsä dokumentissa olevat haitalliset makrot aktivoituivat. (Roy 2019.) Tällaisissa tapauksissa pelkkä dokumentin avaaminen ei käynnistä makroja, vaan yleensä tulee painaa ladatusta Microsoft Office -dokumentista ”Ota sisältö käyttöön” -nappia, jolloin Microsoft Office sallii kaikkien dokumentin makrojen suorittamisen, myös mahdolliset saastuneet makrot.

Haittaohjelma salasi saastuneiden koneiden tiedot käyttäen RSA-4096 ja AES-256 salausmenetelmiä. Benešovin sairaalan hyökkäyksessä dataa ei menetetty ja järjestelmät saatiin palautettua jopa viikossa. Jokaista tietoturvatapausta tulee käsitellä lopputuloksesta huolimatta vakavasti, sillä ne voi laajuudestaan tai vahingoistaan huolimatta enteillä tulevia isompia tietoturvaselkkauksia. (Filipec & Plasil 2021.)

Sairaalassa suojattiin tietokoneita virustentorjuntaohjelmaa sekä palomuuria käyttäen, mutta sairaalan käyttämä palomuuri oli vääränlainen sairaalan järjestelmien suojaustarpeisiin verrattuna. Myöskään päätelaitteiden päivityksiä ei ollut pidetty ajan tasalla. Sairaalan verkossa käytettiin myös seurantaprobeja, joiden avulla pystyy tarkkailemaan ja analysoimaan verkkoliikennettä. Sen kautta voi havaita, jos organisaation verkossa tapahtuu jotakin epäilyttävää ja toimii työkaluna myös tietoturvauhkien huomaamisessa. (Filipec & Plasil 2021.)

Monien muiden organisaatioiden tapaan Benešovin sairaalan IT-osastolla ei ollut tarpeeksi henkilöstöresursseja, jotta kaikki lokitiedot ja suoritetut haut olisi saanut tarkistettua (Filipec & Basil 2021). Tietoturvan ylläpitäminen on kokonaisvaltainen ja pitkäaikainen prosessi, joka tulisi ottaa huomioon osana organisaation turvallisuussuunnitelmaa sekä henkilöstöresursseja. Se tulisi ottaa huomioon ja ylläpitää jo ennen tietoturvauhkien todeksi käymistä. Nopeita, halpoja ja yksinkertaisia yhden kerran ratkaisuja ei valitettavasti ole.

Hyökkäyksen yhteydessä sairaalan taisteluna hyökkäystä vastaan IT-tiimi muutti serveriympäristöä vastaamaan minimaalisimpia saatavilla olevia tietoja ja muuttui hyökkäyksen ajaksi takaisin fyysisen tiedon sairaalaksi. Samaan aikaan se joutui myös rajaamaan tarjoamiaan sairaalapalveluita. (Filipec & Basil 2021.)

Sairaalan IT-tiimi oli pitänyt huolta verkkoympäristön varmuuskopioinneista päivittäisellä tasolla, joten jo muutaman päivän jälkeen hyökkäyksestä salattua dataa päästiin palauttamaan varmuuskopioiden avulla. Vanha palomuuri korvattiin myös uudella, joka mahdollisti datan fragmentoinnin. (Filipec & Basil 2021.) Fragmentoinnilla tietoturvan yhteydessä tarkoitetaan yleensä suuren datan jakamista erillisiin osiin. Hyvä palomuuri voi olla fragmentoinnissa tärkeä työkalu.

Tarkkaa haittaohjelman saastuttamisajankohtaa ei tiedetty, joten National Cyber and Information Security Agency neuvoi sairaalaa aloittamaan tyhjältä pöydältä ja kohtelemaan varmuuskopioituja tietoja saastuneina niin kauan, kun saastuttamisajankohta selviäisi varmaksi. Neljä päivää hyökkäyksen jälkeen IT-osasto oli asentanut puhtaan, turvallisen serverin, johon varmuuskopiot saatiin tuotua sen jälkeen, kun oli varmistettu, että ne ovat puhtaita. (Filipec & Basil 2021.)

3.1.3 Vastaamo

Syksyllä 2020 tuli julki, että psykoterapiakeskus Vastaamon potilastietoja vuodettiin pimeään verkkoon vuoden 2019 tietomurtojen seurauksena, jossa kiristäjä nimimerkillä Ransom_man ei ollut saanut kiristämiään lunnaita Vastaamolta. Kiristäjä uhkasi myös Vastaamon asiakkaita ja vaati lunnaita, jotka saatuaan salaisi aina kyseisen asiakkaan tiedot. Kiristäjä uhkasi vuotaa henkilötietojen lisäksi asiakkaista myös potilaskertomukset. Psykoterapiakeskuksen ollessa kyseessä, ollaan erittäin arkaluonteisen tiedon äärellä potilaskertomustenkin kanssa, joka voi pahimmassa tapauksessa tuhota elämiä päästessään julkisesti saataville. (Kortesoja 2022.)

Vastaamon palvelimen portti oli jätetty yli vuodeksi auki ja palvelimen pääkäyttäjälle ei ollut asetettu salasanaa, jolloin palvelimelle sisäänpääsyn jälkeen normaali käyttäjä pääsi muuttamaan oman statuksensa pääkäyttäjäksi. Palvelimen pääkäyttäjän käyttöoikeudet ei ollut rajattuja. Potilastietokannan tiedot olivat

myös yhdistettävissä potilaisiin eli tiedot eivät olleet anonymisoituja. (Tietosuojakeskus s.a.)

3.1.4 Lontoon kesän 2024 kyberiskut sairaaloihin

Kesäkuussa 2024 usean sairaalan järjestelmiin kohdistui niihin kohdennettu kyberisku. Hyökkäys kohdistui Synnovikseen, joka tarjoaa patologisia palveluita. Iskun takia sairaalat joutuivat perumaan leikkauksia, verikokeita sekä verensiirtoja. (Gecsoyler & Milmo 2024.) NHS:n mukaan kyseessä oli kiristyshaittaohjelmahyökkäys (NHS England 2024). Hyökkääjät väittivät päässeensä Synnoviksen järjestelmiin nollapäivähaavoittuvuuden kautta (Alder 2024).

Nollapäivähyökkäyksessä hyökkääjä hyödyntää järjestelmän tietoturvahaavoittuvuutta, jonka hyökkääjä löytää ennen järjestelmän kehittäjää. Hyökkäyksen avulla pystyy tuottamaan vahinkoa järjestelmiin sekä sen kautta pystyy varastamaan arkaluonteista dataa. Hyväksikäytettyjä, joskin jo korjattuja nollapäivähaavoittuvuuksia on löydetty jokaiselle jo arjenkin tutuista tuotteista, kuten esimerkiksi Chromesta, Zoomista ja Applen iOS-käyttöjärjestelmistä. (Kaspersky s.a. a.)

3.2 Kalasteluviestit ja niiden eri muotojen tunnistaminen

Kalasteluviestien kautta hyökkääjä yrittää kerätä arkaluonteista tietoa kohteeltaan, useimmiten käyttäjä- tai pankkitunnuksia. Nykyään kalasteluviestejä löytyy jo monia erilaisia. (Fortinet s.a. b.)

Useissa huijausyrityksissä, jotka ovat liitoksissa nettisivuihin, kannattaa tarkistaa SSL/TLS-sertifikaatti. SSL/TLS-sertifikaatin avulla käyttäjä pystyy varmentamaan, että hän on oikealla nettisivulla ja SSL/TLS suojaa tietoliikennettä sivuston ja käyttäjän välillä. SSL/TLS-sertifikaatti mahdollistaa organisaatiolle HTTPS:n käytön, joka varmistaa suojatun tiedonsiirron. Kaikkien nykyajan nettisivustojen tulisi käyttää HTTPS-suojausta. Selaimet kertovat, jos olet siirtymässä suojaamattomalle sivustolle (HTTP) ja varmistavat, että haluatko varmasti siirtyä sivulle. Lähtökohtaisesti HTTP-sivustoja ei kannata käyttää, sillä tietoliikenteen suojausta ei pysty varmistamaan ilman HTTPS-suojausta. (Cloudlfare.)

HTTP-yhteydellä olevat sivustot ovat alttiimpia myös sellaisille hyökkäyksille, joissa tietoliikenteen kaappauksen lisäksi hyökkääjä voi lisätä esimerkiksi ylimääräisiä, sivustolle kuulumattomia mainoksia, seurantakoodeja tai huijauslinkkejä sivustolle Man-in-the-middle-hyökkäyksen tapaan. (Cloudflare s.a. a.)

Osana joitain tietojenkalasteluja saatetaan myös hyödyntää liitteitä levittääkseen haittaohjelmaa. Esimerkiksi Microsoft Officen sovelluksissa hyödynnetään makroja ja niitä voi myös hyökkääjät kirjoittaa vahingoittaakseen järjestelmiä, varastaakseen dataa tai sisällyttääkseen dokumenttiin haittaohjelman. Vahingolliset makrot ovatkin yksi isoin uhka Microsoft Officen sovelluksissa, joita edelleen hyökkääjät hyödyntävät. (NCSC s.a.)

Makrot yhdessä tietojenkalastelun ja sosiaalisen manipuloinnin kanssa toimii tehokkaana hyökkäystapana, jonka avulla hyökkääjä voi saada käyttäjän hyväksymään makrot niitä sen enempää miettimättä tai niitä tuntematta. (NCSC s.a.)

Osa organisaatioista hyödyntää makroja, jotta päivittäiset työaskareet sujuvat jouhevammin, mutta jos organisaatiossa tai yksilönä ei ole tarvetta makrojen käyttämiselle, niin ne kannattaa laittaa pois päältä. Microsoft Officen työkaluissa kannattaa myös muistaa sovellusten päivittäminen aina viimeisimpään päivitykseen, jotta sovellusten tietoturva pysyy ajan tasalla. (NCSC s.a.)

Uteliaisuus ja kalasteluviestien kiireellisyydentuntu ovat PhishMen tekemän raportin mukaan toimineet triggeröivinä tekijöinä tietojenkalasteluihin vastatessa. Harkitun päätöksen sijaan ihmiset, jotka kalasteluviesteihin lankeavat, saattavat tehdä päätöksen tunteen perusteella. Myös stressi ja etenkin pitkittynyt stressi vähentää mahdollisten seurauksien harkitsemista päätöksenteossa, myös siis kalasteluviestien kohdalla. (Gururaj, Janhavi & Ambika 2024.)

3.2.1 Kohdennettu tietojenkalastelu

Kohdennettu tietojenkalastelu tunnetaan englanniksi nimellä spear phishing. Hyökkääjän hyödyntäessä kohdennettua tietojenkalasteluja, hän kohdentaa hyökkäyksen johonkin tiettyyn organisaatioon tai henkilöön. Hyökkääjä kerää mahdollisimman paljon tietoa kalastelun kohteestaan, jotta hyökkääjästä

muodostuu mahdollisimman luotettava kuva. Luottamuksen muodostumisen jälkeen hyökkääjän tarkoituksena on hyväksikäyttää luottamusta ja tavoitteena on saada hyökkäyksen kohde syöttämään tietojaan esimerkiksi kalastelulinkin kautta. (Fortinet s.a. b.)

3.2.2 Ääntä hyödyntävä tietojenkalastelu

Ääntä hyödyntävällä tietojenkalastelulla eli voice phishingilla tarkoitetaan sitä, kun hyökkääjä puhelimen välityksellä tekeytyy esimerkiksi hyökkäyksen kohteen läheiseksi tai työkaveriksi saadakseen kalastelemansa tiedot. (Fortinet s.a. b.)

3.2.3 Tietojenkalastelu sähköpostilla

Sähköpostikalastelulla hyökkääjä lähettää esimerkiksi jonkin organisaation nimissä organisaation virallista sähköpostiviestiä mukailevan viestin hyökkäyksen kohteelle. Sähköpostikalastelun avulla yritetään saada hyökkäyksen kohde esimerkiksi kalastelulinkin kautta syöttämään tietojaan, jotka hyökkääjä voi myydä eteenpäin tai hyväksikäyttää tietoja muuten itse. (Fortinet s.a. b.)

3.2.4 HTTPS-kalastelu

HTTPS-kalastelu toimii samalla tapaa kuin sähköpostikalastelu, mutta sähköpostin sijaan viestialustana saattaa toimia mikä vain, esimerkiksi sosiaalisen median alustat. (Fortinet s.a. b.)

3.2.5 Pharming-kalastelu

Pharming-kalastelulla tarkoitetaan tietoturvahyökkäystä, jossa hyökkääjä käyttää erilaisia tekniikoita, joiden avulla sivusto ohjaa käyttäjän väärennetylle verkkosivustolle, vaikka käyttäjä syöttäisi osoitteen oikein. Näin hyökkääjä yrittää saada sivuston käyttäjien tietoja, kuten esimerkiksi salasanoja, pankkitunnuksia tai muuta henkilökohtaista tietoa. (Proofpoint s.a. a.)

3.2.6 Ponnahdusikkunakalastelu

Ponnahdusikkunakalastelun eli pop-up phishingin kohdalla tietoturvarikolliset saattaa saastuttaa esimerkiksi tietoturvaltaan heikkoja sivustoja ponnahdusikkunoilla, joiden kautta yrittää saada käyttäjän tietoja tai saada käyttäjä lataamaan jotakin, joka onkin haittaohjelma. (Hardy 2018.)

3.2.7 Evil Twin -kalastelu

Evil Twin -kalasteluhyökkäys kohdistuu Wi-Fi-verkkoihin, useimmiten jäljitellen julkista Wi-Fi-verkkoa. Hyökkääjä pistää pystyyn väärennetyn Wi-Fi-verkon jäljitellen jonkin todellisen Wi-Fi-verkon tietoja siinä toivossa, että ihmiset yhdistää väärennettyyn verkkoon. Hyökkääjän tavoitteena on tälläkin hyökkäyksellä varastaa hyökkäyksen kohteen tietoja. (Ledesma, 2023.)

Evil Twin -hyökkäystä on vaikea tunnistaa, sillä verkkoihin yhdistäessä käyttäjä näkee yleensä vain verkon nimen. Verkon lisätietoja pääsee tarkastelemaan laitteella vasta siinä kohtaa, kun verkkoon on jo yhdistänyt. Ennen verkkoon yhdistämistä väärennetty Wi-Fi-verkko on lähes mahdotonta tunnistaa oikeasta ja todennäköisyys yhdistää väärään verkkoon on yksi kahdesta. Hyökkääjä pystyy tukkimaan myös oikean verkon palvelunestohyökkäyksillä, jolloin hän epäsuorasti ohjaa käyttäjän käyttämään toista saatavilla olevaa verkkoa, joka tässä tapauksessa olisi väärennetty verkko. (Ledesma, 2023.)

Väärennetyssä verkossa hyökkääjä pystyy seuraamaan käyttäjän toimintaa internetissä sekä pitämään kirjaa käyttäjän näppäinten painalluksista. Myös tämän kalasteluhyökkäyksen avulla hyökkääjä pystyy injektoimaan käyttäjän koneelle haittaohjelman, jonka avulla hyökkääjä saa pahimmassa tapauksessa etänä kontrollin käyttäjän laitteesta. (Ledesma, 2023.)

Käyttäjä voi varovaisen verkkoon yhdistyksen avulla välttää evil twin -hyökkäystä. Automaattinen Wi-Fi-verkkoon yhdistäminen kannattaa ottaa laitteesta pois päältä, nimittäin laitteet yhdistävät verkkoihin verkon nimen perusteella. Automaattinen yhdistäminen saattaisi siis vahingossa yhdistää suoraan

väärennettyyn verkkoon. Kannattaa myös välttää käyttämästä julkista Wi-Fi-verkkoa ja sen sijaan käyttää esimerkiksi oman puhelinliittymän mobiilidatan hotspot-yhteyttä. (Ledesma, 2023.)

3.2.8 Vesiaukkohyökkäys

Vesiaukko- eli watering hole -kalasteluhyökkäys kohdistuu tietyn sivun käyttäjäryhmään. Hyökkääjät yrittävät saastuttaa valitsemansa kohderyhmän usein käyttämän sivun ja tätä kautta saada pääsyn esimerkiksi organisaation verkkoon. Vesiaukkohyökkäykset kohdistuvat yleensä organisaatioihin yksityishenkilöiden sijaan. (Fortinet s.a. c.)

3.2.9 Whaling -kalastelu

Whaling -hyökkäyksessä tietoturvarikolliset valitsevat kohteekseen jonkun korkean position henkilön kohdentaakseen hyökkäyksen häneen. Hyökkääjät hyödyntävät muita kalastelumenetelmiä osana whaling -menetelmää saadakseen haluamansa tiedot käyttäjältä tai saadakseen pääsyn kohteen laitteeseen. Whaling -hyökkäyksen tunnistaa yleensä esimerkiksi oudosta sähköpostiosoitteesta ja organisaation verkon ulkopuolelta tulevat sähköpostit kannattaisi merkata verkon ulkopuolelta tuleviksi, jos organisaation sähköpostissa on siihen mahdollisuus. (Kaspersky s.a. c.)

3.2.10 Kloonauskalastelu

Kloonauskalastelussa hyökkääjä kopioi jonkin käyttäjän jo saaman viestin ja lähettää sen uhrille uudelleen lisäten viestiin esimerkiksi haitallisen linkin. Viestit lähetetään yleensä niin, että ne näyttävät jatkoviesteiltä edellisiin viesteihin. Kloonauskalastelun voi tunnistaa vertaamalla sähköposteja. Käyttäjän kannattaa tarkistaa onko toinen viesti tullut samasta sähköpostiosoitteesta kuin aiempikin viesti. (Proofpoint s.a. b.)

3.2.11 Deceptive phishing -kalastelu

Deceptive phishing on yleisin tietojenkalastelun muoto. Hyökkääjät tekeytyvät uhrin luottamaksi tahoksi, useimmiten joksikin organisaatioksi. Viesteissä on yleensä kiireen tuntu ja hyökkääjät yrittävät ohjata uhrin esimerkiksi väärennetylle verkkosivulle, jonka kautta se saa uhrin henkilökohtaisia tietoja, kuten vaikka pankkitunnukset. (Fortinet s.a. b.)

3.2.12 Tietojen kalastelu sosiaalisessa mediassa

Angler phishing -kalastelussa hyökkääjä esittäytyy tietyn organisaation asiakaspalveluhenkilönä. Hyökkääjän kohderyhmää ovat todellisen organisaation asiakkaat, jotka ovat sosiaalisen median kanavissa ilmaissut tarpeensa asiakaspalvelun kontaktoimiseen. Tällaiselta kalastelulta pystyy välttymään ottamalla itse yhteyttä organisaatioon muuta väylää pitkin ja tarkistamalla onko viesti tullut samalta tililtä, johon käyttäjä alun perin kommentoikin. (Waugh 2025.)

3.2.13 Tekstiviestikalastelu

Smishing -kalastelulla tarkoitetaan tekstiviestikalastelua. Niiden avulla hyökkääjä lähettää tekstiviestejä, joissa on joku haitallinen linkki tai yrittää saada arkaluonteisia tietoja. Viestit tulevat usein luotettavalta taholta. Tekstiviestikalastelun aiheuttamalta vahingolta voi välttyä sillä, että ei esimerkiksi avaa epäilyttäviä linkkejä viestien kautta ja tarkistaa ennemmin organisaation sivuilta verkkoselaimen kautta omalta tililtä, jos siellä on mahdollisesti jotain huomioitavaa. (Kosinski 2024.)

3.2.14 Man-in-the-middle -hyökkäys

Man-in-the-middle -hyökkäyksessä hyökkääjä saa pääsyn kahden osapuolen viestiketjuun ja keskustelun oikeat osapuolet eivät huomaa hyökkäystä mistään. Hyökkääjä pystyy esittäytymään tällöin toisena osapuolena viestiketjussa ja varastamaan osapuolten dataa. (Fortinet s.a. d.)

3.2.15 Verkkosivuhuijaus

Verkkosivuhuijauksessa kalastellaan uhrien tietoja luomalla väärennetty kopio jonkin organisaation sivusta, jonka kautta saadaan kerättyä käyttäjien tietoja. (Fortinet s.a. b.)

3.2.16 Domain-huijaus

Domain spoofing -kalastelulla eli domain-huijauksessa tarkoitetaan kalastelua, jossa väärennetään sivuston nimi tai esimerkiksi sähköpostiosoite, jotta ne näyttäisivät käyttäjälle turvallisilta käyttää ja luottaa niihin. Tämän kalastelun tavoitteena on saada käyttäjän henkilökohtaisia tietoja, pankkitunnuksia, saada käyttäjä lähettämään rahaa hyökkääjille tai lataamaan haittaohjelma. (Cloudflare s.a. b.)

Domain-huijaukselta välttyäkseen kannattaa kiinnittää huomiota URL-osoitteeseen ja jos siinä on esimerkiksi ylimääräisiä merkkejä, joita ei tulisi olla verrattuna aiempaan käyttäjän käyttämään organisaation URL-osoitteeseen. (Cloudflare s.a. b.)

Domain-huijauksessa saatetaan myös hyödyntää homograph-hyökkäystapaa (Cloudflare s.a. b.). Homograph-hyökkäyksessä hyökkääjä on luonut väärennetyn verkkosivuston URL-osoitteella, jossa hyödynnetään normaaleilta kirjaimilta näyttäviä Unicode-merkkejä. Nykyään selaimen tulisi ilmoittaa käyttäjälle sivustosta, jolla käytetään kyseisenlaisia merkkejä normaalien kirjaimien tai merkkien sijaan. (Umawing 2017.)

Homograph-hyökkäystavat ei ole vain yksityishenkilöitä koskettava uhka, vaan ne uhkaavat myös samalla organisaatioita. Organisaatioille uhka liittyy väärennettyjen nettisivujen lisäksi myös mainehaittaan. (Network Solutions Team 2020.)

Domain-huijaus sisältää myös organisaatioihin ja yksityishenkilöihin kohdistuvia mainoshuijauksia (ad spoofing). Huijarit saattavat käyttää hyödykseen esimerkiksi hakukoneiden mainostilaa yrittäen saada käyttäjät jakamaan tietonsa

hyökkääjille kyseisen mainoksen ja väärennetyn sivuston kautta. (Insurance Fraud Bureau s.a.)

Käyttäjä saa suojattua itsensä mainoshuijauksilta jättämällä hakukoneiden mainostilan huomiotta. Hakukoneiden mainosten kautta ei koskaan kannata klikkailla sivustoille. Myös URL-osoite kannattaa aina tarkistaa, että vastaako se URL-osoitetta, joka on aiemmilla asiointikerroilla ollut. Lähtökohtaisesti säännöllisesti käytettävät sivustot kannattaa tallentaa selaimen kirjanmerkkeihin eikä mennä niihin aina hakukoneiden kautta. (Insurance Fraud Bureau s.a.)

3.2.17 Kuvakalastelu

Image phishing eli kuvakalastelussa käytetään kuvia tietojenkalastelun päätyökaluna. Tällaisessa kalasteluyrityksessä teksti on laitettu kuvamuotoon, jolloin tietoturvaohjelmat ei tunnista viestiä roskapostiksi. (Alibe s.a.)

3.3 Sosiaalinen tietoturva

Sosiaalinen manipulointi on tietoturvauhista haastavin, sillä siltä ei voi suojautua erinäisten tietokoneohjelmien avulla. Teknologian ja suojausmenetelmien kehittyessä hyökkääjät ottavat käyttöön uusia menetelmiä, joilla päästä suojausten läpi. (Gururaj ym. 2024.)

Hyökkääjät yrittävät sosiaalisen manipuloinnin avulla saada toinen osapuoli paljastamaan arkaluonteista tietoa ja rikkoa erinäisiä turvallisuusmääräyksiä. Tällaista hyökkäystä saattaa olla myös vaikea huomata organisaation sisällä. (Gururaj ym. 2024.)

Sosiaalisessa manipuloinnissa hyökkääjien tapana on usein herättää ja kerätä luottamusta vastapuolessa, jotta he saavat hyväksikäytettyä heitä joko teoin tai tietojen kautta. Jos hyökkääjät toimisivat aggressiivisemmin, herättäisi se luultavasti huomion ja kysymysmerkkejä uhrissa. (Gururaj ym. 2024.)

Hyökkääjät hyödyntävät kaikkia mahdollisia tietolähteitä kerätäkseen tietoa. Kaikki julkisesti saatavilla oleva tieto esimerkiksi yrityksen nettisivuilla, uutisissa

tai sosiaalisessa mediassa voi toimia tietolähteenä hyökkääjille. Tämän takia organisaatiolla sekä sen henkilöstöllä tulisi olla tarkat käytännöt sen suhteen, että mitä julkisesti saa jakaa organisaatiosta tai omista työtehtävistään. Sosiaalisen manipuloinnin hyökkäys voi tulla myös mitä kautta vaan; kasvotusten, sähköpostilla tai sosiaalisen median kautta. (Gururaj ym. 2024.)

Open Source Intelligence eli OSINT-hyökkäyksissä voidaan osana hyökkäystä hyödyntää erilaisia julkisia saatavilla olevia lähteitä keräämään organisaatiosta tietoa. Tämän takia organisaatioissa tulisikin kiinnittää huomiota ja kouluttaa työntekijöitä siitä, että mitä yrityksestä saa jakaa julkisissa lähteissä. Työntekijän tulisi myös ymmärtää, että yksittäisenä tietona harmittomaltakin vaikuttava tieto työnantajasta, voi olla avuksi organisaatioon kohdistetussa hyökkäyksessä. (Gururaj ym. 2024.)

Organisaation tai yksittäisen henkilön tietoturvakoulutuksen yhteydessä esille nostettavia teemoja voisi olla sellaiset asiat, kuten miten työntekijän jakamaa julkista tietoa voidaan hyväksikäyttää hyökkääjien toimesta, mitä henkilötietoja ei tulisi jakaa julkisesti, käydä läpi sosiaalisen median yksityisyysasetuksia sekä miten siellä tulisi toimia tiedon jakamisen kanssa ja korostaa myös organsiaation omia tietoturvakäytäntöjä, jos tietoturvakoulutus on kohdennettu tietylle organisaatiolle.

Tapoja, miten hyökkääjä pystyy hyödyntämään työntekijöiden antamia tietoja, ovat muun muassa erinäiset palvelut, joihin voi arvostella työnantajia. Yhdysvalloissa tällaisena palveluna on toiminut Glassdoor-niminen verkkosivusto. (Gururaj ym. 2024.) Suomessa vastaava palvelu oli aikoinaan Tunto, mutta sen käyttö lakkautettiin (Alma Media Oyj 2019). Palvelut ovat lähtökohtaisesti tarkoitettu työntekijöitä varten ja heidän tueksi, mutta tieto on saatavilla tuota kautta myös heillekin, jotka saattavat tietoja käyttää hyväksi.

OSINT-hyökkäyksissä hyödynnettävänä työkaluna hyökkääjillä saattaa olla myös palveluita, joiden avulla hyökkääjä pystyy tarkistamaan joko organisaation tai yksittäisen henkilön käyttäjänimen, että onko se käytössä eri sosiaalisen median alustoilla tai verkkosivustoilla. Eli jos hyökkääjällä on tiedossa jokin työntekijän käyttäjätunnuksista, niin tuota kautta hyökkääjä löytää muut samalla nimimerkillä

olevat tilit. Tällä tavoin eri palveluissakin olevia tiedonmuruja hyökkääjä pääsee helposti hyväksikäyttämään isompana kokonaisuutenakin. (Gururaj ym. 2024.)

Hyökkääjien yhtenä tekniikkana on myös Google dorking tai vastaavasti Google hacking, jossa käytetään Googlen hakutoimintoja, joiden avulla hyökkääjä löytäisi esimerkiksi piilotettua tietoa. (Gururaj ym. 2024.)

Organisaation indeksoidessaan verkkosivunsa osaksi Google-hakua, Google saa pääsyn myös sellaisiin osiin organisaatioiden verkkosivuissa, joita normaali internetin käyttäjä ei näe. Google dorkingin tai Google-hakkeroinnin avulla hyökkääjä käyttää hyödyksi tätä haavoittuvuutta. Tällä tavalla hyökkääjät saattavat myös löytää heikkoja nettisivuja, joihin hyökätä. Sen kautta hyökkääjä saattaa myös pahimmassa tapauksessa saada pääsyn organisaation servereille tai vaikka tiedostoihin. (Gururaj ym. 2024.)

3.4 Tekoäly

Tekoälyä hyödynnetään sosiaali- ja terveysalalla jo useissa eri paikoissa. Sairauksien diagnosointi, potilaiden seuranta sekä terveydenhuollon resurssien suunnittelu ovat tänä päivänä osittain tekoälyavusteisia. (Alvarez & Tiainen 2023.) Tässä osassa keskitytään enemmän tekoälyn tietoturvapuoleen sekä siihen, mitä työntekijän tulisi ottaa huomioon, kun käytetään palveluja, joissa viestitään tekoälyn kanssa.

Tietoturvan kannalta tekoälyn kanssa kannattaa muistaa olla laittamatta mitään arkaluonteista tietoa tekoälyn kanssa keskustellessa. Esimerkiksi kuluttajakäyttöön tarkoitettu ChatGPT käyttää viestiprompteja koulutusmateriaalina tekoälylle, joten tällöin mahdolliset arkaluonteiset tiedot voivat vuotaa eteenpäin. Jos siis käyttää tekoälyä arkaluonteisemman tiedon kanssa viestimiseen, niin kannattaa tarkistaa, että viestejä ei käytetä tekoälyn koulutuskäyttöön tai olla tietoinen mahdollisista muista riskeistä, joita siihen liittyy. Hyvänä ohjenuorana on olla jakamatta tekoälylle mitään, mitä ei voisi jollekin organisaation ulkopuoliselle henkilölle jakaa ilman luottamuksellisen tiedon vaarantumista. (Sekine 2024.)

Tekoälyn avulla pystyy luomaan myös deepfake-tekniikkaa hyödyntäen todellista kuvaa tai ääntä luodakseen uutta ja väärennettyä todentuntuista kuvaa tai ääntä. Tällä tuodaan ihan uusi ulottuvuus eri tiedonkalastelukeinoihin. Deepfake-materiaalia luodaan tekoälytyökalun avulla, jolle esimerkiksi ChatGPT:n viestien tapaan syötetään kuvia ja videoita kouluttaen työkalua haluttuun lopputulokseen. Kyseisenlaisen tekoälyn neuroverkkotyön perusteella iso edistysaskel, mutta joissain tapauksissa lopputuloksen puolesta saattaa olla pelottavakin edistysaskel, jota voidaan hyödyntää myös pahoihin tarkoituksiin. (University of Virginia s.a.)

3.5 Lainsäädäntö

Potilastietojen käsittelyyn liittyy sosiaali- ja terveysalallakin useita eri säädöksiä, joiden mukaan tulee toimia henkilötietoja käsitellessä. Yleinen tietosuoja-asetus (GDPR), tietosuojalaki, laki potilaan asemasta ja oikeuksista, laki sosiaalihuollon asiakkaan asemasta ja oikeuksista sekä laki asiakas- ja potilastietojen sähköisestä käsittelystä. (Valvira s.a.)

Tietosuojalaki täydentää Euroopan yleistä tietosuoja-asetusta. Tietosuojalaissa on määrätty muun muassa tietosuojavaltuutetun nimittämisestä organisaatiossa sekä tietosuojavaltuutetun toimivaltuuksista. Tämän lisäksi tietosuojalaissa on säädetty rekisteröidyn oikeuksista, ikärajasta henkilötietojen käsittelyn suostumukseen sekä mahdollista haittaa tai jopa syrjintää aiheuttavien henkilötietojen käsittelystä. Tietosuojalain mukaan ihmisen henkilötietoja voidaan käsitellä kumminkin ilman henkilön omaa suostumusta journalistisessa, taiteellisessa, akateemisessa tai kirjallisessa mielessä, kunhan tieto ei ole harhaanjohtavaa. Henkilön lupaa ei tarvitse myöskään poikkeustilanteissa, joissa esimerkiksi viranomaiset tarvitsevat henkilötietoja. Tietosuojalaki suojaa myös henkilötunnuksen käsittelyä. (Tietosuojavaltuutetun toimisto s.a. a.)

Jos organisaatiossa käsitellään arkaluonteisia tietoja, seurataan ihmisiä tai organisaatio on julkishallinnon toimija, tulee organisaatioon nimittää tietosuojavastaava. Organisaation työntekijöiden lisäksi myös organisaation ulkopuolisilla henkilöillä tulee olla mahdollisuus olla yhteydessä organisaation

tietosuojavastaavaan, joten tietosuojavastaavan yhteystiedot tulisi olla julkisesti saatavilla. Organisaatioon valittu tietosuojavastaava tulisi ilmoittaa tietosuojavaltuutetun toimistoon. (Tietosuojavaltuutetun toimisto s.a. b.)

Rekisteröidyn oikeuksiin kuuluu mahdollisuus saada tietoa omien henkilötietojen käsittelystä, päästä lukemaan tiedot, oikaista tai poistaa tietoja sekä oikeus tulla unohdetuksi. Näiden lisäksi rekisteröidyllä on oikeus rajoittaa omien tietojensa käsittelyä, siirtää halutessaan tiedot muualle, vastustaa tietojen käsittelyä sekä oikeus vaatia, että hänestä tehtävät päätökset eivät voi olla pelkästään automaattisia. (Tietosuojavaltuutetun toimisto s.a. c.)

Rekisteröidyn oikeudet näkyvät siis sosiaali- ja terveysalalla niin, että henkilöllä on oikeus päästä käsiksi omiin potilas- tai asiakastietoihinsa.

Oikeus unohtaa potilas- ja asiakastiedot ovat rajoitettuja vedoten lain potilaan asemasta ja oikeuksista lukuun neljä ja pykälään kaksitoista. Terveydenhuollon yksiköiden on säilytettävä laadittuja asiakirjoja sosiaali- ja terveysministeriön määräysten mukaisesti, jolloin rekisteröidyn tiedot voidaan poistaa vasta määrätyn säilytysajan päätyttyä. (Finlex s.a. a.)

Sosiaali- ja terveysalalla oikeus henkilötietojen käsittelyn rajoittamisesta on sovellettu vain pyyntöön virheellisten tietojen oikaisusta.

Laki sosiaali- ja terveysalan asiakastietojen käsittelystä määrää muun muassa asiakastietojen salassapidosta, vaitiolovelvollisuudesta, asiakastietojen käsittelystä, käyttöoikeuksista sekä tiedon käytön ja luovutuksen seurannasta. Useat näistä koskevat myös sosiaali- ja terveydenhuoltoalan rivityöntekijöiden päivittäistä työarkea. (Finlex s.a. b.)

Asiakas- ja potilastietojen salassapidolla tarkoitetaan asiakastietoja sisältävää asiakirjaa ja sen sisältöä ei saa missään muodossa näyttää tai luovuttaa sellaiselle henkilölle, joka ei vastaa tai osallistu potilaaseen tai asiakkaaseen liittyviin tehtäviin. Terveydenhuollon yksiköissä asiakkaan ja potilaan tietoja saa käsitellä sellainen työntekijä, jolle se on välttämätöntä potilaan tai asiakkaan oikeanlaisen hoidon toteuttamiseksi. Salassapitovelvollisuudesta saa poiketa vain muussa laissa määrätyin ehdoin tai asiakkaan omasta suostumuksesta. (Finlex s.a. b.)

Asiakas- ja potilastietoja käsittelevällä työntekijällä on lain mukaan vaitiolovelvollisuus. Se siis tarkoittaa sitä, että työntekijällä on lain mukaan määrätty velvollisuus pitää salassa työssä tai muussa toimeksiannossaan käsittelemiään asiakas- tai potilastietoja. Vaitiolovelvollisuus on voimassa edelleen työsuhteen päättymisenkin jälkeen. Vaitiolovelvollisuudesta saa poiketa vain muussa laissa määrätyin ehdoin tai asiakkaan omasta suostumuksesta. (Finlex s.a. b.)

Työnantajan tulee huolehtia oikeanlaisten käsittelyohjeiden tiedoksi antamisesta sekä kouluttamisesta työntekijöilleen. (Finlex s.a. b.)

Käyttöoikeus asiakas- tai potilastietoon määrittelee millä perustein tietoja saa käyttää. Yleisenä linjauksena tietojen käyttö on rajoitettu tietoihin, joita työntekijä tarvitsee hoitaakseen työnsä tai potilasta asianmukaisesti. Ne tiedot, jotka ulottuvat tarpeen ulkopuolelle, ovat myös työntekijän käyttöoikeuden ulkopuolella. (Finlex s.a. b.)

Asiakas- ja potilastietojen käsittelyä ja luovutusta seurataan. Tietojen käsittelystä sekä luovutuksesta tulee lain mukaisesti pitää käyttölokirekisteriä. Yksittäistä työntekijää tämä koskee siinä määrin, että käyttölokirekisteriin tulee maininta tietojen käyttäjästä, käyttötarkoituksesta, käyttöajankohdasta sekä ketkä ovat katsoneet tai muuttaneet tietoja. (Finlex s.a. b.)

3.6 Millainen merkitys työntekijällä on tietoturvaprosessissa?

Työntekijällä on organisaation tietoturvaprosessissa iso merkitys. Järjestelmiä käyttävät aina lähtökohtaisesti ihmiset, joiden tietotekniset taustat ovat kovin erilaisia. Tietoturva ei ole yksinomaan organisaation tietoturvavastaavan tai -asiantuntijoiden harteilla, vaan jokainen työntekijä kohtaa päivittäisessä työssään tietoturvaan liittyviä asioita ja valintoja. (Kyberturvallisuuskeskus 2023.)

Oikeanlaisella tietoturvakoulutuksella ja selkeillä organisaation antamilla toimintamalleilla organisaatio pystyy minimoimaan tietoturvaan liittyviä vahinkoja sekä nostamaan tietoturvatietoisuutta isommaksi prioriteetiksi työntekijöidenkin arjessa. (Kyberturvallisuuskeskus 2023.)

3.7 GDPR

Euroopan yleisen tietosuoja-asetuksen eli GDPR:n mukaan jokaisen Euroopan maan kansalaisen kohdalla tulisi toteutua perusoikeus henkilötietojen asianmukaisesta käsittelystä yksityisyyttä kunnioittaen ja noudattaen varovaisuutta. Yleisessä tietoturva-asetuksessa otetaan myös huomioon sananvapaus sekä turvallisuus, jolloin henkilötietojen suojaaminen ei ole rajoitettua. (Euroopan Unioni 2016.)

GDPR:n avulla halutaan myös taata henkilötietojen turvallinen liikkuminen maasta toiseen Euroopan sisällä sekä omien tietojen valvominen. Tietosuoja-asetuksessa korostetaan myös rekisteröityjen oikeuksia sekä tietorekisterien pitäjien velvollisuuksia. Asetuksen avulla halutaan varmistaa kansalaisuudesta riippumatta yhdenvertainen suoja luonnollisen henkilön tiedoille Euroopan sisällä. (Euroopan Unioni 2016.)

3.7.1 Mikä vaikutus GDPR-ohjeistuksilla on yksittäisen työntekijän työhön?

Yksittäisen työntekijän työhön GDPR-asetus vaikuttaa muun muassa henkilötietojen käsittelyn laadun suhteen. Kaikki potilas- ja asiakastiedot ovat arkaluonteisia tietoja, joten niitä tulee käsitellä harkitusti. GDPR-asetuksen mukaan tietojenkäsittely tulee olla aina läpinäkyvää sekä perusteltua. Työntekijän siis tulee tunnistaa työperäinen tarve jokaiselle hakemalleen henkilötiedolle. (Valvira s.a.)

Euroopan Unionin yleisessä tietosuoja-asetuksessa määrätään myös, että työntekijä saa käsitellä vain niitä tietoja, joita tarvitsevat potilaan hoitamiseen ja tutkimiseen. Käyttöoikeuksien tulee kattaa vain työntekijän työtehtävien puitteissa tarvitsemat tiedot. (Euroopan Unioni 2016.)

3.8 Salasanat

Salasanoilla on suuri merkitys tietoturvan kannalta, ja silti useat toistavat vielä nykyäänkin samoja virheitä salasanaa vaihtaessaan tai valitessaan. Jos ottaa oman ja organisaation tietoturvallisuuden tosissaan, ei tulisi käyttää samoja salasanoja eri palveluissa. Samaa salasanaa käyttämällä pelaa väärän joukkueen pussiin edesauttamalla hyökkääjien työtä ja antamalla pääsyn omiin tileihinsä tarjottimella heille.

Myöskään helposti muistettavista tai edellisistä muunnelluista salasanoista ei ole tietoturvan kannalta hyötyä ja lopputulema saattaa olla sama. Vahva salasana on tärkeä osa myös palveluissa, joissa on usean askeleen autentikointi käytössä eikä salasanaa keksiessään tulisi vetää mutkia suoriksi silloinkaan.

Vahvan salasanan luomisessa käyttäjä joutuu valitsemaan turvallisen salasanan tai sitten käyttäjäystävällisen, helposti muistettavan salasanan välillä. (Kaleta, Lee & Yoo 2019)

Tutkimuksissa on todettu, että vahvan ja turvallisen salasanan luomisen kouluttaminen ihmisille ei tuota haluttuja tuloksia. (Kennison & Chan-Tin 2020.)

3.8.1 Salasanan luominen

Hyvällä salasanalla on kaksi tavoitetta. Salasanan tulee olla uniikki ja tarpeeksi monimutkainen, jotta sitä ei saa hakkeroitua, mutta samaan aikaan sen on oltava tarpeeksi yksinkertainen ja helposti käytettävä arjen käytössä. (Wash & Rader 2021, 1.)

1. Monet tietoturvapalveluntarjoajat suosittelevat vähintään viidentoista merkin salasanoja, jossa pitäisi olla mukana numeroita, isoja ja pieniä kirjaimia sekä välimerkkejä. Salasanaa ei myöskään kannata luoda sanoista, vaan mitä enemmän kielellisesti järjettömämpi salasana, sitä vaikeampi se on hakkeroida. (Das 2023, 1.)
2. Älä uudelleen käytä tai luo uusia versioita samasta salasanasta tai salasanalauseesta. (Das 2023, 1.)

3. Älä käytä helppoja näppäinyhdistelmiä, kuten qwerty tai 1234567 salasanana. (Das 2023, 1.)
4. Turvallinen versio salasanasta on keksiä jokin lause, jonka avulla muistaa salasanansa tinkimättä tietoturvasta ja tehdäkseen hakkereiden työn mahdollisimman vaikeaksi. Ravindra Dasin kirjassa The Zero Trust Framework oli esimerkkinä käytetty lausetta ’The Old Duke is my favorite pub in South London’, jonka mukaan muodostui salasanaesimerkki ’ThOl-DuismyfapuinSoLo’. (Das 2023, 1.)

3.9 Tietoturvaloukkauksen tunnistaminen ja raportoiminen vastuuhenkilölle

Tietoturvaloukkauksella tarkoitetaan tilannetta, jossa henkilötietoihin pääsee luvattomaksi käsiksi joku sellainen, jonka ei kyseisiä henkilötietoja tulisi tai tarvitsisi käsitellä tai jos henkilötietoja tuhoutuu, häviää, muuttuu tai niitä luovutetaan luvattomasti. Tällaisia tilanteita voivat olla esimerkiksi tietoturvahyökkäys sekä varastettu tai hävinnyt tiedonsiirtoväline tai laite. Tietoturvaloukkauksena voidaan siis pitää myös tilannetta, jossa työntekijä katsoo potilastietoja ilman perustetta ja tarvetta esimerkiksi työtehtävien puolesta. (Tietosuojavaltuutetun toimisto s.a. d.)

Tietoturvapoikkeaman voi havaita joko organisaation sisäinen työntekijä tai sitten joku ulkopuolinen palvelua käyttävä taho. Poikkeamatilanteiden ilmoittamisesta tulee sopia käytännön tavat, miten tulisi toimia poikkeaman huomatessaan tai sellaista epäillessään. Järjestelmien seuranta on myös tärkeässä roolissa poikkeamien huomaamisessa. Seuranta tulee olla resursoitua sekä järjestelmällistä. (Valtiovarainministeriö 2017, s. 16-23.)

Organisaation henkilöstö tulee kouluttaa asianmukaisesti tietoturvapoikkeamien havaitsemiseen omassa työssään, toimintatapoihin sekä niistä informoimiseen (Valtiovarainministeriö 2017, s. 16-23.). Poikkeamatilanteista tulisi henkilöstölle kouluttaa tilanteet, joista organisaatiossa poikkeamailmoitus tehdään, mihin henkilöstön tulee ilmoittaa poikkeamasta tai muusta epäilyttävästä toiminnasta, mistä henkilöstö pääsee käsiksi poikkeamatilanteiden toimintaohjeisiin ja keneltä

henkilöstö voi kysyä lisätietoa epäselvissä tilanteissa. (Kyberturvallisuuskeskus 2023.)

3.9.1 Tietoturvallisuuden vastuuhenkilöt organisaatioissa

GDPR edellyttää, että organisaatioissa tulisi olla määrätty tietosuojavastaava, jolloin sama pätee myös sosiaali- ja terveysalan toimijoihin. Tietosuojavastaavaan voi olla yhteydessä henkilötietoihin käsittelyyn liittyvissä asioissa sekä tietosuojaan liittyvien oikeuksien kohdalla. Organisaation tietosuojavastaavan yhteystiedot tulisi olla helposti saatavilla myös julkisesti. (Tietosuojavaltuutetun toimisto s.a. e.)

Tietosuojavastaavan tulisi olla tietoinen tietoluojalainsäädännöstä sekä käytännöstä, jotta hän suoriutuu tietosuojavastaavan tehtävistään. Sen lisäksi tietosuojavastaava seuraa, että organisaatio noudattaa tietosuojaan liittyvää lainsäädäntöä ja tekee siitä omavalvontaa. Tietosuojavastaavan tehtäviin kuuluu myös organisaation työntekijöiden ohjeistaminen ja kouluttaminen tietosuoja-asioihin liittyen. (Tietosuojavaltuutetun toimisto s.a. b.)

Tietoturvavastaava tai tietoturvapäällikkö valvoo joko tiimin voimin tai osana omia työtehtäviään teknisiä toimintoja ja ympäristöjä, ylläpitää järjestelmien ja laitteiden tietoturvaa sekä tietoturvaohjelmia, pitää tietoturvakäytännöt työntekijöiden tiedossa. Tehtäviin kuuluu myös lakien ja säädösten noudattamisen seuraaminen sekä organisaation tietoturvakäytänteiden arviointi ja tietoturvan huomioiminen organisaation liiketoimintaprosesseissa. (Cisternelli 2024.)

4 TIETOTURVAKOULUTUKSEN KEHITTÄMINEN

Opinnäytetyön toiminnallinen osuus lähti käyntiin tietoturvakoulutuksen alustavien kustannusten selvittämisellä. Testattavaksi lähtikin datatiedoston sekä tekoälyn ohjeistuksen yhdistäminen, mikä tiedonhaun jälkeen osoittautui kustannuksiltaan tehokkaimmaksi työkaluksi toistuvassa käytössä, johon se koulutuksessa tulisi.

Kustannusarvion lisäksi alussa piti myös testata sitä, miten tekoäly reagoi sille yhdistettyyn datatiedostoon sekä tekstiohjeistukseen. Kustannusarviota ei ilman tätä saisi todenmukaiseksi. Samalla sai testattua tekoälyn ohjeistuksen ja datatiedoston logiikkaa yhdessä eli miten nämä siis toimisi toistensa kanssa. Testaus osoittautui kahdella ensiyrittämällä onnistuneeksi, jonka jälkeen pääsi muovaamaan lopullista datatiedostoa, joka tuli tekoälyn kaveriksi. Testauksen jälkeen loin myös yleispätevän pohjan datatiedostolle, joka toimi samalla datatiedoston dokumentaationa selittäen sen auki sekä tekoälyn ohjeistuksen, jotka pystyisi muokkaamaan tulevaisuudessa eri koulutuksia varten.

Tietoturvakoulutuksen luominen tässä kohtaa vaati teoriaperustan läpikäymistä ja tietojen poimimista sieltä. Tässä opinnäytetyöosuudessa tuli myös edelleen muutoksia teoriaperustaan, joita ei pelkkää teoriaa etsiessä osannut ottaa huomioon. Tietoturvakoulutuksen ja opinnäytetyön sisältöä räätälöitiin koulutukseen osallistujien taustan mukaan, joka siis lähtökohtaisesti tarkoitti tässä koulutuksessa sitä, että teknistä koulutustaustaa ei välttämättä ole, josta olisi saanut tietoonsa eri tietoturvakäytäntöjä ja -huomioita.

5 TULOKSET JA JOHTOPÄÄTÖKSET

Opinnäytetyön teoriaosuudessa keskeisiksi teemoiksi nousi tietoturvauhkien tunnistaminen, työntekijän tärkeys päivittäisessä tietoturvatekemisessä, organisaation rooli henkilöstön kouluttamisessa sekä organisaation tietoturvapolitiikka ja lainsäädäntö. Teoriaosuudesta useammasta lähteestä korostui erityisesti työntekijän oma vastuu ja osaaminen organisaation tietoturvan turvaamisessa.

Koulutukset tulisi suunnitella käyttäjälähtöisesti ja niissä tulisi näyttää esimerkein mikä vaikutus tietoturvatoimilla on koulutettavan arjen työhön tai miten tietoturva tulisi ottaa huomioon arjen työtehtävissä. Tietoturvakoulutukset ovat merkittävä osa organisaation tietoturvajohtamista, mutta ne eivät yksistään ehkäise tietoturvaan liittyviä riskejä.

Koulutusten ja tietoturvajohdon tulisi myös ottaa huomioon työntekijöiden lähtötaso. Kaikki organisaation työntekijät eivät ole samalla lähtötasolla organisaation IT- tai tietoturvatiimin kanssa, jolloin se tulisi ottaa huomioon henkilöstöä kouluttaessa. Tietoturvakouluttajien tai organisaation IT-tiimin olisikin hyvä ottaa selvää organisaation lähtötasosta esimerkiksi jonkin tietoturvatestin avustuksella, jolla arvioida henkilöstön osaamista organisaatiotasolla.

Otanta erilaisista menetelmistä kouluttaa tietoturvaa organisaatioissa, oli tässä opinnäytetyössä vähän, sen keskittyen lähinnä luentopainoitteiseen kouluttamiseen. Teoriakatsauksessa mainittujen luentokoulutusten lisäksi tärkeää olisi tuoda henkilöstölleen esiin tietoturvan tärkeyttä päivittäisessä työssään, käydä läpi yhteistyössä yli osastorajojen arjessa turvallisia tietoturvakäytänteitä, esimerkiksi kalasteluviestien tunnistamista käytännössä.

Sosiaali- ja terveysalan teoriaosuudessa nousi esiin erityisesti lainsäädäntö ja sen mukainen tietojenkäsittely. Kaikkea henkilötietojen käsittelyä määrittää lainsäädäntö, esimerkiksi GDPR tai Suomen tietosuojalaki. Teoriaosuudesta koulutukseen saikin ammennettua ymmärryksen siitä, että mitä ja milloin tietoja saa käsitellä sekä miksi ja miten tietojen turvaaminen tapahtuu.

Tietoturvauhkissa nousi esiin myös kalasteluviestit sekä työntekijän heikko asema tietoturvauhkia kohtaan. Kalasteluviestit ovat sosiaali- ja terveysalalla teoriakatsauksen mukaan yleisin uhka, jolloin organisaatioiden kannattaisi nostaa esiin esimerkkejä kalasteluviestien tuomista uhkista sekä miten ne voi tunnistaa. Työntekijöiden tulisi myös tiiviisti tehdä yhteistyötä viestien tunnistamisessa organisaation IT-osaston kanssa.

Esiin nousi myös työntekijän asema tietoturvauhkissa. Lähtökohtaisesti suurin osa tietoturvauhkista juontaa juurensa työntekijän inhimilliseen virheeseen. Hyökkääjät luottavat siihen, että he saavat hyväksikäytettyä ihmisten erehtyväisyyttä. Se tekeekin ihmisestä heikoimman lenkin tietoturvaketjussa. Omaa tietoturvatietoisuutta voi kasvattaa kasvattamalla riskitietoisuuttaan.

Toiminnallisen työn tuloksena syntyi alustava tietoturvakoulutuspohja, jota pystyy helposti muokkaamaan koulutustarpeiden mukaan ja jonka tarkoituksena on tukea sosiaali- ja terveysalalle kouluttautuvien perehtymistä oikeaoppiseen tietojenkäsittelyyn sekä huomioitavaan tietoturvaan työssään. Koulutuspohjan suunnittelussa hyödynnettiin tietoturvaan liittyvää kirjallisuutta, artikkeleita sekä lainsäädäntöä, jonka pohjalta opinnäytetyön teoriaosuus oli luotu.

Opinnäytetyön toiminnallisessa vaiheessa tärkeänä seikkana oli myös helppo sovellettavuus käytettävissä työkaluissa. Koulutuspohjan yksityiskohtaista sisältöä ei voida julkaista osana opinnäytetyötä.

Alan opiskelijana tietoturva oli kaikessa laajuudessaan tuttu asia, mutta käsitykseni organisaation sisällä tapahtuvasta tietoturvakouluttamisesta avartui. Merkittävänä osana tietoturvakouluttamista toki on kalvosulkeiset, joissa asioita käydään teoriatasolla läpi, mutta yhtä merkittävänä osana siinä voi olla myös tietoturvan harjoittaminen ihan käytännön työssä.

Jos resursseja löytyy, niin organisaation sisäisesti pystytään pitämään luentoja, joissa pureudutaan kunnolla tiettyyn tietoturvakäytäntöön, esimerkiksi sosiaali- ja terveysalalla tämä voisi olla luento kalasteluviesteistä tai vaikka jonkinlainen työpaja, jossa henkilöstö oppii tunnistamaan erilaisia kalasteluviestejä. Perinteisen tietoturvakouluttamisen rinnalle siis pystyisi helposti keksimään eri tapoja, joilla syventää henkilöstön koulutusta.

Opinnäytetyöstä suurin osa ajasta meni oikean tiedon etsimiseen ja löytämiseen koulutusta varten, joka tietenkin näkyi myös toiminnallisen osuuden suppeudessa.

LÄHTEET

Aalto Yliopisto 2022a. Tiivistefunktiot. Tiivistefunktioiden ominaisuudet. Luettavissa: https://plus.cs.aalto.fi/cs-ej4404/2022/07-Tiivistefunktiot/02-HASHominaisuudet/. Luettu: 21.3.2025.

Aalto Yliopisto 2022b. RSA. Johdatus kryptografiaan. Luettavissa: https://plus.cs.aalto.fi/cs-ej4404/2022/08-JulkisenAvaimenMenetelmat/04-RSA/?hl=fi. Luettu: 21.3.2025.

Alder, S. 2024. Ransomware Group Leaks Data from 300 Million Patient Interactions with NHS. The Hipaa Journal. Luettavissa: https://www.hipaajournal.com/care-disrupted-at-london-hospitals-due-to-ransomware-attack-on-pathology-vendor/. Luettu: 24.3.2025.

Alibe, B s. a. Fresh Phish: Clever Image-Based Phishing and Phone Scam is Outwitting Threat Detectors. Inky. Luettavissa: https://www.inky.com/en/blog/clever-image-based-phishing-and-phone-scam-is-outwitting-threat-detectors. Luettu: 26.3.2025.

Alma Media Oyj 2019. Uusi Tunto-palvelu lisää työelämän läpinäkyvyyttä ja tuo vertaisarvioinnit työnantajista kaikkien saataville. Luettavissa: https://www.almamedia.fi/blog/2019/03/12/uusi-tunto-palvelu-lisaa-tyoelaman-lapinakyvyytta-ja-tuo-vertaisarvioinnit-tyonantajista-kaikkien-saataville/. Luettu: 27.3.2025.

Alvarez, A. & Tiainen, M. 2023. Tekoäly mullistaa terveydenhuollon: 5 asiaa, jotka tällä hetkellä on syytä ymmärtää. Aalto Yliopisto. Luettavissa: https://www.aalto.fi/fi/uutiset/tekoaly-mullistaa-terveydenhuollon-5-asiaa-jotka-talla-hetkella-on-syyta-ymmartaa. Luettu: 27.3.2023.

Araujo, M. S. de, Machado, B. A. S. & Passos, F. U. 2024. Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. Luettavissa: https://doi.org/10.3390/app14052116. Luettu: 12.3.2025.

Ashenden, D. s.a. In Their Own Words: Employee Attitudes Towards Information Security. Luettavissa: https://pure.port.ac.uk/ws/portalfiles/portal/11378983/In_Their_Own_Words_Final_.pdf. Luettu: 18.3.2025.

Beato, F. & Saunders, J. 2024. 5 ways to achieve effective cyber resilience. World Economic Forum. Luettavissa: https://www.weforum.org/stories/2024/11/cyber-resilience-risk-threat-attack-defence-cybersecurity-cybercrime/. Luettu: 12.3.2025.

Beyond Identity s.a. Device Trust: A Key Element of Zero Trust Authentication Luettavissa: https://www.beyondidentity.com/resource/device-trust-a-key-element-of-zero-trust-authentication. Luettu: 22.3.2025.

Brook, C. 2023. Data Classification Examples to Help You Classify Your Sensitive Data. Digital Guardian. Luettavissa:

https://www.digitalguardian.com/blog/data-classification-examples-help-you-classify-your-sensitive-data. Luettu: 6.3.2025.

Carlton, M., Levy, Y. & Ramim, M. 2019. Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. Information and Computer Security. Luettavissa: https://doi-org.ezp.oamk.fi:2047/10.1108/ICS-11-2016-0088. Luettu: 11.3.2025.

Chin, K. 2024. What is the Cost of a Data Breach in 2024? Upguard. Luettavissa: https://www.upguard.com/blog/cost-of-a-data-breach-2024. Luettu: 17.3.2025.

Cisternelli, E. 2024. The 2 Roles of IT Security Managers. Bitsight. Luettavissa: https://www.bitsight.com/blog/responsibilities-cybersecurity-manager. Luettu: 1.4.2025.

Cloudflare s.a. a. What is HTTPS? Luettavissa: https://www.cloudflare.com/learning/ssl/what-is-https/. Luettu: 25.3.2025.

Cloudflare s.a. b. What is domain spoofing? | Website and email spoofing. Luettavissa: https://www.cloudflare.com/learning/ssl/what-is-domain-spoofing/. Luettu: 25.3.2025.

Cochran, K. A. 2024. Cybersecurity Essentials: Practical Tools for Today's Digital Defenders. Apress, s. 2. Luettavissa: https://learning.oreilly.com/library/view/cybersecurity-essentials-practical/9798868804328/. Luettu: 5.3.2025.

Counter Threat Unit 2017. WCry Ransomware Analysis. Secureworks. Luettavissa: https://www.secureworks.com/research/wcry-ransomware-analysis. Luettu: 21.3.2025.

Coventry, L. & Branley, D. 2018. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Luettavissa: https://www.maturitas.org/action/showPdf?pii=S0378-5122%2818%2930165-8. Luettu: 20.1.2025.

Cyberark s.a. What is Multi-Factor Authentication (MFA)? Luettavissa: https://www.cyberark.com/what-is/mfa/. Luettu: 13.3.2025.

Das, R. 2023. The Zero Trust Framework. CRC Press, s. 1. Luettavissa: https://learning.oreilly.com/library/view/the-zero-trust/9781000922493/. Luettu: 7.3.2025.

Euroopan Unioni 2016. EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679. Luettavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32016R0679. Luettu: 24.3.2025.

European Information Technologies Certification Academy 2023. What is the significance of the avalanche effect in hash functions?. https://eitca.org/cybersecurity/eitc-is-acc-advanced-classical-cryptography/hash-functions/introduction-to-

hash-functions/examination-review-introduction-to-hash-functions/what-is-the-significance-of-the-avalanche-effect-in-hash-functions/. Luettu: 18.3.2025.

Faria, M. 2020. How SHA (Secure Hash Algorithm) works? Medium. Luettavissa: https://01faria-marcello.medium.com/how-sha-secure-hashing-algorithm-works-ac8de87db9ba. Luettu: 21.3.2025.

Filipec, O. & Plášil, D. 2021. THE CYBERSECURITY OF HEALTHCARE: The Case of the Benešov Hospital Hit by Ryuk Ransomware, and Lessons Learned. Luettavissa: https://www.obranaastrategie.cz/filemanager/files/1492295-en.pdf. Luettu: 14.1.2025.

Finlex s.a. a. Laki potilaan asemasta ja oikeuksista. Luettavissa: https://finlex.fi/fi/lainsaadanto/saadoskokoelma/1992/785. Luettu: 26.3.2025.

Finlex s.a. b. Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä. Luettavissa: https://www.finlex.fi/fi/lainsaadanto/2023/703. Luettu: 26.3.2025.

Fortinet s.a. a. What Is WannaCry Ransomware? Does WannaCry Still Exist? Luettavissa: https://www.fortinet.com/resources/cyberglossary/wannacry-ransomware-attack. Luettu: 21.3.2025.

Fortinet s.a. b. 19 Types Of Phishing Attacks. Luettavissa: https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks. Luettu: 25.3.2025.

Fortinet s.a. c. Watering Hole Attack. Luettavissa: https://www.fortinet.com/resources/cyberglossary/watering-hole-attack. Luettu: 25.3.2025.

Fortinet s.a. d. Man-in-the-Middle Attack: Types And Examples. Luettavissa: https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack. Luettu: 25.3.2025.

Gecsoyler, S. & Milmo, D. 2024. Russian crime group behind London hospitals cyber-attack, says expert. The Guardian. Luettavissa: https://www.theguardian.com/technology/article/2024/jun/05/russian-group-behind-london-hospitals-cyber-attack-says-expert. Luettu: 24.3.2025.

Gururaj, H. L., Janhavi, V. & Ambika, V. 2024. Social Engineering in Cybersecurity. CRC Press, 1. Luettavissa: 10.1201/9781003406716-1. Luettu: 26.3.2025.

Hakatemia s.a. Mitä ovat hajautusfunktiot (hash) ja mihin niitä käytetään? Luettavissa: https://www.hakatemia.fi/courses/kryptografia/hajautusfunktiot-hash. Luettu: 18.3.2025.

Hardy, J. 2018. Scam Alert: What You Need to Know About Pop-Up Phishing. Affinity Technology Partners. Luettavissa: https://www.affinitytechpartners.com/3n1blog/2018/5/3/scam-alert-what-you-need-to-know-about-pop-up-phishing. Luettu: 26.3.2025.

IBM s.a. What is cyber resilience? Luettavissa: https://www.ibm.com/think/topics/cyber-resilience. Luettu: 8.3.2025

IBM 2021. Cost of a Data Breach Report 2021. Luettavissa: https://info.techdata.com/rs/946-OMQ-360/images/Cost_of_a_Data_Breach_Report_2021.PDF. Luettu: 17.3.2025.

IBM 2024. Cost of a Data Breach Report 2024, s. 4. Luettavissa: https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec. Luettu: 17.3.2025.

Insurance Fraud Bureau s.a. Paid Ad Spoofing Scams. Luettavissa: https://www.insurancefraudbureau.org/insurance-fraud/paid-ad-spoofing. Luettu: 28.3.2025.

Irwin, L. 2023. Demystifying the CIA Triad: Why It's Crucial for Cyber Security. IT Governance. Luettavissa: https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important. Luettu: 29.3.2025.

Kaleta, J. P., Lee, J. S. & Yoo, S. 2019. Nudging with construal level theory to improve online password use and intended password choice: A security-usability tradeoff perspective. Information Technology & People, Volume 32 Issue 4. Luettavissa: https://doi-org.ezp.oamk.fi:2047/10.1108/ITP-01-2018-0001. Luettu: 7.3.2025.

Kaspersky s.a. a. Mikä nollapäivähyökkäys on? Määritelmä ja selitys. Luettavissa: www.kaspersky.fi/resource-center/definitions/zero-day-exploit. Luettu: 24.3.2025.

Kaspersky s.a. b. Mikä on WannaCry -kiristysohjelma? Luettavissa: https://www.kaspersky.fi/resource-center/threats/ransomware-wannacry. Luettu: 21.3.2025.

Kaspersky s.a. c. What is a Whaling Attack? Luettavissa: https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack. Luettu: 26.3.2025.

Kennison, S. M. & Chan-Tin, E. 2020. Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. Frontier in Psychology 11/2020 vol. 11, s. 1. Luettavissa: https://oula.finna.fi/oamk/PrimoRecord/pci.cdi_doaj_primary_oai_doaj_org_article_3dd05ab4c090440eb6e073aa1c93f58a?sid=4957812875. Luettu: 9.3.2025.

Kortesoja, M. 2022. Tapaus Vastaamo: Symptomaattinen luenta potilastietosuojan murtumisen yhteiskunnallisista syistä ja seurauksista. Luettavissa: https://doi.org/10.55294/tk.113346 . Luettu: 23.3.2025.

Kosinski, M. 2024. What is smishing (SMS phishing)? IBM. Luettavissa: https://www.ibm.com/think/topics/smishing. Luettu: 26.3.2025.

Kyberturvallisuuskeskus 2020. SHA-1-tiivistefunktio on lopullisesti murrettu. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/sha-1-tiivistefunktio-lopullisesti-murrettu. Luettu: 22.3.2025.

Kyberturvallisuuskeskus 2023. Tietoturva on koko organisaation asia - vinkkejä henkilöstön tietoturvakoulutuksen suunnitteluun. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/tietoturva-koko-organisaation-asia-vinkkeja-henkiloston. Luettu: 28.3.2025.

Kyberturvallisuuskeskus 2024. Turvaa tietosi: Vinkkejä puhelimen tietoturvalliseen käyttöön. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/turvaa-tietosi-vinkkeja-puhelimen-tietoturvalliseen-kayttoon?utm_source=chatgpt.com. Luettu: 17.3.2025.

Laakso, M. 2011. Salasanan murtaminen. Luettavissa: https://tietojesiturvaksi.fi/blogi/salasanan-murtaminen. Luettu: 21.3.2025.

Ledesma, J. 2023. Evil Twin Attack: What it is, How to Detect & Prevent it. Varonis. Luettavissa: https://www.varonis.com/blog/evil-twin-attack. Luettu: 25.3.2025.

Luo, X. R. & Zhdanov, D. 2016. Special issue introduction: A comprehensive perspective on information systems security — technical advances and behavioral issues. Luettavissa: https://www.sciencedirect.com/science/article/pii/S0167923616301798?fr=RR-2&ref=pdf_download&rr=910c93ef8ddf8dc2. Luettu: 20.1.2025.

Malwarebytes s.a. EternalBlue. Luettavissa: https://www.malwarebytes.com/glossary/eternalblue. Luettu: 21.3.2025

Roy, M. 2019. 'Triple threat' malware campaign combines Emotet, TrickBot and Ryuk. Luettavissa: https://www.techtarget.com/searchsecurity/news/252461071/Triple-threat-malware-campaign-combines-Emotet-TrickBot-and-Ryuk. Luettu: 23.3.2025.

Microsoft s.a. What is two-factor authentication? Luettavissa: https://www.microsoft.com/en-ie/security/business/security-101/what-is-two-factor-authentication-2fa. Luettu: 13.3.2025.

Mitnick, K. D. & Simon, W. L. 2002. The Art of Deception: Controlling the Human Element of Security. Wiley Publishing, Inc., s. 41. Luettu: 16.3.2025.

Murray-Watson, Dr. R. s.a. State of Healthcare Cybersecurity. HIPAA Journal. Luettavissa: https://www.hipaajournal.com/healthcare-cybersecurity/. Luettu: 23.3.2025.

NCSC s.a. Macro Security for Microsoft Office. Luettavissa: https://www.ncsc.gov.uk/guidance/macro-security-for-microsoft-office. Luettu: 25.3.2025.

Network Solutions Team 2020. How to Recognize and Prevent Homograph Attacks. Network Solutions. Luettavissa: https://www.networksolutions.com/blog/protect/cybersecurity/how-to-recognize-and-prevent-homograph-attacks. Luettu: 27.3.2025.

Nielson, S. J. 2023. Discovering Cybersecurity: A Technical Introduction for the Absolute Beginner. Apress, s. 1-2. Luettavissa: https://learning.oreilly.com/library/view/discovering-cybersecurity-a/9781484295601/. Luettu: 15.1.2025.

NHS England 2024. NHS London statement on Synnovis ransomware cyber attack – Thursday 6 June 2024. Luettavissa: https://www.england.nhs.uk/london/2024/06/06/nhs-london-statement-on-synnovis-ransomware-cyber-attack-thursday-6-june-2024/?utm_source=chatgpt.com. Luettu: 24.3.2025.

Olmstead, K. & Smith, A. 2017. Americans and Cybersecurity. Pew Research Center. Luettavissa: https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/. Luettu: 9.3.2025.

Pandasecurity 2024. What Is AES Encryption? A Guide to the Advanced Encryption Standard. Luettavissa: https://www.pandasecurity.com/en/mediacenter/what-is-aes-encryption/. Luettu: 21.3.2025

Proofpoint s.a. a. What Is Pharming? Luettavissa: https://www.proofpoint.com/us/threat-reference/pharming. Luettu: 23.3.2025.

Proofpoint s.a. b. What Is Clone Phishing? Luettavissa: https://www.proofpoint.com/us/threat-reference/clone-phishing. Luettu: 25.3.2025.

Raita-aho, S. 2023. Kolme työntekijää urkkinut potilastietoja, kertoo Hus – jopa satoja tietoja katsottu luvatta. Uutissuomalainen. Luettavissa: https://www.uusimaa.fi/uutissuomalainen/6158361. Luettu: 5.3.2025.

Reeves, A., Calic, D. & Delfabbro, P. 2021. “Get a red-hot poker and open up my eyes, it's so boring”1: Employee perceptions of cybersecurity training. Luettavissa: https://doi.org/10.1016/j.cose.2021.102281. Luettu: 15.1.2025.

Sallanmaa, T. 2023. Tietoturva SaaS-palvelukehityksessä – miten huolehdimme tietoturvan eri osa-alueista. Funidata. Luettavissa: https://www.funidata.fi/blogi/tietoturva-saas-palvelukehityksessa. Luettu: 29.5.2025.

Sekine, T. 2024. Security Risks of Generative AI and Countermeasures, and Its Impact on Cybersecurity. Luettavissa: https://www.nttdata.com/global/en/insights/focus/2024/security-risks-of-generative-ai-and-countermeasures. Luettu: 27.3.2025.

Silverfort s.a. Identity Zero Trust. Luettavissa: https://www.silverfort.com/glossary/identity-zero-trust/. Luettu: 22.3.2025.

Tietosuojakeskus s.a. Case Vastaamo. Luettavissa: https://tietosuojakeskus.fi/case-vastaamo/. Luettu: 24.3.2025.

Tietosuojavaltuutetun toimisto s.a. a. Tietosuojalaki. Luettavissa: https://tietosuoja.fi/tietosuojalaki. Luettu: 26.3.2025.

Tietosuojavaltuutetun toimisto s.a. b. Tietosuojavastaavan nimittäminen. Luettavissa: https://tietosuoja.fi/tietosuojavastaavan-nimittaminen. Luettu: 27.3.2025.

Tietosuojavaltuutetun toimisto s.a. c. Rekisteröidyn oikeudet. Luettavissa: https://tietosuoja.fi/rekisteroidyn-oikeudet. Luettu: 28.3.2025.

Tietosuojavaltuutetun toimisto s.a. d. Tietoturvaloukkaukset. Luettavissa: https://tietosuoja.fi/tietoturvaloukkaukset. Luettu: 28.3.2025.

Tietosuojavaltuutetun toimisto s.a. e. Usein kysyttyä tietosuojavastaavista. Luettavissa: https://tietosuoja.fi/usein-kysyttya-tietosuojavastaavista. Luettu: 1.4.2025.

Trevino, A., Cutler, A. & Guccione, D. 2024. What Are the Five Pillars of Zero-Trust Security? Keeper. Luettavissa: https://www.keepersecurity.com/blog/2024/04/10/what-are-the-five-pillars-of-zero-trust-security/. Luettu: 17.3.2025.

University of Virginia s.a. What the heck is a deepfake? Luettavissa: https://security.virginia.edu/deepfakes. Luettu: 29.3.2025.

Umawing, J. 2017. Out of character: Homograph attacks explained. Malwarebytes. Luettavissa: https://www.malwarebytes.com/blog/news/2017/10/out-of-character-homograph-attacks-explained. Luettu: 27.3.2025.

Valtiovarainministeriö 2017. Tietoturvapoikkeamatilanteiden hallinta, s. 16-23. Luettavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79258/VM_8_2017.pdf. Luettu: 1.4.2025.

Valvira s.a. Potilas- ja asiakastietojen ja henkilötietojen käsittely. Luettavissa: https://valvira.fi/sosiaali-ja-terveydenhuolto/potilas-ja-asiakastietojen-ja-henkilotietojen-kasittely. Luettu: 27.3.2025.

Wash, R. & Rader, E. 2021. Prioritizing security over usability: Strategies for how people choose passwords. Journal of Cybersecurity 2021, s. 1. Luettavissa: https://academic.oup.com/cybersecurity/article/7/1/tyab012/6291418. Luettu: 10.3.2025.

Waugh, E. 2025. What Is Angler Phishing? Experian. Luettavissa: https://www.experian.com/blogs/ask-experian/what-is-angler-phishing-and-how-can-you-avoid-it/. Luettu: 25.3.2025.

Yacono, L. 2024. The 3 Zero Trust Principles (and Why They Matter). Cimcor. Luettavissa: https://www.cimcor.com/blog/the-3-zero-trust-principles. Luettu: 17.3.2025.

Yang, K. 2017. WannaCry: Evolving History from Beta to 2.0. Fortinet. Luettavissa: https://www.fortinet.com/blog/threat-research/wannacry-evolving-history-from-beta-to-2-0. Luettu: 21.3.2025.

Yrityksen digitalous 2022. Digitaalinen ekosysteemi. Luettavissa: https://yrityksendigitalous.fi/yrityksen-digitalous-hankkeesta/digitaalinen-ekosysteemi/. Luettu: 22.3.2025.

Zscaler s.a. a. What Is Zero Trust Network Access? Luettavissa: https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust-network-access. Luettu: 17.3.2025.

Zscaler s.a. b. What Is Network Segmentation?. Luettavissa: https://www.zscaler.com/resources/security-terms-glossary/what-is-network-segmentation. Luettu: 1.4.2025.