TYÖTERVEYS JA –TURVALLISUUS NÄKÖKOHDAT KYBERRISKIEN KARTOITUKSESSA

Tiivistelmä

Tässä asiakirjassa käsitellään uutta näkökulmaa ja selvitetään kyberuhkien ja työntekijöiden terveyden ja turvallisuuden välistä suhdetta. Tällaisessa näkökulmassa laajennetaan pelkästään kyberturvallisuuden teknisiin näkökohtiin keskittyvää perinteistä näkemystä koskemaan myös kyberhyökkäysten aiheuttamiin inhimillisiin ja sosiaalisiin seurauksiin.

Organisaatioissa käytetään jatkuvasti enemmän digitaaliteknologiaa ja hyökkäykset tietojärjestelmiä ja verkkoja vastaan lisääntyvät. Tämän vuoksi on myös työntekijöiden terveyteen ja turvallisuuteen kohdistuviin uusiin ja kehittyviin riskeihin puututtava. Kyberriskien myötä työterveydessä ja -turvallisuudessa on tulevina vuosina käsiteltävänä uusia tarpeita ja haasteita.

Kyberturvallisuustilanne

Kyberturvallisuudesta on muutaman viime vuoden aikana tullut ajankohtainen aihe kaikissa yrityksissä ja kaikilla toimialoilla. Kyberrikollisuus kehittyy jatkuvasti ja kyberrikolliset hyödyntävät hyökkäyksissään kaikenlaisia, sekä fyysisiä, teknisiä että inhimillisiä, haavoittuvuuksia.

Cambridge Dictionary -sanakirjassa kyberhyökkäys määritellään laittomaksi yritykseksi vahingoittaa jonkun toisen osapuolen tietokonejärjestelmää tai siinä olevia tietoja verkkoa käyttämällä[1]. Yhdysvaltojen kansallisen standardi- ja teknologiainstituutin (NIST) määritelmä on täsmällisempi. Sen mukaan kyberhyökkäys on kybertoimintaympäristössä tehty hyökkäys, jonka kohteena on yrityksen kybertoimintaympäristön käyttö ja jonka tarkoituksena on häiritä tietojenkäsittely-ympäristöä/-infrastruktuuria, estää sitä toimimasta, tuhota se tai käyttää sitä hyväksi pahantahtoisesti taikka tuhota datan eheys tai varastaa valvottuja tietoja[2].

Maailman jatkuvan digitalisaation myötä kaikki yritykset ovat vaarassa joutua kyberhyökkäyksen kohteeksi. Etenkin vuosi 2020 on osoittautunut vedenjakajaksi sekä digitalisaatio- että kyberturvallisuusasioissa. Yritykset ovat ottaneet entistä enemmän käyttöön joustavuuteen ja etätyöteknologiaan perustuvia organisaation laajuisia toimintamalleja. Tämä johtuu pääasiassa covid-19-pandemiasta, mutta se on myös lisännyt kyberrikollisten toimintamahdollisuuksia niin, että kyberhyökkäysten määrä on kasvanut jopa 78 prosentissa organisaatioista etätyöhön siirtymisen vuoksi.[3]

Maailmanlaajuisesti on organisaatioista 87 prosenttia yritetty käyttää hyväksi hyödyntämällä niiden olemassa olevia haavoittuvuuksia. Turvallisuusalan ammattilaisista 71 prosenttia on ilmoittanut kyberuhkien (verkkourkinnan, haittaohjelmien, kiristyshaittaohjelmien) lisääntyneen koronaviruspandemian puhkeamisen jälkeen.[4]

Sekä kyberhyökkäysten määrä että vaikutus ovat yleisesti kasvaneet (ENISA, 2021a), mutta maiden resurssit ja työkalut kyberturvallisuuden käsittelemiseksi ovat erilaiset. Kyberturvallisuusindeksin kärkeen on esimerkiksi kyberturvallisuuteen sitoutumisen ja lainsäädännön kaltaisten erityistekijöiden perusteella luokiteltu kolme Euroopan maata (Portugali, Liettua ja Slovakia) [5].

Uhkaympäristön laajenemisen vuoksi Euroopan komission piti kiireellisesti laatia toimiva EU:n kyberturvallisuusstrategian digitaaliselle vuosikymmenelle[6]. Sillä taataan turvallinen digitalisaatio parantamalla häiriönsietokykyä, kehittämällä valmiuksia ehkäistä kyberhäiriöitä ja reagoida niihin sekä määrittämällä johdonmukainen kansainvälinen kyberkäytäntö. Strategiassa korostetaan myös sen

[1] https://dictionary.cambridge.org/dictionary/english/cyberattack
[2] https://csrc.nist.gov/glossary/term/cyber_attack
[3] https://atlasvpn.com/blog/cyberattack-volume-grew-in-78-of-businesses-globally
[4] https://www.checkpoint.com/pages/cyber-security-report-2021/
[5] https://www.eset.com/uk/about/newsroom/blog/european-cybersecurity-index-2021/
[6] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

merkitystä, että kaikilla EU:n toimielimillä, elimillä ja virastoilla on kyberturvallisuustietoisuutta lisäävä ohjelma, j jolla saadaan aikaan toimiva kyberturvallisuuskulttuuri.

Nykyiset ja tulevat uhat

Kyberrikollisuuden kustannusten odotetaan nousevan vuoteen 2025 mennessä koko maailmassa 10,5 biljoonaan Yhdysvaltain dollariin vuodessa[7]. Kybertoimintaympäristöä käytetään vihamielisiin tarkoituksiin monista eri syistä. Myös toimijat ovat erilaisia, pääosin taloudellista etua tavoittelevista kyberrikollisista poliittisten ja ideologisten päämäärien ajamiin kyberterroristeihin. Verkossa tehtävät rikokset ovat hyvin monenlaisia, ja niihin kuuluu useita laittomia toimia, jotka ovat tuttuja jo verkon ulkopuolisesta maailmasta. Niitä ovat muun muassa identiteettivarkaus, petos, vakoilu sekä henkistä omaisuutta koskevat rikokset. Myös verkkoväkivaltaa esiintyy monessa muodossa, esimerkiksi ahdistelua ja kiusaamista. Näissä toimissa voidaan hyödyntää digitaalisen ympäristön tarjoamia tehokkaita keinoja. Jatkuvasti verkottuneemman maailman vuoksi kyberrikollisuus onkin yksi kahden seuraavan vuosikymmenen suurimmista riskeistä.[8]

Kyberuhat ovat jokaisen organisaation ja maan tärkeysjärjestyksessä korkealla, koska niiden seuraukset ovat moninaisia ja vakavia: niiden vuoksi voidaan esimerkiksi menettää arvokkaita tietoja, tietokonejärjestelmät ja niihin liittyvät palvelut voivat halvaantua ja ihmisten terveys ja turvallisuus voivat vaarantua vakavasti.

Vaikka jotkin yleisimmät kyberuhat, kuten verkkourkinta ja kiristyshaittaohjelmat (taulukko 1), ovat olleet tiedossa jo vuosia, ne lisääntyvät jatkuvasti[9]. Ne ovatkin erittäin tuottoisia kyberrikollisille ja niiden toteuttamiskustannukset ovat hyvin pieniä verrattuna hyökkääjien kiinnijäämisen riskiin (Hernandez-Castro et al., 2020). Verkkourkinta kuuluu edelleen tietoturvaloukkausten kärkitaktiikoihin (Verizon, 2021), mutta kyberhyökkäysten eri muodoista käy ilmi, miten monitahoinen kyberuhkaympäristö on. Esimerkiksi toimitusketjuihin tehdään hyökkäyksiä entistä enemmän, ja jatkossa ne ovat organisaatioille suuri huolenaihe (ENISA, 2021b)[10].

Taulukko 1: Yleisimpiä kyberuhkia[11]

Tyyppi	Kuvaus
Verkkourkinta ja kohdennettu verkkourkinta	Verkkourkinnassa lähetetään tavallisesti sähköpostitse petosviestejä, jotka vaikuttavat tulevan hyvämaineisesta lähteestä. Tavoitteena on varastaa arkaluonteisia tietoja, kuten luottokortti- ja kirjautumistietoja, tai asentaa haittaohjelma uhrin koneeseen. Verkkourkinnassa on eri muotoja, kuten kohdennettu verkkourkinta. Se on verkkourkinnan kehittyneempi muoto, joka on kohdennettu tiettyyn henkilöön tai organisaatioon.
Haittaohjelma ja kiristyshaittaohjelma	Haittaohjelma on laaja käsite, jolla tarkoitetaan haittaohjelmistoja, kuten vakoiluohjelmia, kiristyshaittaohjelmia, viruksia ja matoja. Haittaohjelmiin kuuluu esimerkiksi kiristyshaittaohjelma, jossa salataan uhrin tiedot ja pyydetään maksua vastineeksi salauksenpurkuavaimesta. Se on tuottoisimpia kyberhyökkäysten muotoja.
Käyttäjän manipulointi	Käyttäjän manipulointi on tekniikka, jossa ihmisiä petetään ja manipuloidaan, jotta heiltä saadaan luottamuksellisia tietoja tai päästään

[7] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
[8] https://www.weforum.org/agenda/2020/12/3-disruptive-frontier-risks-that-could-strike-by-2040/
[9] https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report
[10] Toimitusketju on tuotteen suunnittelemiseen, valmistamiseen ja jakelemiseen tarvittavien resurssien ekosysteemin yhdistelmä. Kyberturvallisuudessa toimitusketjuun kuuluvat laitteistot ja ohjelmistot, pilvitallennus tai paikallinen tallennus ja jakelumekanismit. https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks
[11] Nämä ovat ENISAn (2020; 2021) raportoimia yleisimpiä kyberuhkia. Uhkien kuvaukseen voi tutustua myös osoitteessa https://www.cisco.com/c/en_in/products/security/common-cyberattacks.html#~types-of-cyber-attacks and https://www.itgovernance.co.uk/cyber-threats

Tyyppi	Kuvaus
	heidän tietokoneelleen. Esimerkiksi verkkourkinta on käyttäjän manipulointia.
Palvelunesto	Tämäntyyppisessä hyökkäyksessä järjestelmiin, palvelimiin tai verkkoihin kohdistetaan niin paljon liikennettä, että järjestelmä ei pysty täyttämään oikeita pyyntöjä. Hyökkääjät voivat käyttää hyökkäyksen käynnistämiseen myös useita vaarannettuja laitteita (hajautettu palvelunestohyökkäys)
Tietosuojaloukkaus	Tietosuojaloukkaus on kyberhäiriö, jossa tietoja varastetaan, otetaan järjestelmästä tai käytetään luvatta.
Kybervakoilu	Kybervakoilun tavoitteena on varastaa arkaluonteista tai turvaluokiteltua tietoa tai henkistä omaisuutta, jotta kilpailevaan yritykseen tai valtiolliseen elimeen nähden saadaan etua.
Disinformaatio- ja misinformaatiokampanjat	Disinformaatiossa luodaan ja jaetaan tarkoituksellisesti väärää tietoa haitan aiheuttamiseksi. Misinformaatiossa väärää tai virheellistä tietoa levitetään tahattomasti. Molemmat voivat edeltää muita hyökkäyksiä (kuten käyttäjän manipulointia ja verkkourkintaa), ja niitä voidaan käyttää yhdessä muiden kyberuhkien kanssa.

Onkin ristiriitaista, että innovatiivisia teknologioita voidaan yhtäältä käyttää kyberturvallisuutta parantavien uusien ratkaisujen luomiseen, mutta toisaalta samat teknologiat tuovat lisämahdollisuuksia kyberrikollisille. Siksi tekoälyn myönteisen käytön, kuten hyökkäysten havaitsemisen ja haittaohjelmien tunnistamisen (Truong et al., 2020), rinnalla kehittyy uusia uhkia ja vanhat uhat vahvistuvat (Brundage et al., 2018). Tekoälyteknologioita voidaan esimerkiksi käyttää käyttäjää manipuloivien hyökkäysten automatisointiin sekä haittaohjelmien tehostamiseen. Esineiden internetin laitteiden leviäminen lisää myös käsittelyn haavoittuvuuksia, koska niiden käsittely- ja tallennusvalmiudet ovat tavallista heikompia, minkä vuoksi niiden suojaamiseksi on käytössä vähemmän tietoturvasovelluksia[12].

Tietyt työskentelytilanteet ovat lisänneet kyberrikollisten mahdollisuuksia. Esimerkiksi covid-19-pandemian vuoksi vuonna 2020 laajasti käyttöön otettu etätyö on aiheuttanut yrityksille uusia turvallisuushaasteita. Etätyössä esimerkiksi käytetään aiempaa enemmän päätelaitteita, jotka voivat olla alttiita tietoturvaloukkauksille, ja se on lisännyt myös henkilökohtaisten laitteiden käyttöä työssä (OLM – oma laite mukaan).[13] Siihen, että kaiken halutaan olevan vaivatta saatavilla yhdessä ainoassa laitteessa, liittyykin merkittäviä tietoturvariskejä, kun esimerkiksi digitaalisten laitteiden yksityiseen käyttöön liittyvä huolettomuus leviää työkäyttöön (Disterer & Kleiner, 2013). Puhumattakaan siitä, että digitaalisen laitteen katoaminen vaarantaa omien tietojen lisäksi myös liiketoimintatiedot. Etätyö on näin ollen turvallisuushaaste yrityksille, joiden on tarkistettava yrityksen laajuiset käytäntönsä ja panostettava etätyöntekijöiden määrätietoiseen koulutukseen (Borkovich & Skovira, 2020).

Merkille pantavaa on myös se, että puettavia laitteita (kuten langattomia kuulokkeita tai älykelloja) käyttävät työntekijät voivat tietämättään itse toimia välittäjinä kyberrikollisten toimissa. Puettavat teknologiat voivatkin aiheuttaa kyberriskejä esimerkiksi silloin, kun yrityksen kannettavaan tietokoneeseen on liitetty laitteita, jotka voisivat tuoda viruksia yrityksen järjestelmään. Luvaton käyttö voi myös vaarantaa yksityisyydensuojan (Heembrock, 2015).

Sekä yksityishenkilöille että yrityksille aiheutuu lisähuolia muista kehittyvistä kyberuhista, koska sosiaalinen media vahvistaa niiden vaikutuksia. Esimerkiksi huijausvideoissa ihmisten – usein julkisuuden henkilöiden tai poliitikkojen – video- tai äänitiedostoja on muutettu digitaalisesti, jotta heille

[12] https://www.forbes.com/sites/chuckbrooks/2021/02/07/cybersecurity-threats-the-daunting-challenge-of-securing-the-internet-of-things/
[13] https://www.techrepublic.com/article/how-to-combat-the-security-challenges-of-a-remote-workforce/

voidaan aiheuttaa haittaa, kuten levittää väärää tietoa ja mustata heidän mainettaan. Näiden uhkien aiheuttama huoli ei kuitenkaan kytkeydy vain propagandaan tai vaaleihin. Ne voivat vaikuttaa myös yrityksiin, kun manipuloidaan markkinoita, sabotoidaan tuotemerkkejä, kiristetään ja esiinnytään yrityksen johtohenkilöinä digitaalisessa maailmassa (Westerlund, 2019).

Kun otetaan huomioon vaikuttava edistyminen teknologian innovaatioissa, kvanttilaskenta, jossa tietoa pystytään käsittelemään huomattavasti perinteisiä toimintamalleja tehokkaammin, voisi arvioiden mukaan olla käytössä vuoteen 2025 mennessä[14]. Teoriassa näillä tietokoneilla voidaan purkaa monet nykyisistä tietoturvan salausjärjestelmistä, mutta tämän teknologian käyttö käytännössä edellyttää huomattavaa teknologista edistymistä[15].

Edellä kuvatusta tilanteesta käy selkeästi ilmi, miksi kyberriskit ovat tärkeysjärjestyksessä korkealla muiden maailmanlaajuisten riskien joukossa (WEF, 2021).

Kyberhyökkäysten vaikutus työterveyteen ja -turvallisuuteen

Yrityksiin ja laitoksiin kohdistuneita kyberhyökkäyksiä on yleensä analysoitu teknisestä näkökulmasta, vaikka inhimillinen tekijä on yhtä tärkeä osa kyberturvallisuutta(Corradini et al., 2020). Myös kyberhyökkäysten vaikutusten arvioinnissa keskitytään pääasiassa taloudellisiin näkökohtiin (Cashell et al., 2004; Anderson et al., 2013) ja vain harvoin työntekijöiden terveyteen ja turvallisuuteen. Vaikutusta mitataankin pääosin aineellisina kustannuksina, kuten tietojen menettämisenä ja liiketoimintojen keskeytymisenä, ja aineettomina kustannuksina, kuten teollis- ja tekijänoikeuksien menettämiseen liittyvänä kilpailuedun menettämisenä ja mainehaittana[16].

Kyberhyökkäykset voivat kuitenkin aiheuttaa vammoja, henkisiä ongelmia tai ihmishenkien menetyksiä: siksi on selvää, että kyberriskien arviointia ja työterveys- ja työturvallisuusriskien arviointia ei voida tehdä erillään vaan ne on tehtävä yhdessä (Izuakor, 2016). Yritysten pitäisi siksi tunnistaa kyberuhkiin liittyviä erilaisia vaikutuksia ja alkaa toimia entistä kokonaisvaltaisemmin kyberriskien hallinnan parantamiseksi (Couce-Vieira et al., 2020). Näistä vaikutuksista annetaan esimerkkejä taulukossa 2.

Taulukko 2: Kyberriskien hallintaa koskevia erilaisia vaikutuksia

Luokat	Vaikutukset
Organisaatio	Taloudelliset vahingot (kuten tuotannon väheneminen, koska palvelu ei ole käytettävissä, markkinaosuuden pieneneminen tai kilpailuedun menettäminen)
	Mainehaitta (sidosryhmien luottamuksen heikkeneminen)
	Muut taloudelliset näkökohdat (kuten kybervakuutus)
Työntekijät	Fyysiset vammat (kuten ihmishenkien menetykset kyberfyysisen järjestelmän häiriöiden vuoksi)
	Vauriot mielenterveydelle (kuten ahdistus tai turhautuminen)
	Vaikutus henkilökohtaisiin oikeuksiin (tietosuojaloukkauksista johtuvat yksityisyyden loukkaukset)
	Henkilökohtaiset taloudelliset vahingot
Muut asianosaiset organisaatiot	Maailmanlaajuisen toimitusketjun keskinäisten yhteyksien häiriintymisestä johtuvat vahingot
Ympäristö	Vaikutus luonnonympäristöön (kuten kyberhäiriön seurauksena saastunut maa)

Muokattu lähteestä Couce-Vieira et al. 2020

[14] https://builtin.com/founders-entrepreneurship/quantum-computing-revolution
[15] https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat
[16] https://www2.deloitte.com/nz/en/pages/forensic-focus/articles/cyber-security-is-your-organisation-under-threat-of-a-cyber-attack.html

Näihin vaikutuksiin voi liittyä rahassa mitattavia kustannuksia, kuten markkinaosuuden pieneneminen, sekä kustannuksia, joita ei voida mitata rahassa, kuten fyysiset tai mielenterveyden vauriot.

Seuraavassa jaksossa käsitellään työntekijöiden terveyteen ja turvallisuuteen mahdollisesti kohdistuvien fyysisten ja henkisten vaikutusten merkitystä.

Näkökulmia kyberturvallisuudesta

Kyberturvallisuutta koskevia turvallisuusäkökulmiaa ei ehkä ole otettu kunnolla huomioon siksi, että kyberriskejä pidetään ulkoisina uhkina, kun taas terveys- ja turvallisuusasioita käsitellään organisaatioissa sisäisesti[17]. Kyberuhkien kehittyminen ja organisaatioiden lisääntyvä altistuminen kyberhyökkäyksille edellyttävät kuitenkin, että niiden tehokasta hallintaa varten omaksutaan kokonaisvaltainen toimintamalli, joka sisältää myös työntekijöiden terveyteen ja turvallisuuteenliittyviä näkökulmia .

Kyberhyökkäykset voivat sekä vaarantaa organisaation tietopääoman että uhata työntekijöiden fyysistä ja henkistä terveyttä, kun hakkerit hyökkäävät kriittisiin infrastruktuureihin[18] tai ottavat työntekijöiden teknologiset laitteet hallintaansa. Esimerkiksi laitteen peukalointi voi aiheuttaa ihmisille fyysistä haittaa ja vaarantaa henkilötiedot (Loukas, 2019).

Tätä kysymystä voidaan selventää esimerkeillä. Saksassa hakkeroitiin vuonna 2014 terästehdas, ja hyökkääjät onnistuivat sulkemaan sen uunin[19]. Käytettyjen materiaalien vuoksi oli olemassa suuri riski , että kyberhyökkäys muuttuisi työntekijöiden turvallisuutta uhkaavaksi kriittiseksi tapahtumaksi.

Yhdysvaltain elintarvike- ja lääkevirasto (FDA) veti vuonna 2017 takaisin noin 465 000 sydämentahdistinta turvallisuutta koskevien haavoittuvuuksien vuoksi. Laitteet olivat alttiita hakkeroinnille ja vaaransivat siten potilaiden hengen[20].

Sekä kybertekijöitä että fyysisiä tekijöitä sisältäviin teollisuuden ohjausjärjestelmiin kohdistuvat kyberhyökkäykset uhkaavat ihmishenkiä. Esimerkkejä tästä ovat Stuxnet[21], tietokonemato, joka luotiin vuonna 2010 ottamaan hallintaan uraanin rikastamiseen käytettyjä sentrifugeja Iranissa, ja Triton-haittaohjelma[22], joka tunkeutui vuonna 2017 petrokemian laitoksiin Lähi-idässä ja onneksi kaatui. Tällaisista hyökkäyksistä voi olla vakavia seurauksia myös ympäristölle.

Kun laitteita käytetään vaarallisissa tilanteissa etäyhteydellä, työntekijöiden turvallisuus voi vaarantua. Näin voi käydä esimerkiksi silloin, kun ajoneuvot tai koneet toimivat hallitsemattomasti, koska langattomissa signaaleissa on häiriöitä tai hakkerit hyökkäävät niihin. (Steijn et al., 2016.)

Kun ihmiset ja robotit tekevät valmistusalalla yhteistyötä tuotantolinjoilla, kyberhyökkäykset voivat häiritä fyysisiä teollisuusprosesseja ja aiheuttaa työntekijöille vammoja (Perales Gómez et al., 2020).

Gartnerin mukaan kyberhyökkäysten tekijät pystyisivät vuoteen 2025 mennessä käyttämään operatiivista teknologiaa ja muita kyberfyysisiä järjestelmiä aseena ja aiheuttamaan haittaa ihmisille tai tappamaan heitä[23].

Sairaaloihn tehtävässä kyberhyökkäyksessä hakkerit pystyvät saamaan käsiinsä kaikkien potilaiden ja työntekijöiden arkaluonteiset tiedot, mutta erityisen vakavasti se kuitenkin vaarantaa potilaiden mahdollisuuden saada asianmukaista hoitoa ja tarvittavia lääketieteellisiä toimenpiteitä (Argaw et al., 2020)[24]. WannaCry-kiristyshaittaohjelmalla toukokuussa 2017 tehdyn maailmanlaajuisen hyökkäyksen

[17] https://donesafe.com/2017/06/why-cybersecurity-should-factor-into-every-health-and-safety-plan/
[18] Kriittiset infrastruktuurit ovat elintärkeitä maan toiminnalle, koska niihin kuuluu energian, kansanterveyden, televiestinnän sekä pankki- ja varainhoitotoiminnan kaltaisia aloja.
[19] https://www.wired.com/2015/01/german-steel-mill-hack-destruction/
[20] https://theconversation.com/three-reasons-why-pacemakers-are-vulnerable-to-hacking-83362
[21] https://spectrum.ieee.org/the-real-story-of-stuxnet
[22] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems/
[23] https://www.thehindubusinessline.com/info-tech/cyber-attackers-could-weaponise-tech-to-kill-humans-by-2025-gartner/article35519872.ece
[24] Saksalainen sairaala joutui vuonna 2020 kyberhyökkäyksen uhriksi eikä voinut ottaa saapuvia potilaita vastaan. Sairaalaan hoitoa varten saapunut nainen kuoli matkalla seuraavaan sairaalaan, joka oli yli 30 kilometrin päässä. Tutkinnan perusteella syyttäjät totesivat näytön riittämättömäksi, mutta sairaalan ensiapupoliklinikan sulkeutumisen tiedettiin johtuvan kiristyshaittaohjelmalla tehdystä hyökkäyksestä. https://www.wired.co.uk/article/ransomware-hospital-death-germany

analyysista kävi ilmi, että siitä oli merkittäviä kielteisiä vaikutuksia Yhdistyneen kuningaskunnan kansanterveyspalveluille (Ghafur et al., 2019).

Covid-19-pandemian aikana yhdysvaltalaisiin sairaaloihin kohdistettiin useita kiristyshaittaohjelmilla tehtyjä hyökkäyksiä, jotka keskeyttivät terveydenhoidon useissa sairaaloissa ja vaaransivat vakavasti potilaiden hengen[25]. Kiristyshaittaohjelmien käyttöä terveydenhuoltolaitoksia vastaan käsittelevästä tutkimuksesta käy ilmi, että näillä kyberuhilla voi olla hengenvaarallisia seurauksia (Ponemon, 2021).

Sosiaaliset ja psykologiset vaikutukset

Kyberhyökkäyksistä voi olla myös sosiaalisia vaikutuksia, kuten digitaaliteknologiaa kohtaan tunnetun luottamuksen menettäminen, ja psykologisia vaikutuksia, kuten ahdistusta, vihaa ja masennusta (Bada & Nurse, 2020). Kyberhyökkäysten uhreiksi joutuneet työntekijät voivat myös tuntea häpeää, syyllisyyttä, hämmennystä ja turhautumista, erityisesti silloin, kun kyse on digitaalisten tietojen vuodoista. Näiden vaikutusten merkittävyys riippuu ympäristöstä, jossa kyberhyökkäys tapahtuu. (Agrafiotis et al., 2018.) Esimerkiksi rahoituslaitoksessa, jossa tietosuojaloukkauksen seuraukset ovat todennäköisesti vakavampia kuin joitakin muita palveluja tarjoavassa laitoksessa, henkinen haitta työntekijöille voi olla suurempi. Äärimmäisissä tapauksissa tietovuodon seuraukset voivat ajaa asianomaiset henkilöt itsemurhaan, koska he kokevat itseään koskevien tietojen julkitulon niin häpeälliseksi[26]. Henkinen taakka voi siis osoittautua työntekijöille erittäin raskaaksi.

Yksityisyys ja turvallisuus kietoutuvat näin ollen entistä tiiviimmin yhteen. Yksityisyys viittaa henkilötietojen keräämiseen ja käyttöön, ja turvallisuudella pyritään takaamaan näiden tietojen suoja.[27] Toukokuun 25. päivänä 2018 tuli voimaan yleinen tietosuoja-asetus, jossa organisaatioille asetetaan tietosuojaa ja yksityisyyttä EU:ssa koskevia velvoitteita[28]. Jos tietosuojaloukkaukset aiheuttavat riskin käyttäjien oikeuksille ja vapauksille, yritysten on ilmoitettava 72 tunnin kuluessa niille, joita loukkaus koskee.

On kiintoisaa seurata, mitä kielteisiä vaikutuksia yksityisyyden loukkaamisella voi olla ihmisten mielenterveyteen. Yksityisyys on itse asiassa psykologinen tarve, joka liittyy tiiviisti ihmisen henkilöllisyyden kehittymiseen (Aboujaoude, 2019).

Kyberrikoksen uhriksi joutumista koskevassa tutkimuksessa korostetaan sekä yritysten että yksityishenkilöiden kielteisiä kokemuksia (esimerkiksi Augustina, 2015 ja McGuire & Dowling, 2013). Etenkin silloin, kun organisaatiota vastaan hyökätään kiristyshaittaohjelmilla, se vaikuttaa IT-henkilöstöön, koska hyökkäys vahingoittaa osaavien työntekijöiden ammatillista itseluottamusta ja vähentää heitä kohtaan tunnettua arvostusta[29]. Kiristyshaittaohjelmilla tehtyjen hyökkäysten psykologinen vaikutus työntekijöiden tunteisiin on myös todennäköisesti muita kyberhäiriöitä suurempi. Tämä johtuu siitä, että yritysten maksaessa lunnaat ne ”palkitsevat” hyökkääjät sen sijaan, että rahat sijoitettaisiin henkilöstöön[30].

Inhimillisiin virheisiin on syytä kiinnittää enemmän huomiota, koska niiden katsotaan aiheuttavan 90 prosenttia kyberturvaloukkauksista[31]. Tällaisia virheitä ovat muun muassa verkkourkintatarkoituksessa lähetettyjen sähköpostiviestien avaaminen ja salasanojen hallinnan laiminlyönti, jotka voivat altistaa organisaatiot vakaville seurauksille. Yrityksen verkkoon voidaan muun muassa asentaa tahattomasti haittaohjelma. On helppoa kuvitella, että tapahtuneesta vastuulliset työntekijät tuntevat epäonnistuneensa. Se voi myös estää heitä ilmoittamasta virheestä organisaatiossaan.

Inhimillisten virheiden osalta on tärkeää ottaa huomioon kyberhäiriöihin liittyvät psykologiset tekijät: työntekijöistä 52 prosenttia tekee todennäköisemmin virheitä stressaantuneena, 43 prosenttia

25 https://www.technologyreview.com/2020/10/29/1011436/a-wave-of-ransomware-hits-us-hospitals-as-coronavirus-spikes/

26 Ashley Madison -seuranhakusivuston hakkerointi heinäkuussa 2015 on esimerkki järkyttävistä seurauksista. Hakkereiden julkistamat tiedot sisälsivät nimiä, salasanoja, osoitteita sekä tietoa asiakkaiden seksuaalisista mieltymyksistä. Tästä tietosuojaloukkauksesta seurasi irtisanomisia, avioeroja ja itsemurhia. https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2017/CYB-ET/Pres/8-4%20Waleed%20Hagag_PrivacyVSSecurity.pdf

28 https://gdpr.eu/tag/gdpr/

29 https://www.sophos.com/en-us/content/cybersecurity-the-human-challenge.aspx

30 https://securityintelligence.com/posts/ransomware-response-beyond-money-to-morale/

31 https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/

väsyneenä ja 26 prosenttia silloin, kun he tuntevat olevansa loppuun palaneita[32]. Puhumattakaan siitä, että kyberturvallisuuden asiantuntijat tuntevat itsensä erittäin stressaantuneiksi tai loppuun palaneiksi, kun he pyrkivät estämään ja lieventämään kyberhyökkäyksiä[33].

Sivuhuomautuksena on lopuksi todettava, että on tärkeää seurata kyberulottuvuuden vaikutusta myös väkivaltailmiöihin. Esimerkiksi verkkokiusaaminen on laajimmin tunnettu verkkohäirinnän muoto (Notar et al., 2013). Siinä pyritään nolaamaan, ahdistelemaan ja hallitsemaan ihmisiä digitaalisin keinoin. Vaikka tämä ilmiö ei kuulu tiukasti tulkittuna kyberturvallisuuden alaan, myös haittaohjelmien ja identiteettivarkauksien kaltaisia hyökkäyksiä voidaan käyttää ihmisten vahingoittamiseen. Verkkohäirinnällä voi olla vakavia psykosomaattisia, sosiaalisia ja henkisiä vaikutuksia (Dressing et al., 2014; Betts, 2016). Koska siis verkkokiusaaminen työssä (Corradini, 2019; Farley et al., 2021) voi vaarantaa työntekijöiden terveyden ja turvallisuuden, tähän ongelmaan on puututtava asianmukaisesti.

Kyberhyökkäysten kohde

Jokaisella työelämän alalla on innovaatioteknologiaa. Kaikki organisaatiot – mikroyritykset, pienet ja keskisuuret yritykset (pk-yritykset) sekä suuryritykset – voivat olla kyberrikollisten kohteena ja siten kyberhyökkäysten vaarassa. Monilla mikro- ja pienyrityksillä ei ole tarvittavia resursseja puolustautumiseen. Tästä on osoituksena se, että 43 prosenttia kaikista tietoturvaloukkauksista koskee mikro- ja pienyrityksiä. (Verizon, 2019.)

On selvää, että digitalisoituneessa maailmassa yritykset kytkeytyvät toisiinsa entistä tiiviimmin, mikä kasvattaa hyökkäyspinta-alaa.

IBM:n vuoden 2021 turvallisuusraportissa tarkasteltiin, mitkä toimialat ovat alttiimpia kyberhyökkäyksille. Vuonna 2020 hyökkäyksiä tehtiin eniten rahoitus- ja vakuutusalalla, jonka osuus hyökkäyksistä oli 23 prosenttia. Sen jälkeen tulivat tuotantoteollisuus (17,7 %), energia-ala (11,1 %), vähittäismyyntiala (10,2 %), ammattilaispalvelut (8,7 %), julkishallinto (7,9 %), terveydenhuolto (6,6 %), tiedotusvälineet (5,7 %), liikenne (5,1 %) ja koulutus (4,0 %).

Tutkimuksista, joissa tarkkaillaan kyberhyökkäysten kohteena olevien toimialojen kehitystä, käy ilmi, että terveydenhuoltoala on entistä houkuttelevampi kyberrikollisille,[34] erityisesti potilasasiakirjojen sisältämien arkaluonteisten tietojen vuoksi (Martin et al., 2017). Covid-19-pandemia on pahentanut tilannetta niin, että kyberrikolliset ovat kääntäneet huomionsa rokotekehitystä koskevaan henkiseen omaisuuteen (Muthuppalaniappan & Stevenson, 2021) ja alkaneet lähettää verkkourkintatarkoituksessa covid-19-aiheisia sähköpostiviestejä[35]. Pandemian torjunta on kuitenkin muuttanut terveydenhuoltoalaa huomattavasti. Tulevaisuudennäkymien perusteella sen onkin vahvistettava turvallisuustoimenpiteitään.[36]

Koulutuslaitoksista on myös tulossa houkutteleva kohde kyberrikollisille. Vuonna 2020 44 prosenttia koululaitoksista joutui kiristyshaittaohjelmalla tehdyn hyökkäyksen kohteeksi. ja niistä 35 prosenttia maksoi lunnaat saadakseen tietonsa takaisin.[37] Syynä pidetään pääosin kyberturvallisuudelle osoitettuja vähäisiä määrärahoja ja suurta käyttäjäpohjaa eli opiskelijoita ja henkilökuntaa, jotka voivat lisätä alttiutta hyökkäyksille. Opettajilta ja opiskelijoilta puuttuu myös digitaalista valveutuneisuutta, joten digitaaliteknologioiden vastuullisesta käytöstä on järjestettävä koulutusta (Corradini & Nardelli, 2020).

Kyberhyökkäystilanne muuttuu jatkuvasti, joten päivityksiä on erittäin tärkeää seurata vuosittain. Tilanne on jo muuttumassa huolestuttavammaksi. Haittaohjelmia käyttävät rikolliset testaavat jo uusia kiristystapoja. Sen vuoksi organisaatioiden on tehtävä yhteistyötä ja jaettava tietoja voidakseen reagoida uhkaavaan toimintaan.[38]

Uhriksi joutumisen riskitekijät

[32] https://www.tessian.com/research/the-psychology-of-human-error/
[33] https://news.vmware.com/security/hacking-burnout-for-cybersecurity-awareness-month-2021
[34] https://cybersecurityguide.org/industries/healthcare/
[35] https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home
[36] https://www.protiviti.com/US-en/insights/whitepaper-top-risks-2021-and-2030-healthcare-industry-perspective
[37] https://news.sophos.com/en-us/2021/07/13/the-state-of-ransomware-in-education-2021/
[38] https://www.accenture.com/us-en/insights/security/cyber-threat-intelligence-report-2021

Kyberrikolliset hyökkäävät mieluummin yrityksiin varastetuilla salasanoilla kuin tekevät joukkohyökkäyksiä saadakseen kuluttajien tietoja[39]. Siitä huolimatta 330 miljoonaa aikuista kymmenessä maassa joutui kyberrikoksen kohteeksi vuonna 2020[40], puhumattakaan siitä, että tiettyjen työntekijöiden ottaminen kohteeksi esimerkiksi kohdennetussa verkkourkinnassa voi olla tehokas strategia heidän organisaatioonsa tietovarantoihin tunkeutumiseksi.

Riski erityyppisten kyberrikosten uhriksi joutumiseen riippuu sekä henkilökohtaisista että ympäristöön liittyvistä tekijöistä (Jansen et al., 2017). Uhrien profiilien tutkiminen voi auttaa ymmärtämään paremmin kyberhyökkäysten ja uhrien taustan välistä yhteyttä.

Kun kyberrikosten uhreja analysoidaan esimerkiksi sukupolven perusteella, vaikuttaa siltä, että nuoret aikuiset (alle 25-vuotiaat) ja iäkkäimmät (vähintään 75-vuotiaat) ovat alttiimpia kyberhyökkäyksille[41]. Sukupuoli on tärkeä kyberturvallisuutta koskevaan käyttäytymiseen vaikuttava tekijä (Anwar et al., 2017). Demografisia piirteitä koskevat tämän alan lisätutkimukset voisivat kuitenkin olla erittäin mielenkiintoisia ennaltaehkäisytoimenpiteiden käsittelyssä. Joistakin tutkimuksista on käynyt ilmi, että naiset ovat todennäköisemmin verkkourkintahyökkäysten kohteena (Darwish et al., 2012). Toiset tutkimukset taas osoittavat, että naiset kiinnittävät miehiä enemmän huomiota yksityisyyteen sosiaalisen median sivustoilla (Tifferet, 2019).

Koska työympäristöjä on vahvistettava kyberuhkia vastaan, olisi mielenkiintoista analysoida, miten organisatoriset tekijät, kuten käyttäytymissäännöt ja rutiinit, vaikuttavat työntekijöiden alttiuteen verkkourkintaa ja kohdennettua verkkourkintaa sisältäville sähköpostiviesteille (Williams et al., 2018). Tällaisesta laajasta analyysista voitaisiin saada hyödyllisiä näkemyksiä rajapintojen suunnittelun ja työntekijöille suunnattujen valistusohjelmien parantamiseen.

Tavoitteena kokonaisvaltainen kyberturvallisuus: valveutuneisuuden merkitys

Kyberuhkien vaikutus terveyteen ja turvallisuuteen on erittäin monitahoinen haaste organisaatioille. Niihin on sisällytettävä kaikki tarvittavat toimenpiteet kyberturvallisuutta koskevaan yrityksen laajuiseen toimintamalliin.[42]

Tämä malli edellyttää suojelua ja turvallisuutta koskevien näkökohtien yhdistämistä. Niitä on tavallisesti pidetty erillisinä käsitteinä erilaisten lainsäädännöllisten rajojen, etujen ja käytännön kysymysten vuoksi. (Boustras & Waring, 2020.)

Eri sidosryhmien tietoisuudella on tämän tavoitteen saavuttamisessa keskeinen rooli. Tietoisuutta pitäisikin kehittää sekä kyberturvallisuuden että työsuojelun näkökulmista ja yhdistää nämä näkökulmat tiiviisti toisiinsa.

Kyberturvallisuutta koskevissa tutkimuksissa on tullut esille , että turvallisuustekijöiden ja muiden organisatoristen tekijöiden heikko huomioiminen altistaa organisaatiot kyberhyökkäyksille. Tämä voi tarkoittaa esimerkiksi riittämättömiä vastatoimia. (Hart, 2019.) Myös työntekijöiden tietämättömyys kyberturvallisuudesta on monen kyberhäiriön takana toimialasta riippumatta[43]. Kyberturvallisuustietoisuutta lisäävillä ohjelmilla voi siksi olla merkittävä rooli organisaatioiden tehokkaan kyberturvallisuuskulttuurin kehittämisessä (Corradini, 2020) ja kyberhyökkäysten estämisessä (Aldawood & Skinner, 2018).

Kun kasvatetaan tietoisuutta kyberhyökkäysten mahdollisista seurauksista työterveydelle ja -turvallisuudelle, on kiinnitettävä aiempaa enemmän huomiota sellaisiin haitta ja vaaratekijöihin, joiden ei perinteisesti ole katsottu liittyvän työntekijöiden terveyteen ja turvallisuuteen. Myös työsuojelun riskinhallinnan myönteisistä kokemuksista voi herätä monia uusia oivalluksia. Tämä perustuu siihen, että organisaatioiden terveyttä ja turvallisuutta koskevissa kysymyksissä pystytään hyödyntämään pitkää, monien vuosien kokemusta, toisin kuin kyberturvallisuuden alalla. Lukuisia työympäristöjen

[39] https://www.idtheftcenter.org/identity-theft-resource-centers-2020-annual-data-breach-report-reveals-19-percent-decrease-in-breaches/?utm_source=email&utm_medium=TMIEmail012821&utm_campaign=2020DBRReport
[40] https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf
[41] https://risk.lexisnexis.co.uk/about-us/press-room/press-release/20200223-biannual-cybercrime-report
[42] https://app.croneri.co.uk/feature-articles/health-safety-and-cyber-threats?topic=3682&product=154&section=3511
[43] https://www.techrepublic.com/article/awareness-of-cyberattacks-and-cybersecurity-may-be-lacking-among-workers/

turvallisuutta lisääviä sovelluksia ja ohjelmia käytetään jatkuvasti menestyksekkäästi. Lisäksi inhimillisten virheiden hallinta katsotaan työsuojelun alalla keskeiseksi tapaturmien ennaltaehkäisyssä.

Koska tietoturvapalvelut/-osastot/-asiantuntijat eivät myöskään tavallisesti ole perehtyneitä työterveyteen ja -turvallisuuteen eikä työsuojeluyhteisö ole perehtynyt kyberuhkiin, näiden kahden alan välinen yhteistyö on olennaisen tärkeää. Jos esimerkiksi yhteistyö työsuojelu-, henkilöstö- ja tietoturvayksikköjen välillä on mahdollista, kyberuhkakysymystä voidaan tarkastella eri näkökulmista ja löytää entistä tehokkaampia ja innovatiivisempia ratkaisuja, joilla uhkia voidaan estää ennalta.

Sidosryhmien tietoisuuden kasvattaminen

Edellä kuvatun perusteella ensimmäiseksi on valistettava eri sidosryhmiä kyberuhkiin liittyvistä työsuojeluriskeistä, jotta sidosryhmät saadaan toimimaan vastuullisesti.

Valistusohjelmat voivat olla erittäin hyödyllisiä, mutta ne on suunniteltava hyvin ja räätälöitävä nimenomaisiin tilanteisiin, jotta ne ovat tehokkaita ja jotta ne soveltuvat eri sidosryhmille. Niiden pitäisi myös sisältää erilaisia työkaluja ja menetelmiä, kuten kampanjoita, työpajoja, konferensseja, koulutusmateriaaleja ja muita viestintätoimia. Mikroyritysten ja pk-yritysten tueksi olisi myös toteutettava erityisiä hankkeita niiden ominaisuuksien ja rajallisten resurssien vuoksi.

Valistusohjelmiin olisi saatava mukaan vähintään seuraavat sisäiset ja ulkoiset sidosryhmät:

- **Työnantajat**, jotka ovat oikeudellisesti vastuussa työntekijöidensä turvallisuudesta ja terveydestä, ja **johtajat**, jotka ovat johtoasemansa vuoksi ensisijaisia toimijoita organisaatioissa. Terveys- ja turvallisuuslainsäädännön mukaan työnantajilla on laajat velvollisuudet suojella työntekijöitään kaikilta työperäisiltä vaaroilta ja hallita näitä riskejä tehokkaasti. Koska kyberuhat voivat vaikuttaa työntekijöiden terveyteen ja turvallisuuteen, ne olisi otettava yksiselitteisesti huomioon riskien hallintatoimissa.
- **Työntekijöille** on tiedotettava kaikista turvallisuus- ja terveysvaaroista, joita heillä voi olla työtehtävien aikana, ja kyberriskit pitäisi sisällyttää niihin: siksi on selvää, että tietojen antaminen työntekijöille ja heidän kouluttamisensa tästä nimenomaisesta kysymyksestä ovat keskeisiä ennaltaehkäisytoimenpiteitä.
- **Työsuojelutoimijat** olisi otettava mukaan valistushankkeisiin, koska heillä ei yleensä ole tietämystä kyberturvallisuudesta. Heillä voisi olla keskeinen rooli työntekijöiden terveyteen ja turvallisuuteen vaikuttavien kyberhyökkäysten ennaltaehkäisyssä. . Heidät olisi myös pidettävä ajan tasalla organisaation tilanteiden kehittymisestä ja sen kyberturvallisuudelle aiheuttamista vaaroista.
- **Työsuojeluviranomaisilta** edellytetään kyberuhkien työterveydelle- ja -turvallisuudelle aiheuttamien uusien uhkien myötä myös uusien menetelmien ja työkalujen käyttöönottoa. Kyberuhkiin liittyvien turvallisuusriskien tunnistaminen on siksi keskeistä sekä niiden tutkinnassa että ennaltaehkäisyssä.
- **Tietoturvajohtajat** eivät useinkaan ole perehtyneitä kyberturvallisuutta koskeviin suojelunäkökohtiin, koska he luonnostaan keskittyvät työssään pääosin verkko- ja tietoturvallisuuteen sekä oman organisaationsa tehokkaiden IT-käytäntöjen suunnitteluun ja hallintaan. Lisäämällä heidän tietoisuuttaan työterveys- ja -turvallisuusuhkista voitaisiin edistää yhteistyötä työsuojeluasiantuntijoiden kanssa ja saada uusia ajatuksia organisaatioiden turvallisuussääntöjen ja -käytäntöjen laatimiseen.

Koska kyberturvallisuuteen liittyvät haitat ja vaarat laajenevat jatkossa työpaikan turvallisuuteen, muidenkin sidosryhmien olisi oltava tietoisia kyberturvallisuuden vaikutuksista työterveyteen ja -turvallisuuteen ja osallistuttava ennaltaehkäisystrategioiden laatimiseen. Näitä sidosryhmiä ovat esimerkiksi ihmisen ja tietokoneen välisen vuorovaikutuksen asiantuntijat ja ohjelmistokehittäjät.

Ihmisen ja tietokoneen välinen vuorovaikutus on monitieteinen tutkimusala, jossa alun perin keskityttiin käyttäjien ja tietokoneen väliseen vuorovaikutukseen ja jossa nyt käsitellään useita tietotekniikan suunnittelun puolia[44]. Koska työskentelylaitteiden verkottuminen lisääntyy, on olennaisen tärkeää, että alan asiantuntijat suunnittelevat ihmisen ja tietokoneen välisen rajapinnan

[44] https://www.interaction-design.org/literature/topics/human-computer-interaction

asianmukaisesti, jotta vaikutus kyberturvallisuuteen ja työterveyteen ja -turvallisuuteen voidaan minimoida (Korfmacher, 2019).

Myös **ohjelmistokehittäjillä** voi olla tärkeä rooli, koska yhä suurempi osa työssä käyvästä väestöstä hoitaa tehtävänsä tietojärjestelmien avulla riippumatta siitä, tehdäänkö työ itse paikalla vai etäyhteydellä. Siksi on tärkeää lisätä ohjelmistokehittäjien tietoisuutta kyberhyökkäysten vaikutuksista työntekijöiden turvallisuuteen ja terveyteen, jotta voidaan varmistaa, että nämä järjestelmät suunnitellaan ja toteutetaan huolellisesti kyberriskeiltä suojautumisen kannalta. Tällä on myönteinen vaikutus työntekijöiden hyvinvointiin, sillä sen ansiosta he tuntevat olevansa suojassa hyökkäyksiltä.

Keskeisenä suosituksena on siis **käyttäytymistieteiden asiantuntijoiden** ottaminen mukaan kyberturvallisuustietoisuutta lisäävien ohjelmien suunnitteluun ja toteuttamiseen. Tällaisten aloitteiden onnistuminen riippuu itse asiassa osallistujien motivaatiosta sekä menetelmistä ja niiden toteuttamiseen käytettävistä työkaluista. Siksi tarvitaan riittävää pätevyyttä ja tietämystä ihmisten käyttäytymisestä.

Kyberturvallisuudessa on ennen kaikkea kysymys ihmisestä. Siksi monialaiset ryhmät, joissa tekniset taidot yhdistetään inhimillisiin ja sosiaalisiin taitoihin, ovat entistä tarpeellisempia, jotta kyberturvallisuutta voidaan hallita tehokkaasti.

Seuraavat vaiheet

Tulevissa tutkimuksissa pitäisi keskittyä kyberturvallisuuden ja työterveyden ja -turvallisuuden välisiin yhteyksiin. Tarpeiden ja puutteiden määrittäminen auttaa tunnistamaan työntekijöille aiheutuvat mahdolliset haitat ja vaarat kyberhyökkäysten kannalta sekä määrittämään asianmukaiset toimintalinjat ja ennaltaehkäisystrategiat organisaatioissa. Kirjallisuudessa on jo käsitelty suojelun ja turvallisuuden välisiä kiinnostavia yhteyksiä, kuten turvallisuuskulttuurin, työtyytyväisyyden ja vaatimukset täyttävän turvallisuuskäyttäytymisen välistä myönteistä suhdetta (Green & D'Arcy, 2010).

Kyberturvallisuuden ja turvallisuusriskien välistä suhdetta koskevassa nykyisessä tutkimuksessa keskitytään pääasiassa terveydenhuoltoalaan (esimerkiksi, Martin et al., 2017) ja itseohjautuviin ajoneuvoihin (esimerkiksi Taeihagh & Lim, 2019). Lisätutkimuksia tarvitaan kuitenkin selventämään kaikkia mahdollisia kyberhyökkäysten vaikutuksia työntekijöiden terveyteen ja turvallisuuteen kaikilla työelämän eri osa-alueilla.

Koska myös upotettuja järjestelmiä käytetään jatkossa entistäkin enemmän, on varmistettava turvallisuuden ja suojelun asianmukainen yhdistäminen. Nämä järjestelmät voitaisiin suunnitella sekä vastaamaan turvallisuustavoitteisiin (kuten hakkerien hyökkäysten estämiseen) että takaamaan suojelutoiminnot, jotta käyttäjille (työntekijöille) ei aiheudu haittaa. Suojelun ja turvallisuuden yhdistäminen on ajankohtainen aihe tehtävän kannalta kriittisten järjestelmien kehittämisessä[45]. Organisaatiot voivat saada siihen hyödyllistä tukea kansainvälisistä standardeista[46].

Hybridityöskentelyn eli kotona ja toimistossa työskentelyn yhdistämisen voidaan olettaa jatkossa yleistyvän entisestään. Tämä pätee myös esineiden internetin teknologioihin ja kyberfyysisiin järjestelmiin perustuviin älykkäisiin työskentely-ympäristöihin. (Podgórski et al., 2017). Organisaatioiden on siksi päivitettävä riskinarviointejaan, jotta kaikki työntekijöille mahdollisesti aiheutuvat haitat- ja vaarat voidaan tunnistaa ja ryhtyä asianmukaisiin toimenpiteisiin. Tämän aikaansaamiseksi on otettava käyttöön uusia menetelmiä ja työkaluja.

Päätelmät

Digitalisaatio on vääjäämätön prosessi, ja siihen liittyy useita haasteita, jotka jokaisella maalla on edessään. Kyberturvallisuus on tällä hetkellä valtava huolenaihe kaikenkokoisille yrityksille ja laitoksille kaikilla toimialoilla, ja jatkossa huoli vain kasvaa.

Kyberturvallisuuden hallintaa ei voida kuitenkaan pelkistää ainoastaan järjestelmien ja tietojen tekniseen hallintaan. Koska kyberhyökkäykset voivat vaikuttaa myös työntekijöiden terveyteen ja turvallisuuteen, organisaatioiden on otettava käyttöön kyberturvallisuutta koskeva kokonaisvaltainen

[45] https://insights.sei.cmu.edu/blog/integrating-safety-and-security-engineering-for-mission-critical-systems/
[46] Ks. esim. ISO/TR 22100-4, Safety of machinery – Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects; IEC TR 63074:2019 Safety of machinery – Security aspects related to functional safety of safety-related control systems.

toimintamalli. Jotta kyberuhkien eri vaikutuksiin voidaan puuttua, tulee **omaksua monitieteinen näkemys, sekä yhdistää teknistä ja sosiaalista osaamista**.

Suurissa organisaatioissa on erittäin suositeltavaa tehdä yhteistyötä tietoturvallisuus- ja työsuojelutoimintojen kesken, jotta voidaan saada aikaan innovatiivinen riskinarviointiprosessi sekä suojella aineellisia ja aineettomia varoja ja, ennen kaikkea, ihmisiä. Tärkeä kysymys on myös se, miten tehokkaita strategioita voidaan panna täytäntöön mikro- ja pk-yrityksissä, joilla ei usein ole erityisiä sisäisiä resursseja[47] mutta jotka kuitenkin altistuvat kyberuhkien seurauksille.

Tulevaisuuden haaste on erittäin kova. Jotta siihen vastaamisessa päästäisiin hyvin alkuun, näistä aiheista on ensin laadittava määrätietoinen ja laaja valistusohjelma. Sen avulla valmistellaan työnantajia, työntekijöitä ja työsuojeluyhteisöä sekä tietoturvajohtajia ja muita asiaankuuluvia toimijoita kohtaamaan entistä digitaalisempi tulevaisuus ja kehittyvät kyberuhat. Näitä toimijoita ovat ihmisen ja koneen vuorovaikutuksen asiantuntijat, ohjelmistokehittäjät ja inhimilliseen käyttäytymisen asiantuntijat.

Laatijat: Isabella Corradini, Themis-tutkimuskeskuksen tieteellinen johtaja (Italia),

Hankehallinto: Emmanuelle Brun ja Annick Starren sekä Ana Cayuela Euroopan työterveys- ja työturvallisuusvirastosta (EU-OSHA).

Tausta-asiakirjan tilasi Euroopan työterveys- ja työturvallisuusvirasto (EU-OSHA). Sen sisällöstä sekä siinä mahdollisesti esitetyistä näkemyksistä ja päätelmistä vastaavat yksin laatijat, eivätkä ne välttämättä vastaa EU-OSHAn kantaa.

[47] https://www.oecd-ilibrary.org/sites/cb2796c7-en/index.html?itemId=/content/component/cb2796c7-en

Viitteet

Aboujaoude, E. (2019). Protecting privacy to protect mental health: The new ethical imperative. *Journal of Medical Ethics*. *45*(9), 604–607.

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S. & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1).

Aldawood, H. & Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review. Julkaisussa IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE). IEEE, 62–68.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T. & Savage, S. (2013). Measuring the cost of cybercrime. Julkaisussa R. Böhme (toim.) *The economics of information security and privacy* (265–300). Springer-Verlag.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L. & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437–443.

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B. & Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 20*(146).

Augustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology*. *9*(1), 35–54.

Bada, M. & Nurse, J. R. C. (2020). The social and psychological impact of cyber-attacks, psychology. Julkaisussa V. Benson & J. Mcalaney (toim.), *Emerging cyber threats and cognitive vulnerabilities* (s. 73–92). Academic Press.

Betts, L. R. (2016). Cyberbullying: Approaches, consequences, and interventions. Julkaisussa J. Binder (toim.), *Palgrave studies in Cyberpsychology*. Palgrave Macmillan.

Borkovich, D. J. & Skovira, R. J. (2020). Working from home: Cybersecurity in the age of covid-19. *Issues in Information Systems*. *21*(4), 234–236.

Boustras, G. & Waring, A. (2020). Towards a reconceptualization of safety and security, their interactions, and policy requirements in a 21st century context. *Safety Science*, 132.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B. et al. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation.* https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

Cashell, B., Jackson, W. D., Jickling, M. & Webel, B. (2004). The Economic Impact of Cyber-Attacks. *CRS Report for Congress*.

Corradini, I. (2020). *Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology.* Springer.

Corradini, I. (2019). *Crimini relazionali nell'era digitale. Conoscere per prevenire. Cyber-bullismo-mobbing-stalking.* Themis.

Corradini, I., Nardelli, E. & Ahram, T. (toim.) (2020). *Advances in human factors in cybersecurity*. AHFE 2020. Advances in Intelligent Systems and Computing. Vol 1219, Springer.

Corradini, I. & Nardelli, E. (2020). Developing digital awareness at school: A fundamental step for cybersecurity education. Julkaisussa I. Corradini, E. Nardelli & T. Ahram (toim.) *Advances in human factors in cybersecurity*. AHFE 2020. Advances in intelligent systems and computing. Vol 1219, Springer.

Couce-Vieira, A., Insua, D. R. & Kosgodagan, A. (2020). Assessing and forecasting cybersecurity impacts. *Decision Analysis. 17*(4), 356–374.

Darwish, A., El Zarka, A. & Aloul, F. (2012). Towards understanding phishing victims' profile. *International Conference on Computer Systems and Industrial Informatics*. 1–5.

Disterer, G. & Kleiner, C. (2013). BYOD - Bring Your Own Device. *HMD*. 50, 92–100.

Dressing, H., Bailer, J., Anders, A., Wagner, A. & Gallas, C. (2014). Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberpsychology, Behavior, and Social Networking,* 17: 61–67.

ENISA. (2020). *Threat Landscape 2020*. https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

ENISA. (2021a). Threat Landscape 2021, 27.10.2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA (2021b). Threat Landscape for Supply Chain Attacks, 29.7.2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Farley, S., Coyne, I. & D'Cruz, P. (2021). Cyberbullying at Work: Understanding the influence of technology. Julkaisussa P. D'Cruz, E. Noronha, G. Notelaers & C. Rayner (toim.), *Handbooks of workplace bullying, emotional abuse and harassment*. Vol 1, Springer.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digital Medicine*. *2*(98).

Hamlyn-Harris, J. H. (2017). *Three reasons why pacemakers are vulnerable to hacking.* The Conversation. http://theconversation.com/three-reasons-why-pacemakers-are- vulnerable-to-hacking-83362

Hart, D. V. (2019). Factors influencing the adoption of cybersecurity situational awareness programs. *Isaca Journal*. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/factors-influencing-the-adoption-of-cybersecurity-situational-awareness-programs

Heembrock, M. (2015). The risks of wearable tech in the workplace. *Risk Management Magazine.* https://www.rmmagazine.com/articles/article/2015/02/02/-The-Risks-of-Wearable-Tech-in-the-Workplace-

Hernandez-Castro, J., Cartwright, A. & Cartwright, E. (2020). An economic analysis of ransomware and its welfare consequences. Royal Society Open Science. 7(3), 190023.

Izuakor, C. (2016). Understanding the impact of cyber security risks on safety. ICISSP 2016 – tietojärjestelmien turvallisuutta ja yksityisyyttä käsittelevä toinen kansainvälinen konferenssi.

Jansen, J., Junger, M., Kort, J., Leukfeldt, R., Veenstra, S., van Wilsem, J. & van der Zee, S. (2017). Victims. Julkaisussa R. Leukfeldt (toim.), *Research agenda. The human factor in cybercrime and cybersecurity*, Eleven International Publishing.

Kavallieratos, G., Katsikas, S. & Gkioulos, V. (2020). Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey. *Future Internet*. *12*(4), 65.

Korfmacher, S. (2019). The relevance of cybersecurity for functional safety and HCI. Julkaisussa V. Duffy (toim.), *Digital human modeling and applications in health, safety, ergonomics and risk management human body and motion HCII 2019 lecture notes in computer science*. 11581. Springer.

Loukas, G. (2019, marraskuu). Cyber-physical security threats to Occupational Safety and Health (OSH) in Industry 4.0. https://www.safe-machines-at-work.org/fileadmin/user_upload/pdf/LOUKAS.pdf

Martin, G., Martin, P., Hankin, C., Darzi, A. & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? British Medical Journal (Clinical research ed.), 358, j3179.

McGuire, M. & Dowling, S. (2013). Cybercrime: A review of the evidence. Summary of key findings and implications (Home Office Research Report, 75). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. *International Journal for Quality in Health Care*, *33*(1).

Notar, C. E., Padgett, S. & Roden, J. (2013). Cyberbullying: A review of the literature. *Universal Journal of Educational Research, 1*(1), 1–9.

Perales Gómez, Á.L., Fernández Maimó, L., Huertas Celdrán, A., García Clemente, F.J., Gil Pérez, M. & Martínez Pérez, G. (2020). SafeMan: A unified framework to manage cybersecurity and safety in manufacturing industry. *Software: Practice and Experience 51(3),* 607–627.

Podgórski, D., Majchrzycka, K., Dąbrowska, A., Gralewicz, G. & Okrasa, M. (2017). Towards a conceptual framework of OSH risk management in smart working environments based on smart PPE, ambient intelligence and the Internet of Things technologies. *International Journal of Occupational Safety and Ergonomics*, *23*(1), 1–20.

Ponemon. (2021). The impact of ransomware on healthcare during covid-19 and beyond. https://www.censinet.com/wp-content/uploads/2021/09/Ponemon-Research-Report-The-Impact-of-Ransomware-on-Healthcare-During-COVID-19-and-Beyond-sept2021-1.pdf

Stacey, N., Ellwood, P., Bradbrook, S., Reynolds, J., Williams, H. & David, L. (2018). *Tieto- ja viestintätekniikassa sekä työskentelypaikassa tapahtuvien muutosten keskeiset suuntaukset ja niihin myötävaikuttavat tekijät Työterveyden ja -turvallisuuden uusien ja kehittyvien riskien ennakointi.* Euroopan työterveys- ja työturvallisuusvirasto. https://osha.europa.eu/en/publications/foresight-new-and-emerging-occupational-safety-and-health-risks-associated

Steijn, W., van der Vorm, J., Luiijf, E., Gallis, R. & van der Beek, D. (6.9.2016). Emergent risks to workplace safety as a result of IT connections of and between work equipment. *TNO report*.

Taeihagh, A. & Lim, H. S. M. (2019). Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews*, 39, 103–128.

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior*, 93: 1–12.

Truong, T. C., Diep, Q. B. & Zelinka, I. (2020). Artificial Intelligence in the Cyber Domain: Offense and Defense. *Symmetry, 12*(3), 410.

Verizon. (2019). 2019 Data breach investigations report. https://www.key4biz.it/wp-content/uploads/2019/05/2019-data-breach-investigations-report.pdf

Verizon. (2021). 2021 Data breach investigations report. https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-data-breach-investigations-report.pdf

WEF. (2021). These are the top cybersecurity challenges of 2021. https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 9*(11), 40–53.

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120, 1–13.