KYMEN LAAKSON LIITTO

SATAMALOGISTIIKAN KYBERHYGIENIA

Kyberuhkatekijät satamalogistiikan työturvallisuudessa

Projektinumero: 13300047

Vesa Tuomala & Tuomas Heikkinen

2023

XAMK
Kaakkois-Suomen ammattikorkeakoulu

SISÄLLYS

1 JOHDANTO

Suomen taloutta pyörittävä voima on pienet ja keskisuuret yritykset, joissa työskentelee alle 250 henkilöä. Nämä PK-yritykset työllistävät 99,9 % työvoimasta.

Kyberpuolustuksen ja kansallista turvallisuutta vaarantavien kyberuhkien torjuntaan on kiinnitettävä nykyistä enemmän huomiota myös pk-yrityksissä. Yhteiskuntamme kriittiseen infrastruktuuriin kohdistuu tällä hetkellä turvallisuuden uhkia ja riskejä kyberrikollisuudesta, vakoilusta, eri valtioiden tiedustelupalvelusta ja hybridivaikuttamisesta, sekä henkilöstön inhimillisistä virheistä. Kriittisten yritysten, tuotantolaitoksien, satamien ja merenkulun tulee hyödyntää enenevässä laajuudessa kyberhygieniaa ja inhimillisiä tekijöitä turvallisuuden lisäämisessä.

Kyberturvallisuus on kokonaisturvallisuutta

Kyberturvallisuus on osa jokaisen organisaation ja yksilön sosiaalista vastuuta. Euroopan Unionin (EU) uusi NIS2-kyberturvallisuusdirektiivi tulee vaikuttamaan useiden suomalaisten, kriittisen infrastruktuurin ja tärkeitä yhteiskunnallisia toimintoja tekevien yritysten toimintojen suojaamiseksi jo lokakuussa 2024. Kriittiseksi infrastruktuuriksi luokitellaan energia-, liikenne-, pankki- ja rahoitusmarkkinat, terveydenhuolto, juomavesi- ja jätehuolto, digitaaliset ICT-palvelut ja julkishallinon lisäksi jopa avaruussektori.

Kriittisiksi aloiksi luetaan myös posti- ja kuriiripalvelut, jätehuolto. kemikaali-, elintarvike- ja valmistusteollisuus. Kriittinen tarkoittaa, että vahinkoa voi aiheutua omaisuudelle ja jopa ihmishenkien menetyksiä toiminnan häiriintymisen myötä. EU:n NIS2 -direktiivillä suojellaan ja turvataan henkilöstöä, organisaatioita ja kriittistä infrastruktuuria kyberhyökkäyksiä vastaan. Direktiivin mukaan kyberhyökkäyksiä vastaan tulee valmistautua, harjoitella ja noudattaa kyberhygieniaa koko organisaation voimin.

2 SATAMALOGISTIIKAN KYBERHYGIENIA

Euroopan turvallisuustilanteen ja Suomen Nato-hakuprosessin yhteydessä nousi kyber- ja hybridivaikuttamisen uhka Suomessa keväällä 2022. Uhka kohdistuu kaikkiin yhteiskunnallisesti merkittäviin toimijoihin, myös kriittiseen infrastruktuuriin. Kriittinen infrastruktuuri on yhteiskunnan hyvinvointiin, toimintaan ja turvallisuuteen liittyvät elintärkeät palvelut, järjestelmät ja rakenteet.

Satamat kuuluvat kriittiseen infrastruktuuriin ja ovat Suomen elinkeinoelämän kannalta erittäin tärkeitä huoltovarmuudellemme. Toiminnan hidastaminen, lamauttaminen ja sekasorron lisääminen satamissa aiheuttaisivat myös uhkia niissä toimivien työntekijöiden kokonaisturvallisuudelle.

Tämä raportti on osa ”Kyberuhkatekijät satamalogistiikan työturvallisuudessa” -projektin tehtäviä, jolla kehitetään satamalogistiikan yritysten turvallisuutta ja varautumista kyberuhkatekijöihin. Projektin nimi lyhennettiin muotoon ”Satamalogistiikan kyberhygienia” suuntautuen kehittämään satamassa toimivan työntekijän vastuuta kyberuhkien torjumisessa ja lisäten samalla satamalogistiikan työturvallisuutta.

Raportissa analysoidaan ja osoitetaan kehityskohdat työntekijöiden turvallisuutta lisääville toimenpiteille, jotka tulivat esiin kevään 2023 haastatteluissa Kaakkois-Suomessa toimiville satamalogistiikan yrityksille. Tämän raportin perusteella on tuotettu myös kyberhygienia -infopaketti satamissa toimiville yrityksille. Kyberhygienia-infopaketin avulla yritykset voivat kehittää toimintatapojaan, sekä kouluttaa, ohjeistaa ja harjoitella toimintaa kyberuhkia vastaan.

Työpaketin tehtävänä oli selvittää yritysten ja työntekijöiden tarpeita kyber- ja hybridivaikuttamisen varautumiseen. Henkilöhaastatteluilla löydettiin kriittisiä kehityskohtia, jotka voivat olla aiheuttaa merkittäviä turvallisuusongelmia.

3 SATAMAYRITYSTEN HAASTATTELUIDEN ETENEMINEN

Haastatteluja varten luotiin ensin kysymyspohja, jota käytettiin haastatteluiden runkona. Kysymyspohjassa käsiteltiin yrityksen digitalisaatiota, yrityksen ja henkilöstön kyberturvallisuutta, informaatiovaikuttamista ja valtiollista toimintaa. Haastattelut litteroitiin, eli nauhoite kirjoitettiin tekstiksi, analysoitiin ja kirjattiin auki tähän raporttiin.

Haastattelut lähtivät käyntiin harjoitushaastatteluilla. Harjoitushaastattelujen jälkeen totesimme, että haastateltavien valintaan tulee asettaa kriteerit. Haastateltavien tulee toimia joko yrityksen johtoryhmätason tehtävissä tai yrityksen asiantuntijatason informaatiotekniikan (IT), tietohallinnon tai kyberturvallisuuden tehtävissä. Kriteerien asettaminen mahdollisti sen, että haastateltavat kykenivät vastaamaan asettamiimme kysymyksiin monipuolisesti.

Ensimmäinen haastateltava yritys valittiin satunnaisesti. Seuraavat haastateltavat valittiin satunnaisotoksella niin, että valitsimme joka viidennen (5.) Hamina-Kotka Sataman alueella toimivan yrityksen. Aloitimme valinnan ensimmäisestä valitsemastamme yrityksestä. Satunnaisotoksen tavoitteena oli kerätä monipuolisia näkökulmia ilmiöön ja pienentää haastattelijoiden vaikutusta tuloksiin.

HaminaKotka Satama Oy:n alueella on toimivia yrityksiä 119 kappaletta (HaminaKotka Satama 2023). Haastatteluihin valitsimme joka viidennen yrityksen haastateltavaksi, toteuttaen yhteensä 17 yrityshaastattelua ”Satamalogistiikan kyberhygienia” -hankkeessa. Haastatteluissa alkoi toteutumaan kyllääntyminen viimeisimpien haastatteluiden kohdalla. Kyllääntyminen tarkoittaa sitä, että haastatteluiden tulokset alkoivat toistamaan itseään, eikä uusi haastateltava tuonut lisää uutta tietoa aiempien haastatteluiden joukkoon.

Yleisen tietosuoja-asetuksen (GDPR, General Data Protection Regulation) mukaisesti emme julkaise haastateltujen yrityksien tietoja julkisesti. Haastatellut yritykset kattavat kaikki pienet ja keskisuuret satamassa toimivat yritykset.

4 KOOSTE HAASTATTELUISTA

4.1 Digitalisaatio

4.1.1 Digitalisaatio ja kyberturvallisuus

Digitalisaatiolla on ollut merkittäviä vaikutuksia satamassa toimivien yrityksien toimintaan. Pääosin kaikki toiminta perustuu sähköiseen tiedonsiirtoon, ja tieto nähdään yrityksen pääomana. Digitalisaatio on sujuvoittanut toimintaa ja haastatteluiden mukaan myös nopeuttanut tiedonkulkua, mahdollistaen paremman ennakkosuunnittelun ja raportoinnin. Digitaalisten järjestelmien ja laitteiden määrä on haastatteluiden mukaan lisääntynyt selvästi logistiikassa. Satamatoimijoiden integraatiota, eli yhdistämistä on myös tehty paljon. Valtaosa työstä tehdään digitaalisilla taustajärjestelmillä.

Digitalisaatio tehostaa toimintaa ja tiedonkulkua, joskin järjestelmien monimutkaisuus ja ihmisten tietotaito järjestelmien käyttämisessä aiheuttaa haittaa käyttäjille. Digitalisoituminen korostaa tämän takia kyber- ja tietoturva-asioiden merkitystä. Erään haastateltavan mukaan päivittäinen järjestelmien käyttäminen on mennyt käyttäjän kannalta vaikeaksi. Käyttäminen on toki turvallista, mutta vastassa on järjestelmän turvallisuus ja sen käytettävyys. Tietosuojan merkitystä myös korostetaan, sillä moni yritys käsittelee asiakkaiden tietoja.

Uhkien varautumisastetta on huomattavasti nostettu ja jatkuvasti parannettu. Tieto- ja kyberturva ovat mukana eri yrityksien kehityshankkeissa ja niihin kiinnitetään huomiota – parannettavaakin vastaajien mukaan vielä on. Digitalisaation avulla monet asiat ovat saatavilla koko ajan ympäri maailmaa, mikä aiheuttaa vaatimuksia turvallisuudelle. Myös operatiivisen teknologian (OT) merkitys on noussut ja sen turvallisuuteen panostetaan.

Pilvipalveluita tarjotaan yrityksille ja niitä käytetään osassa haastatelluissa yrityksissä. Haastatteluissa osa totesi, että riskiä on vähemmän, kun IT:tä ulkoistetaan ammattilaisille. Yritykset ovat logistiikan, eikä kyberturvallisuuden osaajia – eivätkä ymmärrä sen takia kaikkia heihin kohdistuvia uhkia.

4.1.2 Kehityskohdat digitalisaation lisääntyessä

Yritysten tulee seurata tilannekuvaa, missä maailmalla mennään kyberturvallisuusasioissa ja sen avulla kehittää omaa toimintaansa varautuen paremmin uhkakuviin. Digitalisaation lisääntyessä tulee ainakin kolmeen asiaan kiinnittää huomiota: henkilöstön kouluttamiseen, harjoitteluun ja tiedon jakamiseen satamatoimijoiden kesken.

Haastatteluissa korostetaan henkilöstön kouluttamista ja tietoisuuden lisäämistä, jotta he osaavat toimia turvallisesti kybermaailmassa. Henkilöstön tulee siis tietää, miten järjestelmiä käytetään oikein, jolloin järjestelmien haavoittuvuuksia pienennetään käyttäjien avulla. Toisaalta myös keskustellaan käyttäjän näkökulmasta digitalisaatiossa, eli mahdollisimman paljon asioista tulisi pystyä hoitamaan teknisillä ratkaisuilla, jotta käyttäjien ei tarvitsisi olla huolissaan kyber- tai tietoturvallisuudesta. Samalla ymmärretään, että ihmisten on tärkeää tiedostaa riskit.

Kehityskohteeksi nähdään myös, että satamassa voisi jakaa paremmin tietoa kyberturvallisuuteen liittyvistä asioista yrityksien kesken. Haastatteluissa nousee esille, ettei kukaan halua jakaa tietoa digitalisaatiosta ja IT-asioista eteenpäin. Tieto pidetään itsellä ja yritykset kehittävät omaa digitalisaatiotaan. Hyväksi todettuja parhaita käytäntöjä kannattaa jakaa satamaien yrityksien välillä, jolloin tiedonjaosta olisi hyötyä kaikille uhkiin vastaamisessa.

4.1.3 Toiminta yleensä pysähtyy, jos järjestelmät pettävät

Vastaukset vaihtelivat, voiko toiminta jatkua, jos digitaaliset järjestelmät lakkaavat toimimasta. Käytännössä yritystoiminta pysähtyy kokonaan, tai jatkuu enintään muutaman päivän. Toiminnan jatkuessa se ei olisi kovinkaan tehokasta, eikä pitkässä juoksussa toiminta olisi myöskään kannattavaa. Toimitusketjun katkeaminen johtaa yleensä myös kulujen kasvuun ja aiheuttaa yritykselle sanktioita. Satamalogistiikassa iso osa toiminnasta liittyy tietokoneilla ja -järjestelmillä tehtävään työhön.

Kyberhyökkäyksessä satamalogistiikan yrityksen toiminta voi pysähtyä haastatteluiden perusteella hyvinkin nopeasti, jopa välittömästi. Tämä johtuu siitä, että

tietomassa on valtava, mikä yrityksissä liikkuu. Tieto voi liittyä esimerkiksi käsiteltäviin lasteihin. Toimintaa voi osassa yrityksissä hoitaa hetken työskennellen manuaalisesti paperilla, mutta ei kovin pitkään – on erittäin oletettavaa, että satamaan tulevat ja lähtevät tavaralastit menevät nopeasti sekaisin, jos logistiikkaa yritetään hoitaa paperilla. Digitaalisten järjestelmien toiminnan pysähtymisessä fyysinen tavara voi liikkua, mutta toiminta menee nopeasti sekaisin volyymien ollessa satamissa suuria. Yritykset ovat järjestelmiensä varassa.

Tietoliikenneyhteydet ovat merkittävässä roolissa niin yrityksien sisäisesti, kuin myös sidosryhmien suuntaan. Ongelmat toimitusketjun yhdessä kohdassa vaikuttavat laajasti myös koko ketjuun, esimerkiksi lastinkäsittelyn eri vaiheissa. Vaikutukset sidosryhmiin nähdään esimerkiksi silloin, jos lasteja ei voi käsitellä satamissa, terminaaleissa, varastoissa tai logistiikkakeskuksissa yhteysongelmien takia. Tällöin laivoja ei voi purkaa eikä lastata. Digitalisaatio on tehostanut toimintaa ja samalla lisännyt yrityksien haavoittuvuutta järjestelmien toiminnalle. Tämä korostaa kyberturvallisuuden merkitystä satamalogistiikassa.

4.2 Yrityksen kyberturvallisuus

4.2.1 Satamat ovat osa yhteiskunnan kriittistä infrastruktuuria

Satamat ovat osa yhteiskuntamme kriittistä infrastruktuuria. Tästä huolimatta moni satamatoimijoista kokee, ettei se vaikuta niihin uhkakuviin, joihin he ovat varautuneet. Haastateltavat kokevat, etteivät olisi sataman lamaannuttamisessa ensimmäinen kohde, eikä hyökkääjillä olisi motiiveja heidän toimintojansa kohtaan – he ovat enemmän palveluiden käyttäjiä, kuin infran omistajia. Osa ei tiedä vaikuttaako varsinaisesti satamassa toimiminen uhkakuviin; yritys voi olla osa isoa kansainvälistä yritystä ja uhkakuvat tulevat sitä kautta.

Osa kuitenkin kokee, että satamassa toimiminen vaikuttaa varautumiseen. Tietyillä toimialoilla, kuten kemianteollisuudessa, kiinnitetään tähän erityistä huomiota. Yritys ei voi ottaa samalla tavoin riskejä kuin muiden toimialojen yritykset. Haastatteluissa myös korostuu, että yritykset ovat osa isompaa kokonaisuutta ja suurempiin toimijoihin kohdistettu hyökkäys voi selvästi vaikuttaa sidosryhmiin. Nähdään, että pieneen yksikköön pääsee helpommin sisälle kuin isoon

yritykseen, mutta toisaalta pienyritykseen kohdistettu vaikuttaminen ei välttämättä ole merkityksellistä infrastruktuurille. Tämän vuoksi suuremmista toimijoista ollaan kiinnostuneempia.

Eräässä haastattelussa todetaan, että toimiminen kriittisen infrastruktuurin osana, kyseinen yritys tekee kyberturvallisuuden kehittämisessä tiiviimpää yhteistyötä yhteistyökumppaniensa kanssa. Tietoja vaihdetaan ja yhdessä harjoitellaan erilaisia tilanteita varten.

4.2.2 Yrityksien kyber- ja hybridiuhkia

Konkreettisia kyberuhkia:

- kiristyshaittaohjelmat
- tietojen kalastelu
- käyttäjän manipulointi
- järjestelmien lamauttaminen
- tiedon häviäminen ja väärinkäyttö, sekä tietovuodot
- palvelunestohyökkäys
- sidosryhmiin kohdistuvat hyökkäykset

Haastatteluissa tietojenkalastelu nousi todennäköisimmäksi kyberuhkaksi yrityksille. Tietojenkalastelusähköposteja tulee säännöllisesti valtavia määriä. Ne voivat hidastaa palveluita ja niiden kautta voi päästä myös yrityksen tietoverkkoon sisään. Yrityksen työntekijä nähdään heikoimmaksi lenkiksi, jolloin eniten hyökkäyksiä kohdistetaan heihin. Samassa yhteydessä korostetaan myös käyttäjän manipulointia, eli henkilön harhauttamista, häneen vaikuttamista tai hallitsemaan hänen ajatteluansa, tuntemuksia tai käyttäytymistä. Ulkopuolinen henkilö tai manipuloitu työntekijä voi syöttää esimerkiksi haitallisen USB-tikun tai -median yrityksen tietojärjestelmän laitteisiin.

Kyberuhkia lähestytään haastatteluissa myös sitä kautta, että yrityksellä on tietyt ”kyberviholliset”, jotka voidaan jakaa kolmeen tekijään:

1) Taloudellisen edun tavoittelijat, esimerkiksi kiristyshaittaohjelmilla, jotka pääsevät yrityksen tietojärjestelmään

2) Valtiollinen toiminta, sillä satamien yritykset ovat osa kriittistä infrastruktuuria – jotkut jopa huoltovarmuuskriittisiä yhtiöitä. Tällöin yritys on siis houkutteleva kohde valtiolliselle toimijalle

3) Aktivistit/haktivistit nähdään uusimpana ja pienimpänä uhkana, eli esimerkiksi ilmastoasioiden takia jokin taho voi kohdistaa hyökkäyksiä yritykseen kansalaisaktivismin muodossa

Haastatteluiden perusteella pahin konkreettinen kyberuhka on, että joku onnistuu pääsemään yrityksen järjestelmiin lamauttaen ne. Konkreettinen kyberuhka on hyökkäykset erilaisiin järjestelmiin, järjestelmien manipulointi ja se, etteivät järjestelmät ole käytettävissä. Palvelunestohyökkäysien vakavuutta korostetaan, sillä niiden avulla voidaan aiheuttaa merkittävää haittaa tietoliikenneyhteyksille ja lamauttaa yrityksen toiminnan.

Konkreettisia hybridiuhkia:

- fyysinen vaikuttaminen
- hyökkäys sähköverkkoon
- kiristäminen ja pelottelu
- informaatiovaikuttaminen
- mainehaitta

Isona hybridiuhkana nähdään fyysiseen turvallisuuteen vaikuttamisen, esimerkiksi huolintakonttorin tuhoaminen lopettaa yritystoiminnan. Sataman portit ja kulunvalvonta on helppo kiertää. Sähkökatkoilla voi olla merkittäviä vaikutuksia niiden kestäessä pitkään, jolloin ne johtavat järjestelmien lamaantumiseen. Haastatteluissa pohditaan myös, että alueelle on mahdollista saada kulkulupa yrityksien kautta. Satamien yritykset ”kulkuluvittavat” oman liikenteensä, joten rikollisella tai epärehellisellä taholla voi olla motiivina saada yrityksen kautta kulkulupa alueelle.

Hybridiuhkana pohditaan myös perheenjäsenen kiristämistä – samalla todeten, että varmasti helpompiakin keinoja on. Haastatteluissa nostetaan myös esille mahdollisuus, että rikollinen voi yrittää pyrkiä työtehtäviin yritykselle. Lisäksi hybridiuhkana nähdään fyysisen maailman teot, eli esimerkiksi pelottelu fyysisellä vaikuttamisella tai pelottelu kyberaseella.

Konkreettiseksi hybridiuhkaksi nostetaan myös informaatiovaikuttaminen; joku taho alkaa syöttämään negatiivista informaatiota, jolloin työaika menee muuhun kuin liiketoiminnan hoitamiseen. Tähän liittyvä hybridiuhka on mainehaitta, joka voidaan toteuttaa esimerkiksi levittämällä yrityksestä väärää tietoa esimerkiksi sosiaalisessa mediassa.

4.2.3 Kriittisiä työvaiheita

Kriittisiksi työvaiheiksi kuvataan pääasiassa tilanteet, joissa tietoa siirretään yrityksen ja asiakkaiden, tai yrityksen ja yhteistyökumppanien välillä. Moni yritys näkee riskiksi myös sen, että järjestelmät pettävät sataman päässä. Kriittisten sähköpostien käsitteleminen on toinen merkittävä asia. Usealle yritykselle säännöllinen tiedon liikuttaminen on kriittistä toimintaa – esimerkiksi sanomaliikenne tulliin, vaikka varajärjestelmät ovatkin olemassa.

Ihmisten välinen kanssakäyminen nähdään myös kriittiseksi työvaiheeksi, esimerkkinä asiakaspalvelu. Yritykselle voi tulla asiakkailta paljon sähköposteja ja välillä asiakkaat toimittavat yritykselle liitetiedostoja. Asiakaspalvelu ja yrityksen työntekijät ovat siis ensimmäinen rajapinta yrityksessä. Satamayrityksillä on myös paljon ulkomaisia asiakkaita. Riskinä on se, että hyökkäys tehdään asiakkaan kautta, jos heidän tietojärjestelmiinsä päästään ensin sisään.

Näiden lisäksi korostetaan, että yrityksen järjestelmät ovat kriittisiä. On hyvin haitallista, jos hyökkääjä pääsee käsiksi esimerkiksi yrityksen ohjelmistoihin. Automaatiojärjestelmien turvallisuus korostuu myös haastatteluissa. Niiden kanssa toimiminen on tarkkaa ja niiden pysähtyminen haittaa merkittävästi yrityksen toimintaa. Ohjelmistoissa ja automaatiojärjestelmissä nähdään myös merkittäviä riskejä kyber- ja hybridivaikuttamiselle.

4.3 Henkilöstön kyberturvallisuus

4.3.1 Henkilöstön digitaidot ja kyberturvatietoisuus on vaihtelevaa

Haastatteluiden perusteella yritysten henkilöstön digitaidot ja kyberturvatietoisuus on vaihtelevaa; moni vastaaja toteaa, että henkilöstön digitaidot ja kyberturvatietoisuus ovat huonolla tai jopa matalalla tasolla. Toisaalta joissain yrityksissä osaamisen taso on kohtuullinen, tai jopa hyvä. Osaamistaso on siis kirjavaa ja se nähdään riippuvan työtehtävästä, sekä yrityksen toimialasta.

Satamien yritysten henkilöstön ikäjakauma on laaja ja haastatteluiden perusteella keski-ikä on korkea. Tämän nähdään vaikuttavan osaamistasoon. Osa henkilöstöstä ei ole juurikaan käyttänyt tietokonetta elämänsä aikana. He ovat

saattaneet tehdä pitkän uran esimerkiksi ahtaajana aikana, jolloin tietokonetta ei ole tarvittu. Osa henkilöstöstä on siis ongelmissa tietokoneiden kanssa, mikä kasvattaa esimerkiksi tietojenkalastelun onnistumisen todennäköisyyttä. Lisäksi on esiintynyt muutosvastaisuutta esimerkiksi silloin, kun uusia laitteita on pitänyt ottaa käyttöön.

Haastateltavien mukaan tarvitaan henkilöstölle enemmän ohjeistusta ja tietoisuuden lisäämistä kyberuhkatekijöiden tietoisuuden lisäämiseksi. Yrityksien pitää viedä asiaa eteenpäin ja jalkauttaa sitä henkilöstölleen. Osaamista tulee kehittää tarpeen kasvaessa jatkuvasti.

Osaamista tulisi kehittää, mutta miten?

Haastatteluiden perusteella osaamista tulisi kehittää säännöllisesti. Toisaalta korostetaan, että jos asioita tapahtuu paljon jatkuvasti, siihen ”turrutaan”. Voi käydä niin, ettei esimerkiksi kalasteluviesteistä enää ilmoiteta IT-henkilöstölle. On selvää, että kyberturvallisuusasiat tulee pitää mahdollisimman yksinkertaisina henkilöstölle. Kovin montaa muistettavaa asiaa ei pidä olla – yhden haastateltavan mukaan asioita saisi olla korkeintaan kolmesta neljään.

On tärkeää korostaa varsinkin ikääntyneemmälle henkilöstölle, että tietokone ei mene rikki käytettäessä. Lisäksi henkilöstön tulee ymmärtää, että tietokone on ammattikäyttöä varten, sillä ei siis mennä minne tahansa internet-sivuille. Kyberturvallisuusasioita tulee harjoitella konkreettisissa harjoituksissa. Harjoituksessa voi esimerkiksi levittää USB-muistitikkuja työpaikalle ja seurata, yhdistetäänkö niitä laitteisiin kiinni.

Haastatteluissa myös korostui, että osaamisen kehittäminen on resursseista kiinni ja siitä, miten asiaa koulutetaan henkilöstölle. Kouluttajan tulee olla asiantuntija, mutta hänen tulee myös kyetä puhumaan asioista kohderyhmälleen ymmärrettävästi. Lisäksi ison yrityksen henkilöstön kyberturvatietoisuuden lisääminen ei ole ongelmatonta; asioiden läpikäyminen kaikkien kanssa on hankalaa, vaatien yritykseltä resursseja ja henkilöstöltä työaikaa.

4.3.2 Henkilöstöön kohdistuvia kyber- ja hybridiuhkia

Tietojenkalastelu on selkeästi suurin henkilöstöön kohdistuva kyberuhka, joka nousi esille useassa haastattelussa. Tietojenkalastelussa esimerkiksi henkilöstön käyttäjätunnuksia ja salasanoja voidaan kalastella haitallisten verkkosivujen, linkkien ja liitetiedostojen kautta. Suurin uhkakuva on se, että joku henkilöstöstä käyttäytyy huolimattomasti, ja sitä kautta esimerkiksi haittaohjelma pääsee leviämään yrityksen järjestelmiin. Myös haitalliset USB-tikut mainitaan vakavaksi uhaksi.

Uhaksi tunnistetaan myös se, että järjestelmien käyttäjät eivät pidä huolta salasanoistaan. Sähköpostien kautta tapahtuvien hyökkäyksien lisäksi kyberuhaksi nähdään se, että käyttäjä voi internet-verkkoa selaamalla saada haittaohjelmatartunnan. Perinteiset huijaussoitot, esimerkiksi ”Microsoftin tukipuhelut” mainitaan myös uhkana. Osa haastateltavista ei kuitenkaan koe, että henkilöstöön kohdistuisi kyberuhkia, vaan koetaan, että uhka kohdistuu isompiin toimijoihin ja siellä avainasemassa oleviin henkilöihin.

4.3.3 Kyberturvallisuus ja työturvallisuus

Useat vastaajat näkevät joko osittain tai täysin, että kyberturvallisuus on osa työturvallisuutta, osa taas ei. Vaihtelu vastauksissa riippuu siitä, millaista työtä yrityksessä tehdään. Toimistotyössä fyysiseen turvallisuuteen ei päästä vaikuttamaan, mutta henkiseen turvallisuuteen kyllä. Operatiivisessa työssä taas fyysinen ja psyykkinen turvallisuus ovat molemmat tärkeitä.

Monissa yrityksissä kaikki toiminta perustuu tiedon välittämiseen ja sen hyväksi käyttämiseen. Normaalissa tilanteessa työntekijän tulee kyetä keskittymään kentällä työn suorittamiseen, eli tiedon tulee olla oikeassa muodossa ja käsiteltävissä. Kesken fyysisen suorituksen (esimerkiksi työkoneella ajaminen) ei siis aleta ratkaisemaan ongelmia. Tällä tavalla luodaan myös turvallisuuden tunnetta henkilöstölle.

Kyberturvallisuus voi siis liittyä työturvallisuuteen henkisen hyvinvoinnin kautta. Osa yrityksiä ei näe, että fyysisiä vaaratilanteita voisi aiheuttaa järjestelmien

väärinkäytöllä, osassa yrityksissä tämä taas on hyvinkin mahdollista. Esimerkiksi kemianteollisuudessa vaarallisten aineiden kanssa operoidessa ja automaatiojärjestelmien käytössä tämä on oleellinen riski.

Miten kyberuhkat voivat vaikuttaa työturvallisuuteen?

Asioiden mennessä hyvin, kyber- ja hybridiuhkat eivät vaikuta työntekoon. Ongelman aikana henkilöstö ei vain voi tehdä töitä, jolloin ei synny fyysisiä, eikä henkisiä vaikutuksia. Vakavissa tapauksissa työturvallisuuteen voi olla vaikutuksia, esimerkiksi automaatiojärjestelmässä ilmenevän virheen kohdalla. Kyberhyökkäyksen vaikutuksia voidaan siis nähdä myös fyysisessä maailmassa.

Hybridiuhka voi aiheuttaa ongelmia työturvallisuudelle. Tämä voi tapahtua esimerkiksi fyysisen maailman vaikuttamisella tai väsyttämällä henkisesti työntekijä, jolloin suoriutuminen työstä heikkenee. Lisäksi osa haastateltavista pohti, että henkilötietomurto voisi liittyä työturvallisuuteen.

4.4 Informaatiovaikuttaminen

Haastatteluissa nousi esille, että informaatiovaikuttaminen koetaan yrityksissä mahdolliseksi, mutta epätodennäköiseksi uhaksi. Moni haastateltava toi esiin sen, että eivät koe yrityksen olevan kiinnostavin kohde informaatiovaikuttamiselle. Osassa yrityksissä informaatiovaikuttamisesta ei ole ollut puhetta.

Informaatiovaikuttaminen voi esiintyä väärän tiedon levittämisenä – voidaan esimerkiksi väittää, ettei yritys toimi turvallisesti. Yritystä voidaan myös mustamaalata, jotta asiakkaat suhtautuisivat yritykseen toisella tavalla. Informaatiovaikuttamista voi kohdistaa yritykseen sen toimialan mukaisesti. Mitä ylemmäs organisaatiossa mennään, sitä suurempi intressi vaikuttamiselle on haastatteluiden mukaan. Sosiaalinen media erityisesti antaa mahdollisuuden informaatiovaikuttamiselle. Vaikuttaminen voi levitä myös tämän jälkeen sisäisesti yrityksessä.

Haastatteluissa korostui, että informaatiovaikuttaminen koetaan erittäin hankalaksi, sillä se voi olla huomaamatonta, koska on henkilökohtaista, mihin kukakin

uskoo. Useasti työntekijät ovat kuitenkin olleet pitkään talossa, joten luottamus henkilöstöön on korkea ja väärä tieto voidaan nopeasti korjata.

Viestinnällä taistellaan informaatiovaikuttamista vastaan

Yrityksen tulee kyetä tunnistamaan informaatiovaikuttaminen ja vastata siihen viestinnällä. Usea haastateltava kokee, että sillä on väliä, millä tavalla yritys viestii asioista, sekä miten asiat tuodaan esille. Yrityksellä tulee olla selkeä viestintästrategia ja -taktiikka laadittuna informaatiovaikuttamistilannetta varten, eli selkeä tapa toimia silloin, kun informaatiovaikuttamista havaitaan.

Yrityksen on kyettävä viestimään selkeästi asioiden oikea laita ja mahdollisimman nopeasti, kriisiviestintäsuunnitelman mukaisesti. Yrityksen sisällä tulee tehdä selkeää viestintää, etteivät asiat jää epäselviksi. Tiedon tulee olla avointa ja läpinäkyvää, koska sillä on merkittävä vaikutus siihen, miten työntekijät ajattelevat yrityksestä. Yrityksen johdon tulee ottaa vastuu tilanteessa ja viestiä asiasta henkilöstölle. Henkilöstön pitäminen ajan tasalla on keskeistä.

Henkilöstön tulee olla tarkkaavaisia ja ilmoittaa organisaatiossa ylöspäin poikkeamista. On myös tärkeää korostaa, että työntekijät eivät reagoi itse mihinkään, vaan ylempi johto hoitaa informaatiovaikuttamiseen liittyvät asiat. Yrityksen tulee seurata eri medioita ja tutkia, minkälaisia asioita siellä liikkuu yrityksestä. Avoimuus viestinnässä, virheiden korjaaminen ja nopea reagointi ovat keskeisiä asioita palautumisessa. Tärkeää informaatiovaikuttamisen torjumisessa on olla lähellä henkilöstöä ja ymmärtää, mitä tietoa siellä liikkuu päivittäin.

4.5 Valtiollinen toiminta

Venäjän hyökkäyssodan vaikutukset ovat olleet merkittäviä suoraan ja välillisesti yrityksiin. Useat yritykset ovat myös vetäytyneet Venäjän toiminnasta. Euroopan kriisi on vaikuttanut operatiiviseen toimintaan valtavasti; energian hinta on noussut merkittävästi, mikä näkyy liiketoiminnan kustannuksissa.

Keskeinen huomio on, että kukaan haastateltavista yrityksistä ei ole tunnistanut kyberuhkia, jotka johtuvat kriisistä. Toisaalta, jos Venäjän hyökkäystä ei olisi

tapahtunut, olisi joka tapauksessa voinut kyberhyökkäyksiä kohdistua Suomeen. On vaikeaa todeta, onko juuri Ukrainan kriisi synnyttänyt nykyisiä kyberuhkia. Vaikka kyberuhkia ei olisi syntynyt, on kriisi kuitenkin konkretisoinut uhkakuvat tehden selväksi, että ne eivät ole enää vain hypoteettisia uhkia.

Kybervakoilu koetaan epätodennäköiseksi

Haastatteluissa korostui, että kybervakoilu koetaan kuten informaatiovaikuttaminen: mahdolliseksi, mutta epätodennäköiseksi. Kybervakoilu satamalogistiikan yrityksille nähdään monesti marginaalisena asiana, eli satamien yritykset eivät ole sen ensimmäinen kohde. Usea yritys kokee, että vakoilua tehdään, mutta se ei kohdistu juuri heidän yritykseensä. Syynä on se, että yritykset ovat pieniä toimijoita, tai heillä ei ole merkittävää tietoa.

Jotkut toimijat kuitenkin kokevat kybervakoilun hyvin merkitykselliseksi ja mahdolliseksi uhaksi – asia on siis yrityskohtainen. Yritykset kokevat myös, että kybervakoilua kohdistetaan pääsääntöisesti niihin satamien kriittisiin yrityksiin, jotka ovat satamien infrastruktuurissa kunnolla mukana. Moni satamalogistiikan yritys toimii kyllä sataman alueella, mutta ei satamaliikenteessä. Lisäksi koetaan, että terminaalitasolla ei olisi suuria salaisuuksia, joita kybervakoilulla yritettäisi saavuttaa.

4.6 Yhteenveto

Digitalisaatio

Digitalisaatiolla on ollut merkittäviä vaikutuksia satamalogistiikan toimintaan. Digitaalisten järjestelmien ja laitteiden määrän kasvaminen on monimutkaistanut työntekoa korostaen kyberturvallisuuden merkitystä. Varautumista parannetaan jatkuvasti, mutta haastatteluiden mukaan parannettavaa vielä on. Monessa yrityksessä koetaan, että he ovat logistiikan, eivät kyberturvallisuuden osaajia, minkä takia yritykset eivät ymmärrä kaikkia heihin kohdistuvia uhkia.

Haastatteluissa korostetaan, että yrityksien tulisi seurata, mitä kyberturvallisuuden tilannekuvassa tapahtuu. Yrityksien tulisi keskittyä henkilöstön kouluttami-

seen ja tiedon jakamiseen satamatoimijoiden kesken. Toiminta pysähtyy pääsääntöisesti yrityksissä, jos järjestelmät lakkaavat toimimasta. Joissakin yrityksissä toiminta voi jatkua muutaman päivän ajan, ollen kannattamatonta aiheuttaen kuluja yrityksille. Satamalogistiikan toimijat ovat siis järjestelmiensä ja yhteyksiensä varassa. Satamatoimijat eivät halua kehittää yhteistyötä myöskään IT:n osalta – moni toimija miettii vain omaa ympäristöään. Useasti yrityksissä on vain yksittäinen henkilö, jonka harteilla on IT ja sen kehitys, eikä resursseja ole kehittää kyberturvallisuutta tai digitalisaatiota – asia nähdään vain kustannustekijänä yrityksessä.

Yrityksen kyberturvallisuus

Satamat ovat osa yhteiskuntamme kriittistä infrastruktuuria, mutta tämän ei pääsääntöisesti nähdä vaikuttavan uhkakuviin, joihin satamalogistiikan yritykset varautuvat. Kyberturvallisuus ei ole ollut monelle yritykselle se liiketoiminnan pääasia, vaan se, että osaavat käyttää laitteistoja ja hyödyntää digitalisaatiota yrityksen toiminnoissa.

Kolme keskeisintä haastatteluissa noussutta kyberuhkaa ovat tietojen kalastelu, järjestelmien lamauttaminen ja palvelunestohyökkäys. Pinnalla olevat hyökkäystavat koetaan perinteisiksi ja henkilöstöön kohdistuvat hyökkäykset ovat yleisimpiä. Kolme keskeisintä haastatteluissa noussutta hybridiuhkaa ovat fyysinen vaikuttaminen, kiristäminen ja pelottelu sekä informaatiovaikuttaminen. Keskeisimpiä kriittisiä työvaiheita ovat ne, joissa tietoa siirretään yrityksen ja asiakkaiden, tai yrityksen sekä yhteistyökumppanien välillä.

Henkilöstön kyberturvallisuus

Satamalogistiikan yrityksien henkilöstön digitaidot ja kyberturvatietoisuus ovat haastatteluiden perusteella vaihtelevilla tasoilla – paikoin ne arvioitiin heikoiksi ja paikoin kohtuullisiksi, tai jopa hyviksi. Osaamistaso on siis kirjavaa, kuten on myös henkilöstön ikäjakauma. Keski-ikä on korkea ja se vaikuttaa haastateltavien mukaan osaamistasoon. Osalle tietokone on vain ”pakollinen paha” ja osa taas käyttää sitä mielellään. Henkilöstölle tarvitaan enemmän ohjeistusta ja tie-

toisuuden lisäämistä. Koulutuksen tulisi olla säännöllistä ja kouluttamisen ymmärrettävyyteen tulisi kiinnittää huomiota. Kommunikointihaasteet ja resurssikysymys ovat keskeisiä hidasteita osaamisen kehittämisessä.

Merkittävin henkilöstöön kohdistuva kyberuhka haastatteluiden perusteella on tietojenkalastelu, seuraavaksi merkittävimmäksi nähtiin käyttäjän manipulointi. Kyberturvallisuus nähdään osana työturvallisuutta osassa yrityksistä, osassa ei. Vaihtelu riippuu siitä, millaista työtä yrityksessä tehdään. Kyberturvallisuudella voi olla vaikutuksia henkilöstön fyysiseen ja psyykkiseen turvallisuuteen. Henkilöstölle tulee taata turvallinen ympäristö, myös kyberturvallisuuden osalta. Tämä korostuu etenkin operatiivisessa työssä.

Informaatiovaikuttaminen

Informaatiovaikuttaminen koetaan epätodennäköisenä, mutta mahdollisena. Informaatiovaikuttaminen voi olla esimerkiksi väärän tiedon levittämistä yrityksestä. Tunnistaminen koetaan hankalaksi, koska se on monesti huomaamatonta. Viestinnällä taistellaan informaatiovaikuttamista vastaan. Yrityksen tulee olla ajan tasalla siitä, mitä tietoa heistä liikkuu verkossa ja kyetä vastaamaan viestinnällä informaatiovaikuttamiseen. Yrityksellä tulee olla selkeä tapa viestiä, kun yritykseen kohdistuvaa vaikuttamista havaitaan.

Valtiollinen toiminta

Venäjän hyökkäyssodan vaikutukset ovat olleet merkittäviä yrityksiin sekä suoraan, että välillisesti. Haastateltavat eivät kuitenkaan koe, että sodan seurauksena olisi välttämättä syntynyt kyberuhkia. Kriisi on kuitenkin konkretisoinut ja tehnyt selväksi, että uhka on todellinen. Uhkakuviin varaudutaan tällä hetkellä oikeasti ja sitä vastaan tehdään myös toimenpiteitä. Kybervakoilu koetaan kuten informaatiovaikuttaminen; mahdolliseksi, mutta epätodennäköiseksi. Kybervakoilun nähdään kohdistuvan niihin toimijoihin, jotka ovat syvällä sataman infrastruktuurissa mukana – osa yrityksistä toimii sataman alueella, mutta ei satamaliikenteessä.

5 MIHIN TULEE OTTAA KANTAA

Haastatteluiden keskeiseksi tulokseksi voidaan todeta, että satamalogistiikan yrityksien yleisimmät kyberuhkat keskittyvät inhimillisiä heikkouksia hyödyntäviin hyökkäyksiin – eli käytännössä tietojenkalasteluun ja käyttäjän manipulointiin. Merkittävimmäksi uhkakuvaksi nähtiin järjestelmien lamaantuminen. Tämä voi tapahtua juuri henkilöstöön kohdistetun hyökkäyksen kautta. Tämän takia henkilöstön osaamistasolla on tärkeä rooli yrityksen kyberturvallisuudessa.

Haastateltavien yrityksien henkilöstön digitaidot ja kyberturvaosaaminen kuvattiin hyvin vaihtelevaksi. Osa työntekijöistä osaa toimia turvallisesti, osalle tietokoneen käyttäminen tuottaa haasteita. Haastatteluiden perusteella voidaan todeta, että henkilöstölle tulisi tuottaa helposti lähestyttävää ja helposti ymmärrettävää materiaalia, jonka avulla he voivat kehittää omaa osaamistaan. Materiaalin tulee olla yleistajuista, eli sisältö tulee räätälöidä kohderyhmälle ymmärrettäväksi. Yksilöiden roolia turvallisuuden tekijöinä tulee tuoda vahvemmin esille ja heille tulee tarjota keinot kehittää ja ylläpitää omaa osaamistaan.

Tarve osaamista kehittävälle oppaalle korostui niin haastateltavien yrityksien johtotason henkilöiden, kuin operatiivisessa toiminnassa toimivien henkilöiden vastauksissa. Tarve kyberhygieniaa opettavalle oppaalle on siis olemassa ja siihen tulisi ottaa kantaa jatkossa. Kyberhygieniaopas vastaa osaamisen kehittämistarpeeseen, joka haastatteluissa nousi esille ja joka on tunnistettu myös laajemmin esimerkiksi Huoltovarmuuskeskuksen Digipoolin (2020) selvityksessä. Selvityksen mukaan satamien ja merenkulun kehityskohde on kyberturvallisuustietoisuuden lisääminen ja logistiikan kehityskohde on kyberturvallisuuteen liittyvän tiedon jakaminen.

Seuraavaksi tulee luoda kyberhygieniaa käsittelevä opas, joka on ymmärrettävä ja ihmislähtöinen. Oppaassa tulee selkeästi avata, millä tavalla kyberturvallisuus koskettaa jokaista ihmistä roolista riippumatta. Oppaan tulee myös tarjota konkreettisia keinoja kehittää omaa kyberhygieniaa, eli kertoa, miten turvallisuudesta saa tehtyä itselleen rutiinin. Kohderyhmää ei tulisi pelotella toimimaan tietyllä tavalla, vaan kannustavasti kuvata, miten pienillä päivittäisillä asioilla omaa ja yrityksen turvallisuutta voi lisätä. Opas ei saa myöskään olla liian laaja, jotta sen sisäistäminen on helppoa.

Oppaan lisäksi helposti lähestyttävä videokurssi

Oppaan lisäksi toteutetaan videokurssi, jonka idea on käydä ytimekkäästi ja ymmärrettävästi läpi mitä työntekijän tulisi tietää kyberturvallisuudesta ja kyberhygieniasta. Ytimekkäästi ja ymmärrettävästi tarkoittaa lyhyttä, viiden minuutin mittaista tietoiskua, jossa kyberturvallisuudesta puhutaan yleistajuisesti. Keskeinen tavoite on konkretisoida vertauskuvien avulla, mitä kyberturvallisuus oikeasti tarkoittaa ja miksi siihen tulisi kiinnittää huomiota. Lisäksi tavoite on välttää ”pelottelupuhetta” ja sen sijaan kannustaa kuuntelijoita panostamaan kyberturvallisuuteen.

Kyberturvallisuuden perusteet käydään siis läpi kolmen videon kautta, joissa käsitellään seuraavia aiheita: 1) mitä kyberturvallisuus tarkoittaa, 2) mitä kyberuhkia työntekijä voi kohdata ja 3) miten omaa kyberhygieniaa voi parantaa. Videokurssissa käydään ensimmäiseksi läpi kyberturvallisuuden perusteet. Tämän jälkeen kuvataan keskeisimpiä kyberuhkia, joita työntekijä voi työssään kohdata. Lopuksi puhutaan kyberhygieniasta ja kerrotaan, miten jokainen voi pienillä teoilla parantaa kyberturvallisuutta. Seuraavaksi käydään läpi lyhyt yhteenveto tietoiskujen sisällöstä.

Video 1: Kyberturvallisuus – tätä se tarkoittaa kansankielellä

Ensimmäisessä tietoiskussa kyberturvallisuutta lähestytään konkreettisen vertauskuvan kautta; kyberturvallisuuden idea on sama kuin fyysisen omaisuuden suojelemisessa – pidämme kotioven lukittuna, koska kodissa on jotakin, jolla on arvoa ja jota halutaan suojella. Vertauskuvan avulla perustellaan myös sitä, miksi kyberturvallisuus koskettaa jokaista meistä. Tämän jälkeen perustellaan, että ihmiset ovat yleensä hyökkäyksen kohteita, koska meissä ihmisissä on inhimillisiä heikkouksia. Omaa osaamista tulee myös kehittää, jotta emme ole helppoja kohteita rikollisille.

Video 2: Kyberuhka – tunne kyberviholisesti

Toisessa tietoiskussa tutustutaan kyberuhkiin, joita erityisesti työntekijä voi työssään kohdata. Edelleen hyödynnetään vertauskuvaa kodin ja kyberturvalli-

suuden välillä; jos koteihin ei murtauduttaisi, niitä ei tarvitsisi suojella – jos kyberuhkia ei olisi, kyberturvallisuudelle ei olisi tarvetta. Tietoiskussa nostetaan esille kolme keskeistä työntekijän kyberuhkaa: tietojenkalastelu, haittaohjelmat ja käyttäjän manipulointi. Ideana ei ole pelotella, vaan korostaa selkeästi, millaisia uhkakuvia työpaikalla voi kohdata.

Video 3: Kyberhygienia – mitä voimme oppia oikean elämän hygieniasta

Kolmas tietoisku keskittyy keinoihin, joilla aiemmin esitellyiltä kyberuhkilta voi suojautua – siis kyberhygieniaan. Kyberhygieniaa lähdetään avaamaan vertaamalla sitä oikean elämän hygieniaan. Se on sitä päivittäistä turvallista toimintaa, jonka avulla pidämme esimerkiksi laitteemme turvassa. Kyberhygienia on hygieniaa verkossa. Tietoiskussa nostetaan esille viisi tapaa parantaa ja ylläpitää omaa kyberhygieniaa: 1) salasanahygienia, 2) sähköposti- ja linkkihygienia, 3) laitteiden lukitseminen ja paperiton työpöytä, 4) vieraiden laitteiden välttäminen ja 5) verkossa näkemiensä asioiden kyseenalaistaminen. Pienillä teoilla on lopulta suuri vaikutus.

6 INHIMILLISET TEKIJÄT TYÖTURVALLISUUDESSA

6.1 Kyberhygienia on yrityksen tietoturvan suojaamisen perusedellytys

Euroopan Unionin kyberturvallisuusviraston ENISA:n kanta on selvä; kyberhygienia on ratkaiseva tekijä yritysten tietojen suojaamisessa. Kyberhygieniaan tulee suhtautua kuin henkilökohtaiseen hygieniaan, joka näkyy yksilön yksinkertaisina päivittäisinä rutiineina ja hyvänä tietoturvakäyttäytymisenä, sekä yritysten omina tarkastuksina, joilla varmistetaan kyberturvallisuus. Kyberhygienia on käyttäjän parhaita toimintoja (Best Practices) henkilökohtaisen turvallisuuden varmistamiseksi verkkomaailmassa, yrityksen ohjelmistojen ja laitteistojen päivittämistä, sekä tietoverkkojen suojauksen parantamista. Kyberhygienia on yhdistelmä yksilön ja yrityksen kyberturvallisuutta järjestelmien sekä tietojen suojaamiseksi.

6.2 Inhimillinen tekijä huomioitava turvallisuuden luomisessa

Monet sekoittavat inhimillisen tekijän ja inhimillisen virheen toisiinsa. Inhimillisillä tekijöillä tarkoitetaan ihmisen yksilöllisiä ominaisuuksia (asenteet, henkinen vahvuus, taidot ja päätöksentekokyky) ja työhön, organisaatioon, sekä ympäristöön liittyviä turvallisuuteen, terveyteen, hyvinvointiin, käytettävyyteen että suorituskykyyn vaikuttavia tekijöitä. Inhimillinen virhe on puolestaan ihmisen aiheuttama onnettomuus.

Inhimillinen tekijä kuvastaa siis ihmisen ja koneen välistä toimintaa. Työntekijöitä pyydetään tekemään työtehtäviä ryhmässä yksilön osaamisen mukaisesti. Ihmisen persoonallisuuteen voi harvoin vaikuttaa, mutta toimintaa ja taitoja voidaan parantaa. Organisaation työtapoja ja -menetelmiä, kulttuuria, resursseja, viestintää, johtajuutta (leadership) ja asioiden johtamista (management) tulee kehittää, sillä niillä on suuri vaikutus yksilön ja ryhmän edellytyksiin menestyä työssään. Inhimilliset tekijät tulee sisällyttää yrityksen hyvään turvallisuusjohtamis- ja riskienhallintajärjestelmään.

Inhimillisiin tekijöihin vaikuttavat ihmisen käyttäytymiseen vaaratilanteissa kokemus, koulutus, kulttuuri, osaaminen, stressi, terveys, tilannetietoisuus, työolot, viestintä ja väsymys (fatigue). Väsymys (fatigue) johtaa virheisiin ja onnettomuuksiin ollen usein suuronnettomuuksien juurisyy.

6.3 Inhimilliset tekijät kyberturvallisuudessa

Kyberhyökkäyksistä, tietomurroista ja kiristyshaittaohjelmista yli 80 % johtuu inhimillisistä tekijöistä. IBM raportoi vuonna 2015 inhimillisen tekijän aiheuttavan 95 % kaikista kyberturvallisuustapauksista harkitsemattomista työtavoista, tietämättömyydestä, suojaamattomista verkkoyhteyksistä, riittämättömästä viestinnästä arkaluontoisten tietojen käsittelystä, haittaohjelmistoista ja kehnosta ohjelmistopäivityksien hallinnasta. Osa työntekijöistä siirtää kyberturvallisuuden vastuun tietokonejärjestelmille, ylläpitäjille ja yrityksen johdolle. Nykyiset kyberturvallisuuskoulutukset eivät pysty muokkaamaan loppukäyttäjän käyttäytymistä, joten organisaatioiden koulutusilmapiiri tulee muuttaa aktiiviseksi oppimiseksi turvallisuuskulttuurin muuttamiseksi.

Inhimilliset tekijät aiheuttavat yrityksissä kasvavaa huolta tietoturvasta, sillä inhimilliset virheet aiheuttavat eniten tietomurtoja, kiristysohjelma- ja kyberhyökkäyksiä. Yritykset ja organisaatiot investoivat teknologiaan vähentääkseen inhimillisiä virheitä kyberturvallisuudessa ja jättävät huomioimatta inhimillisen virheen taustalla olevat käyttäytymis- ja kognitiiviset ongelmat. Kognitio tarkoittaa lyhyesti ihmismielen tiedon käsittelemistaitoja ja -toimintoja suoritustilanteissa (ajattelua, havaitsemista ja muistamista).

Kyberturvallisuuden kulmakivet ovat ihmiset, prosessit ja teknologiat. Uuden teknologian hankinnat eivät ole vähentäneet ihmisten aiheuttamia virheitä kyberturvallisuuden osalta. Työntekijöiden riskialtista toimintaa ovat aikapaineet, työtaakka ja organisaatioissa käytettävät ”nopeammat työskentelytavat”, jolloin kyberrikolliset pääsevät käyttämään työtekijöiden suorituskykyä heikentävää stressiä, uupumusta ja väsymystä, sekä tilannetietoisuuden puutetta (situational awareness) hyväkseen hyökkäyksissään. Inhimillisiä virheitä aiheuttavat työntekijän apatia, huolimattomuus, kokemattomuus, turvallisuustietoisuuden puute ja jopa vastustus parempaan työskentelykulttuuriin. Nämä johtavat usein tietoturvakatastrofeihin, kuten tietomurtoihin, kiristyshaittaohjelmiin ja kyberhyökkäyksiin.

6.4 Kyberrikollisten hyökkäystavat yritysten tietoverkkoihin

Yrityksiin kohdistuvat kyberhyökkääjät ovat valtioiden tukemia kyberhyökkääjiä, kyberrikollisia, palkattuja epäeettisiä hakkereita tai ”haktivisteja”. Haktivisti-termi muodostuu sanoista hakkeri ja aktivisti, joka viittaa kansalaisaktivismin poliittista tai sosiaalista agendaa ja yhteiskunnallista kansalaistottelemattomuutta jonkin yrityksen tietoverkkoa kohtaan.

Tärkeimmät hyökkäystavat ovat tietojenkalastelu haittaohjelmilla, palvelunestohyökkäykset (DDoS) ja kiristyshaittaohjelmat. Myös ”nollapäivähyökkäys”, joka johtuu ohjelmistojen haavoittuvuudesta ennen kuin valmistaja ehtii korjaamaan ohjelmointivirhettään. Huijauspuhelut ja huijaustekstiviestit ovat varsin yleisiä tänä päivänä. Myös tietoverkkojen välistä viestiliikennettä ja yrityksen dokumentteja voidaan seurata ja salakuunnella. Käyttäjien manipulointi ja seuraaminen, vaikuttaminen ja hämääminen on kasvava ongelma turvallisuudessa. Tavoitteena tässä on hyökkääjällä huijata käyttäjää paljastamaan arkaluonteista

tietoa, käyttäjätunnuksia tai varastaa rahaa tai arvokasta omaisuutta. Ransomware-, eli kiristyshaittaohjelmat ovat tällä hetkellä viheliäisimpiä tapoja yrityksiä kohtaan hyökätä salaamalla yrityksen tiedostot ja lukitsemalla laitteet. Yleensä hyökkääjät pyytävät Bitcoin-kryptovaluuttana lunnaita avatakseen tiedot yritykselle. Digitaaliset toimitusketjuhyökkäykset tapahtuvat luotettavilta tahoilta kuten yrityksen yhteistyökumppaneilta tulevien hyökkäyksien muodossa, jossa luotettuun ohjelmistoon tai tiedostoon on lisätty haittakoodi, joka tarjoaa pääsyn yrityksen tietoverkkoon. Kyberhyökkäyksen motiivina ovat useimmiten taloudellinen hyöty, hyökkäyksen saava julkisuus jotain aatetta kohtaa, yritysvakoilu tai jopa kybersota valtioiden välisissä kahnauksissa.

6.5 Koulutusta, oppimista ja harjoittelua!

Kyberturvallisuusongelmat johtuvat inhimillisistä tekijöistä ja käyttäjän persoonallisuudesta sekä asenteesta, jotka vaikuttavat turvallisuuteen (security) ja työturvallisuuteen (safety). Tietoturvan ammattilaiset luottavat liikaa teknologiaan vähentääkseen inhimillisiä virheitä kyberturvallisuustapahtumissa. Turvallisuuskoulutuksen kehittämiseen ja muuttamiseen yritykset tarvitsevat koulutusta, oppimista ja harjoittelua.

MUISTA AINAKIN TÄMÄ!

Kyberturvallisuushäiriöiden riskin vähentämiseksi yritysten tulee ottaa käyttöön turvallisuuskulttuurin muutos aktiivisella oppimisella ja parhailla käytännöillä, sekä huomioitava työntekijän riittävä lepo, että oikeat työtavat ja -menetelmät väsymyksen ja stressin vähentämiseksi.

Yrityksien on huomioitava hyvä tilannetietoisuus ja riskinhallintajärjestelmä, sekä valmistelu-, suojaus, reagointi- että palautussuunnitelma kyberhyökkäyksiä varten. Kokonaisturvallisuuden parantaminen vaatii jatkuvaa koulutusta organisaation kaikilla tasoilla. Viestintä on erittäin tärkeää sisäisessä ja ulkoisessa tiedottamisessa. Yritysten tulee parantaa omaa johtajuuttaan, viestintää ja resursseja turvallisuuden sekä riskien hallinnassa.

On myös hyvä pitää mielessä englanninkielinen sanonta:
“If you think safety is expensive, try having an accident.”

LÄHTEET

HaminaKotka Satama. 2023. Kaikki sataman yritykset Saatavissa: Sataman yritykset | HaminaKotka [viitattu 25.5.2023].

Huoltovarmuusorganisaation Digipooli. 2020. Kyberturvallisuuden nykytila eri toimialoilla -kartoituksen keskeiset havainnot. PDF-dokumentti. Saatavissa: https://www.huoltovarmuuskeskus.fi/files/b3671ecb5d0b5b431174fec9350e0251b75227ba/kyberturvallisuuden-nykytila-eri-toimialoilla2-verkkosivuille.pdf [viitattu 26.4.2023].

Tuomala, V. (2023). Kyberhygienia ja inhimilliset tekijät huomioitava suomalaisissa yrityksissä. XAMK READ 2/2023-verkkojulkaisuartikkeli. Saatavissa: https://read.xamk.fi/2023/logistiikka-ja-merenkulku/kyberhygienia-ja-inhimilliset-tekijat-huomioitava-suomalaisissa-yrityksissa/ [viitattu 31.5.2023]