Uhkatiedon hyödyntäminen organisaation tietoturvatietoisuuden ja riskienhallinnan kehittämisessä

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tieto- ja viestintätekniikka, insinööri (AMK)

Syksy 2023

Ulla Yli-Kiehelä

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tieto- ja viestintätekniikka, insinööri Tiivistelmä
Tekijä Ulla Yli-Kiehelä Vuosi 2023
Työn nimi Uhkatiedon hyödyntäminen organisaation tietoturvatietoisuuden ja riskienhallinnan kehittämisessä
Ohjaaja Ismo Turve

Opinnäytetyön tavoitteena on selvittää miten toimeksiantaja organisaatiossa hyödynnetään ja analysoidaan uhkatietoa, sekä miten uhkatietoa sovelletaan tietoturvatietoisuuden ja riskienhallinnan kehittämisssä. Tavoitteena on selvittää, kuinka uhkatietoa kerätään ja analysoidaan, ja kuinka saatua tietoa voisi hyödyntää tehokkaammin.

Opinnäytetyön toimeksiantaja on valmistavan teollisuuden organisaatio. Opinnäyteytön taustalla on organisaation tarve yhtenäistää jokaisen yksikön toimeenpanoa ISO 27001-standardin vaatimusten mukaisesti. Taustalla on myös tarve selvittää, kuinka eri yksiköt saavat ja soveltavat uhkatietoa, ja ovatko tavat kullekkin yksikölle toimivia ja tehokkaita.

Opinnäytetyö sisältää teoriaa tietoturvallisuudesta, kyberturvallisuudesta, uhkatiedosta ja riskienhallinnasta. Opinnäytetyö sisältää tietoa siitä, miten organisaatiot voivat suojautua erilaisilta hyökkäyksiltä, ja kuinka organisaatiot voivat lisätä tietoturvallisuuttaan ja parantaa tietoturvatietoisuuttaan.

Opinnäytetyön tuloksena saatiin selville, että toimeksiantaja organisaatio on tietoturvatietoinen, sekä tietoinen useista erilaisista tietoturvauhista. Heillä on käytössään muun muassa ISO 27001 -standardi, jonka mukaan toimiminen antaa hyvän pohjan organisaation tietoturvallisuudelle. Opinnäyteytön tuloksena selvisi, että toimeksiantaja organisaatiolla on tietoturvassaan aihealueita, jotka vaativat kehittämistä. Näistä aihealueista toimeksiantaja organisaatio on tietoinen ja niiden kehittämiskeinoja mietitään.

Johtopäätöksinä voidaan todeta, että toimeksiantaja organisaatio hyödyntää monipuolisesti keräämäänsä uhkatietoa, ja soveltaa sitä tietoturvatietoisuuden ja riskienhallinnan kehittämisessä. Voidaan myös todeta, että koska tietoturvallisuus on kasvava ala, ei toimeksiantaja organisaatiolta tule loppumaan kehitettävät aihealueet. Toimeksiantaja organisaatiossa ollaan tietoisia heitä kohtaan uhkaavista uhista, mutta kaikkiin uhkiin ei ole löytynyt ratkaisua.

Toimeksiantaja organisaation edustaja kommentoi toteutunutta opinnäytetyötä selkeänä ja ymmärrettävänä. Edustaja kommentoi, että työtä voidaan käyttää tietoturvatietoisuuden parantamiseen niin toimeksiantajan organisaatiossa, kuin organisaation ulkopuolellakin. ”Työssä ehdotetut parannusehdotukset ovat asianmukaisia, ja näitä tullaan toteuttamaan käytännössä tietoturvan ja tietoturvatietoisuuden kehittämisessä.”

Avainsanat Uhkatieto, riskienhallinta, tietoturvallisuus, kyberturvallisuus
Sivut 44 sivua

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Information and Communication Technology
Author Ulla Yli-Kiehelä
Subject Utilizing Threat Intelligence in Improving Organizational Awareness and Risk Management
Supervisor Ismo Turve

Abstract
Year 2023

The goal of this thesis is to explore how an organization uses and analyses threat intelligence, and how it is utilized to improve information security awareness and risk management development. The aim is to clarify how threat intelligence is gathered and analyzed, and how it could be capitalized more efficiently.

The organization in this thesis is in the manufacturing industry and the motivation for this study is to unify all units' work execution according to ISO 27001 -standard. Another reason is to examine how each units gathers and uses threat intelligence, and whether the methods for each unit are applicable and efficient.

This thesis includes theory about information security, cybersecurity, threat intelligence and risk management. Thesis also includes information about how an organization can shield against different types of attacks and how to improve their information security and information security awareness.

The result of this thesis shows that the employer organization is aware of information security and is aware of multiple information security threats. The employer organization is using ISO 27001 -standard among other standards, which provide a good base for an organization's information security awareness. The results show that the employer organization's information security has areas that need to be improved. The employer organization is aware of these areas and development work is in progress.

In conclusion it can be stated that the employer organization uses the gathered threat intelligence in multiple ways and utilizes it to improve awareness and risk management. It can also be stated that as information security is a growing field, there will always be areas for improvement. The employer organization is aware of the threats targeted towards them but has not found a solution for all of them.

The employer organization's representative described the actualized thesis as clear and understandable. The representative commented that the thesis can be used to improve organizational awareness in the organization as well as outside of the organization. According to the representative, the listed propositions in the thesis are appropriate, and they will be executed in practice to improve information security and awareness.

Keywords Threat intelligence, risk management, information security, cybersecurity
Pages 44 pages

Sisällysluettelo

Kuvat, taulukot ja kaavat

Sanasto

APT-ryhmä on organisoitunut hakkeriryhmä, joka toimii joko valtiollisen toimijan ohjauksessa tai itsenäisesti. Kohdistetut haittaohjelmahyökkäykset ovat usein APT-ryhmien suunnittelemia ja toteuttamia. APT-ryhmiä voidaan tunnistaa analysoimalla niiden toimintatapoja sekä tekniikoita. (Sanastokeskus, 2018)

Haavoittuvuus on alttius tietoturvaan kohdistuville uhkille. Haavoittuvuus voi olla mikä tahansa heikkos, joka mahdollistaa, tai jota voidaan käyttää vahingon aiheuttamisessa. Haavoittuvuuksia voi olla henkilöiden toiminnassa, prosesseissa tai tietojärjestelmissä. (Sanastokeskus, 2018)

Haittaohjelma (engl. malicious software) on ohjelma, joka tarkoituksellisesti aiheuttaa ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa. Haittaohjelmia ovat esimerkiksi madot, virukset sekä troijalaiset hevoset. (Sanastokeskus, 2018)

Kiristyshaittaohjelma (engl. ransomware) on kyberhyökkäys, jossa hyökkääjät pyrkivät salaamaan organisaation dataa, ja vaativat lunnaita tietojen palauttamiseksi. (Microsoft, n.d -a)

Kohdistettu haittaohjelmahyökkäys (engl. advanced persistent threat, APT) on monivaiheinen tietoverkkohyökkäys, joka kohdistuu rajattuun kohteeseen, ja joka tehdään esimerkiksi haittaohjelmien avulla. (Sanastokeskus, 2018)

Kriittiseen infrastruktuuriin kuuluu niin fyysisiä laitoksia ja rakenteita, kuin digitaalisia toimintoja ja palveluita. Kriittisiä infrastruktuureja ovat esimerkiksi energian tuotanto-, siirto- ja jakelujärjestelmät, liikenne ja logistiikka, sekä tieto- ja viestintäjärjestelmät. (Sanastokeskus, 2018)

”Kyberhyökkäyksiksi kutsutaan laajaa kirjoa erilaisia tapoja, joilla pyritään muun muassa lamauttamaan järjestelmiä, varastaamaan tietoja tai muuten vain tekemään haittaa.” (F-secure, n.d)

Kyberturvallisuus on tavoitetila, jossa sen toimintaympäristöön voidaan luottaa, ja jossa toiminta turvataan. Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan hallita ja sietää erilaisia uhkia ja niiden vaikutuksia. Tietoturvan tarkoittaessa tiedon luottamuksellisuutta, eheyttä ja saatavuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen organisaation ja yhteiskunnan turvallisuutta ja vaikutusta sen toimintoihin. (Sanastokeskus, 2018)

Käyttäjän manipulointi (engl. social engineering) on pyrkimys hankkia luottamuksellista tietoa tekeytymällä tiedon käyttöön oikeutetuksi henkilöksi, tai tietoon oikeutetun henkilön hyväksi käyttämistä. (Sanastokeskus, 2018)

Käyttöoikeuksien hallinnalla tarkoitetaan menetelmiä, joilla myönnetään, evätään tai käsitellään käyttöoikeuksia järjestelmiin ja palveluiin. (Sanastokeskus, 2018)

Nollapäivähaavoittuvuudella (engl. zero day vulnerability) tarkoitetaan tietojärjestelmässä olevaa haavoittuvuutta, johon ei ole saatavilla korjausta. (Sanastokeskus, 2018)

Palvelunestohyökkäys (engl. denial of sevice, DoS) on tietoverkkohyökkäys, jonka pyrkimys on kuormittaa ja lamauttaa palvelu tai tietojärjestelmä. (Sanastokeskus, 2018)

Pääsynhallinta on kaikki ne menetelmät, joilla varmistetaan että käyttäjät, järjestelmät, laitteet ja sovellukset pääsevät käyttämään tietojärjestelmässä olevaa tietoa roolinsa mukaisesti. (Sanastokeskus, 2018)

Riskillä tarkoitetaan myönteistä, kielteistä tai molempien vaikutusta odotetusta poikkeamasta. Riski voi käsitellä tai saada aikaan mahdollisuuksia ja uhkia. (Sanastokeskus, 2018)

Riskienhallinta on prosessi jolla identifioidaan, arvioidaan ja kontrolloidaan uhkia organisaatiota ja sen hankintoja kohtaan. (Tucci, 2023)

Tietojenkalastelulla (engl. phising) pyritään huijaamaan uhria ja huijauksen avulla varastamaan vaikka käyttäjätunnukset. Tietojenkalastelu voi olla esimerkiksi sähköposti jonkun tunnetun yrityksen nimissä. (F-secure, n.d)

Tietoturvalla tarkoitetaan järjestelyitä, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. (Sanastokeskus, 2018)

Tietoturvauhka (engl. security threat) on mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu tietoturvaan, ja toteutuessaan vaarantaa sen. (Sanastokeskus, 2018)

Tietoverkkohyökkäys (engl. network attack) on tietoverkon kautta tapahtuva teko tai toiminta, joka pyrkii tietoverkon tai -järjestelmän, laitteen tai datan vahingoittamiseen tai oikeudettomaan käyttöön. Tietoverkkohyökkäyksiä ovat esimerkiksi palvelunestohyökkäys ja haittaohjelma. (Sanastokeskus, 2018)

Tietoverkkovalvonnalla (engl. data network monitoring) tarkoitetaan oman verkon tietoliikenteen seurantaa sekä analysointia. (Sanastokeskus, 2018)

Todennus (engl. authentication) on menettely, jolla pyritään varmistamaan kohteen totuudenmukaisuus, oikeellisuus ja alkuperä. (Sanastokeskus, 2018)

Uhkatieto (engl. threat intelligence) on yksityiskohtaista tietoa uhista, joilla pyritään estämään ja vastaamaan organisaatioon kohdistuviin kyberuhkiin. (Ibm, n.d)

Vakoiluohjelmien tavoitteena on vakoilla kohdettaan. Jos uhri lataa vakoiluohjelman laitteelleen, ohjelma voi seurata käyttäjän toimintaa esimerkiksi tallentamalla näppäimistön painalluksia. (F-secure, n.d)

Väliintulohyökkäys (engl. man-in-the-middle) on hyökkäys, jossa hyökkääjä kaappaa kahden osapuolen välisen keskustelun verkosta, ja esiintyy keskustelun yhtenä osapuolena. Näin hyökkääjä voi esimerkiksi yrittää saada salasanoja tietoonsa, tai saada uhrin asentamaan haittaohjelman laitteelleen. (F-secure, n.d)

Väsytyshyökkäys (engl. brute force) on ”hyökkäys, jossa kokeillaan systemaattisesti kaikkia mahdollisia salausavaimia ja salasanoja salauksen avaamiseksi tai salasanan löytämiseksi.” (Termipankki, n.d).

1 Johdanto

Opinnäytetyö tehtiin valmistavan teollisuuden organisaatiolle, joka toimii työn toimeksiantajana. Toimeksiantajalla oli tarve selvittää, miten heillä käsitellään ja analysoidaan uhkatietoa eri yksiköissä, ja miten saatua tietoa voitaisiin paremmin hyödyntää riskienhallinnan ja tietoturvatietoisuuden kehittämisessä. Toimeksiantaja halusi selvittää, kuinka tehokkaasti eri yksiköt käsittelevät uhkatietoa, ja miten saatu tieto parhaiten integroituisi jokaisen työntekijän päivittäiseen työhön.

Tutkimuksen taustalla on toimeksiantajan tarve selvittää mitkä ovat eri yksiköiden tarpeet uhkatiedon käsittelylle, ja kuinka tehokasta tarvittavien toimeenpiteiden käyttöönotto on. Tutkimuksen avulla haluttiin myös selvittää, kuinka saataisiin parhaiten sovellettua tietoturvallisuutta toimeksiantajan eri yksiköissä.

Tutkimuksen tavoitteena on tutkia millaista uhkatietoa missäkin yksikössä kerätään ja miten sitä käsitellään. Tavoitteena on selvittää, mitä saadulla uhkatiedolla tehdään, ja miten se olisi paremmin hyödynntettävissä. Tavoitteena on myös selvittää, miten uhkatietoa voisi soveltaa ja mikä olisi sopivin tapa hyödyntää uhkatietoa kussakin yksikössä.

Tutkimus koostuu kysymyksistä, joita esitettiin eri yksiköissä uhkatiedon kanssa työskenteleville henkilöille. Saatujen tietojen perusteella voidaan parantaa organisaation tietoturvatietoisuutta, kun tavat tiedon välittämiseen tarkentuvat koskemaan yksityiskohtaisesti kutakin yksikköä.

Tutkimus toteutettiin valmistavan teollisuuden organisaatiolle. Organisaatiolla on käytössään jo ennestään usea eri tietoturvallisuuden standardi, kuten ISO 27001 sekä NIS2 -direktiivi. Tutkimuksen tavoitteena on tarkistaa, kuinka myös standardeissa vaadittuja kohtia saisi paremmin toteutettua organisaatiossa. Tutkimuksessa selvitettiin keinoja hyödyntää uhkatietoa aikaisemmasta tehokkaammalla tavalla.

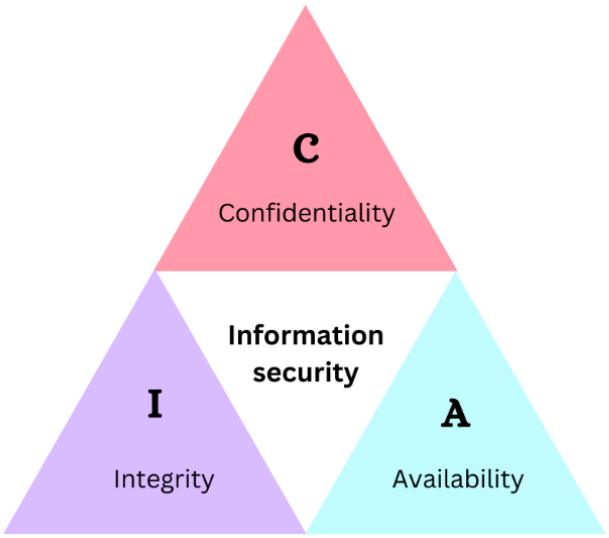
2 Kyberturvallisuus ja tietoturvauhat

Kyberturvallisuus ja tietoturvauhat -luvussa käsitellään yleisestä näkökulmasta tietoturvallisuutta ja siihen liittyviä aiheita, kuten tietoturvauhkia valmistavalle teollisuudelle, riskienhallintaa, sekä kyberturvallisuuden eettisiä näkökulmia.

Tietoturvauhat ovat keskeinen osa lukua, ja niitä käsitellään niin ulkoisesta, kuin sisäisestäkin näkökulmasta. Tietoturvauhkien tunnistaminen on keskeinen osa organisaation kykyä puolustautua negatiivisesti vaikuttavilta tietoturvatapauksilta, kuten hyökkäyksiltä tai datan menetykseltä.

Tietoturvallisuuden malli on tehty suojelemaan herkkää tietoa datavuodoilta. CIA-kolmio on tärkeä konsepti tietoturvallisuuden alalla, ja se on käytössä ISO 27001 -standardissa. ISO 27001 -standardia käytetään maailmanlaajuisesti tietoturvallisuuden hallitsemiseksi (Irwin, 2023). Kolmion jokainen sakara kuvaa eri asioita englannin kielisten termien mukaan, kuten kuvasta (kuva 1) näkee. Saatavuudella (engl. availability) tarkoitetaan sitä, että tieto on hyödynnettävissä haluttuna ajankohtana. Eheys (engl. integrity) tarkoittaa tiedon yhteenpitävyyttä alkuperäisen tiedon kanssa. Luottamuksellisuus (engl. confidentiality) tarkoittaa, että tieto pysyy sille tarkoitettujen henkilöiden keskuudessa.

Kuva 1. Tietoturvallisuuden CIA-kolmio.



Tietoturvallisuuden konkreettisia toimia ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi, sekä virustorjuntaohjelman, palomuurin ja varmenteen käyttäminen (Sanastokeskus, 2018). Kulunvalvonnalla voidaan käsittää että organisaatiolla on tiedossaan kuka pääsee ja minne. Tilat tulee olla lukittuna, ja vain asiaan kuuluvien henkilöiden tulee päästä sisään. Asiakirjat tulee säilyttää ja hävittää asianmukaisesti, esimerkiksi asiakkaiden tietoihin liittyvät asiakirjat tulee pitää salassa ja hävittää silppuamalla. Tietoja tulee salata ja varmuuskopioida, esimerkiksi asiakastietoja ei saa luovuttaa kolmansille osapuolille. Tietojen varmuuskopiointi varmistaa tietojen säilyvyyden vaikka tulipalon sattuessa, ja varmuuskopioita tulee säilyttää turvallisessa tilassa. Virustorjuntaohjelma ja palomuuri ehkäisee muun muassa haittaohjelmien leviämisen organisaation järjestelmiin, ja varmenteen käyttäminen estää ulkopuolisten pääsyn käsiksi työntekijän käyttäjätunnuksiin. (organisaation sisäinen lähde)

2.1 Tietoturvauhat

Tietoturvauhkia löytyy monenlaisia, ja yleensä niiden tarkoitus on saada jollain tavalla organisaation toiminta häiriintymään. Digiturvamalli (n.d) listaa heinäkuussa 2023 suurimmiksi tietoturvauhiksi muun muassa tietojen kalastelun, salasanahyökkäykset, työntekijöiden huolimattomuuden, haittaohjelmat, sähköpostin vaarantumisen,

sisäpiirihyökkäykset, kiristyshaittaohjelmat, väärät pääsyoikeudet ja väärin konfiguroidut pilvitallennustilat.

Listatut esimerkit tietoturvauhista koskevat myös valmistavan teollisuuden organisaatioita. Tietojen kalastelulla voidaan päästä käsiksi työntekijän käyttäjätunnuksiin, ja huolimattomuus voi olla tietojen kalastelussa osatekijänä. Huolimattomuus voi myös olla salattujen asiakirjojen jättämistä näkyville, esimerkiksi työpöydälle tai tietokoneen lukittamattomalle näytölle.

Enisa (n.d) listaa yleisimmät kyberuhat ja -trendit kahdeksaan eri kategoriaan niiden yleisyyden ja vaikutusten mukaan. Kategorioita ovat kiristyshaittaohjelmat (engl. ransomware), haittaohjelmat (engl. malware), käyttäjän manipulointi (engl. social engineering), uhat datalle (engl. threat against data), uhat saatavavuudelle (engl. threat againts availability), disinformaatio-misinformaatio ja tuotantoketjun hyökkäykset (engl. supply chain targeting).

Disinformaatio on väärää tietoa, jolla tarkoituksellisesti halutaan aiheuttaa vahinkoa. Misinformaatio taas on väärä tietoa, jota on luotu tai levitetty tahattomasti (Eurooppa-neuvosto, n.d). Enisan (n.d) mukaan tekoälyn levittämä disinformaatio on nousussa, kuten myös syvävääreennökset (engl. deepfake), jotka ovat keinotekoisesti tehty jäljittelemään aitoa ääntä ja videota. Enisa (n.d) listaa myös nousevaksi trendiksi disinformaation palveluna (engl. disinformation-as-a-service), jossa kuka tahansa voi ostaa valeuutisia tai misinformaatio kampanjoita levittääkseen niitä esimerkiksi netissä (Smirnoff, 2022).

Nousevana trendinä on tuotantolinjan hyökkäykset (engl. Supply chain attack), jossa hyökkäys yritetään kohdistaa organisaation heikkoihin kohtiin sen tuotantoketjussa. (Tucci, 2023) Tuotantolinjan hyökkäys voi esimerkiksi kohdistua organisaation tavarantoimittajaan kaataen toimittajan palvelimet, jolloin tavarantoimittajan palvelut pysähtyvät. Tavarantoimittajan palveluiden pysähtyminen vaikuttaa tavaran tilanneesseen organisaatioon negatiivisesti, kun organisaatio ei pysty toimittamaan omia tuotteitaan eteenpäin. (organisaation sisäinen lähde) Enisan (n.d) mukaan kolmannen osapuolen kybertapaukset ovat nousseet 17 %:iin vuonna 2021, kun ne olivat vielä vuonna 2020 alle yhden prosentin.

2.1.1 Haittaohjelmat

Haittaohjelma on laaja käsite, joka kattaa haitalliset sovellukset ja koodin, joilla pyritään haittaamaan tai vahingoittamaan laitteiden normaalia käyttöä (Microsoft, n.d -a). Enisan (n.d) mukaan vuonna 2021 havaittiin 66 nollapäivähaavoittuvuutta joihin ei löytynyt ratkaisua. Nollapäivähaavoittuvuudella tarkoitetaan haavoittuvuutta, jonka hyökkääjä löytää ennen kuin haavoittuvuudesta ollaan tietoisia. Organisaatio ei siis tiedä haavoittuvuudesta, eikä organisaatiolla näin ollen ole keinoja suojautua, joten hyökkäyksen onnistuminen on todennäköinen. (Kaspersky, n.d -a) Enisa (n.d) listaa yhdeksi nousevaksi trendeiksi tällä hetkellä nollapäivähyökkäykset (engl. zero-day exploits), jossa hyökätään käyttöjärjestelmän haavoittuvuuteen.

Haittaohjelman saa ujutettua työntekijän tietokoneeseen sisäpiirihyökkäyksen avulla, esimerkiksi hyökkäyksen toteuttajan liittäessä haittaohjelman sisältävän USB-tikun työntekijän koneeseen. Haittaohjelman saa ujutettua työntekijän tietokoneelle myös sähköpostissa olevan linkin kautta, jota klikkaamalla työntekijän tietokoneelle latautuu haittaohjelma. Haittaohjelma voi tallettaa salasanoja, joiden kautta organisaation salattuihin tietoihin pääsee käsiksi. Väärät pääsyoikeudet, joilla tarkoitetaan esimerkiksi liian laajoja pääsyoikeuksia, edesauttavat hyökkääjää levittämään haittaohjelmansa haluttuun paikkaan organisaation sisällä. Väärin konfiguroidut pilvitallennustilat mahdollistavat hyökkääjän vapaan liikkumisen organisaation sisäisissä tiedoissa, kun hyökkääjällä on mahdollisuus päästä niin työntekijän tietokoneelle, kuin pilvitallennustiloihinkin. (organisaation sisäinen lähde)

2.1.2 Kiristyshaittaohjelmat

Haittaohjelma voi olla kiristyshaittaohjelma, jossa kiristyshaittaohjelma vaatii lunnaita ennen kuin työntekijä pääsee takaisin tarvitsemiinsa tiedostoihin. Kiristyshaittaohjelmaa käytetään uhrien laitteiden lukitsemiseen tai heidän pääsyn estämiseen esimerkiksi tiettyihin tiedostoihin. Lukitut laitteet tai tiedostot saa takaisin käyttöönsä vain maksamalla hyökkääjälle. Maksaminen ei kuitenkaan takaa, että pääsyoikeutensa saa takaisin. (F-secure, n.d) Enisan (n.d) mukaan 60 % kiristyshaittaohjelman vastaanottaneista organisaatioista on maksanut vaaditut lunnaat.

2.1.3 Käyttäjän manipulointi

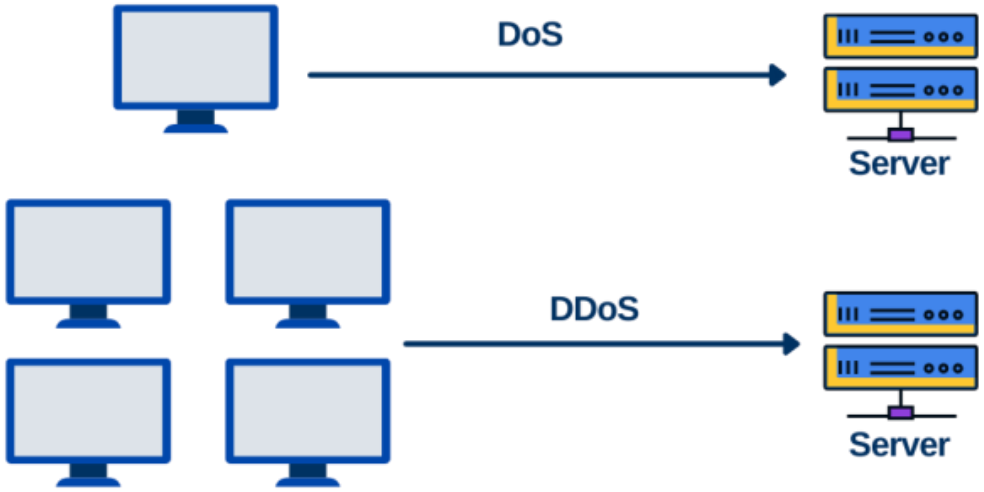
Käyttäjän manipulointi on pyrkimys hankkia luottamuksellista tietoa tekeytymällä tiedon käyttöön oikeutetuksi henkilöksi, tai pyrkimys käyttää hyväksi tietoon oikeutettua henkilöä. Käyttäjän manipulointi voi kohdistua yhteen tai useampaan henkilöön. Toiminnalla pyritään usein selvittämään käyttäjän käyttäjätunnus (Sanastokeskus, 2018). Enisan (n.d) mukaan kalastelu pysyy edelleen suosittuna tekniikkana manipuloida käyttäjää, mutta uusia kalastelumuotoja on jo näkyvissä. Näitä ovat esimerkiksi kohdennettu tietojenkalastelu (engl. spear-fishing), valaanpyyntihyökkäys (engl. whaling), tekstiviestihyökkäys (engl. smishing), sekä puhelun avulla hyökkäys (engl. vishing).

2.1.4 Palvelunestohyökkäys ja hajautettu palvelunestohyökkäys

Uhkia on myös dataa ja datan saatavuutta kohtaan. Palvelunestohyökkäys (engl. denial of service) on tietoverkkohyökkäys, jonka pyrkimys on kuormittaa ja lamaannuttaa palvelu tai tietojärjestelmä. Palvelunestohyökkäys voi lamaannuttaa esimerkiksi sähköpostin suurella määrällä palvelupyyntöjä palvelimeen tai reitittimeen, tai lähettemällä liian suuren määrän sähköpostiviestejä. (Sanastokeskus, 2018) Enisan (n.d) mukaan suurin palvelunestohyökkäys tähän asti toteutui Euroopassa heinäkuussa 2022. Hyökkäyksessä internetin rakenne tuhoutui väliaikaisesti, syntyi katkoksia ja internet-liikenne tuli ohjata uudelleen. Hyökkäys havaittiin ja tunnistettiin 21.7.2022, ja se kohdistui Akamai:n eurooppalaiseen asiakkaaseen. Hyökkäys kohdistui asiakkaan IP-osoitteisiin, muodostaen suurimman hyökkäyksen joka on havaittu Prolexic-alustalla. (Sparling, Gebhardt, 2022)

Palvelunestohyökkäyksiä on myös hajautettuja (engl. distributed denial of service attack, DdoS attack), eli hyökkäys tulee useasta eri lähteestä. Kuvassa (kuva 2) on selvennetty, miten kohdistettu palvelunestohyökäys eroaa palvelunestohyökkäyksestä. Hajautettuun palvelunestohyökkäykseen voidaan käyttää hyökkääjän tietoverkon kautta haltuunsa saaduista tietokoneista muodostuvaa bottiverkkoa.

Kuva 2. Palvelunestohyökkäys (DoS) ja hajautettu palvelunestohyökkäys (DDoS) (Wong, 2022).



Enisan (n.d) mukaan palvelunestohyökkäykset suurentuvat koko ajan, ja ne muuttuvat monimutkaisimmiksi. Palvelunestohyökkäykset kehittyvät kohti mobiiliverkkoja ja esineiden internettiä, joita käytetään jo nyt kybersodankäyntiin. Nousussa on myös tekoälyn levittämä disinformaatio ja syvävääreennökset, joita voi hyödyntää sääntelyiden prosesseissa, sekä yhteisön kanssakäymisessä levittämällä väärää tietoa ja kommentteja esimerkiksi hallituksesta. (Enisa, n.d)

2.1.5 Hyökkäykset esineiden internettiin

Esineiden internet (engl. Internet of things) laitteiden käyttö on laajasti yleistynyt, ja niissä piileviä tietoturvauhkia ei aina huomioida. Tärkeimmät keinot esineiden internet laitteen turvaamiselle on vahva salasana, päivitykset sekä tunnistautuminen. Useimmat laitteet myös käyttävät pientä määrää dataa, joka koituu ongelmaksi jos laitteeseen ei voi asentaa palomuuria tai virussuojaa. Myös jaettu internet yhteys on tietoturvauhka. Jos esineiden internet laite käyttää esimerkiksi samaa WiFi:ä kuin älypuhelin, on esineiden internet laitteen kautta mahdollista päästä käsiksi tietoverkkoon ja siihen yhdistettyihin laitteisiin, kuten älypuhelimeen. Lisäksi esineiden internet laitteiden tietojen lähettämisessä ei

useinkaan käytetä suojausta, ja laitteet voivat olla ominaisuuksiltaan vanhentunteita. Vanhoihin laitteisiin ei välttämättä pysty asentamaan nykyaikaisia turvallisuusvaatimuksia. (Henke, 2023)

2.1.6 Uhat valmistavan teollisuuden organisaatiolle

Esimerkkejä tietoturvauhista valmistavan teollisuuden yritykselle ovat yllä esitettyjen lisäksi mustassa pörssissä myytävät käyttäjätunnukset, vääränlainen materiaalien ja salasanojen toimitus työntekijälle, sekä asiakirjojen huolimaton jakaminen tai talletus. Kaikki nämä voivat olla seurausta työntekijän huolimattomuudesta tai koulutuksen ja tietämyksen puutteesta. Työntekijän perehdyttämisellä on suuri rooli siinä, että tällaiset mahdollisesti kriittiset tapahtumat vähenisivät. Organisaation on mahdollista vähentää tietoturvauhkien aiheuttamien riskien voimakkuutta ennakoivilla toimenpiteillä. (organisaation sisäinen materiaali)

Tietoturvauhkana organisaatiolle voi olla asiakastietojen liiallinen jakaminen. Asiakastietoja ei saa lähtökohtaisesti nähdä kukaan muu kuin tietoa välttämättä tarvitsevat työntekijät, sillä asiakastiedot ovat salattavaa tietoa. Liian laajat käyttöoikeudet ovat myös tietoturvauhka organisaatiolle. Käyttöoikeuksilla tulee päästä vain työntekijälle ennalta määrättyihin palveluihin, ei kaikkiin. Käyttöoikeuksien rajaamisella voidaan pienentää käyttäjätunnuksien avulla tehtyjen tietovuotojen riskiä, sekä minimoida vahinkoja joita esimerkiksi organisaatioon soluttautuminen aiheuttaisi. Muun muassa soluttautujien ja kyberhyökkäysten varalta on tärkeää tehdä erillisiä varmuuskopioita ja säilyttää niitä suojattuna verkon ulkopuolella (engl. offline), jotta minimoidaan vahingot jota datan poistaminen aiheuttaa. Datan poistaminen tai salaus voi vaarantaa koko organisaation toiminnan, jos esimerkiksi tehtaan tuotantolinjan ohjelmisto tietoineen ei ole käytettävissä.

Luottamattomuuden periaate (engl. zero trust) perustuu ajatukseen, että luottamus on nolla kaikilla ajan hetkillä. Laitteet ja käyttäjät tulisi tunnistaa kaikissa tilanteissa, ja päätös pääsyn sallimisesta perustuu riskiarvioon. Yksi perusasioista on vahva tunnistautuminen. Mallissa käytetään kolmea pääkohtaa, käyttäjän varmistamista, minimi-käyttöoikeuksia ja sitä, että oletetaan aina pahinta. Mallin mukaan tietoturvan kehitys on jatkuvaa. (Elisa yrityksille, 2021)

Työntekijöitä tulee kouluttaa, ja heille tulee pitää jatkuvia tiedotuskampanjoita siitä, miten tiedostoja jaetaan, ja miten tiedostot jaetaan turvallisesti niin, etteivät tiedot päädy ulkopuolisten nähtäville. Työntekijälle toimitettavat materiaalit ja salasanat tulee suojata niin, että vaikka toimitusketju katkeaisi, ei ulkopuolisten ole mahdollista aktivoida tunnuksia itselleen. Työntekijöiden tulee olla tietoisia siitä, että salasanoja tai käyttäjätunnuksia ei tule säilyttää esimerkiksi tietokoneen muistiossa tai paperilla. Jos kyseiset materiaalit on toimitettu fyysisellä paperilla, tulee tämä paperi tuhota. Salasanan säännöllinen vaihtaminen tulee olla käytäntö, ja yhteiskäyttötunnuksia tulee välttää. Työntekijät tulee myös ohjeistaa lukitsemaan tietokoneensa aina sen äärestä poistuessaan. (organisaation sisäinen materiaali)

Pääsynhallinnan väärinkäyttö on tärkeää minimoida. Työntekijät tulee kouluttaa olemaan tietoisia siitä, että organisaation tiloihin ei saa päästää ketään asiattomia henkilöitä. Kaikkien tulee kulkea organisaation tiloihin omalla kulkukortillaan, ja kulkukortittomat tulee ohjata paikkaan jossa he voivat tunnistautua. Sosiaalisen manipuloinnin yritykset voivat kohdistua myös organisaation tiloihin pääsemiseksi. (organisaation sisäinen materiaali)

Sosiaalinen manipulointi on tekniikka joka hyödyntää ihmisen tekemiä virheitä saadakseen yksityistä tietoa, käyttöoikeuksia tai arvoesineitä. Kyberrikollisuudessa manipulointi usein houkuttelee uhria paljastamaan dataa, levittämään haittaohjelmaa tai antamaan oikeuksia rajattuihin systeemeihin. Hyökkäykset voivat tapahtua netissä, kasvokkain tai muiden yhteyksien avulla. Hyökkäysprosessi voi toteutua yhdellä sähköpostilla, tai kuukausia kestäneellä sosiaalisen median keskustelulla. (Kaspersky, n.d -b)

Työntekijöiden on tärkeää ymmärtää tietoturvauhkien ja sosiaalisen manipuloinnin riskit jokapäiväisessä työssään. Yksi käytetyimmistä sosiaalisen manipuloinnin keinoista on tietojen kalastelu. Ei ole merkitystä kuinka vahva salasana on, sillä hyökkääjät osaavat käyttää hyväkseen organisaation haavoittuvuuksia, kuten työntekijää. Hyökkääjät käyttävät hyväkseen erilaisia väärennöksiä ja huijauksia. Sosiaalisen manipuloinnin hyökkäys on kohtuullisen suoraviivainen, hyökkääjän tarkoitus on saada huonosti informoitu, stressaantunut tai helposti luottava henkilö luottamaan siihen mitä hyökkääjä sanoo (Cisco, n.d).

Useimmat sosiaalisen manipuloinnin hyökkäykset perustuvat kommunikaatiolle hyökkääjän ja uhrin välillä. Hyökkääjä yrittää motivoida uhria paljastamaan tietojaan, sen sijaan että hyökkääjä käyttäisi esimerkiksi väsytyshyökkäystä (engl. brute force). (Kaspersky, n.d -b)

Sosiaalisen manipuloinnin hyökkäys etenee usein tietyssä järjestyksessä. Ensimmäisenä on valmisteluvaihe. Valmisteluvaiheessa kerätään taustatietoa uhrista, tai isommasta ryhmästä jonka jäsen uhri on. Taustatietojen keräämiseen käytetään usein avoimien tietolähteiden tiedustelua (engl. Open source intelligence). Tiedustelun tavoitteena on muodostaa vapaasti löydettävistä tiedoista kontekstin ja kokonaisuuden kautta tilannekuva, joka paljastaa enemmän kuin organisaatio haluaa tai tiedostaa. Tietojen yhdisteleminen ja johtopäätöksien tekeminen voi paljastaa organisaatiosta haavoittuvaisuuksia ja heikkoja kohtia. (Mintsecurity, n.d)

Toisessa vaiheessa soluttaudutaan. Soluttautumisessa yritetään luoda suhde uhriin, ja yritetään rakentaa luottamusta. Kolmas vaihe on hyväksikäyttö. Uhrin hyväksikäytössä luottamuksesta on tullut uhrin heikkous, jota hyödynnetään hyökkäyksen toteuttamisessa, kuten käyttäjätunnusten haltuun saamisessa. Viimeinen vaihe on irrottautuminen. Irrottautumisessa hyökkääjä on saanut haluamansa, ja hyökkääjä yrittää poistua jättämättä jälkiä. (Kaspersky, n.d -b)

Sosiaalisella manipuloinnilla yritetään hämmentää uhria. Työntekijät eivät välttämättä ymmärrä, että pienelläkin tiedon luovuttamisella he saattavat antaa hyökkääjälle pääsyn useille tileille ja sisäiseen verkkoon. (Kaspersky, n.d -b)

Työntekijöiden tulee olla varuillaan sosiaalisen manipuloinnin varalta, ja esimerkiksi työntekijöiden tulee olla avaamatta mitään linkkejä joiden alkuperästä ei ole täyttä varmuutta. Sähköpostit joissa on epäilyttäviä linkkejä, tiedostoja tai tietoja, tulee heti raportoida eteenpäin. (organisaation sisäinen materiaali)

Valmistavan teollisuuden organisaatiolle suurin sosiaalisen manipuloinnin uhka on erilaiset kalasteluhyökkäykset. Kalastelua voi tehdä esimerkiksi sähköpostin kautta, kuten myös tekstiviestien ja pikaviestipalveluiden kautta (engl. smishing). Englanninkielistä termiä ”vishing” käytetään puhelimitse tehtävistä huijauksista. (F-secure, n.d)

Sosiaaliselta manipuloinnilta on mahdollista suojautua. Ratkaisevin suojauskeino on tiedotus, jolla lisätään yleistä tietoturvatietoisuutta. Tiedotuksen tulee sisältää demonstraatioita siitä, millä tavoin hyökkääjä voi yrittää manipuloida työntekijää. Tiedotus auttaa jokaista työntekijää suojautumaan manipuloinnilta, ja auttaa ymmärtämään miten ja miksi heidän roolinsa organisaation turvallisuudelle on tärkeää. (Cisco, n.d)

Organisaatioilla tulee olla myös käytössään selvät turvallisuuskäytänteet, jotta työntekijöiden on mahdollista tehdä järkeviä valintoja sosiaalisen manipuloinnin yrityksissä. Selkeitä ja tärkeitä tapoja ovat esimerkiksi salasanojen hallinta, kaksivaiheinen todennus (engl. Multi factor authentication) ja sähköpostien turvallisuus. Salasanan hallinnassa tulee olla vaatimukset ja ohjeet millainen on turvallinen salasana. Tämä voi sisältää ohjeet millaisia merkkejä ja numeroita tulee käyttää ja kuinka pitkä salasanan tulee olla. Organisaation käyttämien järjestelmien ei pidä hyväksyä salasanoja jotka eivät täytä vaatimuksia. Ohjeiden tulee sisältää tieto siitä, kuinka usein salasana tulee vaihtaa, ja painottaa tärkeyttä, että salasanaa ei tule missään tilanteessa jakaa kenellekään. Jos organisaatiossa on käytössään salasanan hallintatyökalu, tulee työkalusta olla oma ohjeistuksensa. Kaksivaiheinen todennus vähentää hyökkäysten mahdollisuutta, ja todennus tulee olla työntekijöillä käytössä. Organisaatiossa tulee olla käytössään monen kerroksen sähköpostien suojaus, joka minimoi mahdollisuuden kalasteluun ja sosiaaliseen manipulointiin. (Cisco, n.d)

Kun organisaatiossa tehdään muutoksia jotka ovat julkisesti tiedossa, on uhkana että organisaatioon yritetään hyökätä vielä aktiivisemmin. Yksi näistä hyökkäyksen keinoista on kalastelusähköpostit. Organisaatioille tähdätyt sähköpostit uskottelevat lähettäjän olevan itse organisaatio tai joku sen tunnettu toimija tai asiakas. Myös kaapattuja organisaation sähköpostitilejä voidaan käyttää kalastelusähköpostien lähettämiseen. Sähköpostiin sisällytetty linkki vie saastuneelle (engl. malicious) sivustolle, joka voi ulkoasultaan muistuttaa organisaation käyttämää kirjautumispalvelua tai nettisivua. Jos uhri kirjoittaa tunnuksensa tälle sivustolle yrittäessään kirjautua sisään, hyökkääjä saa hänen tunnuksensa. Sähköpostin lisäksi hyökkääjä voi yrittää saada tietoonsa organisaation tietoja tai tunnuksia LinkedIn:n kautta tai muussa sosiaalisessa mediassa. Tällaiset yritykset tulee aina raportoida eteenpäin. Sähköpostien raportoimiseen löytyy ohjeet organisaatiosta, ja esimerkiksi LinkedIn:n huijaukset tulee raportoida sovelluksen ylläpitäjille. Linkkejä ei tule klikata, eikä omia tunnuksiaan tule kirjoittaa mihinkään ellei ole varma nettisivun aitoudesta. Kaikista

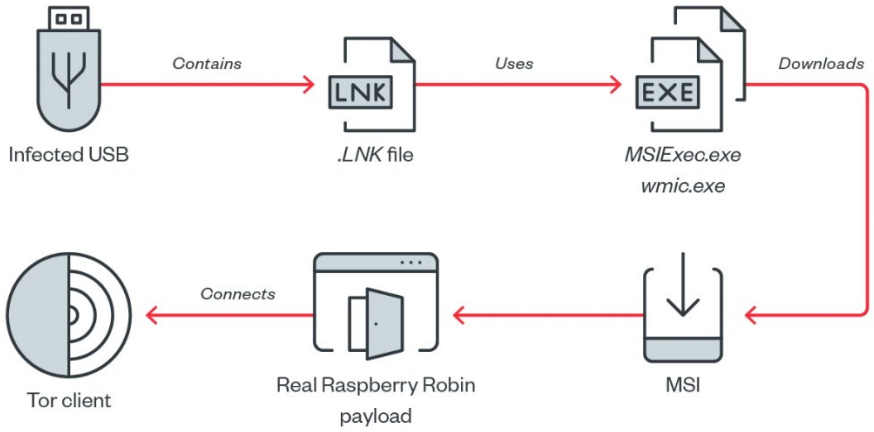
epäilyksistä tai epäilyttävistä sähköposteista, sivustoista ja LinkedIn profiileista voi puhua vapaasti esimiehen kanssa, tai raportoida niistä organisaation tietoturvakäytänteiden mukaisesti. (organisaation sisäinen lähde)

Tunnettuna tietoturvauhkana valmistavan teollisuuden organisaatiolle on kohdistettu haittaohjelmahyökkäys (engl. targeted malware atack). Hyökkäys voi kohdistua yritykseen, toimialaan, valtion hallinoimaan organisaatioon tai rajattuun henkilöjoukkoon. Tavoitteena on kriittisen tiedon haltuun saaminen tai kohteen toiminnan muuttaminen. Kohdistetun haittaohjelmahyökkäyksen tekijä pyrkii hyväksikäyttämään kohteestaan hakemiaan tietoja, joiden avulla haittaohjelma on mahdollista saada kohteen järjestelmiin. Hyökkääjä pyrkii toimimaan huomaamatta, jäljet pyritään poistetaan tietojärjestelmistä hyökkäyksen lähteen selvittämisen vaikeuttamiseksi. Hyökkäykset ovat usein pitkäkestoisia ja niissä käytetyt haittaohjelmat voivat olla yksilöllisesti suunniteltuja. (Sanastokeskus, 2018)

Yksi tunnetuista tietoturvauhista toimeksiantajalle on Raspberry Robin, joka on madon kaltainen haittaohjelma. Haittaohjelma leviää järjestelmiin saastuneen USB-tikun kautta saastuttaen laitteen, kun haittaohjelman sisältämää .LNK-tiedostoa tuplaklikataan. Seuraavaksi haittaohjelma lataa saastuneen asennusohjelman, joka asentaa laitteelle Raspberry Robinin tietosisällön. Haittaohjelma on edistynyt, sillä se osaa piilottaa koodinsa viruksentorjuntaohjelmilta ja tutkijoilta. (Toulas, 2022)

Raspberry Robin on paketoitu useaan eri kerrokseen. Haittaohjelman tietosisällön ensimmäisten kerrosten alta on mahdollista löytää väärennös haittaohjelmasta. Vielä syvemmälle mentäessä kerrosten alta löytyy haittaohjelman oikea tietosisältö. Tietosisältöön on kovakoodattu yhteys Tor tietoverkkoon, jonka avulla hyökkääjä voi esimerkiksi kommunikoida haittaohjelman kanssa. Kuvassa 3 on esitetty Raspberry Robinin reitti Tor tietoverkkoon pääsemiseksi. (Toulas, 2022)

Kuva 3. Raspberry Robinin tartuntareitti (So, 2022).

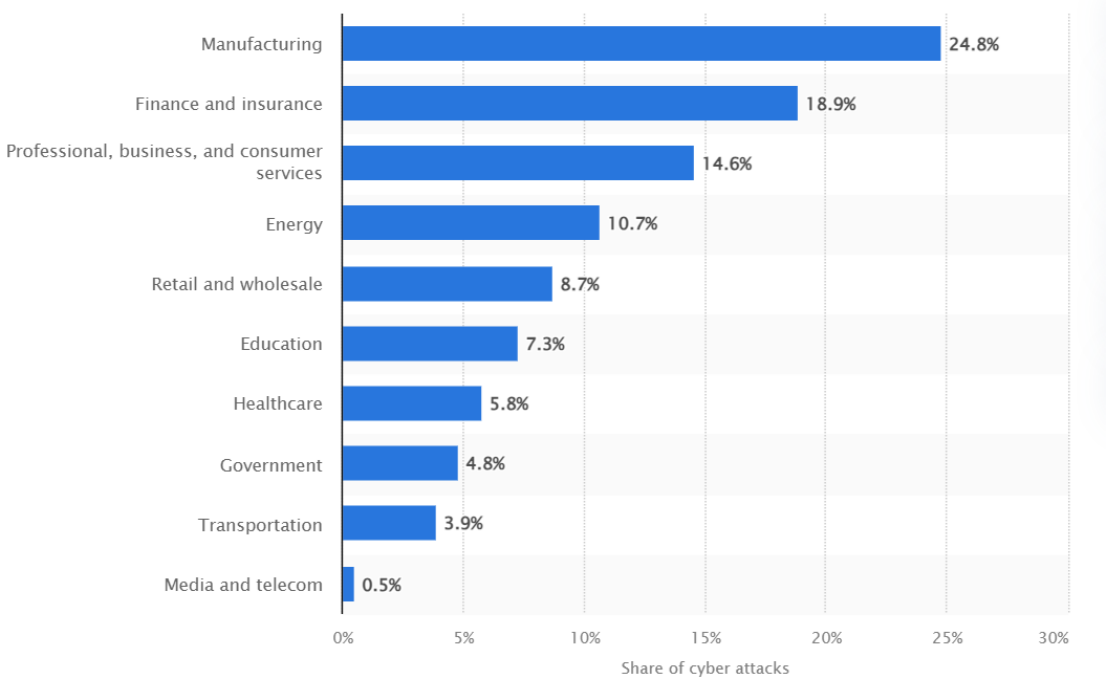


Tunnetuista APT-ryhmistä toimeksiantajasta voi olla kiinnostunut APT5-ryhmä. APT5-ryhmä sijaitsee todennäköisesti Kiinassa, ja se hyökkää muun muassa valmistavan teollisuuden organisaatioihin Euroopassa ja Aasiassa. Ryhmä on ollut aktiivinen ainakin vuodesta 2007 lähtien. Ryhmä hyökkää useiden eri alojen organisaatioihin, mutta pääasiassa telekommunikoinnin ja teknologian organisaatioihin. Ryhmä käyttää hyväkseen haittaohjelmaa joka tallentaa näppäimistön painalluksia. Haittaohjelman avulla ryhmä hyökkää yritysten tietoverkkoihin, työntekijöihin ja johtotasoon. Ryhmä on näyttänyt merkittävää kiinnostusta tietoverkossa olevien laitteiden vaarantamiseen ja näitä ylläpitävien ohjelmistojen manipuloimiseen. (Mandiant, n.d)

2.2 Kyberturvallisuus ja kyberhyökkäykset

Kyberturvallisuutta tarvitaan kaikessa organisaation toiminnassa. Toimeksiantaja on hyvin altis kyberhyökkäyksille, sillä se on valmistavan teollisuuden organisaatio. Alttiuden takia kyberturvallisuuden tulee korostua kaikessa organisaation toiminnassa. Kuvasta (kuva 4) näkee, kuinka valmistavan teollisuuden organisaatiot ovat olleet eniten kyberhyökkäysten kohteena.

Kuva 4. Maailmanlaajuinen kyberhyökkäysten jakautuminen alakohtaisesti (Statista, 2023).



Kyberhyökkäyksiä on monia erilaisia, joiden tavoitteet, kohteet ja toimintatavat vaihtelevat. Hyökkäysten tavoite voi olla esimerkiksi taloudellinen hyöty tai poliittinen motiivi. Osa hyökkäyksistä voi kohdistua yksityishenkilöihin, jotta huomio poistuu joltain suuremmalta kohteelta, kuten yrityksiltä tai valtioilta. (F-secure, n.d)

Yritysten on mahdollista suojautua erilaisilta kyberhyökkäyksiltä useilla eri tavoilla. Yksi tärkeä suojautumiskeino on virussuoja. Virussuoja havaitsee troijalaisia, vakoiluohjelmia sekä muita haittaohjelmia. Jos jokin haittaohjelma on jo päässyt laitteelle, on virussuojan mahdollista havaita ja poistaa se. (F-secure, n.d)

Ajantasaiset ohjelmistopäivitykset ovat myös osa puolustautumista kyberhyökkäyksiltä. Hyökkääjä osaa hyödyntää aukkoja ohjelmistojen tietoturvassa, ja hyökkääjät etsivät tietoturva-aukkoja aktiivisesti. Palveluntarjoajat julkaisevat säännöllisesti ohjelmistopäivityksiä, joiden tarkoituksena on korjata havaittuja haavoittuvuuksia. Pitämällä laitteen ohjelmistot ja käyttöjärjestelmä ajan tasalla, on niitä mahdollisimman turvallista käyttää. (F-secure, n.d)

Tärkeää on myös kiinnittää huomiota omaan käyttäytymiseensä laitteella. Varautuminen ja varovaisuus netissä on tapa ehkäistä joutumista hyökkäyksen uhriksi. Monet kyberuhat

vaativat toimia uhriltaan. Esimerkiksi troijalainen ei voi päästä laitteelle jos laitteelle ei lataa tiedostoa johon haittaohjelma on piilotettu. Myös linkkien klikkaamatta jättäminen suojelee laitetta erilaisilta hyökkäyksiltä. Hyökkäyksen mahdollistavia, saastuneita linkkejä voi olla erilaisilla nettisivuilla, laitteelle lähetetyissä tekstiviesteissä tai sähköposteissa. (F-secure, n.d)

On tärkeää kiinnittää huomiota omaan käyttäytymiseen netissä, kuten siihen, että ei jaa liikaa tietoa itsestään. Käyttäjien tietoja, kuten henkilötunnuksia, salasanoja ja osoitteita keräävät palvelut voivat joutua tietomurron uhriksi. Yksilö ei voi vaikuttaa siihen, kuinka hyvin tietoja keräävät palvelut on suojattu. Yksilöllä on kuitenkin mahdollisuus rajoittaa itsestään jakamiaan tietoja. Salasanojen vaihtaminen ja vahvat salasanat auttavat siinä, että vaikka yritys joutuisi tietomurron kohteeksi, eivät yksilön tiedot välttämättä ole vaarantuneet. (F-secure, n.d)

Vahvat salasanat ja kaksivaiheinen tunnistautuminen suojelevat kyberhyökkäyksiltä. Samoja salasanoja ei tule käyttää useassa eri kohteessa, koska yhden salasanan murrettua hyökkääjän on mahdollista päästä muihinkin palveluihin. Tunnusten suojausta voi vahvistaa kaksivaiheisella tunnistautumisella (engl. Multifactor authentication, MFA), tai käyttämällä salasanojen hallintaan tarkoitettuja työkaluja. (F-secure, n.d)

Kirjautuessa sisään erilaisille tileille netissä, todistetaan palvelulle että kirjautuja on kuka väittää olevansa. Yleisesti tämä on tapahtunut käyttämällä salasanaa ja käyttäjätunnusta, mutta se ei ole nykyään enää riittävä keino. Käyttäjänimi on helppo löytää, sillä se saattaa olla vain sähköpostiosoite. Salasanoja on vaikea muistaa, joten henkilöt ovat taipuvaisia valitsemaan helppoja salasanoja, tai käyttävät samaa salasanaa useassa eri paikassa. (Microsoft, n.d -b)

Melkein kaikki nettipalvelut, kuten pankit, sosiaaliset mediat sekä organisaatiot, ovat lisänneet keinon, jolla tilit olisivat turvallisempia. Tätä keinoa nimitetään kaksivaiheiseksi todennukseksi. Kaksivaiheinen todennus toimii usein samalla kaavalla; kun tilille kirjautuu ensimmäistä kertaa uudella laitteella tai sovelluksella, tarvitsee muutakin kuin salasanan ja käyttäjätunnuksen. Tämä tekijä (engl. factor) tunnistusprosessissa varmistaa kirjautujan identiteetin. Esimerkiksi salasana on yksi tekijä, jonka lisäksi tarvitsee toisen tekijän. Kolme

yleisintä tekijää identiteetin varmistamiseen ovat salasana tai pin, älypuhelin tai USB-avain, sekä sormenjälki tai kasvojen tunnistus. (Microsoft, n.d -b)

Kaksivaiheinen todennus toimii niin, että henkilö syöttää salasanan ja käyttäjätunnuksensa. Jos nämä olisivat ainoat asiat joita vaaditaan sisäänkirjautuessa, kuka tahansa mistä sijainnista tahansa voisi kirjautua sisään tilille. Kaksivaiheinen todennus pyytää salasanan ja käyttäjätunnuksen syöttämisen jälkeen toisen tunnistustavan varmistaakseen kirjautujan identiteetin. Yksi tapa on Todennus-sovellus (engl. Authenticator), joka näyttää uniikin ja dynaamisesti luodun 6-numeroisen koodin älypuhelimella. Tämä koodi kirjoitetaan kirjautumisen yhteydessä. Tilille ei ole mahdollista päästä ilman tilin haltijan älypuhelinta, jossa 6-numeroinen koodi sijaitsee. Useat todennus-sovellukset myös vaihtavat koodeja hyvin usein, jokaiselle kirjautumisyritykselle, joten edellisen koodin tietäminen ei auta seuraavalla kirjautumisyrityksellä. (Microsoft, n.d -b)

2.3 Riskienhallinnan perusteet ja menetelmät

Riskienhallinta on prosessi jolla identifioidaan, arvioidaan ja kontrolloidaan uhkia organisaatiota ja sen hankintoja kohtaan. Riskit voivat tulla useasta eri lähteestä, kuten taloudellisista epävarmuuksista, laillisista velvollisuuksista, teknologiaongelmista, strategisista johdon virheistä, vahingoista, onnettomuuksista ja luonnon katastrofeista. (Tucci, 2023)

Työntekijä on lain mukaan velvoitettu suojelemaan työntekijöitä ja muita vahingoilta. ”Työntekijän on myös kokemuksensa, työnantajalta saamansa opetuksen ja ohjauksen sekä ammattitaitonsa mukaisesti työssään huolehdittava käytettävissään olevin keinoin niin omasta kuin muiden työntekijöiden turvallisuudesta ja terveydestä” (Finlex, 2002). Minimivelvoite on tunnistaa mikä voi aiheuttaa vahingon henkilölle tai organisaatiolle, päättää kuinka todennäköistä on että joku loukkaantuu ja kuinka vakavasti, sekä tehdä toimenpiteitä jolla voi ehkäistä vahingon jos se on mahdollista, tai hallita riskiä. Riskin arviointi on vain yksi osa prosessista jolla hallitaan riskejä työympäristössä. (Health and safety executive, n.d)

Onnistunut riskienhallinta auttaa organisaatiota kohtaamaan riskejä jokaisesta näkökulmasta. Riskienhallinta myös tutkii riskien ja niiden vaikutusten suhdetta, jotka voivat vaikuttaa organisaation strategisiin tavoitteisiin. (Tucci, 2023) Kolme tärkeää vaihetta riskienhallinnan prosessissa on riskien tunnistaminen (engl. identifying risks), riskianalyysi ja arviointi (engl. risk analysis and assessment) sekä riskien vähentäminen ja seuranta (engl. risk mitigation and monitoring) (Ibm, n.d).

Riskien tunnistaminen on prosessi, jossa identifioidaan ja arvioidaan uhkia jotka vaikuttavat organisaatioon, sen toimintaan ja työvoimaan. Riskien tunnistaminen voi sisältää tietotekniikan turvallisuuden määrittämistä, kuten onnettomuudet, haittaohjelmat, luonnon katastrofit ja muut potentiaalisesti haitalliset tapahtumat, jotka voivat häiritä yritystoimintaa. (Ibm, n.d)

Riskianalyysi ja arviointi sisältää vakiintuneen ajatuksen, että riskitapahtuma voi esiintyä, ja potentiaalisesti jokainen tapahtuma voi näkyä ulospäin. Riskien arviointi vertaa jokaisen riskin merkitystä ja sijoittaa jokaisen riskin niiden todennäköisyyden ja vakavuuden mukaan. (Ibm, n.d)

Riskien vähentäminen ja seuranta osoittaa prosessiin, jossa suunnitellaan ja kehitetään menetelmiä ja vaihtoehtoja jotka vähentävät uhkia projektille. Projektiryhmä voi toteuttaa riskien vähentämisen strategioita identifioidakseen, monitoroidakseen ja arvioidakseen riskejä ja seuraamuksia tai suorittaakseen tietyn projektin, kuten uuden tuotteen luomisen. Riskien vähentäminen myös sisältää ne toimenpiteet, jotka tehdään projektia koskevien ongelmien ja vaikutusten käsittelemiseksi. (Ibm, n.d)

Riskeihin vastaamiseen on eri tapoja. Näitä ovat muunmuassa riskien välttäminen (engl. risk avoidance), riskien vähentäminen (engl. risk mitigation), riskien jakaminen (engl. risk sharing), riskien siirtäminen (engl. transferring risk) ja riskien hyväksyminen ja säilyttäminen (engl. risk acceptance and retention). Riskien välttäminen on keino, jossa riskejä yritetään minimoida. Riskejä voi esimerkiksi välttää siten, että ei tee sijoitusta tai aloita uutta tuotantolintaa. Riskien vähentäminen on tapa, jolla yritetään minimoida menetys täydellisen eliminaation sijaan. Riski voidaan joissain tilanteissa hyväksyä, erityisesti jos riski on pieni. Jos riskiä ei pysty kokonaan poistamaan, riskille tehdään seurantaa jotta mahdollinen riskin aiheuttama menetys tai haitta pidetään hallittuna. Terveydenhuollossa tällainen toiminta on

esimerkiksi ennakoivaa hoitoa. Riskin voi myös siirtää komannelle osapuolelle, kuten vakuutusyhtiölle, joka mahdollisesti korvaa omaisuuden vahingot tai tapaturmat. Riskin hyväksyminen ja säilyttäminen on toimenpide, joka tehdään kun muut tavat on kokeiltu. Kaikkia riskejä ei voi kokonaan eliminoida. Jäännösriskiksi kutsutaan riskiä, jolle on jo tehty kaikki mahdolliset korjaavat toimenpiteet. (Ibm, n.d)

Riskien todennäköisyyttä ja sen vaikutusta voidaan arvioida riskien arvioinnin taulukon avulla. Taulukon avulla lasketaan, millaiset vaikutukset riskillä olisi organisaatioon. Kuvassa (kuva 5) on esimerkki millaisen taulukon avulla riskejä voidaan laskea. Taulukolla voidaan laskea tapahtuman todennäköisyyden ja vaikutuksen perusteella kuinka riski tulisi vaikuttamaan organisaatioon.

Kuva 5. Riskiarvio-taulukko (Aven, Cox. n.d).

Risk Assessment Table

		Severity of Harm (Impact)		
		Low (L)	Medium (M)	High (H)
Likelihood	High (H)	3	4	5
	Medium (M)	2	3	4
	Low (L)	1	2	3

2.4 Eettiset näkökulmat

Kyberturvallisuus kasvaa hurjaa vauhtia teknologian kehittyessä, ja samalla kasvavat myös tietoturvahyökkäykset sekä turvallisuusuhat. Kyberturvallisuustoiminnan lisääntyessä korostuu myös se, että ammatinharjoittajat toimivat eettisellä tavalla. (UK Cybersecurity council, 2023)

Kyberturvallisuuden ensimmäinen eettinen sääntö on suojella yksilön yksityisyyttä. Tämä tarkoittaa sitä, että kaikki kerätty data on kerätty organisaation tai yksilön suostumuksella. Kaikki kerätty data tulisi varastoida turvallisesti, ja sitä ei saa jakaa ilman suostumusta. Tämä varmistaa sen, että kaikki arkaluontoinen data, kuten pankkikortin tiedot ja muu henkilökohtainen tieto, ei tule kerätyksi ilman henkilön tietämystä asiasta. (UK Cybersecurity council, 2023)

Eettiset toimet ovat välttämättömiä datan suojelemiseksi ja luottamuksen säilyttämiseksi. Kun teknologia kehittyy, tulee pitää yllä tiettyjä standardeja kun käsitellään arkaluontoista dataa. Ilman näitä ohjeistuksia voi tulla vakavia seuraamuksia niin taloudellisesti kuin laillisesti. (UK Cybersecurity council, 2023)

Yhtenäisyyden (engl. integrity) mukaan toimiminen sisältää esimerkiksi datan salaamisen mahdollisilta hyökkäyksiltä suojaamiseksi. Lisäksi organisaatioilla tulisi olla ohjeet kuinka he käsittelevät dataa, jotta asiakkaat tietävät että heidän tietonsa pysyvät turvassa. Lisäksi käyttäjiä tulisi aina informoida etukäteen muutoksista, jotta he voivat päättää, haluavatko he että heidän tietojaan kerätään uusien ehtojen mukaan vai eivät. (UK Cybersecurity council, 2023)

Toinen tärkeä sääntö eettisestä toiminnasta on ammattimaisuus ja läpinäkyvyys siitä, mitä dataa organisaatio kerää ja mihin he tarvitsevat kerättyä tietoa. Organisaatioiden täytyy varmistaa, että heidän käyttäjänsä ymmärtävät millaista tietoa organisaatio kerää ja kuinka sitä käytetään ennen kuin keräämiseen on kysytty lupaa. Organisaatioiden tulee käyttää dataa vain ilmoittamiinsa tarkoituksiin. (UK Cybersecurity council, 2023)

Kolmas eettinen sääntö on uskottavuus (engl. credibility), joka sisältää säännön vastuullisesta käytöksestä. Pitää varmistaa, että jokainen asiaan liittyvä ottaa vastuun teoistaan. Esimerkiksi organisaatioiden tulisi säännöllisesti tehdä auditointeja identifioidakseen aihealueita joissa tulisi tehdä parannuksia. Työntekijöiden tulisi myös ilmoittaa mistä tahansa epäilyttävästä toiminnasta välittömästi. Toimitusjohtajien tulisi näyttää esimerkkiä kiinnittymällä tiukasti organisaation käytänteisiin kyberturvallisuusprotokollista. On jokaisen velvollisuus välttää laiminlyöntejä datan käsittelyssä. Näiden pääohjeistusten seuraaminen auttaa käyttäjiä ja ammatinharjoittajia pitämään luottamuksen yritysten ja kuluttajien välillä, pitäen digitaalisen puolen turvattuna. (UK Cybersecurity council, 2023)

2.5 Uhkatieto

Uhkatieto (engl. threat intelligence) on yksityiskohtaista tietoa uhista, joilla pyritään estämään ja vastaamaan organisaatioon kohdistuviin kyberuhkiin (ibm.com). Uhkatieto on

dataa jota on kerätty, prosessoitu ja analysoitu, jotta ymmäretään uhan tekijän motiiveita, kohteita ja hyökkäyksen toimintatapoja. Uhkatieto mahdollistaa nopeammat ja informatiivisemmat päätökset jotka perustuvat kerättyyn dataan. Uhkatieto myös mahdollistaa käytöksen muuttumisen ennakoivammaksi. (Baker, 2023)

Uhkatieto on yksityiskohtaista dataa, joka sisältää tietoa organisaatiota uhkaavista tietoturvallisuusuhista. Uhkatieto auttaa turvallisuusvastaavia ennakoimaan, mahdollistaen tehokkaita ja datavetoisia toimia tietoturvahyökkäyksien estämiseksi jo ennen kuin niitä ilmenee. Uhkatieto myös auttaa organisaatiota havaitsemaan hyökkäyksiä, sekä vastaamaan paremmin jo käynnissä oleviin hyökkäyksiin. (Ibm, n.d)

Kaikki uhkatieto ei ole keskenään samanarvoista, sillä kaikki valmistavalle teollisuudelle tärkeät tiedot eivät välttämättä ole tärkeitä esimerkiksi organisaatioille jotka työskentelevät logistiikan parissa. Uhkatiedon arvo lisääntyy tarpeellisuuden ja saatavuuden mukaan. Tietoa tulee suodattaa sen mukaan, millainen organisaatio on, missä se sijaitsee, sekä toimintaympäristön ja infrastruktuurin mukaan. Suodatukseen vaikuttaa myös kenen kanssa organisaatio on tekemisissä, sekä organisaation riskiprofiili. Tärkeää on päättää kuka pääsee dataan ja erilaisiin tietoihin käsiksi. Kaikkea uhkatietoa ei kannata julkaista julkisesti, vaan uhkatieto kannattaa analysoida ja lajitella. (Llorens, n.d)

Uhkatietoa kerätään usein useasta eri lähteestä. Lähteitä voivat olla esimerkiksi aikaisemmat hyökkäykset, uutiset ja artikkelit, blogit, tweetit, turvallisuusalan raportit sekä viitteet hyökkäyksistä. Turvallisuusanalyytikot luovat uhkatietoa keräämällä uhkiin ja turvallisuuteen liittyvää tietoa useista eri lähteistä, ja sitten vertailevat ja analysoivat dataa paljastaakseen trendejä, kaavoja ja suhteita. Uhkatietoa kerätään, jotta voidaan tuottaa syvällistä ymmärtämistä todellisista ja potentiaalisista uhista. (Llorens, n.d)

Uhkatiedossa on neljä päätyyppiä, strateginen, taktinen, teknillinen sekä operaattinen (DNSstuff, 2022). Kuvassa (kuva 6) on esitetty uhkatiedon eri päätyypit.

2.5.1 Strateginen uhkatieto

Strateginen uhkatieto on termi, jota käytetään analysoidessa trendejä ja kasvavia riskejä, jotta voidaan luoda yleinen kuva mahdollisen kyberhyökkäyksen vaikutuksista. Strateginen

uhkatieto kysyy kysymyksen ”mikä on pahin mitä voi tapahtua”. Tämä tieto on usein esitetty organisaatiossa korkean tason päätöksen tekijöille, kuten hallituksen jäsenille. (DNSstuff, 2022) Strategista uhkatietoa käytetään hyväksi muun muassa suunniteltaessa liiketoiminnan jatkuvuuden varmistamista.

2.5.2 Taktinen uhkatieto

Taktinen uhkatieto antaa yksityiskohtaisempaa tietoa uhkatekijän taktiikasta, tekniikasta ja menetelmistä. Se on lähinnä tarkoitettu tekniselle yleisölle, ja auttaa ymmärtämään kuinka tietoverkkoon mahdollisesti hyökätään, pohjautuen hyökkääjien viimeisimpiin menetelmiin saavuttaa tavoitteensa. Taktisessa uhkatiedosssa etsitään indikaattoreita vaarantumisesta ja mahdollisista poikkeamista, kuten IP-osoitteita, URL-osoitteita ja sisäänkirjautumisia. Tieto vaarantumisesta auttaa tulevaisuudessa havaitsemaan mahdollisuudet varastaa dataa. Taktinen, todisteisiin pohjautuva uhkatieto on usein osoitettu turvallisuustiimeille tai organisaation henkilöille jotka vastaavat suoraan tietoverkkojen turvaamisesta. (DNSstuff, 2022)

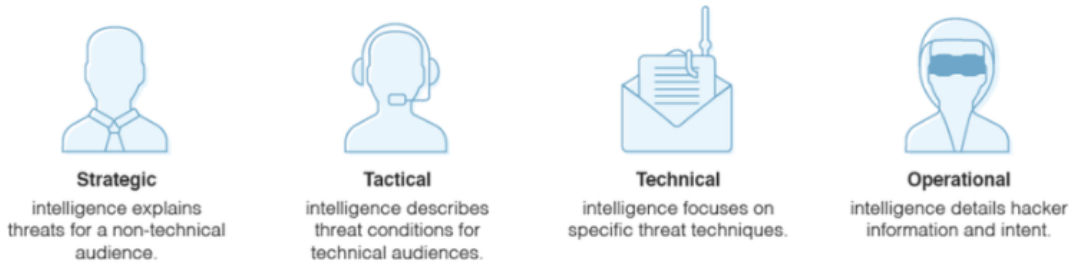
2.5.3 Tekninen uhkatieto

Tekninen uhkatieto keskittyy teknisiin vihjeisiin, kuten kalastelusähköpostin aihe-kenttään tai petollisiin URL-osoitteisiin. Tämän tyyppinen uhkatieto on tärkeää, sillä se antaa idean mitä etsiä, ja tekee sosiaalisen manipuloinnin analysoinnista hyödyllistä. Kuitenkin koska hyökkääjät vaihtavat usein heidän taktiikoitaan, tekniikoitaan ja menetelmiään, teknisen uhkatiedon tutkinnan elinkaari on lyhyt. (DNSstuff, 2022)

2.5.4 Operatiivinen uhkatieto

Operatiivinen uhkatieto auttaa tietoteknistä puolustajaa ymmärtämään yksittäisten kyberhyökkäyksien luonnetta erittelemällä oleellisia tekijöitä, kuten luonnetta, aikeita, ajoitusta sekä hyökkääjän ryhmän kehitteneisyyttä. Operatiivinen uhkatieto on esimerkiksi hyökkääjän käyttämiin chat-palveluihin soluttautumista. Kaikki näkökulmat kyberuhkatiedosta ovat tarpeellisia kattavan uhka-arvion toteuttamiseksi. (DNSstuff, 2022)

Kuva 6. Uhkatieto voidaan jakaa neljään päätyyppiin, strategiseen, taktiseen, tekniseen ja operatiiviseen (Dnsstuff, 2022).



Uhkatiedon käsittelyyn löytyy monia työkaluja, ja netissä on saatavilla hyviä artikkeleita joissa on vertailtu eri yhtiöiden kaupallisia työkaluja. Uhkatiedon työkalut voidaan kuitenkin karkeasti jakaa niitten käyttötavan perusteella neljään kategoriaan; lokien hallintaan, turvallisuustapauksien analysointiin, raportointiin sekä automaattiseen vastatoimeen. (DNSstuff, 2022)

2.5.5 Uhkatieto ISO 27001 -standardissa

ISO 27001 on maailmanlaajuinen tietoturvallisuuden hallintaan liittyvä standardi. ISO 27001 -standardi velvoittaa organisaatiota kerämään ja analysoimaan tietoa, joka liittyy tietoturvallisuusuhkiin ja käyttämään tätä tietoa pienentääkseen haitallista toimintaa. Uhkatietoa käytetään uhkien torjumiseen, tunnistamiseen tai uhkiin vastaamiseen. ISO 27001 -standardi on ennakoiva, huomioiva ja korjaava toimenpide, jotta varmistetaan, että tuotetaan tietoisuutta organisaation uhkaympäristöstä, jotta tarvittavat toimet voidaan ottaa käyttöön (Hightable, 2023). Sertifikaatti on virallisen ulkopuolisen toimijan myöntämä todistus siitä että organisaatio toimii standardin mukaisesti.

ISO 27001 -standardissa sanotaan: “Information relating to information security threats should be collected and analyzed to produce threat intelligence” (Barker, 2023). Kyseinen alakohta standardissa varmistaa, että:

- Päämäärät uhkatiedon tuotantoon on varmistettu
- Sisäiset ja ulkoiset tietolähteet on tunnistettu, valittu ja ennakkotarkistettu, mikä on tarpeellista ja sopivaa tietoa

- Tietoa on kerätty valituista lähteistä
- Tieto on valmisteltu analyysia arten, esimerkiksi kääntämällä se
- Tieto on analysoitu, jotta tiedetään mikä koskee organisaatiota
- Kommunikointi ja tiedon jakaminen on tehty niin, että tietoa tarvitsevat ihmiset ymmärtävät sen

Kun käsitellään uhkatietoa, uhkatieto analysoidaan ja sisällytetään riskienhallintasuunnitelmaan. Uhkatietoa käytetään tiedoitukseen, miten hyödyntää ja konfiguroida teknisiä kontrolleja. Uhkatiedon perusteella sopeutetaan tietoturvallisuustestejä ja -tekniikoita.

3 Tietoturvatietoisuuden kehittäminen

Tietoturvatietoisuuden kehittäminen on jatkuva kehityskohde isoissa kansainvälisissä organisaatioissa. Jokaisen työntekijän työpanosta tarvitaan tietoturvallisuuden ylläpitämiseksi, ja näin ollen tietoturvatietoisuus on tärkeä jatkuvan kehittämisen kohde. Tehokkaita tietoturvatietoisuuden lisäämisen keinoja ovat muun muassa tiedotukselliset tapahtumat, koulutukset, logojen ja sloganien käyttö sekä yleinen tiedottaminen esimerkiksi kiinnittämällä tiedotteita organisaation tilojen oviin, mainostauluihin ja käytäville.

3.1 Toimeksiantajan tietoturvakulttuuri

Toimeksiantaja on tietoturvatietoinen. Toimeksiantajalla on käytössään tietoturvallisuuteen liittyen useampi eri standardi ja sertifikaatti. Näitä ovat esimerkiksi ISF standard of good practice, kuten myös ISO 27001 -standardi, sekä IEC 62443. ISF of good practice on laaja ja maailmanlaajuisesti hyväksyttu turvallisuuden viitekehys (ISF, n.d). IEC 62443 -sarja on automaatiolle ja ohjausjärjestelmille kehitetty kyberturvallisuus standardi (International society of automation, n.d). Toimeksiantaja järjestää kaikille työntekijöilleen pakollisia koulutuksia tietoturvallisuudesta, sekä velvoittaa työntekijänsä toimimaan standardeissa ja organisaatiossa olevien ohjeistuksien mukaisesti. Toimeksiantaja tiedottaa tietoturvaan liittyvistä asioista esimerkiksi webinaarien muodossa, sekä yksiköille järjestetään vuosittain ja tarpeellisuuden mukaan spesifioituja tietoturvaharjoituksia. Toimeksiantajalla on käytössään tietoturvakuukautena erilaisia kampanjoita, ja tietoturvallisuudesta tiedotetaan sisäisissä viestintäkanavissa. Toimeksiantajan työntekijät ovat hyvin valppaina lähettämään turvallisuustiimille kysymyksiä oman työnkuvansa tietoturvallisuuteen liittyen, jos toimeksiantajan tietoturvakäytänteissä ei ole suoraan otettu kantaa asiaan.

Tietoturvallisuus linkittyy useisiin toimeksiantajan tuotteisiin ja toimintaan. Eri teollisuussektoreilla, kuten energia- ja laivasektorilla (engl. marine), on omia tietoturvallisuusvaatimuksia. Esimerkiksi laivojen rakennuksessa on standardit ja vaatimukset, joita valvovat luokituslaitokset, kuten DNV ja Lloyds. Riskiarviointi on tiukka. Puolustusvoimien kanssa työskennellessä on voimassa KATAKRI-vaatimukset, joka on kansallinen turvallisuusvaatimuskriteeristö. KATAKRI-vaatimuksessa arvioidaan organisaation turvallisuuspolitiikkaa, ja sen arviointiin käytetään kysymyksiä, kuten ”Toimivatko

organisaation kaikki tasot turvallisuuspolitiikan mukaisesti?” (KATAKRI, 2011, s.10) Eri teollisuusektorien tietoturvavaatimukset asettavat vaatimuksia myös tuotteisiin liittyen.

Toimeksiantaja tekee sisäisiä auditointeja, kuten toimeksiantajalla oleva ISO 27001 -standardi vaatii tehtävän. Sisäisissä auditoinneissa voidaan levittää hyviä käytänteitä toimeksiantajan eri toimipisteiden kesken, kuten mitä materiaaleja voisi kehittää ja millä tavalla. Sisäiset auditoinnit ovat hyvin vuorovaikutusperustaisia, ja niissä pyritään parantamaan jokaisen toimipisteen toimintaa. ISO 27001 -standardi vaatii sisäisten auditointien lisäksi yhteistyökumppaneiden auditoinnin. Standardin toimivuus varmistetaan virallisen ulkopuolisen toimesta.

ISF standard of good practice -standardi vaatii säännöllisen turvallisuuskatsauksen. Toimeksiantaja tekee myös sisäisiä auditointeja esimerkiksi tuotteille ja laatujärjestelmille. Myös toimeksiantajan asiakkailla on mahdollisuus tehdä auditointeja organisaatioon ja näin varmistua sen käytänteiden asianmukaisuudesta.

3.2 Koulutus- ja tiedotuskampanjat

Toimeksiantajalla on käytössä useita erilaisia koulutus- ja tiedotuskampajoita. Näihin lukeutuu muun muassa vuosittain suoritettavat pakolliset tietoturvallisuuskoulutukset, joita on useasta eri aiheesta. Osa koulutuksista koskee kaikkia työntekijöitä, ja osa koulutuksista on tehty koskemaan vain tiettyjen asioiden parissa toimivia työntekijöitä. Lisäksi toimeksiantajan sisäisillä nettisivuilla on paljon ohjeistuksia miten erilaisissa tilanteissa tulee toimia tietoturvan näkökulmasta, kuten asiakasvierailuilla tai etäyhteyksien kanssa toimiessa. Toimeksiantaja osallistuu CyberSecurityMonth-kampanjaan vuosittain lokakuussa, ja yrittää tämän kuukauden aikana lisätä tietoturvatietoisuutta ja kiinnittää erityistä huomiota tietoturvaan liittyvissä asioissa. Kampanjan tarkoituksena on muistuttaa työntekijöitä mihin toimeksiantaja on sitoutunut ISO 27001 -standardillaan. Kampanjan tarkoituksena on myös kiinnittää työntekijöiden huomio siihen, että toimeksiantaja vaatiii jokaista työntekijää huomioimaan tietoturvallisuuden työssään, vaikka ei suoranaisesti työskentelisikään tietoturvan parissa. Pääkohtia CyberSecurityMonth-kampanjassa ovat esimerkiksi organisaation tiloissa liikkuminen, tilojen pääsyoikeudet, luotamuksellisten

asiakirjojen salassapito, epäilyttävien linkkien sekä sähköpostien avaamattomuus ja poikkeamista ilmoittaminen.

Toimeksiantaja järjestää myös webinaareja tietoturvallisuuteen liittyen, sekä tarvittaessa erilaisia koulutuksia yksiköille ja tiimeille. Toimeksiantaja järjestää spesifejä tietoturvaharjoituksia, jossa voisi olla esimerkiksi skenaario, missä asiakkaan kriittisen infrastruktuurin laitokseen on hyökätty. Harjoituksessa voidaan käsitellä kehen ollaan yhteydessä, mitä tilanteessa tehdään, sekä mikä on palautumisstrategia. Harjoituksessa kerrataan poikkeamiin vastaamisen suunnitelma (engl. incident response plan), joka sisältää kirjoitetut ohjeet, kuinka toimeksiantajan organisaatiossa toimitaan tietovuotojen, datan menetyksen ja kyberhyökkäysten suhteen. Poikkeamiin vastaaminen (engl. incident response) sisältää yksityiskohtaista tietoa jokaista erilaista skenaariota kohtaan, kuten hyökkäykset, lisävahinkojen estäminen, palautumisajan lyhentäminen, sekä kyberturvallisuusriskien lieventäminen (Tyas Tunggal, 2023).

Poikkeamiin vastaamisen suunnitelma on tärkeä työkalu, sillä se korostaa kuinka minimoidaan turvallisuustapahtuman kesto sekä vaikutus. Suunnitelmalla myös identifioidaan sidosryhmä, tehostetaan digitaalista forensiikkaa, lyhennetään palautumisaikaa, vähennetään negatiivista julkisuutta, sekä otetaan asiakkaan huolet huomioon. Jo pieni turvallisuustapaus, kuten haittaohjelma, voi lumipalloefktinä luoda suuria ongelmia, kuten tietovuotoja, datan menetystä sekä keskeytyneen tuotannon. (Tyas Tunggal, 2023)

Poikkeamiin vastaamisen suunnitelma auttaa hyödyntämään parhaita ratkaisuita poikkeamien käsittelyssä, sekä parantamaan kommunikointisuunnitelmaa. Suunnitelma auttaa lakitiimin, työntekijöiden ja muiden asiaan liittyvien sidosryhmien tiedottamisessa. (Tyas Tunggal, 2023)

3.3 Sisäiset viestintäkanavat ja -käytännöt

Toimeksiantajalla on käytössään useampi eri kanava viestinnälle. Suurin osa viestinnästä tapahtuu Microsoft365-palveluiden kautta, jotka ovat lähtökohtaisesti hyvin suojattuja ja niissä on kaksivaiheinen todennus käytössä. Toimeksiantaja käyttää myös esimerkiksi

tiedostojen jakamiseen palveluita, joissa kaksivaiheinen todennus on käytössä. Toimeksiantaja kieltää oman puhelinnumeron käytön esimerkiksi asiakasyhteyksissä. Työtehtäviä kirjataan tiketti-palveluun.

Toimeksiantajalla on käytössään intra-palvelu, sekä sisäiset nettisivut viestintää ja tiedotusta varten. Nettisivuilta löytyy yleistä tietoa työntekijälle toimeksiantajasta, toimeksiantajan tiloista, sekä yksityiskohtaisempia ohjeistuksia, esimerkiksi kuinka ottaa turvallinen etäyhteys tai kuinka työskennellään tietoturvallisella tavalla. Tietotekniikan puolella tiedotusta välitetään muun muassa sähköpostin kautta.

Toimeksiantaja järjestää paljon erilaisia webinaareja, joissa jaetaan tärkeää tietoa työntekijöille. Webinaareissa aiheita voi olla esimerkiksi ”mitä voi oppia kyberturvallisuustapauksista” tai ”kuinka minut hakkeroitiin”.

Lisäksi toimeksiantajalla on käytössään Sharepoint, jossa on paljon projekteihin liittyvää dokumentaatoita. Tämän lisäksi toimeksiantaja käyttää projektien hallintaan ja tapausten seurantaan tikettipalvelua Jiraa, sekä Confluencea, joka on yhteistyön ja tietojen yhdistävä työtila tiimeille.

3.4 Johdon sitoutuminen ja esimerkki

Johtamis- ja esimiesviestintä on suuressa roolissa organisaation sisäistä viestintää. Työyhteisöviestintä on tärkeä kohde johdolle kehittää koko ajan (Helsingin yliopisto, 2019)

Toimeksiantaja on johtotasoa myöten tietoinen tietoturvallisuudesta ja mahdollisten poikkeamien vaikutuksesta toimeksiantajan organisaatioon ja sen asiakkaisiin. Johto edesauttaa tietoturvallisuuteen liittyvissä asioissa, ja esimerkiksi tietoturvallisuudelle on oma budjettinsa. Johto ottaa tietoturvallisuusasiat esille kokouksissa ja päätöksen teossa.

Johtoryhmän kanssa on jatkuvaa kommunikointia ja prosessien käsittelyä. Yksi johtoryhmän henkilöistä on myös tietoturvavastaava. Ennen johtoryhmän kokouksia tietoturvavastaava käy tietoturvatiimien kanssa asioita läpi, ja tarvittaessa vie asiat johtoryhmän käsiteltäviksi ja hyväksyttäviksi. Johtoryhmä on myös mukana tietoturvahavaintojen raportoimisessa. Johtoryhmän henkilöt osallistuvat arkipäiväisiin tietoturvallisuusasioihin ja raportoivat

poikkeamia kuten muukin henkilökunta, esimerkiksi jos ilmenee jokin ongelma organisaation tilojen lukituksessa.

Edistettävät tietoturvallisuusasiat etenevät sujuvammin kun johtoryhmä on päätöksenteossa ja toteutuksessa mukana. Ylipäällikön ohjatessa työntekijät ovat taipuvaisia toteuttamaan ja noudattamaan tietoturvallisuusvaatimuksia tehokkaammin.

4 Uhkatiedon hyödyntäminen riskienhallinnassa

Uhkatiedon pääasiallinen käyttötarkoitus on ehkäistä tulevia poikkeamia, kuten hyökkäyksiä ja datan menetystä. Uhkatieto on siis tärkeää tietoa riskienhallinnan näkökulmasta. Uhkatietoa käytetään muun muassa riskien tunnistamisen, riskianalyysin ja riskien vähentämisen prosesseissa.

4.1 Uhkatiedon kerääminen ja analysointi

Toimeksiantajan organisaatiossa uhkatietoa kerätään ja analysoidaan useilla eri tavoilla. Uhkatietoa kerätään paljon julkisia reittejä pitkin, kuten Kyberturvallisuuskeskuksen antamista tiedoista, sekä useista ulkoisista lähteistä. Uhkatietoa saadaan myös sisäisistä lähteistä.

Organisaatiossa uhkatiedon keräämiseen on erikoistunut tiimi tietotekniikassa (IT). Tiimi tietotekniikassa kerää tietoa useista lähteistä, kuten Kyberturvallisuuskeskukselta, keskustelupalstoilta, mustasta marketista (engl. black market) ja pimeästä verkosta (engl. dark web), erilaisilta asiaan liittyviltä servereiltä sekä erilaisista tietoturvaraporteista, kuten Microsoftin Defense -raportti. Lisäksi uhkatietoa saadaan asiakkailta, datavuodoista, sekä haavoittuvuusskannauksista saaduista tiedoista.

Tiimi tietotekniikassa analysoi uhkatietoa. Tietotekniikan tiimi lajittelee uhkatietoa sen mukaan onko tieto relevanttia toimeksiantajalle. Uhkatietoa välitetään eteenpäin sitä tarvitseville yksiköille. Yksiköissä arvioidaan yksityiskohtaisemmin koskeeko saatu uhkatieto kyseistä yksikköä, ja mitä toimenpiteitä uhkaan vastaaminen vaatii.

Uhkatiedon perusteella kartoitetaan mitkä tiedoista ovat mahdollisia riskejä toimeksiantajalle. Uhan ollessa riski toimeksiantajalle, tehdään tarkempi riskien arviointi. Riskien arvioinnin jälkeen mietitään toimenpiteitä riskien hallitsemiseksi, asetetaan vastuuhenkilöt ja määritellään aikataulu. Havaittua riskiä, toimenpiteiden toteutumista ja vaikutusta seurataan säännöllisesti.

4.2 Uhkien arviointi ja priorisointi

Toimeksiantajan prioriteetteina ovat uhat jotka vaikuttavat suoraan toimeksiantajan toimintaan tai asiakkaisiin. Kukin yksikkö arvioi saadun uhkatiedon perusteella, mitkä uhat vaativat toimenpiteitä, ja mitkä uhat eivät koske kutakin yksikköä. Merkittävät uhat jollekin toiselle yksikölle välitetään eteenpäin sitä koskevalle yksikölle. Toimeksiantajan organisaatiossa uhkatietoa kerää eniten tietotekniikan yksikkö, joka jakaa saamansa tiedot eteenpäin tietoa tarvitseville yksiköille. Yksiköissä johdossa oleva henkilö päättää mitä uhalle tehdään, jos uhka vaatii toimenpiteitä.

4.3 Seuranta ja päivitykset

Toimeksiantajan tiedonvälityksen tiedon oikeellisuutta seurataan aina sitä käsitellessä. Tietoturvallisuuskursseja päivitetään tarpeen mukaan, mutta myös tasaisin aikavälein. Kurssien suorittamisprosentteja seurataan koko organisaation tasolla, ja suorittamattomista kursseista pidetään kirjaa ja lähetetään muistutuksia.

Toimeksiantajan organisaatiossa seurataan tietoturvatavoitteita ja niiden toteutumista kuukausittain. Kuukausittain seurattaviin aiheisiin kuuluu myös tietoturvallisuuskoulutuksien, riskien, poikkeamien ja dokumenttien tilanteiden seuranta. Johtotasolla varmistetaan että standardien mukaiset vaatimukset tulee käsiteltyä ja toteutettua. Turvallisuustiimi seuraa miten tietoturvatavoitteet toteutuvat vuositasolla sekä mikä on riskien tilanne. Yksiköiden pitää tehdä turvallisuuskatsaus neljännesvuosittain, jossa yksiköstä riippuen seurataan esimerkiksi poikkeamia, turvallisuushavaintoja, tapauksia, tietoturvallisuuskoulutuksia, turvallisen ohjelmistokehityksen tilannetta sekä tuotehaavoittuvuuksia. Tietoturvallisuustapauksissa asioita käsitellään useasta eri näkökulmasta, kuitenkin sisältäen aina vähintään kolme komponenttia, teknologian, tuotteet sekä ihmiset.

5 Tutkimus toimeksiantajaorganisaatiossa

Tutkimuksen aiheena on kuinka toimeksiantajan organisaatiossa kerätään uhkatietoa, ja miten sitä voisi paremmin hyödyntää riskienhallinnan ja tietoturvatietoisuuden parantamisessa. Aihe valikoitui toimeksiantajan tarpeen perusteella. Toimeksiantaja halusi selvittää, miten eri yksiköissä uhkatietoa kerätään ja analysoidaan, ja kuinka tehokkaita tavat ovat. Toimeksiantajan organisaatiossa ei ole ollut aikaisempaa tutkimusta aiheesta.

Tutkimusongelma on kuinka uhkatietoa voitaisiin hyödyntää toimeksiantajan tietoturvatietoisuuden ja riskienhallinnan kehittämisessä. Tutkimuksessa käytetään teoriaa tietoturvallisuudesta, kyberturvallisuudesta, uhkatiedosta sekä riskienhallinnasta. Teoriaa on kerätty useista eri ulkoisista lähteistä, standardeista sekä toimeksiantajan sisäisistä lähteistä.

Tutkimuksen keskeisiä käsitteitä ovat uhkatieto, tietoturvallisuus, riskienhallinta ja kyberturvallisuus. Tutkimuksen aineistona käytetään haastattelussa kerättyä tietoa. Haastattelut pidettiin toimeksiantajan eri yksiköissä uhkatiedon parissa työskenteleville henkilöille. Haastattelut kirjoitettiin ylös kokonaisuudessaan, jonka perusteella aineistoa käsiteltiin.

Tutkimusta voidaan käyttää hyväksi toimeksiantajan tietoturvatietoisuuden ja riskienhallinnan parantamisessa. Toimeksiantaja voi tutkimuksen perusteella tarkastella toimiaan uhkatietoon liittyen, ja tarvittaessa tehdä parannuksia ja muutostoimenpiteitä. Tutkimukselle ei tarvinnut rahoitusta.

Tutkimus toteutettiin haastattelemalla uhkatiedon parissa työskenteleviä henkilöitä eri toimeksiantajan organisaation yksiköissä. Tutkimukseen osallistuneita olivat yksiköt tietotekniikassa, asiakaspalvelussa ja liiketoiminnassa. Tutkimus toteutettiin lähi- ja etäpalavereilla. Tutkimus sisälsi tutkimuskysymyksiä. Kysymyksien vastausten perusteella kerättiin aineistoa. Tutkimuskysymykset olivat:

- Mistä organisaation eri yksiköt saavat uhkatietoa ja kuinka niitä tällä hetkellä käsitellään ja analysoidaan?
- Mitä käytännön toimenpiteitä organisaation eri yksiköt voisivat toteuttaa tietoturvallisuuskäytänteiden integroimiseksi päivittäiseen työhön?

Ennen tutkimuskysymyksiin menemistä, tutkimukseen osallistuneille kerrottiin miksi tutkimusta tehdään, ja mitkä tutkijan lähtökohdat tutkimukselle olivat. Tutkimukseen osallistujat olivat tietoisia opinnäytetyön aiheesta, ja kiinnostuneet haastateltavat saivat myös nähdä työn silloisen sisällysluettelon. Tutkimukseen osallistuneille kerrottiin missä yksikössä ja tiimissä opinnäytetyön kirjoittaja työskentelee, ja tutkimukseen osallistuneet ovat myös tietoisia kyseisen tiimin toiminnasta toimeksiantajan organisaatiossa.

Tutkimukseen osallistujien kanssa varattiin palaveriaika, joka sijoittui kesä-elokuun välille vuonna 2023. Palaverit toteutettiin pääosin lähipalavereina, mutta tutkimukseen oli myös mahdollista osallistua etäyhteydellä. Tutkimukseen osallistuttiin yksitellen eri ajankohtina. Tutkimukseen osallistuvat eivät nähneet kysymyksiä itse, vaan he kuulivat ne suullisesti. Tutkimuskysymyksiin oli mahdollista kysyä tarkennusta ja keskustella aiheesta. Lisäksi haastattelussa oli epävirallisempia liitännäis- tai apukysymyksiä, esimerkiksi ”Kerrotko tarkemmin miten yksikössä kerätään uhkatietoa?” ja ”Miten itse johtajan roolissa ottaisit esille tietoturvan esimerkiksi projektissa tai sen säännöllisissä palavereissa?”.

Tutkimukseen osallituneille myös kerrottiin mitä opinnäytetyössä käsiteltävä uhkatieto tarkoittaa, ja mikä sen merkitys on toimeksiantajan organisaatiossa. Uhkatiedon käsitteestä ja siihen liittyvistä aiheista keskusteliin tutkimukseen osallistuneiden kanssa, jotta varmistui, että ymmärrys on molemmin puoleinen.

5.1 Tutkimusasetelma ja osallistujat

Toimeksiantajan organisaatiosta tutkimukseen osallistui yksikkö tietotekniikasta, asiakaspalvelusta ja liiketoiminnasta. Yksiköt valikoituivat sen perusteella, missä yksiköissä työskennellään uhkatiedon parissa. Tutkimukseen haluttiin yksiköitä, joista jokainen toimii uhkatiedon kanssa eritavoin. Yksiköt on lajiteltu niin, että mukaan tutkimukseen tulee yksikkö jossa uhkatiedon kanssa työskennellään tiiviisti ja konkreettisesti. Yksikkö kerää, analysoi ja välittää uhkatietoa eteenpäin. Kyseinen yksikkö on tietotekniikka. Sen lisäksi tutkimukseen otettiin yksikkö missä uhkatiedon vaatimien toimien mukaan toimitaan, mutta päätökset toimien suhteen eivät ole yksikön tekemiä. Yksikössä ei kerätä uhkatietoa. Kyseinen yksikkö on liiketoiminta. Viimeiseksi valikoitunut yksikkö on tältä väliltä. Yksikössä kerätään osa uhkatiedosta, ja osa uhkatiedosta saadaan muualta. Uhkatiedon vaatimiin

toimiin reagoidaan yksikön sisällä, mutta apua saa myös asiaan perehtyneemmältä taholta. Tämä yksikkö on asiakaspalvelu.

Tutkimukseen osallistui kolme henkilöä, yksi henkilö kustakin yksiköstä. Henkilöt valikoituivat sen perusteella, että henkilö toimi uhkatiedon parissa, tai valvoi uhkatiedon prosesseja. Kaikki valikoituneet henkilöt olivat yksikön johtotasossa, joten heillä on kokonaiskuvallinen näkemys miten yksikössä toimitaan.

Analyysi tehtiin tutkimusvastauksien perusteella. Haastattelun vastauksia verrattiin teoriaan, ja teorian sekä vastauksien perusteella kirjoitettiin analyysi. Analyysissä käsitellään haastattelun vastauksia teoriaan pohjautuen.

5.2 Aineistonkeruu

Aineistoa kerättiin vastauksien perusteella. Palaverien aikana käyty keskustelu kirjattiin ylös, ja keskustelu kirjoitettiin myöhemmin puhtaaksi.

5.2.1 Tietotekniikka

Uhkatietoa saadaan haavoittuvuusskannauksista, joita on muutaman kerran kuukaudessa. Uhkatietoa saadaan myös virheilmoituksista esimerkiksi asiakkaan järjestelmissä, julkisista raporteista, kuten Verizon, sekä tietomurroista saadusta datasta. Uhkatietoa kerätään Microsoftin Defence-raportista, uhkatietoa käsitteleviltä keskustelupalstoilta, sekä avoimen lähdekoodin palveluista, kuten Shodanin Shadow-serveriltä.

Toimeksiantajan tietoturvalle on tärkeää huomioida, onko joku jo järjestelmän sisällä, kuinka kiinnostava toimiala on, sekä mitä organisaatiosta on tarjolla pimeillä markkinoilla. Tärkeä aspekti toimeksiantajaa vastaan hyökkäämisessä on miettiä, kuinka kannattavaa hyökkääminen on, kuinka paljon kuluja ja tuottoa hyökkäys tuottaisi, sekä kuinka suuri on hyökkäyksen onnistumisprosentti. Hyökkääjää usein kiinnostaa isot organisaatiot, sillä niissä tietoturva ei välttämättä ole ajantasalla. Hyökkääjää kiinnostaa tietysti myös valmistavan teollisuuden organisaatiot.

Uhkatietoa hyödynnetään välittämällä olennaiset asiat palvelupäällikölle. Palvelupäällikkö kerää havainnot ja toimii niiden mukaisesti. Kaikki uhkatieto jossa odotetaan toimenpiteitä, kuten sovelluksen turvaaminen tai haavoittuvuus, ohjataan tietoturvallisuuden tukitiimien käsiteltäväksi.

Uhkatiedon parantamiseksi toimeksiantajan organisaatiossa voitaisiin sisäisesti käyttöönottaa käyttötapaustyyppinen (engl. use case) lähestyminen tiedotuksen suhteen. Jokainen tiimi hyötyisi roolipohjaisesta tiedoituksesta tai harjoituksista, koska esimerkiksi uhat laskuttajalle eivät ole samat kuin tuotantohenkilöstölle. Uhkien ja koulutusten kohdistaminen lisää tietoisuutta ja osaamista. Kustannustehokkuus laskee, jos koulutettavat asiat eivät koske koulutuksessa olevia henkilöitä.

Uhkatietoon reagoinnissa tulisi ottaa huomioon käyttötapaus. Tulisi pohtia mitä asialle voidaan tehdä, asian tiedottamista, teknistä puolta sekä organisaation käytänteitä. Täytyy ottaa huomioon voisiko kyseessä olla sosiaalisen manipuloinnin yritys, eli varmistetaan tuleeko tieto oikealta henkilöltä ja oikeasta osoitteesta, sekä kenelle tili oikeasti kuuluu.

Haavoittuvuusskannauksen kompastuskivi voi olla viive, eli kuinka nopeasti haavoittuvuus tulee palveluun näkyviin jos esimerkiksi asiakkaan järjestelmässä on virhe. Jos skannauksia on vain viikon tai kahden välein, usea virhe saattaa jäädä huomaamatta, tai virheisiin ei ehdi reagoimaan yhtä nopeasti kuin pitäisi, jotta voitaisiin välttyä vahingoilta.

Nopea uhkatiedon hyödyntäminen kriittisissä palveluissa on tärkeää. Toimeksiantajan pitää tunnistaa ulkoverkon kriittiset haavoittuvuudet. Tärkeää on pohtia, kuinka voidaan monitoroida haavoittuvuuksia paremmin. Tärkeää on myös huomioida mitä on suoraan internettiin päin avoinna, esimerkiksi mihin tietoihin tietokoneiden etähallintapalveluista pääsee käsiksi. Huomion arvoinen aihe on myös mihin tietoihin Faviconin kautta pääsee käsiksi. Favicon on määritelty internetsivulle, ja se näkyy usein osoiterivin vasemmassa laidassa. Nykyiset Python koodit osaavat laskea Faviconille hash luvun, jonka avulla voidaan etsiä sivun haavoittuvuksia ja nähdä mitkä palvelut ovat avoinna internettiin. Shodan.io-sivustolta löytyy tietoa, miten Faviconin avulla voidaan hyödyntää organisaation tietoja.

5.2.2 Asiakaspalvelu

Asiakaspalvelu saa uhkatietoa asiakkailta, esimerkiksi asiakasprojekteissa sekä myös tietotekniikan tiimien kautta. Jos tieto liittyy asiakaspalveluun, tieto välitetään eteenpäin. Uhkatietoa saa myös julkisista lähteistä, kuten Kyberturvallisuuskeskukselta, ja ulkomaisia tietoja kerätään myös Kyberturvallisuuskeskukselta. Asiakaspalvelu pitää sisäisiä palavereita, joissa käydään löydettyjä tietoja ja tietoihin liittyviä skenaarioita lävitse.

Tärkeää on huomata, että kaikkeen uhkatietoon ei tarvitse reagoida. Jos esimerkiksi asiakasrajapinnassa on uhka tai tapahtuma, kutsutaan kyberturvallisuuden tapauksista vastaava tiimi koolle. Kyseisen tiimin tehtävänä on miettiä kuinka vakavasti tieto liittyy toimeksiantajan organisaation tai asiakkaan toimintaan, ja kuinka vakavasti. Asiakaspalvelu järjestää myös haavoittuvuuksien hallintaan liittyviä palavereita, joissa käydään läpi tunnettuja haavoittuvuuksia. Palaveriin osallistuu automaation puolelta laaja kirjo edustajia, kuten eri tuotteista ja maanosista.

Jos haavoittuvuus liittyy tuotteeseen tai palveluun, mietitään pitääkö tehdä uusi versio ja uuden version testaus, ja kuinka nopealla aikataululla. Tärkeää on myös informoida asiakasta ja kumppaneita haavoittuvuudesta ja tehtävistä toimenpiteistä.

Turvallisuuskäytänteiden parempaa integroimista päivittäiseen työhön helpottaisi tehokkaammat koulutukset. Koulutuksia on monta, ja niistä tulee sekava kokonaiskuva. Asiakaspalvelulle voisi olla oma tekniseen tietoon painottuva koulutus. Koulutuspaketit voisivat olla yksinkertaisempia. Erilaiset kampanjat ja tapahtumat ovat hyviä, varsinkin ovissa ja ikkunoissa esiintyvät kampanjat ovat tehokkaita. Myös projekteissa, niin myynnin kuin suunnittelun puolella, olisi tulevaisuudessa hyvä kiinnittää huomiota tietoturva-aiheisiin.

5.2.3 Liiketoiminta

Yksikössä uhkatietoa saadaan hallinnolliselta kyberturvallisuustiimiltä, joka vastaa toimeksiantajan organisaatiossa tietoturvallisuudesta, tietoturvallisuuden standardeista, sekä asiakastiedotteista. Kaikki palautteet tutkitaan heti, ja jos niissä ilmenee jotain uhkaavaa, tiedoitetaan heti myös esimerkiksi asiakkaita. Kyberturvallisuustiimi tiedottaa yksikköä siitä, mitä tapahtuu toimeksiantajan organisaation ulkopuolella. Tähän lukeutuu

esimerkiksi löydetyt haavoittuvaisuudet kyberturvallisuudessa. Löydetyt kyberhaavoittuvuudet, löytyivät ne sitten asiakkaalta tai kilpailijalta, käydään läpi johtoryhmän kanssa. Johtoryhmän kanssa pohditaan koskeeko uhka yksikköä, ja näin ollessa uhkaan pyritään löytämään suojautumiskeinot.

Uhkatiedon osalta yksikössä ei suoraan kerätä tietoa. Yksikkö saa suodatetut ja heitä koskevat tiedot sisäisesti. Yksikkö vastaa asiakaskunnasta ja muualta tulee tieto siitä mitä toimenpiteitä vaaditaan. Yksikön tehtävänä on toteuttaa vaaditut toimenpiteet.

Päivittäisiä tietoturvatoimia yksikössä on kaikki asiakkaan tietojen suojaaminen, sillä asiakastietoja on paljon. Tietoturvatoimia ovat esimerkiksi omien USB-tikkujen ja tietokoneiden käyttökielto, päivitysten on oltava ajantasalla, sekä toimeksiantajan sisäiset tietoturvallisuuskoulutukset on käytävä säännöllisesti. Tietoturvallisuutta voidaan parantaa yksikössä niin, että tiedotusta lisätään, johtoryhmällä olisi tietoturvallisuus vakioagendanaan, sekä että tiedon kulkua sujuvoitetaan toimeksiantajan organisaation sisällä. Tietoturvallisuutta voidaan parantaa ottamalla aihe samalla vakavuudella kuin asiat jotka liittyvät terveyteen, työympäristöön ja työturvallisuuteen.

Yksikössä tärkeitä päivittäiseen tietoturvallisempaan työskentelyyn liittyviä asioita on muun muassa turvalliset etäyhteydet asiakkaan kanssa, ohjeiden sisäistäminen, osaaminen miten asiakkaan tiloissa tulee toimia ja liikkua, linkkien klikkaamisen välttäminen, sekä asiakkaan tietojen oikeanlainen säilytys.

6 Yhteenveto ja jatkotutkimusmahdollisuudet

Tuloksena voidaan todeta, että toimeksiantaja hyödyntää hyvin uhkatietoa, ja soveltaa saatua tietoa tietoturvatietoisuuden ja riskienhallinnan kehittämisessä. Eri yksiköt toimivat uhkatiedon keräämisen, analysoinnin ja uhkatietoon reagoimisen kanssa hyvin eri tavoin.

Liiketoiminnan ylätasolla uhkatiedon kerääminen ja analysoiminen on vähäistä. He saavat tiedon suoraan, kuten myös ehdotukset korjaavista toimenpiteistä, ja heidän vastuulla on hyväksyä mahdolliset toimenpiteet ja niiden vaatimat kustannukset. Liiketoiminnan toiminta uhkatiedon suhteen on suoraviivaista, he saavat valmiiksi lajitellut tiedot, joiden mukaan he miettivät toimintasuunnitelman.

Asiakaspalvelussa uhkatiedon kerääminen ja käsittely on myös suhteellisen suoraviivaista. Asiakaspalvelussa uhkatietoa kerätään itse, mutta saadaan myös julkisia reittejä pitkin. Uhkatietoa voidaan saada myös asiakkaalta. Uhkatietoa käsitellään sisäisesti asiakaspalvelussa, ja mahdollisten uhkien mukaan tehdään toimintasuunnitelma. Asiakaspalvelussa ratkaisuita mietitään sisäisesti huollon kesken, mutta tarvittaessa he saavat apua aiheeseen perehtyneeltä tiimiltä. Ratkaisut toteutetaan yhteistyössä muiden kanssa.

Tietotekniikan rooli uhkatiedon keräämisessä ja analysoimisessa on suuri. Yksikössä kerätään uhkatietoa useista eri lähteistä, niin ulkoisesti kuin sisäisestikin. Yksikössä kerätään uhkatietoa myös pimeästä verkosta, ja muualta jossa uhkatieto ei ole suoraan valmiiksi raportoituna. Tietotekniikka analysoi tietoja ja välittävät uhkatietoa eteenpäin koko toimeksiantajan organisaatiolle ja oikeille yksiköille. Tietotekniikka vastaa itse mahdollisiin uhkiin. Tietotekniikan rooli uhkatiedon keräämisessä ja tiedon välittämisessä eteenpäin on merkittävä. Ilman tietotekniikan työpanosta toimeksiantajan organisaation uhkatiedon kerääminen ja analysointi olisi vähäistä.

Työssä haastateltavat yksiköt olivat pääosin tyytyväisiä nykyisiin toimiin uhkatiedon keräämisen ja analysoinnin suhteen. Muutamia kehitysalueita nousi myös esiin. Tietotekniikan yksikkö haluaisi nopeammat reagointiajat havaittuihin uhkiin, ja lisätä haavoittuvuusskannauksia. Nämä toimet ovat tärkeitä aiheita tietoturvallisuuden ylläpitämiseksi. Yksikkö asiakaspalvelussa haluaisi konkreettisempia ja teknisempiä

tietoturvallisuuskoulutuksia. Asiakaspalvelun näkökanta on se, että koulutukset keskittyvät liian paljon yleiseen tietoturvallisuuden teoriaan. Asiakaspalvelu haluaisi oman koulutuksen, jossa käsiteltäisiin heille tärkeitä tietoturvallisuuden näkökulmia. Liiketoiminta on hyvin tyytyväinen tietoturvallisuuskoulutuksiin, ja koulutukset täyttävät heidän tarpeensa loistavasti. Liiketoiminnan yksikköä koskevia tietoturvallisuuskoulutuksia on useampi, ja koulutuksissa on monipuolisesti ja seikkaperäisesti käyty läpi liiketoiminnan tarvitsemia tietoturvallisuustietoja. Liiketoiminta on myös tyytyväinen nykyiseen toimintapolkuun uhkatiedon keräämisen, ja mahdollisiin uhkiin reagoimisen suhteen.

Yleisesti toimeksiantajan organisaatiossa tietoturvallisuus on nostettu hyvin esille. Toimeksiantajan organisaatiossa on käytössä monia tapoja tietoturvallisuuden edistämiseksi ja nykyisten ohjeistusten noudattamiseksi. Valmistavan teollisuuden organisaationa tulee kuitenkin käyttöönottaa yllä mainittuja tehokkaampia keinoja tietoturvallisuuden lisäämiseksi. Toimeksiantajan organisaatiossa voidaan myös parantaa ja tehostaa valvontaa, niin että vaadittuja keinoja myös toteutetaan jokaisen työntekijän toimesta.

6.1 Johtopäätökset ja niiden merkitys

Johtopäätöksinä voidaan todeta, että roolipohjainen tiedotus lisää työntekijöiden osaamista. Uhkien ja koulutusten kohdistaminen on kustannustehokkaampaa, kuin kaiken kouluttaminen kaikille. Haavoittuvuuksien löytymisen, ja niihin reagoimisen viivettä tulee lyhentää. Tämä onnistuu esimerkiksi useammin suoritettavilla haavoittuvuusskannauksilla. Pääsyoikeudet ja tiedostojen jakaminen tulee olla ajantasalla. Turhat pääsyoikeudet tulee poistaa. Tiedostojen jakamiseen tulee olla selkeät ohjeistukset ja käytännöt, jotta kukaan ei esimerkiksi vahingossa jaa sisäisiä tai salattuja tiedostoja avoimeksi internettiin. Tietoturva-aiheet tulee olla jatkuvasti huomioituna kaikessa toiminnassa. Tietoturvallisuus tulee myös ottaa vakavasti jokaisen työntekijän toimesta jokapäiväisissä työtehtävissä.

Johtopäätöksien merkitys on painava. Johtopäätöksien avulla voidaan merkittävästi parantaa toimeksiantajan tietoturvallisuutta. Johtopäätökset ovat mahdollisesti olleet toimeksiantajan tiedossa, mutta tutkimuksen perusteella niitä varten tehtävät toimenpiteet konkretisoituvat. Johtopäätöksien avulla on mahdollista parantaa tietoturvatietoisuutta ja riskienhallintaa toimeksiantajan organisaatiossa.

6.2 Mahdolliset jatkotutkimusaiheet

Mahdollisia jatkotutkimusaiheita on useita, joista kaikki liittyvät siihen, miten valmistavan teollisuuden organisaatiossa voitaisiin parantaa vielä entisestään tietoturvallisuutta. Jatkotutkimuksen voisi tehdä esimerkiksi pääsynhallinnan parantamisesta. Tutkimusaiheita voisi myös olla kuinka tietoisia työntekijät ovat heidän tekojen vaikutuksesta organisaation alttiuteen kyberhyökkäyksille, tai kuinka organisaation asioissa pilvipalveluiden käyttäminen olisi turvallisempaa. Jatkotutkimuksen arvoinen aihe olisi myös miettiä, kuinka suuri riski kunkin työntekijän tunnuksien vuotaminen olisi organisaation tietoturvallisuudelle.

6.3 Tutkimuksen tulosten yhteenveto

Toimeksiantaja on hyvällä tasolla tietoturvatietoisuuden suhteen, mutta aiheessa on myös kehityskohteita. Uhkatietoa käsitellään usealla tavalla, ja tietoa sovelletaan eri tavoin eri yksiköissä. Tutkimuksessa kerättyjä tietoja voidaan käytännössä hyödyntää siirryttäessä ISO 27001:2013 versiosta ISO 27001:2022 versioon. ISO 27001:2022 versiossa organisaation on avattava kuinka tietoturvauhkia kerätään ja analysoidaan, jotta saadaan tuotettua uhkatietoa. (ISO 27001, 2022)

Tutkimuksen tuloksissa selvisi, että tietotekniikalla on merkittävä rooli uhkatiedon keräämisessä, analysoimisessa, ja tiedon välittämisessä eteenpäin sitä tarvitseville yksiköille. Tietotekniikka kerää uhkatietoa monesta ajankohtaisesta lähteestä, ja heillä on suuri työpanos tiedon jakamiseen sitä tarvitseville yksiköille. Jotta uhkatiedon hyödyntämisestä saataisiin vielä tehokkaampaa, tulee esimerkiksi haavoittuvuusskannauksia suorittaa useammin.

Koulutusten spesifioiminen koskemaan tiettyä yksikköä lisää tiedon parempaa sisäistämistä ja käyttöönottamista. Webinaarit ovat toimiva tapa lisätä työntekijöiden tietoturvatietoisuutta, ja johdon panoksella on suuri merkitys tietoturvatietoisuuden käyttöönottamisessa. Tapauskohtaiset harjoitukset ovat tehokas keino työntekijöiden kouluttamiseen esimerkiksi tietoturvavuodon kanssa toimiessa. Tapauskohtaisia harjoituksia on hyvä toteuttaa toimeksiantajan organisaation eri yksiköille, jotta myös työntekijät jotka eivät toimi suoranaisesti tietoturvallisuuden parissa olisivat tietoisia miten tilanteessa tulee

toimia. Tapauskohtainen koulutus myös realisoisi työntekijöille heidän tekemiensä toimien mahdolliset seuraukset tietoturvalle.

Edustaja toimeksiantaja organisaatiosta kommentoi opinnäytetyötä seuraavasti:

”Valittu aihepiiri on erittäin laaja. Tästä huolimatta opinnäytetyössä on onnistuttu jaottelemaan ja käsittelemään aihetta selkeästi ja ymmärrettävästi. Työn laatu on korkea ja tekijä täytti hyvin työlle asetetut tavoitteet liittyen uhkatiedon hallintaan ja hyödyntämiseen tietoturvan ja riskienhallinnan kehittämisessä. Tekijä osasi myös hyödyntää uusimpia kirjallisuuslähteitä.

Työtä käytiin säännöllisesti läpi yhdessä ohjaajan kanssa ja tekijä otti kiitettävästi palautteen ja kehitysehdotukset vastaan. Myös yleisissä tiimin kanssa käydyissä keskusteluissa tekijä pystyi osallistumaan tietoturvan ja tietoturvatietoisuuden parantamiseen liittyviin ideointeihin ja antamaan omat uudet selkeät ehdotuksensa, esimerkiksi Kyberturvallisuuskuukauden tietoturvakampanjoihin liittyen.

Työssä vahvistettiin tarve tehostaa ja yhtenäistää uhkatiedon käsittelyyn liittyviä käytäntöjä. Työssä ehdotetut parannusehdotukset ovat asianmukaisia, ja näitä tullaan toteuttamaan käytännössä tietoturvan ja tietoturvatietoisuuden kehittämisessä. Kokonaisuutena työ on selkeä ja ymmärrettävä, ja sitä voidaan käyttää yleisemminkin aiheesta tiedottamiseen ja tätä kautta tietoturvatietoisuuden parantamiseen, mahdollisesti myös tilaajan organisaation ulkopuolelle, esimerkiksi Suomen Automaatioseuran verkkosivujen kautta.”

Lähteet

Aven, T. & Cox, L., A. (n.d.) *Riskiarvio-taulukko* [kuva]. Wiley online library. https://onlinelibrary.wiley.com/page/journal/15396924/homepage/special_issue__simple_characterisations_and_communication_of_risks.htm

Baker, K. (2023). *What is cyber threat intelligence*. Crowdstrike. https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

Barker, S. (2023). *ISO27001 Annex A 5.7 Threat Intelligence*. HighTable. https://hightable.io/iso-27001-annex-a-5-7-threat-intelligence/

Cisco. (n.d). *What is social engineering*. https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html#~types-of-attacks

Digiturvamalli. (n.d). *Top 15 tietoturvauhkat tänään*. https://www.digiturvamalli.fi/tietoturvauhkat

DNSstuff. (2020). *What is threat intelligence, definition and types*. https://www.dnsstuff.com/what-is-threat-intelligence

Dnsstuff. (2020). *Uhkatieto voidaan jakaa neljään päätyyppiin, strategiseen, taktiseen, tekniseen ja operatiiviseen* [kuva]. https://www.dnsstuff.com/what-is-threat-intelligence

Elisa yrityksille. (2021). *Zero trust – nollaluottamus modernin turvallisen ICT-ympäristön perustana*. https://yrityksille.elisa.fi/ideat/zero-trust-nollaluottamus-turvaa-ict-ymparistosi/

Enisa. (n.d). *Threat Landscape*. https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends

Eurooppa-neuvosto. (n.d). *Disinformaation torjunta*. https://www.consilium.europa.eu/fi/policies/coronavirus/fighting-disinformation/

F-secure. (n.d). *Mikä on kyberhyökkäys*. https://www.f-secure.com/fi/articles/what-is-a-cyber-attack

Health and safety executive. (n.d). *Managing risks and risk assessment at work*. https://www.hse.gov.uk/simple-health-safety/risk/index.htm

Helsingin yliopisto. (2019). *Sisäinen viestintä: 10 perusohjetta johtajille ja esimiehille*. https://hyplus.helsinki.fi/sisainen-viestinta-10-perusohjetta-johtajille-ja-esimiehille/

Henke, C. (2023). *What is IoT security? Risks, examples and solutions*. Emnify. https://www.emnify.com/iot-glossary/iot-security

Ibm. (n.d). *What is risk management*. https://www.ibm.com/topics/risk-management

International society of automation. (n.d). *The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards*. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Irwin, L. (2023). *What is CIA triad and why is it important.* It governance. https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important

ISF. (n.d) *Standard of good practice for information security*. https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security/

ISO 27001. (2022). *Information security management systems*. Osa 5.7: Threat intelligence. SFS-online.

Kaspersky. (n.d -a). *Mikä nollapäivähyökkäys on*? Määritelmä ja selitys. https://www.kaspersky.fi/resource-center/definitions/zero-day-exploit

Kaspersky. (n.d -b). *What is social engineering*. https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering

KATAKRI ll. (2011). *Kansallinen turvallisuusauditointikriteeristö*. Puolustusministeriö. Osa: Hallinnollinen turvallisuus. https://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

Llorens, A. (n.d). *5 best practices to get more from threat intelligence*. Threat Quotient. https://www.threatq.com/5-best-practices-more-threat-intelligence/

Mandiant. (n.d). *Advanced persistent threats*. https://www.mandiant.com/resources/insights/apt-groups

Microsoft. (n.d -a). *Mitä ovat haittaohjelmat*. https://www.microsoft.com/fi-fi/security/business/security-101/what-is-malware

Microsoft. (n.d -b). *What is Multifactor Authentication*. https://support.microsoft.com/en-gb/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661

Mint security. (n.d). *OSINT lyhyesti*. https://www.mintsecurity.fi/osint/

Sanastokeskus. (2018). *Kyberturvallisuuden sanasto*. https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf?file=pdf/Kyberturvallisuuden_sanasto.pdf

Smirnoff, V. (2022). *Disinformation as a service: Content marketing's evil twin*. Hackernoon. https://hackernoon.com/disinformation-as-a-service-content-marketings-evil-twin

So, C. (2022). *Rasberry Robinin tartuntareitti* [kuva]. Trendmicro. https://www.trendmicro.com/en_us/research/22/l/raspberry-robin-malware-targets-telecom-governments.html

So, C. (2022). *Rasperry Robin malware targets telecom, governments*. Rasberry Robinin tartuntareitti. Trendmicro. https://www.trendmicro.com/en_us/research/22/l/raspberry-robin-malware-targets-telecom-governments.html

Sparling, C., Gebhardt, M. (2022). *Largest European DDoS attack on record*. Akamai. https://www.akamai.com/blog/security/largest-european-ddos-attack-ever

Statista. (2023). *Maailmanlaajuinen kyberhyökkäysten jakautuminen alakohtaisesti vuonna 2022* [kuva]. https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/

Termipankki. (n.d). *Brute force-hyökkäys*. https://termipankki.fi/tepa/fi/haku/brute-force-hy%C3%B6kk%C3%A4ys

Tietoturvallisuuden CIA-kolmio [kuva].

Toulas, B. (2022). *Raspberry robin worm drops fake malware to confuse researchers*. Bleeping computers. https://www.bleepingcomputer.com/news/security/raspberry-robin-worm-drops-fake-malware-to-confuse-researchers/

Traficom. (2022). *Uusi ohje auttaa kiristyshaittaohjelman kohteeksi joutunutta organisaatiota*. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uusi-ohje-auttaa-kiristyshaittaohjelman-kohteeksi-joutunutta-organisaatiota

Tucci, L. (2023). *What is risk management and why is it important*. TechTarget. https://www.techtarget.com/searchsecurity/definition/What-is-risk-management-and-why-is-it-important

Tyas Tunggal, A. (2023). *What is incident response plan*. UpGuard. https://www.upguard.com/blog/incident-response-plans

Työturvallisuuslaki 738/2002. https://www.finlex.fi/fi/laki/ajantasa/2002/20020738#L4P18

UK Cybersecurity council. (2023). *Why do we need ethics in cyber*. https://www.ukcybersecuritycouncil.org.uk/news/news/why-do-we-need-ethics-in-cyber/

Wong, C. (2022). *Palvelunestohyökkäys (DoS) ja hajautettu palvelunestohyökkäys (DDoS)* [kuva]. Cobalt. https://www.cobalt.io/blog/what-is-denial-of-service-attack

Wong, C. (2022). *What is denial of service attack*. Cobalt. https://www.cobalt.io/blog/what-is-denial-of-service-attack