Kyberturvallisuuden kehittäminen pk-yrityk-sessä – Case HNR-Konepaja

Teemu Pirkkalainen

2023 Laurea

Laurea-ammattikorkeakoulu

Kyberturvallisuuden kehittäminen pk-yrityksessä – Case HNR-Konepaja

Teemu Pirkkalainen

Turvallisuus ja riskienhallinta

Opinnäytetyö

Heinäkuu, 2023

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuuden ja riskienhallinnan koulutus
Tradenomi (AMK)

Teemu Pirkkalainen
Kyberturvallisuuden kehittäminen pk-yrityksessä – Case HNR-Konepaja
Vuosi 2023 Sivumäärä 54

Tämän opinnäytetyön toimeksiantaja oli HNR-Konepaja Oy. Yritys lukeutuu pieniin ja keskisuuriin yrityksiin ja ei toimi kyberturvallisuuden kannalta kriittisellä alalla. Työn tavoitteena oli kartoittaa kohdeorganisaation kyberturvallisuuden nykytila ja lisätä kyberturvatietoisuutta yrityksen toimihenkilöiden keskuudessa.

Opinnäytetyön tietoperustassa tarkasteltiin yritysturvallisuuden, riskienhallinnan sekä kyber- ja tietoturvallisuuden perusteita, viitaten alan keskeisiin standardeihin ja viitekehyksiin. Teoriaosuudessa esiteltiin pk-yritysten kannalta keskeisiä kyberturvallisuuden haasteita.

Kehittämistyön aineisto kerättiin haastattelemalla viittä yrityksen toimihenkilöä, havainnoimalla heidän toimintaansa päivittäisessä työssä ja käyttämällä Traficomin julkaisemaa Kybermittari- työkalua. Haastattelumenetelmänä käytettiin puolistrukturoitua haastattelua. Kybermittarin tiedonkeruu toteutettiin neljänä eri kertana ja vastaukset saatiin yrityksen toimitusjohtajalta. Havainnointeja suoritettiin kolmena kertana.

Kybermittarin avulla selvitetty nykytilan kartoitus kertoi, että organisaatio ei toteuta lainkaan tai toteuttaa tapauskohtaisesti kyberturvallisuuden hallintaan liittyviä käytäntöjä, mutta tekeminen ei ole säännöllistä. Havainnoinnilla ei saatu näyttöä kyberturvallisuutta merkittävästi vaarantavista seikoista. Haastatteluiden perusteella organisaatiossa on tietoisuutta kyberturvallisuuden perusasioista, ja yrityksen toimihenkilöt ovat kohdanneet kyberturvallisuuden yleisimpiä häiriöitä työssään tai vapaa-aikana. Opinnäytetyön osana tuotettu tietoturvaohjeistus toimii yrityksen toimihenkilöiden tukena tavoiteltaessa parempaa kyberturvallisuutta yrityksen liiketoiminnassa.

Asiasanat: kyberturvallisuus, kybermittari, tietoturvallisuus, tietoturvaohje

Laurea University of Applied Sciences **Abstract**
Degree Programme in security, Safety and Risk Management

Bachelor's Degree

Teemu Pirkkalainen
Developing cybersecurity in a small and midsized company – Case HNR-Konepaja Oy
Year 2023 Pages 54

The commissioner organization of this thesis was HNR-Konepaja Oy. The company is placed at the small and midsize enterprise section and its business is not related to critical cybersecurity matters. The purpose of the thesis was to find out the current state of cyber security in the organization and to upgrade the cyber security awareness level of the office personnel.

The theoretical framework of the thesis introduces the basics of corporate safety, risk management and cyber and information security. Also, common cybersecurity frameworks and cyber security threats and challenges to small and midsize organization industry are introduced in the theory part of the thesis.

The information for this development work format thesis was collected by interviewing five office workers of the company and observing their daily routines at work and using a specific tool called Kybermittari, developed by the National Cyber Security Center in the Finnish Transport and Communications Agency Traficom. The method used for interviews was half-structured interview. The observation was made in three sessions and the data collection using Kybermittari took four sessions with company's CEO.

Results of Kybermittari showed that the organization does not follow cybersecurity procedures or follows them only in some cases. Based on the results of the observation, there were no cybersecurity endangering threats detected. The interviews showed that the company's office personnel have knowledge about the cybersecurity basics, and that they have also encountered common cybersecurity interferences at their work or outside the office. The thesis also produced information security instructions for the commissioner organization to help the office personnel in the future for seeking higher level of cybersecurity awareness.

Keywords: cybersecurity, kybermittari, information security, information security instructions

Sisällys

1 Johdanto

Meitä ympäröi fyysinen maailma, johon kuuluu konkreettisia asioita, kuten kädessäsi oleva kello, ajamasi auto ja työpöytäsi. Tämän maailman rinnalle ihminen on luonut keinotekoisen bittien maailman. Siihen kuuluu esimerkiksi internet, sosiaalinen media ja erilaiset tietoverkot ja sovellukset. Tätä maailmaan kutsutaan digitaaliseksi maailmaksi. (Limnéll, Majewski & Salminen 2014, 21.)

Myös yritysten ja organisaatioiden toiminta on erittäin riippuvaista erilaisista järjestelemistä ja palveluista, jotka toimiakseen, vaativat yhteyden verkkoon. Digitalisaatio helpottaa yritysten työtä, mutta tuo mukanaan myös uudenlaisia uhkia, joihin on syytä varautua.

Helsingin seudun kauppakamarin tutkimuksen ”Yrityksiin kohdistuvat kyberuhkat 2019” mukaan suomalaisten yritysten mukaan suurimmat kyberturvallisuuden uhat ovat phishing, eli tietojenkalastelu sekä haittaohjelmahyökkäykset, yhtiön luottamuksellisen tiedon vuotaminen, palvelunestohyökkäykset, tunkeutumiset, yhtiön omien työntekijöiden aiheuttama uhka ja hyökkäykset, jotka kohdistuvat teollisiin tuotantoprosesseihin. Saman selvityksen mukaan merkittävimmät esteet tehokkaan kyberturvallisuuden toteuttamisessa ovat, käyttäjien piittaamattomuus, kyberuhkiin liittyvän tiedon riittämättömyys, nykyisen henkilökunnan tietotaidon ylläpito ja turvallisuustoimiin ja menetelmiin liittyvän tiedon riittämättömyys. (Kauppakamari, 2019.)

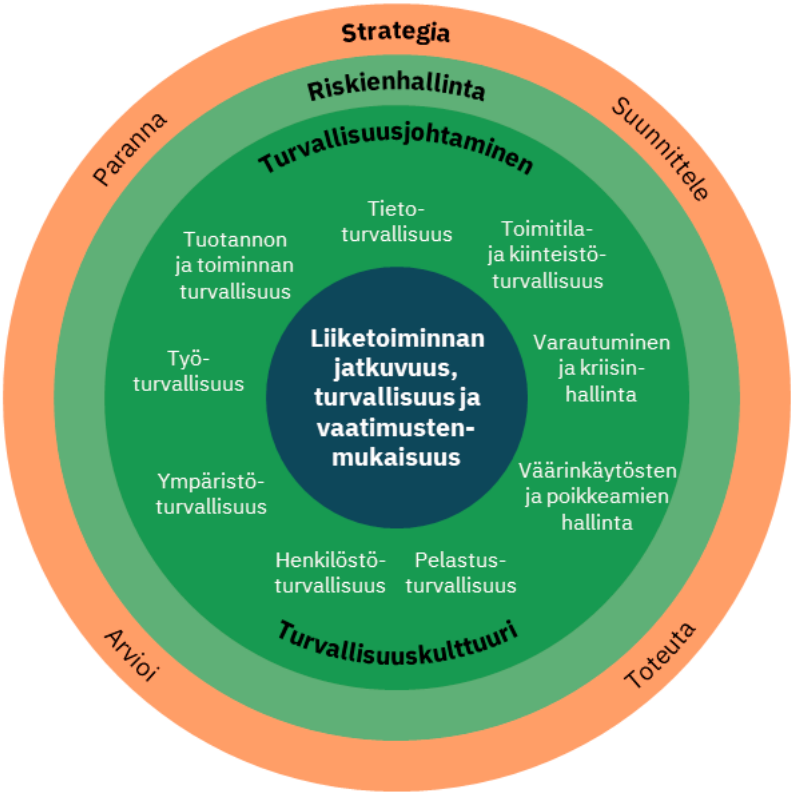
HNR-Konepaja Oy on Kotkassa toimiva metallialan yritys, joka on kiinnostunut kehittämään turvallisuuttaan ja riskienhallintaa. Yrityksessä on toteutettu mm. ISO 9001- laadunhallintajärjestelmän sertifiointi vuonna 2021 ja tämän myötä riskienhallinnan kehittäminen on erittäin ajankohtainen aihe yritykselle. Opinnäytetyössä kartoitetaan HNR-Konepaja Oy:n kyberturvallisuuden tila ja suunnitellaan kehittämistoimia sen parantamiseksi. Tavoitteena on saada selvitys nykytilasta ja huomioida jatkossa kyberturvallisuus osana yrityksen päivittäistä liiketoimintaa. Opinnäytetyö tuottaa kohdeyritykselle tietoturvaohjeistuksen, jonka avulla kyberturvallisuutta voidaan ylläpitää päivittäisessä liiketoiminnassa.

2 Kyberturvallisuus osana yritysturvallisuutta

Tämän päivän yritysten ydinliiketoimintaa ohjaa tai mahdollistaa bitit ja kyberavaruudessa ohjataan yritysten tuotantoa, jakelua, talousasioita, myyntiä ja markkinointia. Näin ollen kyberturvallisuus tarkoittaa yrityksille toimintavarmuutta ja sen tulee olla osa yrityksen strategiaa. (Limnéll ym. 2014, 40.)

2.1 Yritysturvallisuus

Yritysturvallisuudesta puhuttaessa tarkoitetaan yrityksen kaikkien toimintojen turvallisuutta. Yritysturvallisuuden tehtävänä on edistää ja parantaa yrityksen kilpailukykyä, tuottavuutta ja suojata henkilöstöä, tietoa, mainetta, omaisuutta tai ympäristöä niihin kohdistuvilta riskeiltä. Yritysturvallisuustoiminnan tavoitteena on jatkuvuuden, turvallisuuden ja vaatimuksenmukaisuuden varmistaminen kaikissa tilanteissa osana yrityksen riskienhallintaa. Elinkeinoelämän mukaan turvallisuus on jatkuva prosessi ja myös osa yrityksen laatujärjestelmää. Turvallisuuden kehittämistoiminnan kannalta keskeisiksi teemoiksi muodostuvat henkilöstön kouluttaminen ja turvallisuustietoisuuden lisääminen sekä hyvän turvallisuuskulttuurin luominen yritykseen. (Elinkeinoelämän keskusliitto 2023)



Kuvio 1 Elinkeinoelämän yritysturvallisuusmalli (Elinkeinoelämän keskusliitto, 2023)

Elinkeinoelämän kehittämän yritysturvallisuusmallin (Kuvio 1) avulla on helppoa tarkastella yrityksen turvallisuuskenttää. Ylätason teemat mallissa ovat strategia, riskienhallinta, turvallisuuskulttuuri, turvallisuusjohtaminen. Mallin keskiössä on tavoite ja ympärillä on esitetty mitä elementtejä tulee huomioida, jotta tavoitteeseen päästään. Malli on yleisluontoinen ja siinä esitettyjen osa-alueiden merkitys eri yrityksissä vaihtelee. Tärkeää on tunnistaa mallista oman organisaation kannalta keskeiset kohdat.

2.2 Tieto- ja kyberturvallisuus yrityksissä

Kyberturvallisuudella tarkoitetaan digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin. Kyberturvallisuutta ovat toimenpiteet, joilla voidaan hallita ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia. Häiriö kybertoimintaympäristössä johtuu monesti toteutuneesta tietoturvauhkasta. Pyrittäessä hyvään kyberturvallisuuteen, tietoturva on erittäin keskeinen tekijä. (Turvallisuuskomitea, 2018).

Nykyisessä tietoyhteiskunnassa toimivien organisaatioiden keskeiset toiminnot ovat riippuvaisia järjestelmien toiminnasta. Tieto- ja viestintätekniikan hyödyntäminen tuo mukanaan tietoa koskevia riskejä. Yritysten tulee suojata omat ja asiakkaidensa tiedot erittäin hyvin ja se edellyttää monesti yrityksen ulkopuolista tietoturvaosaamista. (Juvonen ym., 2014,150.)

Järvisen (2022, 13) mukaan tietoturva kiteytyy kolmeen tavoitteeseen: luottamuksellisuuteen, eheyteen ja saatavuuteen. Luottamuksellisuudella hän tarkoittaa tietojen suojaamista siten, etteivät ulkopuoliset pääse niihin käsiksi. Tällaisia tietoja ovat esimerkiksi liikesalaisuudet, palkanmaksutiedot ja sähköpostien sisältö. Eheydellä tarkoitetaan sitä, että tietojen täytyy olla oikein ja niihin kohdistuu vain oikeutettuja muutoksia. Esimerkkinä Järvinen mainitsee, että työntekijöillä ei saa olla pääsyä talousosaston palkkatietoihin, etteivät he pysty korottamaan omia palkkojaan tai sen, että hakkerit pääsevät murtautumaan firman verkkosivulle ja tekemään sinne ei toivottuja muutoksia. Kolmantena tavoitteena on tiedon saatavuus. Laitteiden ja palvelujen saatavuusongelmia ovat esimerkiksi verkkoyhteyden pätkiminen tai rikkinäinen kone. Saatavuus on Järvisen mukaan tekninen ongelma, jolloin saatavuusongelmia vastaan suojaudutaan myös teknisin keinoin.

Järvisen (2022, 32) mukaan tietoturvallisuus liittyy nykyään enemmän inhimillisiin asioihin ja ihmisten ollessa huolimattomampia, väsyneempiä ja piittaamattomampia, heitä on helpompi huijata. Tärkeimmäksi tavoitteeksi tietoturvallisuudessa on saada ihmiset toimimaan oikein ja noudattamaan ohjeita.

Tietoturvallisuus on läsnä jokaisen yrityksen työntekijän tehtävissä. Tietoturvallisuus tulee saada liitettyä luontevasti osaksi jokapäiväistä toimintaa, kuten tiedotustilaisuuksiin,

kokouksiin ja kehityskeskusteluihin. Tietoturvakoulutustakin tehokkaampi tapa lisätä henkilöstön tietoturvatietoisuutta ja motivaatiota turvallisuusasioihin, on osallistaa henkilöstö näihin asioihin ja antaa henkilöstölle vaikuttamismahdollisuuksia. Myös viestintä ja koulutus lisäävät henkilöstön sitoutumista. (Juvonen ym., 2014,159.)

2.3 Riskienhallinta yrityksissä

Riskillä tarkoitetaan yleensä vaaraa tai uhkaa ja se kuvaa jotakin epäedullista tapahtumaa henkilölle tai omaisuudelle. Riski koetaan kolmen tekijän kautta: tapahtumaan liittyvä epävarmuus, tapahtumaan liittyvät odotukset ja tapahtuman laajuus ja vakavuus. (Juvonen ym. 2014, 8.)

Yritystoimintaan sisältyy aina riskejä. Riskienhallinnan hyvä suunnittelu turvaa liiketoimintaa ja sillä voidaan saavuttaa myös kilpailuetua ja imagohyötyjä työmarkkinoilla. Riskienhallinta tulee integroida kiinteästi yrityksen muihin toimintoihin, jolloin yritys voi tunnistaa, analysoida ja varautua riskeihin parhaan kykynsä mukaan. (Juvonen ym. 2014, 7.)

ISO 9001 on kansainvälinen laadunhallintajärjestelmän standardi. Standardi määrittää laadunhallintajärjestelmiä koskevat yleiset vaatimukset organisaatioille, joita se voi hyödyntää, kun tulee tarve osoittaa organisaation kyky tuottaa asiakasvaatimukset täyttäviä tuotteita tai palveluja sekä tuotteita tai palveluja koskevat viranomaisvaatimukset ja lakien vaatimukset. Organisaatio voi hyödyntää ISO 9001 standardia myös, kun se pyrkii lisäämään asiakastyytyväisyyttä soveltamalla järjestelmään, joka sisältää järjestelmän parantamisen prosessit ja asiakasvaatimusten ja sekä tuotetta koskevien lakien ja viranomaisten vaatimusten täyttämisen prosessit. (SFS-EN-9001:2015,10.) Kohdeyrityksessä on toteutettu kevään 2021 aikana standardin ISO 9001 mukainen laadunhallintajärjestelmän käyttöönotto. Kohdeorganisaation riskienhallintaa on jo tarkasteltu ISO 9001 laatujärjestelmän käyttöönoton yhteydessä.

Organisaatiot kohtaavat sisäisiä ja ulkoisia haasteita, joiden vuoksi on epävarmaa, saavuttavatko organisaatiot tavoitteitaan. ISO 31000 standardi antaa ohjeita organisaatioiden kohtaamien riskien hallintaa, sovellettuna organisaatioon ja sen toimintaympäristöön. (SFS-ISO-EN-31000:2018, 5.). ISO 31000 käyttäminen syventää riskienhallintaa entisestään ja auttaa kyberriskien hallinnan tuomista osaksi päivittäistä liiketoimintaa.

2.4 Tieto- ja kyberuhkat yrityksissä

ENISA:n (Euroopan unionin kyberturvallisuusvirasto ja tietoverkkojen ja digitaalisen toimintaympäristön turvallisuusasiantuntija EU:ssa) laatiman raportin mukaan yleisimmät kyberuhkat on esitetty oheisessa kuviossa (Kuvio 2). Valtaosa uhkista on sellaisia, jotka voivat koskettaa yksittäistä tietoverkkoja käyttävää kansalaista, tai ne voivat esiintyä usean yrityksen päivittäisessä liiketoiminnassa yrityksen kokoon tai toimialaan katsomatta. (Enisa, 2023.)

Haittaohjelmat ovat ohjelmistoja tai laiteohjelmistoja, joiden on tarkoitus suorittaa luvaton prosessi tavoitteena aiheuttaa haitallisia vaikutuksia järjestelmän luottamuksellisuudelle, eheydelle tai saatavuudelle. Verkkopohjaiset hyökkäykset kohdistuvat pääasiassa tietojen eheyteen ja saatavuuteen. Tietojenkalastelulla eli phishingillä tarkoitetaan yhteydenottoja, joiden tavoitteena on saada kohde luovuttamaan arkaluonteista materiaalia, kuten salasanoja tai käyttäjätunnuksia hyökkääjälle. Yhteydenotot ovat yleensä yleisiä, eivät kohdennettuja tietylle henkilölle tai organisaatiolle. (Enisa, 2023.)

Verkkopohjaisilla hyökkäyksillä tarkoitetaan hyökkäyksiä, joiden sovellukset ovat internetin palvelujen ytimessä. Käyttäjiä ja sovelluksia on paljon ja hyökkääjät pyrkivät löytämään niistä heikkoja kohtia, päästäkseen tunkeutumaan käyttäjän tietoihin. (Enisa, 2023.)

Roskapostit ovat sähköisiä viestejä, jotka toimitetaan pyytämättä vastaanottajalle. Spam-viestejä voidaan käyttää myös muiden kyberhyökkäysten apuna, kuten phishing-kampanjat. Palvelunestohyökkäyksellä tarkoitetaan hyökkäystä, jossa hyökkääjät kohdistavat suuren määrän verkkoliikennettä tietylle sivustolle, estäen tai haitaten sen toimintaa. (Enisa, 2023.)

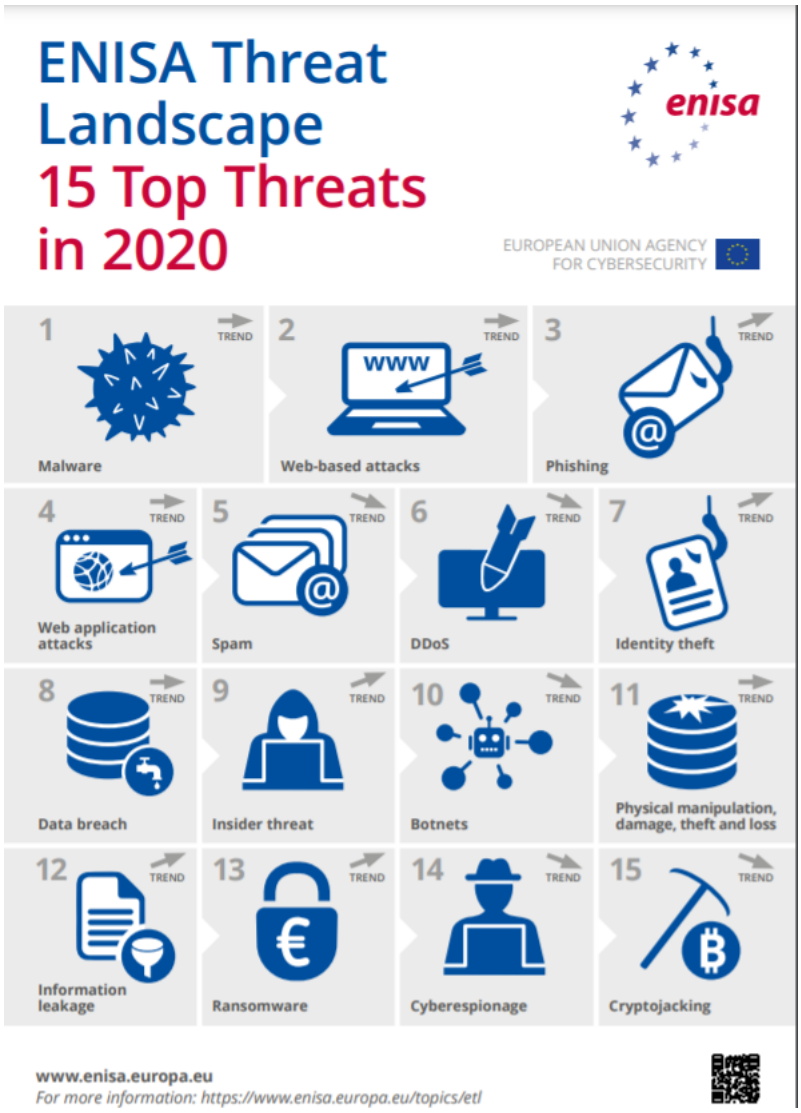
Identiteettivarkaudet ovat varkauksia, joissa esiinnytään toisen henkilöllisyydellä, esim. käytetään toisen henkilötietoja tai tunnistamistietoja. Identiteettivarkauden tiedot on monesti saatu haltuun tietomurtojen yhteydessä. (Enisa, 2023.)

Tietomurto on kybertapahtuma, jossa tietoon päästään käsiksi ilman oikeutta ja useimmiten tarkoituksena on käyttää tietoja väärin tai hävittää niitä. Esim. tunkeutuminen tietokantaan ja tietojen anastaminen. Sisäpiiriuhkalla tarkoitetaan tilannetta, jossa organisaation sisäpuolinen työntekijä tahallisesti tai tahattomasti toimii siten, että organisaation turvallisuus vaarantuu. (Enisa, 2023.)

Bottiverkko on joukko tietokoneohjelmia, jotka ovat kytkeytyneet toisiinsa verkon välityksellä. Saastunutta bottiverkkoa voidaan käyttää esim. palvelunestohyökkäyksien toteuttamisessa. Laitteiden joutuessa haitallisen toimijan käsiin, tietoturva vaarantuu. Tällainen toimija voi myös pyrkiä tuhoamaan fyysisesti laitteita, jolloin niissä olevat tiedot voivat kadota. (Enisa, 2023.)

Tietovuoto kohdataan usein tietomurron jälkeen, eli tietomurrolla saadut tiedot vuodetaan jonnekin, esim. tietylle verkkosivustolle. Kiristyshaittaohjelmat ovat ohjelmia, joiden avulla hyökkääjät vaativat käyttäjää maksamaan tietyn summan, jotta tiedot eivät katoa tai joudu julkaistuksi. Kybervakoilulla tarkoitetaan tilannetta, missä hankitaan tietoja toiselta organisaatiolta verkon kautta käyttämällä organisaation laitteita hyväksi. Kybervakoilu kohdistuu usein valtioon tai kriittisen infrastruktuurin alan yrityksiin. (Enisa, 2023.)

Laitteiden luvatonta käyttöä kryptovaluutan louhimiseen kuvataan englanninkielisellä termillä cryptojacking. Tämän tyyppinen toiminta ei ole samalla tavalla herättänyt lainvalvontaviranomaisten kiinnostusta verrattuna muihin kybermaailman uhkiin. Käyttäjälle cryptojacking näyttäytyy hitaampina koneina ja lisääntyneenä sähkönkulutuksena. (Enisa, 2023)



Kuvio 2 Enisa Top 15 Kyberuhkat (Enisa, 2021)

Kyberuhkia kohdistuu kaikkiin organisaatioihin ja yrityksiin ja niiden konkretisoiduttua yrityksen liiketoiminnalle voi aiheutua merkittävää haittaa tai jopa koko liiketoiminta voi keskeytyä. Traficomin Kyberturvallisuuskeskus saakin päivittäin kaikenkokoisia organisaatioita koskevia ilmoituksia kyberturvallisuuden vaarantumisesta. Pienyritysten kyberturvallisuusoppaan mukaan yleisimpiä kyberuhkia ovat tietojenkalastelu, eli phishing, haittaohjelmat ja kiristyshaittaohjelma. (Traficom, Pienyritysten kyberturvallisuusopas, 2021.)

Helsingin seudun kauppakamarin ja Avarn Security Oy:n vuonna 2022 teettämän selvityksen mukaan, jopa 77 prosenttia kyselyyn vastanneista arvioi suurimmaksi kyberuhkaksi tietojenkalastelun ja haittaohjelmat. Tietoisuus ja taitojen puute nousivat myös esiin selvityksessä. Vastanneista 50 prosenttia kertoi, että kyberturvallisuuden tietotaidon ylläpito nousee suurimmaksi ongelmaksi kyberturvallisuuden parantamiseksi, 40 prosentin mielestä työntekijöiden piittaamattomuus on esteenä kyberturvallisuuden edistämiseksi ja 34 prosentin mielestä yritysten on vaikeaa löytää riittävää tietoa kyberturvallisuusasioista. Selvitys ”Yrityksiin kohdistuvat kyberuhkat” on tehty syyskuussa 2022 ja siihen vastasi 258 suomalaisyritystä. 75 prosenttia vastanneista oli yrityksiä, jotka työllistävät alle 50 henkilöä, 10 prosenttia vastaajayrityksistä työllisti 50-200 henkilöä ja 15 prosenttia yli 200 henkilöä. (Kauppakamari, 2023.)

Yritysten, erityisesti pk-yritysten näkökulmasta uhkat ovat pysyneet viime vuosina varsin samankaltaisina ja tuorein selvitys korostaa henkilöstön asenteiden ja osaamisen merkitystä hyvän kyberturvallisuuden tason saavuttamisessa.

2.5 Kyberturvallisuuden hallinta ja kehittäminen yrityksissä

Kyberuhkia voidaan hallita ja kehittää mm. erilaisten standardien ja viitekehyksien avulla. Valtaosa niistä on alun perin kehitetty palvelemaan kriittisen infrastruktuurin yrityksiä, mutta niiden laatijoiden mukaan ne toimivat myös pienempien organisaatioiden kyberturvallisuuden parantamisessa.

2.5.1 Standardit ja viitekehykset

ISO 27001 standardi (Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.) määrittää vaatimukset koskien tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista organisaation toimintaympäristössä. Se sisältää myös tietoturvariskien arviointia ja käsittelyä koskevat vaatimukset. Tietoturvallisuuden hallintajärjestelmän tehtävänä on suojata tiedon luottamuksellisuutta, eheyttä sekä saatavuutta riskienhallintaprosessin avulla. Sen tarkoitus on myös osoittaa sidosryhmille, että riskienhallinta on asianmukaista. Tietoturvallisuuden hallintajärjestelmän on tärkeää olla osa organisaation prosesseja ja yleisiä rakenteita, kuten johtaminen ja hallinta. SFS-EN-ISO/IEC 27001:2017, 5.)

Yhdysvaltalainen National Institute of Standards and Technology on julkaissut viitekehyksen, Framework for Improving Critical Infrastructure Cybersecurity. Ensimmäinen versio julkaistiin vuonna 2014 ja päivitetty tällä hetkellä käytössä oleva 1.1 versio on vuodelta 2018. Kuten viitekehyksen nimikin kertoo, se on kehitetty kriittisen infrastruktuurin organisaatioiden kyberturvallisuuden kehittämiseen. Malli ei ole velvoittava, vaan se on vapaasti käytettävissä. Mallin pohja-aineistona on kansainvälisiä standardeja, joten sitä voidaan käyttää laajasti ja myös Suomessa. NIST kertoo verkkosivuillaan, että mallin avulla kaikenkokoiset yritykset voivat

käyttää sitä parantamaan kybertuvallisuuden riskienhallinnan tasoa. NIST- mallin kyberturvallisuusriskien hallintamalli koostuu seuraavista viidestä pääkohdasta: Uhkien tunnistaminen, uhkilta ennalta suojautuminen, uhkien havaitseminen/etsiminen, hyökkäykseen vastaaminen ja hyökkäyksestä toipuminen. (NIST,2021.)

Toinen kyberturvallisuuden viitekehysmalli, Cybersecurity Capability Maturity Model C2M2 on kehitetty Yhdysvalloissa energiasektorilla vuonna 2012. Mallia oli luomassa myös Department of Energy (DOE). C2M2- mallin tarkoitus on auttaa kaikentyyppisiä ja -kokoisia organisaatiota kaikilta toimialoilta arvioimaan ja kehittämään kyberturvallisuutta ja vahvistamaan resilienssiään. Nykyinen käytössä oleva versio 2.0 on ollut saatavilla heinäkuusta 2021 asti. (Department of Energy, 2021.)

C2M2- mallin pääkohdat ovat kyberriskien hallintastrategian luominen ja ylläpitäminen, kyberriskien tunnistaminen, kyberriskien analysointi, kyberriskeihin vastaaminen ja hallintatoimenpiteet. (Department of Energy, 2021.)

Kybermittari ei varsinaisesti ole viitekehys eikä standardi, mutta se pohjautuu ylempänä esitettyihin kansainvälisiin kyberkyvykkyyksien mittausmalleihin NIST Cybersecurity Framework sekä Cybersecurity Capability Maturity Model. Kybermittari on työkalu, jonka Traficomin kyberturvallisuuskeskus on kehittänyt parantamaan yritysten, organisaatioiden ja koko yhteiskunnan kykyä torjua kyberuhkia. Mittari on räätälöity Suomessa toimivien yritysten ja organisaatioiden tarpeisiin. Se pohjautuu kansainvälisiin kyberkyvykkyyksien mittausmalleihin NIST Cybersecurity Framework sekä Cybersecurity Capability Maturity Model. Työkalun avulla organisaatio voi mitata omaa kyberturvallisuuden kypsyystasoa. Mittari kertoo tulokset eri osa-alueilla ja esittää kehityskohteet. Ensisijaisesti mittari on suunniteltu huoltovarmuuden kannalta kriittisten yritysten käyttöön, mutta sitä voi käyttää myös muiden yritysten, järjestöjen ja julkisten toimijoiden kyberturvallisuuden kartoittamiseen. (Traficom, 2021.)

2.5.2 Kyberuhkilta suojautuminen

Täydellistä kyberturvallisuutta ei ole olemassa, mutta yleisimmiltä kyberuhkilta suojautuminen ei ole vaikeaa. Paras tapa on lisätä kaikkien tietoisuutta, toimintakykyä ja pitämällä tietoturva ajan tasalla. Tärkeää on tunnistaa haasteet ja reagoida niihin. (Limnéll ym. 2014, 84.)

Pienyritysten kyberturvallisuusopas käsittelee yleisimpiä kyberturvallisuuden uhkia tietojenkalastelu, haittaohjelmat ja kiristyshaittaohjelmat. Tietojenkalastelurikoksen kohteeksi voi joutua kuka hyvänsä ja suojautua siltä voi kiinnittämällä erityistä huomiota tileihin liittyviin pyyntöihin ja vastaanotettuun tietoon, erityisesti linkkeihin. Jos epäilet vastaanottajaa tai linkkiä, varmistu vastaanottajasta esimerkiksi soittamalla tälle puhelimella. Myöskään epäilyttävää linkkiä ei saa avata. (Traficom, Pienyritysten kyberturvallisuusopas, 2021.)

Haittaohjelmilta ja kiristyshaittaohjelmilta voi parhaiten suojautua pitämällä käyttöjärjestelmät ja ohjelmistot päivitettynä ja ottamalla tiedoista varmuuskopiot. Myös sähköpostilla saapuneita linkkejä ja liitteitä tulee lähestyä terveellä epäluulolla. Käyttöoikeuksien suhteen tulee noudattaa niin sanottua vähemmän oikeuden periaatetta, eli älä käytä järjestelmiä pääkäyttäjän oikeuksilla ja jokaiselle käyttäjälle tulee luoda omat tilit. (Traficom, Pienyritysten kyberturvallisuusopas, 2021.)

Ohjelmistopäivityksillä korjataan haavoittuvuuksia ja ne on syytä asentaa laitteille mahdollisimman pian niiden julkaisun jälkeen. Päivitykset ovat saatavissa sovelluskaupoista, palvelun sivuilta tai automaattisesti koneen tarjotessa niitä. Päivittämätön laite on aina rikollisien kannalta kiinnostavampi, koska rikolliset pyrkivät hyödyntämään näitä haavoittuvuuksia. Automaattiset päivitykset ovat tehokkain ja helpoin keino välttää tunkeutumisia koneelle. Tärkeimmistä tiedoista ja palveluista tulee tehdä varmuuskopiot, jotka säilytetään erillään suojattavista kohteista, kuten järjestelmät ja tiedot. Hyvä tapa on säilyttää niitä esimerkiksi erillisellä kiintolevyllä. Varmuuskopioiden palauttamista tulee myös testata säännöllisesti, koska silloin pystytään varmistumaan, että tiedot on varmasti kopioitu ja palauttaminenkin onnistuu. Tärkeä suojautumiskeino on myös monivaiheinen tunnistautuminen järjestelmiin. Tällä tarkoitetaan sitä, että järjestelmään kirjautuvan henkilön identiteetti varmistetaan useammalla eri tavalla, esimerkiksi sähköisessä tunnistautumisessa se perustuu kolmeen kohtaan: jotain mitä tiedän (salasana), jotain mitä omistan (päätelaitteeseen lähettävä varmenne) ja jotain mitä olen (sormenjälki). Jos kaksi kolmesta edellä mainituista toteutuu, tunnistusta voidaan pitää riittävänä. (Traficom, Pienyritysten kyberturvallisuusopas, 2021.)

Työpaikan tietoturvaoppaan tietoturvan kymmenen kohdan huoneentaulu (taulukko 1) auttaa parantamaan työpaikan tietoturvaa ja tiivistää tärkeimmät kohdat.

Tiedon luokittelu	Luokittele tiedot julkisiin ja salassa pidettäviin. Käsittele henkilötietoja saamiesi ohjeiden mukaisesti.
Tietoaineistojen tallentaminen	Huolehdi, että käsittelemistäsi tiedoista löytyy varmuuskopiot. Varmista, että tiedot eivät katoa teknisen ongelman, laitevian tai inhimillisen virheen takia.
Salasanojen käyttö	Älä käytä töissä ja vapaa-ajan palveluissa samoja salasanoja. Laadukas salasana sisältää isoja aakkosia, kirjaimia, numeroita ja erikoismerkkejä.

Laitteiden käyttö	Ole huolellinen käyttäessäsi erilaisia päätelaitteita. Suhtaudu terveellä epäilyksellä liitteisiin ja linkkeihin, joita vastaanotat.
Arkaluontoisista asioista keskustelu	Älä keskustele salassa pidettävistä työasioista tai pidä sellaista materiaalia julkisella paikalla.
Tietojen säilytys	Sammuta tai lukitse laitteet, jos et käytä niitä, tai poistuessasi paikalta. Säilytä salassa pidettävää tietoa lukitussa tilassa.
Organisaation tietoturvaohjeet	Lue organisaatiosi tietoturvaohjeet ja noudata niitä.
Toiminta häiriötilanteessa	Häiriötilanteessa tiedät kehen ottaa yhteyttä ja miten tulee toimia, kun havaitset tietoturvallisuutta uhkaavan asian.
Kysy ja varmista	Jos et tiedä, aina voit kysyä. Jos olet ilmoittanut poikkeamasta, varmista, että asia etenee ja sen eteen tehdään korjaustoimenpiteitä.
Älä ota turhia riskejä tai hölmöile	Jos jokin asia vaikuttaa liian hyvältä ollakseen totta, näin se myös yleensä on. Esimerkiksi sähköpostiviestin tai muun yhteydenoton sisältö.

Taulukko 1 Tietoturvan kymmenen kohtaa

Tiedon luokittelu julkisiin ja salassa pidettäviin tietoihin ja henkilötietojen oikeaoppinen käsittely suojaavat tietoja. Kaikista tarpeellisista tiedoista tulisi olla varmuuskopiot ja tietoja tulisi tallentaa siten, että teknisen vian tai muun häiriön sattuessa tiedot ovat kuitenkin palautettavissa. Salasanakäytännöt tulisi opetella siten, että kotona ja työpaikalla käytetään eri salasanoja, jotta toisen mahdollinen vuotaminen ei johda toisen palvelun helppoon sisäänpääsyyn käyttäen samoja tunnuksia. Salasana tulee olla myös tarpeeksi laadukas sisältää erilaisia elementtejä, kuten isoja kirjaimia, numeroita ja erikoismerkkejä. Päätelaitteita on erilaisia ja niiden käytön suhteen kannattaa olla huolellinen ja opetella laitteen oikea käyttö turvallisen toiminnan takaamiseksi. Laitteet tulee lukita tai sammuttaa, kun työskentely on päättynyt tai taukoaa. Päätelaitteiden huolellisen käytön lisäksi myös muun fyysisen

materiaalin käsittely on tärkeää turvallisuuden kannalta. Arkaluonteiset ja salassa pidettävät materiaalit tulee pitää pois näkyvistä ja tarvittaessa lukitussa tilassa, jotta ne eivät päädy vääriin käsiin. Näistä arkaluonteisista tiedoista ei saa myöskään keskustella paikoissa, joissa kuulemassa voi olla ulkopuolisia henkilöitä. Päätelaitteilla työskenneltäessä kohtaa jatkuvasti sähköistä materiaalia, kuten sähköposteja ja linkkejä. Kaikkeen poikkeavaan kannattaa suhtautua terveellä epäilyksellä ja miettiä aina uudestaan tai kysyä työkaverilta, jos epäilee huijausta tai muuta häiriötä. Useassa organisaatiossa on myös laadittu tietoturvaohjeet, joita seuraamalla selviää monesta epäselvästä tilanteesta. Järvisen ja Rouskun huoneentaulun mukaan turhien riskien välttämistä kannattaa välttää ja moni liian hyvältä vaikuttava asia on monesti huijausyritys. (Järvinen ja Rousku, Työpaikan tietoturvaopas, 2017, luku 6.)

3 Opinnäytetyön toteutus ja menetelmät

Opinnäytetyö on tyypiltään tutkimuksellinen kehittämistyö. Tutkimukselliseen kehittämistyöhön liittyy monesti tarve ratkaista käytännön ongelmia sekä tuottaa ja toteuttaa uusia ideoita, käytäntöjä, palveluita tai tuotteita. Tutkimuksellinen kehittämistyö saa alkunsa tyypillisesti organisaation muutoksen tarpeesta tai kehittämistarpeesta. Tutkimuksellista kehittämistä ohjaavat siis ensi sijassa käytännölliset tavoitteet, joita tuetaan teorialla. Keskeistä on, että ongelmia havaitaan ja niitä kyetään ratkaisemaan. (Ojasalo, Moilanen & Ritalahti 2014, 19-20.) HNR-konepajalla kehittämistarpeena oli kyber- ja tietoturvallisuuden parantaminen. Tässä luvussa kuvataan lähtötilannetta ja menetelmiä, joilla saadaan koottua tarvittavat tiedot tutkimuksen suorittamiseksi. Tietoa kerättiin haastattelemalla yrityksen toimihenkilöitä, havainnoimalla kolmena eri kertana yrityksen toimitiloissa ja kartoittamalla Kybermittari-työkalua hyödyntäen yrityksen kyberturvallisuuden nykytila.

3.1 Opinnäytetyön toimeksiantaja

Toimeksiantajana on Kotkassa toimiva HNR-Konepaja Oy. Yritys on perustettu vuonna 1983 palvelemaan lähialueen teollisuuden kunnossa- ja käynnissä pitoa. Kunnossapito alkoi siirtyä 1990- luvulla yrityksille itselleen ja HNR- Konepajassa keskityttiin enemmän valmistamaan osakomponentteja teollisuudelle.

Vuodesta 2004 kunnossapitotöitä ei ole enää tehty, yritys tarjoaa nykyisin prosessiteollisuuden energiataloudellisia ratkaisuja globaaleille pörssiyrityksille. Pääasiakkuudet ovat viime vuosina olleet pääasiassa samoja, pientä vaihtuvuutta asiakkaissa toki on. Liiketoiminnasta 90 prosenttia koostuu suuremmista asiakkaista, 10 prosenttia pienemmistä, yksityisasiakkaita ei juuri ole.

HNR-Konepaja Oy työllistää 27 henkilöä, kaikki työskentelevät vakituisessa työsuhteessa. 22 työntekijää toimii tuotantotehtävissä ja viisi toimihenkilötehtävissä. Toimihenkilöt

työskentelevät toimistossa ja käyttävät työssään tietoteknisiä laitteita päivittäin työtehtävien hoitamiseksi. Tuotannon työntekijät eivät juuri käytä verkossa olevia tietokoneita.

HNR-Konepaja on kehittänyt toimintaansa vuosien varrella, kehityksen jatkuessa edelleen. Viimeisen viiden vuoden sisällä yrityksen tuotantotiloja on muokattu, logistiikkakeskus rakennettu, asioiden sähköinen kirjaaminen on myös lisääntynyt ja mm. työnseurannan tuntikirjaukset tulevat siirtymään mobiilikirjauksiksi. Yritys haki ja sai Business Finlandin koronatukea vuonna 2020 ja tuen myötä yritys sai luotua laatujärjestelmän ISO9001, joka mahdollistaa liiketoiminnan kehittämisen edelleen, esimerkiksi uusien vaativampien asiakkaiden hankinnan.

HNR-Konepajan toimitusjohtajana toimii Joni Rinne, joka on toiminut tehtävässä vuodesta 2011 alkaen. Hän on toisen polven yrittäjä ja on työskennellyt laajasti yrityksen eri tehtävissä ennen toimitusjohtajan tehtäviä.

HNR-Konepaja on kehittänyt riskienhallintaansa muun muassa ISO9001- standardin sertifioinnin yhteydessä. Kriittisimpien kehityskohteiden yhteydessä ei ole kuitenkaan käsitelty kyberturvallisuutta, eikä juurikaan tietoturvallisuutta. Keskusteluissa yrityksen toimitusjohtajan kanssa käy ilmi, että kyberturvallisuusasiat on tiedostettu, mutta syvällistä osaamista kyberturvallisuudesta ei ole. Halukkuutta kyberturvallisuuden tietämyksen nostamiseen yrityksestä löytyy.

3.2 Aineistonkeruu haastattelemalla

Ojasalon ym. (2014, 106–107) mukaan haastattelu on erittäin yleinen tiedonkeruumenetelmä kehittämistyössä, koska haastatteluiden avulla voidaan saada muun muassa hyvin yksityiskohtaistakin tietoa kehittämisen kohteesta. Haastattelulla korostetaan yksilöä, jolloin häntä koskevia asioita sillä voidaan helpommin käsitellä. Haastattelun tehtävänä on monesti asioiden selventäminen ja syventäminen, jonka vuoksi haastattelun lisänä on kehittämistyössä hyvä käyttää myös muita tiedonhankintamenetelmiä.

Haastattelun valinta tiedonkeruumenetelmäksi vaatii suunnitelmallisuutta. Haastattelijan tulee miettiä millaista tietoa hän tulee tarvitsemaan kehittämistehtävää varten, joka tulee vaikuttamaan haastattelun rakenteeseen ja haastattelutyyppiin. Haastattelun tyyppejä ovat strukturoitu, puolistrukturoitu ja avoin haastattelu. Strukturoidussa haastattelussa kysymykset on laadittu valmiiksi ja ne esitetään tietyssä järjestyksessä, puolistrukturoidussa haastattelussa ennalta laadittujen kysymysten paikkaa voi vaihdella haastattelun kulun perusteella ja tilanteeseen liittymättömiä kysymyksiä ei ole tarpeen kysyä tai voidaan kysyä kysymyksiä, mitä tulee mieleen haastattelun aikana. Avoimessa haastattelussa osapuolet (haastattelija ja haastateltava) keskustelevat aktiivisesti aiheesta ilman ennalta laadittuja kysymyksiä. (Ojasalo ym. 2014, 108–109.)

Haastattelu on vuorovaikutusta, joka perustuu osapuolten väliseen luottamukseen. Haastattelija kertoo haastateltavalle kehittämistyön tarkoituksen ennen haastattelun aloittamista. Haastattelun kesto voi vaihdella kymmenistä minuuteista useisiin tunteihin. Usein haastattelut äänitetään, jolloin haastattelija voi paremmin keskittyä tilanteeseen ja haastattelun voi myös jälkikäteen kuunnella, joka saattaa avata uusia näkökulmia. Haastattelut on hyvä myös kirjoittaa auki, eli litteroida, jolloin niiden analysointi helpottuu. (Ojasalo ym. 2014, 107–108.)

Haastattelun analysointi riippuu haastattelujen laajuudesta ja haastateltavien lukumäärästä. Strukturoidun haastattelun tulokset suositellaan analysoitavan tietokoneohjelmalla, kuten Excelillä tai SPSS- ohjelmalla, teemahaastattelut ja avoimet syvähaastattelut analysoidaan lukemalla litteroinnit useaan kertaan ja luokittelemalla aineisto. (Ojasalo ym. 2014, 110.)

Luotaessa haastattelukysymyksiä HNR- konepajan toimihenkilöille, on huomioitu yrityksen toimiala (metalliteollisuus), yrityksen koko (pk-yritys) ja henkilöstön tarve olla tietoinen kyberturvallisuuden asioista. Kysymykset on pyritty tarkentamaan kyseiselle yritykselle sopivaksi. Rouskun (2014, s.63-64) mukaan tietoturvaohjeistukset vaihtelevat organisaatioissa, eikä ohjeistuksia välttämättä ole lainkaan. Vaihtelu johtuu organisaatioissa käsiteltävien tietojen, organisaation toimialan ja sen ydinprosessien erilaisuudesta. Esimerkiksi valtion viraston prosessit ovat varsin erilaiset, kuin pienyrityksessä. Kuitenkin myös pienyrittäjältä edellytetään tiettyjä tietoturvavelvoitteita mm. asiakkaiden ja alihankkijoiden suuntaan.

Haastattelumetodiksi valittiin puolistrukturoitu haastattelu, koska haastateltavien kanssa haluttiin keskustella varsin avoimesti kyberturvallisuudesta ja kuulla heidän näkemyksiään aiheesta. Ennakkoon laadituilla kysymyksillä kuitenkin pysytään rajoitetummassa aihepiirissä ja saadaan olennaisinta tietoa kyberturvallisuuden nykytilan kannalta. Haastattelukysymykset luotiin opinnäytetyön teoriaosuudessa esitettyjen tietojen pohjalta. Kysymysten avulla kerättiin tietoa yrityksen työntekijöiden kyberturvallisuusosaamisesta ja kehittymishalukkuudesta. Haastatteluilla saatua tietoa hyödynnettiin kehittämistoimien suunnittelussa.

Toimitusjohtaja haastateltiin kaksi kertaa, ensimmäisellä haastattelulla 6.10.2021 selvitettiin yleisiä asioita yrityksestä, joilla osaltaan muodostettiin yrityksen henkilöstölle kohdennettuja haastattelukysymyksiä ja sitä käytettiin myös rajaamaan myöhempien haastateltavien joukkoa. Toisessa haastattelussa 30.11.2021 toimitusjohtajalta selvitettiin samoja asioita, kuin toimihenkilöiltä.

Toimihenkilöiden haastattelut jakautuivat kolmeen pääteemaan: *yleiset, termistö, häiriöt*. Yleinen osa käsitti kysymyksiä työhistoriasta, koulutuksesta, käytössä olevasta tietoteknisestä laitteistosta, salasanojen hallinnasta, fyysisen materiaalin käsittelystä ja oman arvion kyberturvallisuusosaamisesta haastatteluhetkellä (asteikolla 0-5). Termistö- osiossa selvitettiin haastateltavien tietämystä yleisimmistä kyberturvallisuuteen liittyvistä termeistä, jotka ovat

oleellisia myös turvallisen työskentelyn kannalta. Häiriöt- osiossa selvitettiin, ovatko haastateltavat kohdanneet työurallaan kyberhäiriöitä ja jos ovat, miten niihin on reagoitu. Haastattelukysymykset löytyvät opinnäytetyön liitteistä (liite 1). Haastateltavia toimihenkilöitä on toimitusjohtajan lisäksi neljä. Haastatteluihin saatiin haastateltavien suostumus ja ne suoritettiin yrityksen toimitiloissa 11.10.-30.11.2021. Haastatteluilla saatu aineisto litteroitiin analysointia varten. Haastattelujen rakenteen vuoksi niistä on helppo etsiä tiettyjä teemoja. Haastatteluiden analysointi suoritettiin teemoittelemalla.

3.3 Aineistonkeruu havainnoimalla

Kyselyt ja haastattelut eivät kerro mitä todella tapahtuu. Havainnointia voidaan käyttää, kun halutaan tietoa siitä, toimivatko ihmiset, kuten he kertovat toimivansa. (Hirsjärvi, Remes & Sajavaara 2009, 212.) Havainnointi sopii käytettäväksi myös silloin, kun kohteena on esine tai sen käyttäminen. (Ojasalo ym. 2014, 114).

Vierailin kolme kertaa kohdeyrityksessä kirjaten samalla ylös, kuinka kohdehenkilöt työskentelivät työympäristössään. Tavoitteena oli saada selville, onko työskentely tietoturvallista myös todellisuudessa. Havainnointi kohdistettiin tietoturvalliseen työskentelyyn laitteiden kanssa ja fyysiseen turvallisuuteen työpisteillä ja niiden läheisyydessä. Havainnointien päivämäärät 6.10.2021, 25.11.2021 ja 26.11.2021.

Havainnointilomake on osittain strukturoitu Word-asiakirja, jossa runkona toimi taulukossa 1 esitetyt aihealueet. Muodostin havainnointiasiakirjaan aihealueet: työtiloihin saapuminen, tilojen suunnittelu ja työpisteiden suunnittelu, henkilöiden käyttäytyminen, henkilöiden työskentely, tiloissa sijaitseva fyysinen materiaali, ulkopuolisten henkilöiden vierailu tiloissa ja tiloista poistuminen. Lomakkeen otsikoiden alle kirjattiin havainnot jokaisen havainnointikerran jälkeen. Analysoin havaintojen tuloksia jokaisen havainnointikerran jälkeen lukemalla asiakirjat.

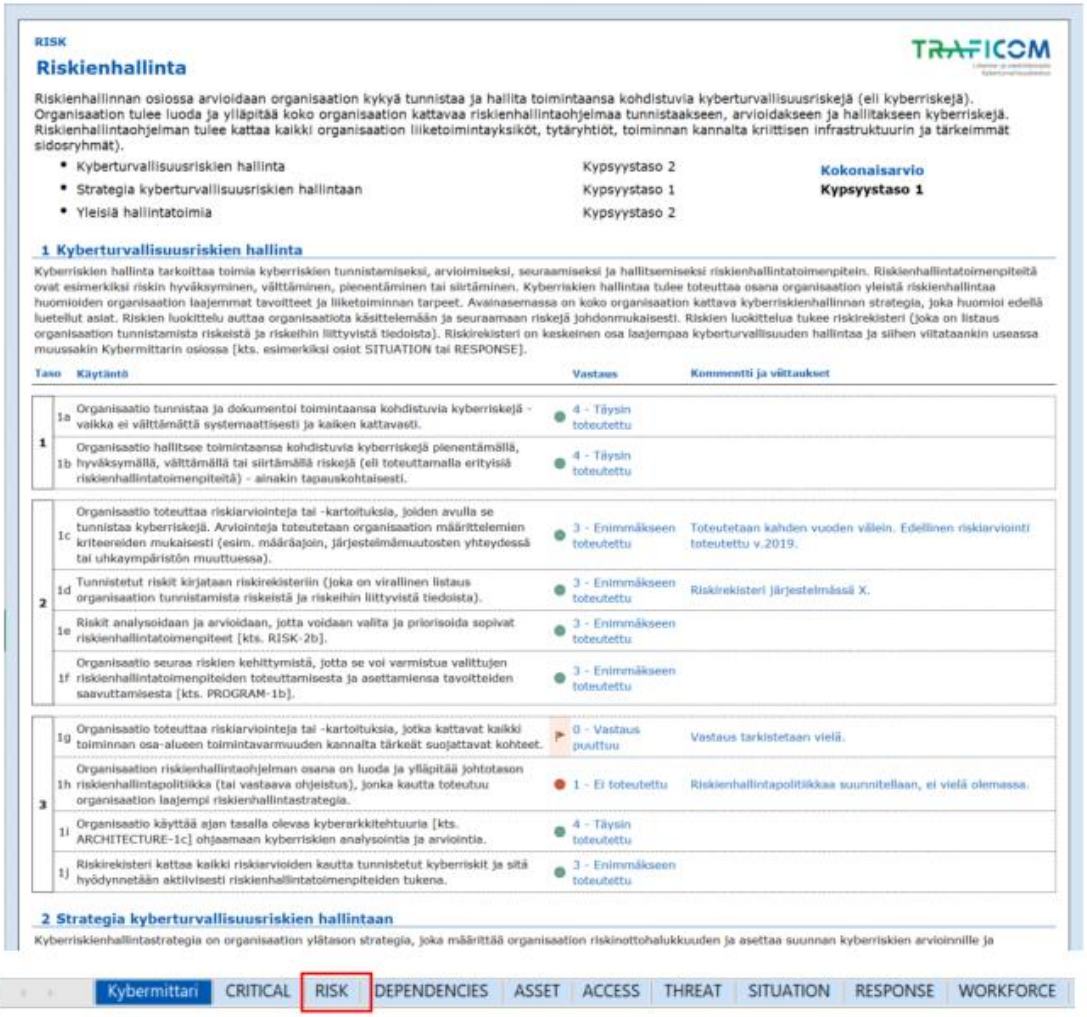
Havainnoitava aihe-alue	**Mitä havainnoitiin?**
Työtiloihin saapuminen	Ovien lukitus, vastaanotto
Tilojen suunnittelu ja työpisteiden sijoittelu	pöydät, tietokoneet, muut verkkolaitteet, kansiot, tulostimelle pääsy
Henkilöiden käyttäytyminen	koneiden ja laitteiden käyttö, läsnäolo työpisteellä

Henkilöiden työskentely	millaisia tehtäviä, keskustelu kollegoiden kanssa, mahdolliset häiriöt ja reagointi niihin
Tiloissa sijaitseva fyysinen materiaali	mitä tulosteita, mitä materiaalia työpöydillä, onko arkaluontoista, onko salasanoja esillä, seinien ilmoitustaulujen materiaalit, kansioiden sisällöt
Ulkopuolisten henkilöiden vierailu tiloissa	miten otetaan vastaan, miten saa kulkea tiloissa
Tiloista poistuminen	ovien lukitus, koneilta uloskirjautuminen

Taulukko 2 Havainnointitaulukko

3.4 Aineistonkeruu Kybermittaria käyttämällä

Tässä opinnäytetyössä kybermittaria käytettiin organisaation kyberturvallisuuden nykytilan kartoittamiseen. Mittarin tulosten avulla organisaatio voi tarkastella kyberturvallisuuden tilaansa ja suunnitella kehittämistoimia sen parantamiseksi. Kybermittari-työkalua ei ollut vaikea käyttää, koska siihen oli valmistauduttu lyhyellä Traficomin koulutuksella ja lukemalla mittarin ohjeistus. Työkalu on excel-pohjainen ja se on saatavilla kaikille vapaasti Traficomin Kyberturvallisuuskeskuksen verkkosivuilta. Kybermittari muodostuu yhdestätoista kyberturvallisuuden osiosta. Osiot on kuvattu omilla välilehdillään. Esimerkki kuviossa 3. Jokainen osio sisältää noin 20-40 kysymystä kohdeorganisaatiolle.



Kuvio 3 Esimerkki kybermittarin välilehdestä RISK. (Traficom, 2021)

Toteutus eteni loogisesti välilehti kerrallaan ja mittari laski itse kypsyystasot, kun vaadittavat tiedot oli syötetty. Toteutin kybermittarin tiedonkeruun yhdessä kohdeorganisaation toimitusjohtajan kanssa alkuvuonna 2022. Sovimme toimitusjohtajan kanssa, että ensimmäinen tiedonkeruu suoritetaan paikan päällä kohdeyrityksessä ja jos tiedonkeruu jää kesken, seuraavat keruut voidaan suorittaa Teams-palaverien muodossa. Tiedonkeruu jäi ensimmäisen tapaamisen jälkeen kesken ja tapasimme tämän asian parissa vielä kolme kertaa Teamsissa siten, että heijastin oman näyttöni toimitusjohtajalle, ohjasin keskustelua ja siten sain tarvittavat tiedot mittarin eri kohtiin. Työmäärä koettiin suureksi ja jokainen tiedonkeruutapahtuma vei useita tunteja.

Kybermittarin kysymykset olivat pääosin ymmärrettäviä, mutta usean kysymyksen vastausvaihtoehdot eivät kohdanneet kohdeyrityksen toimintojen kanssa. Voidaan todeta, että pk-yrityksen, jonka ydintoiminta ei ole kyberturvallisuuden kannalta kriittisellä alalla, kannattaa mitata kyberkyvykkyyttään jollakin toisella mittaustavalla. Näkemykseni mukaan Kybermittari

toimii varmasti erittäin hyvin esim. valtion organisaation tai jonkin finanssialan toimijan kyberturvallisuuden mittaamisessa ja on selkeän rakenteensa vuoksi helposti toistettavissa, kun halutaan seurata organisaation kyberkypsyyden kehityssuuntaa.

4 Tulokset

Luvussa esitetään havainnoinnin, haastatteluiden ja Kybermittarin avulla kerätyt tulokset. Havainnointikertoja oli yhteensä kolme 6.10.2021, 25.11.2021 ja 26.11.2021. Haastatteluita suoritettiin viidelle toimihenkilölle (toimitusjohtaja, kaksi työnjohtajaa, toimistopäällikkö ja toimistoapulainen). Haastatteluiden ajankohdat olivat 11.10.-30.11.2021. Kybermittarin tulokset kerättiin neljällä eri kerralla 10.-17.1.2022.

4.1 Haastattelut

Toimitusjohtajan ensimmäisen haastattelun perusteella toimihenkilöt käyttävät päivittäin verkossa olevia laitteita ja kommunikoivat asiakkaiden kanssa sähköisillä viestivälineillä. Toimitusjohtajan arvion mukaan toimihenkilöiltä löytyy kyberturvaosaamista sen verran, että kriittiset päivitykset saadaan suoritettua ja tietoturvaohjelmistot pysyvät ajan tasalla. Hänen mukaansa henkilöstöllä ei ole erityistä kyberturvakoulutusta ja yleisesti osaaminen kyberasioissa ei ole hyvällä tasolla. Varmuuskopiot tärkeistä asioista on saatavilla pilvipalveluista ja ulkopuoliselta palveluntarjoajalta.

Haastateltavien koulutustaso on tasoilla ammatillinen perustutkinto (2 henkilöä) ja AMK (3 henkilöä). Neljä haastateltavaa on työskennellyt yrityksessä useamman vuoden ja yksi haastateltava alle yhden vuoden, hänelläkin on työelämästä jo pidempi kokemus toiselta alalta. Kaikilla haastateltavilla on suoritettuna erilaisia työtehtäviä tukevia kursseja. Kyberturvallisuuteen tai tietotekniikkaan liittyviä erityisiä kursseja tai koulutuksia ei ole kenelläkään suoritettuna.

Haastatteluiden tulokset esitetään teemoittain. Teemat ovat yleiset kyberturvallisuusasiat ja henkilöiden taustat, kyberturvallisuuden termit ja kyberturvallisuuden häiriöt. Ensimmäinen teema ”Yleiset kyberturvallisuusasiat”, piti sisällään kysymyksiä henkilöiden tyypillisistä työtehtävistä, millaisia laitteita henkilöt käyttävät työssään, laitteiden päivityksistä, virustorjunnasta, salasanoista ja fyysisen materiaalin käsittelystä. Toisessa teemassa ”Kyberturvallisuuden termit” käsiteltiin keskeistä termistöä ja haastateltavia pyydettiin kuvaamaan käsitteitä kyberturvallisuus, phishing, haittaohjelma, kiristyshaittaohjelma, palvelunestohyökkäys, toimitusjohtajapetos CEO-fraud ja suojattu verkkoyhteys. Kolmas teema ”Kyberturvallisuuden häiriöt” käsitteli henkilöiden kohtaamia kyberhäiriöitä töissä, kuten epämääräisiä sähköposteja, kalasteluyrityksiä ja reagointia tämän kaltaisissa tilanteissa.

4.1.1 Yleiset kyberturvallisuusasiat

Haastatteluiden perusteella yrityksen henkilöstöllä on käytössään Windows-pohjaiset tietokoneet ja Android-käyttöjärjestelmällä varustetut älypuhelimet. Myös kaksi iOs-käyttöjärjestelmän omaavaa laitetta on käytössä. Kaikkien haastateltavien tietokoneet ja puhelimet on säädetty suorittamaan automaattisia päivityksiä, päivitykset ovat ajan tasalla ja niiden kanssa ei ole ollut ongelmia.

Kaikilla haastateltavilla on kirjoitettuna salasanoja paperilapuille, joilla pääsee kirjautumaan koneelle tai johonkin käytössä olevaan järjestelmään. Kaksi haastateltavaa säilyttää salasanoja siten, että ne ovat saatavilla työpisteeltä, mutta haastateltavien mukaan lapuissa ei suoraan lue, mihin tarkoitukseen salasanat ovat. Kolme haastateltavaa kertoo säilyttävänsä salasanapaperit lukitussa tilassa. Yhtä lukuun ottamatta haastateltavat eivät käsittele arkaluontoista materiaalia.

Haastateltavilta kysyttiin omaa arviota kyberturvallisuusosaamisesta asteikolla 0-5. Vastaukset olivat välillä 2-4, keskiarvon ollessa 3.

4.1.2 Kyberturvallisuuden termit

Neljä viidestä haastateltavasti osasi kuvata kyberturvallisuustermiä ymmärrettävästi. Haastateltavat määrittelevät kyberturvallisuuden sähköisen maailman ja internetin turvallisuudeksi, joka voi käsittää myös laajempia valtakunnallisia asioita. Toimihenkilö kertoo kyberturvallisuus-termistä:

> Kyberturvallisuus on bittiavaruus, syvällistä tietotekniikkaa, kaikki on alustoilla. Tämän kaiken turvaaminen.

Kaikki viisi haastateltavaa osasivat kuvata phishing-termiä ymmärrettävästi. Haastateltavat kertovat phishing-termin olevan tietojenkalastelua, roskaposteja, joiden linkkiä klikkaamalla pyritään saamaan tietoja haltuun, esimerkiksi pankkitunnuksia. Kalastelua voidaan tehdä myös puhelimitse.

Kaikki viisi haastateltavaa osasivat kuvata haittaohjelma-termiä ymmärrettävästi. Haastateltavien mukaan haittaohjelmat ovat seurantaohjelmia, jotka voivat esimerkiksi lähettää käyttäjän sähköpostista tietoja eteenpäin. Haastateltavien mukaan haittaohjelmia ovat virukset tai epämääräiset linkit, joita klikkaamalla tietokone jumiutuu.

Neljä viidestä haastateltavasta osasi kuvata kiristyshaittaohjelma-termiä ymmärrettävästi. Haastateltavien mukaan kiristyshaittaohjelma lukitsee käyttäjän tietokoneen ja ohjelma voi pyytää rahaa tai muussa tapauksessa se lähettää tietoja eteenpäin.

Neljä viidestä haastateltavasta osasi kuvata palvelunestohyökkäys-termiä ymmärrettävästi. Haastateltavat kuvasivat termiä hyökkäyksenä sivuille, jotta ne menevät tukkeeseen ja saadaan estettyä joku palvelu tai pääsy palveluun. Haastateltava kertoo termistä:

> Olen kuullut tästä, siinä pommitetaan jotain sivua ja sitten se menee tukkeeseen.

Kolme viidestä haastateltavasta osasi kuvata CEO-fraud, toimitusjohtajapetos-termiä ymmärrettävästi. Haastateltavien mukaan toimitusjohtajapetoksessa esiinnytään firman johtajana ja pyydetään palvelusta kuten firman tilitietojen tarkastamista. Toimitusjohtajapetoksia kohdistuu erityisesti uusille työntekijöille ja loma-aikoina.

Neljä viidestä haastateltavasta osasi kuvata suojattu verkkoyhteys-termiä ymmärrettävästi. Haastateltavat kertovat, että suojatun verkkoyhteyden tunnistaa https-merkinnästä sivulla ja selaimessa on lukon kuvan tai sivustolla maininta suojauksesta. Vastaavasti turvattomilla sivustoilla on maininta, että sivusto ei ole turvallinen.

4.1.3 Kyberturvallisuuden häiriöt

Kyberturvallisuutta vaarantavia häiriöitä oli kohdannut kaksi viidestä haastateltavasta. Organisaatioon kohdistui toimitusjohtajapetoksen yritys, joka tunnistettiin hyvin ja vahinkoa ei päässyt syntymään. Lisäksi yhteistyökumppanin nimissä on tullut sähköpostin välityksellä hieman erilaiselta näyttävä viesti, johon ei reagoitu. Myöhemmin yhteistyökumppani ilmoitti, että heidän nimissään on lähetetty epäilyttäviä viestejä, joita ei saa avata. Toimihenkilö kommentoi häiriötä:

> Tuli sähköposti, jossa vastapuoli ei noudattanut vanhaa mallia. En avannut linkkiä ja myöhemmin sieltä tulikin viesti, että älkää avatko viestiä.

Haastatteluiden perusteella kenenkään haastateltavan työasemalla ei ole ollut viruksia. Epämääräisiä sähköposteja oli saanut kolme viidestä haastateltavasta. Sähköpostit ovat olleet sijoituksiin tai bitcoineihin liittyviä.

Soittoja ATK-tuesta tai muusta epäilyttävästä lähteestä oli saanut kolme viidestä haastateltavasta. Soitot ovat koskeneet mm. Microsoft-tukea ja vaikuttivat tulevan Intiasta. Osa puheluista on koskenut tuotteen tai palvelun tilaamista ja vaikuttanut haastateltavan mielestä tilausansalta. Myös erilaisten tutkimusten tekijät ovat kyselleet yrityksen tiedoista, osa on vaikuttanut epäilyttävältä. Toimihenkilö kertoo saapuneesta puhelusta:

> Kovasti se halusi yrityksen tietoja tarkastaa, mutta minua epäilytti ja suljin puhelun.

Sosiaalisen median kautta epämääräisiä lähestymisyrityksiä oli kohdannut yksi haastateltavista. Nämä lähestymiset ovat olleet linkkejä, jotka ovat koskeneet tuotteen tai palvelun hankintaa (tilausansa).

Kolme viidestä haastateltavasta on antanut salasanoja tai käyttäjätunnuksia toiselle henkilölle. Salasanoja on luovutettu organisaation sisällä kollegalle. Salasanat ovat kuitenkin lukitussa tilassa. Kaikki haastateltavat kertovat, että heillä on eri salasanat eri palveluihin. Haastateltava kertoo:

> Samankaltaisia ne salasanat voivat olla, mutta ei samoja.

Kolme viidestä haastateltavasta kertoo, että työpaikalla puhutaan kyberturva- ja tietoturvaasioista. Yleisesti koetaan, että asioista voisi puhua enemmän.

Yrityksen toimihenkilöt ovat kohdanneet työuransa varrella tyypillisiä kyberturvallisuuden häiriöitä. Häiriöihin on osattu reagoida ja vahinkoja liiketoiminnalle ei ole syntynyt. Kyberturvallisuusasioista halutaan ymmärtää enemmän ja toivotaan lisää keskustelua aiheesta.

4.2 Havainnointi

Havainnot esitetään taulukoissa siten, että jokaisen havainnointikerran muodostavat oman taulukkonsa. Taulukoissa kerrotaan havainnoitava aihealue ja mitä siitä tarkemmin havainnoitiin, sekä millaisia havaintoja kohteessa tehtiin.

Havainnoitava aihealue	**Mitä havainnoitiin?**	**Havainnot 6.10.2021**
Työtiloihin saapuminen	Ovien lukitus, vastaanotto	Ulko-ovi avoinna, tiloissa yksi henkilö. Hän havaitsee minut heti ja alamme jutella. 10 min päästä saapuu lisää henkilökuntaa.
Tilojen suunnittelu ja työpisteiden sijoittelu	pöydät, tietokoneet, muut verkkolaitteet, kansiot, tulostimelle pääsy	Työtilat ovat rakennuksen toisessa kerroksessa (ylin krs.), kaksi työpistettä

		oikealla, kaksi vasemmalla, tj;n tilat hieman pidemmällä, valvontakameralaitteisto, monitoimitulostin, modeemit aivan kahden toimihenkilön läheisyydessä,
Henkilöiden käyttäytyminen	koneiden ja laitteiden käyttö, läsnäolo työpisteellä	Toimihenkilöt käyttivät omia koneitaan, omilla työpisteillä, soittivat ja vastaanottivat puheluita, hetkellisiä poistumisia koneilta.
Henkilöiden työskentely	millaisia tehtäviä, keskustelu kollegoiden kanssa, mahdolliset häiriöt ja reagointi niihin	Toimihenkilöiden työskentely oli normaali toimistotyötä koneella ja puhelimitse, välillä keskustelua kollegoiden kanssa työasioista, häiriöitä ei havaittu.
Tiloissa sijaitseva fyysinen materiaali	mitä tulosteita, mitä materiaalia työpöydillä, onko arkaluontoista, onko salasanoja esillä, seinien ilmoitustaulujen materiaalit, kansioiden sisällöt	Pöydillä ei ole arkaluontoista materiaalia tai salasanoja.
Ulkopuolisten henkilöiden vierailu tiloissa	miten otetaan vastaan, miten saa kulkea tiloissa	Havainnoinnin aikana ulkopuolisia ei vieraillut toimistossa.
Tiloista poistuminen	ovien lukitus, koneilta uloskirjautuminen	Tilojen jäädessä tyhjäksi, kaikilta koneilta oli kirjauduttu

		ulos, ulko-ovi lukittiin lounastauon ajaksi.

Taulukko 3 Ensimmäinen havainnointi 6.10.2021

Ensimmäisellä havainnointikerralla 6.10.2021 saatiin seuraavat tulokset. Tapaamisesta oli sovittu toimitusjohtajan kanssa. Yrityksen toimihenkilöiden tiloihin tullaan ulkoa, ulko-ovi on avoinna. Paikalla on yksi toimihenkilö, hän havaitsee minut heti ja keskustelen hänen kanssaan. Alle 10 min kuluttua paikalle saapuu toimitusjohtaja ja kaksi muuta toimihenkilöä. Toimihenkilöiden tilat sijaitsevat yläkerrassa, kaksi työpistettä oikealla, kaksi vasemmalla ja toimitusjohtajan tilat hieman pidemmällä neuvottelutilan yhteydessä. Lisäksi tiloissa on WC ja keittiötila. Toimihenkilöiden tilat on sijoitettu siten, että ulkopuolelta tulevien henkilöiden saapuminen huomataan ja esim. selän taakse ei yllättäen pääse ulkopuolinen henkilö. Tiloissa sijaitsee näkyvästi myös modeemi, monitoimilaite ja valvontakameralaitteisto. Laitteiden sijoittelu on välittömästi kahden toimihenkilön työpisteen vieressä, etäällä portaikosta. Ensimmäisen havainnoinnin yhteydessä suoritettiin myös toimitusjohtajan ensimmäinen haastattelu ja selvitettiin paikalla oleville toimihenkilöille opinnäytetyön prosessia ja saatiin suostumukset haastatteluille. Toimitusjohtajan haastattelun jälkeen toimihenkilöiden tilat jäivät tyhjäksi ja tiloista poistumisen yhteydessä kaikilta koneilta oli kirjauduttu ulos ja ulko-ovi lukittiin lounastauon ajaksi. Pöydillä ei ole esillä arkaluontoista materiaalia eikä salasanoja.

Havainnoitava aihealue	**Mitä havainnoitiin?**	**Havainnot 25.11.2021**
Työtiloihin saapuminen	Ovien lukitus, vastaanotto	Ulko-ovi avoinna, tiloissa yksi henkilö. Hän havaitsee minut heti ja alamme jutella. Hetken päästä myös toinen toimihenkilö saapuu paikalle tuotantotiloista.
Tilojen suunnittelu ja työpisteiden sijoittelu	pöydät, tietokoneet, muut verkkolaitteet, kansiot, tulostimelle pääsy	Jos aulatilojen työpisteillä ei ole henkilöitä

		työskentelemässä, voi tiloihin päästä kenenkään huomaamatta ulko-ovelta. Näin on mahdollista seurata toisessa tilassa olevien työskentelyä tai muuten liikkua tiloissa.
Henkilöiden käyttäytyminen	koneiden ja laitteiden käyttö, läsnäolo työpisteellä	Toimihenkilöt käyttivät omia koneitaan, omilla työpisteillä, soittivat ja vastaanottivat puheluita, hetkellisiä poistumisia koneilta. Koneet jäivät lukitsematta.
Henkilöiden työskentely	millaisia tehtäviä, keskustelu kollegoiden kanssa, mahdolliset häiriöt ja reagointi niihin	Toimihenkilöiden työskentely oli normaalia toimistotyötä koneella ja puhelimitse, välillä keskustelua kollegoiden kanssa työasioista, häiriöitä ei havaittu.
Tiloissa sijaitseva fyysinen materiaali	mitä tulosteita, mitä materiaalia työpöydillä, onko arkaluontoista, onko salasanoja esillä, seinien ilmoitustaulujen materiaalit, kansioiden sisällöt	Pöydillä ei ole arkaluontoista materiaalia tai salasanoja.
Ulkopuolisten henkilöiden vierailu tiloissa	miten otetaan vastaan, miten saa kulkea tiloissa	Yksi työhaastattelu päivän aikana. Toimitusjohtaja hoiti tämän omissa

		tiloissaan. Tiloissa käy myös firman omia tuotannon työntekijöitä.
Tiloista poistuminen	ovien lukitus, koneilta uloskirjautuminen	Havainnoinnin aikana tiloista ei poistuttu siten, että ne olisivat jääneet tyhjiksi.

Taulukko 4 Toinen havainnointi 25.11.2021

Toisella havainnointikerralla 25.11.2021 saatiin seuraavat tulokset. Saapuessani paikalle, ulko-ovi on auki. Jälleen saapuessani toimistolle, paikalla on toimihenkilö, joka havaitsee minut heti. Myös toinen toimihenkilö tulee tiloihin hetken kuluttua tuotantohallin puolelta. Havaitsin, että jos aulatilojen yhteydessä olevilla työpisteillä ei ole henkilöitä työskentelemässä, tiloihin voi päästä ulkoa kenenkään huomaamatta ja portaiden yläpäästä aulatilasta, voi seurata toimihenkilön työskentelyä selän takaa ja nähdä näytöllä esillä olevat asiat. Päivän aikana tiloissa käy yrityksen omia tuotannon työntekijöitä, tuovat tai hakevat tavaroita, esim. piirustuksia valmistettaville tuotteille tai käyvät kysymässä neuvoja työhön liittyen. Toimihenkilöt poistuvat välillä omilta työpisteiltään, koneet jäävät lukitsematta, henkilöt eivät poistu kauas koneiltaan. Päivän aikana tiloissa käy yksi ulkopuolinen henkilö, hänellä oli ennalta sovittu työhaastattelu, jonka toimitusjohtaja suorittaa tämän omissa neuvottelutiloissa. TJ työskenteli omissa tiloissaan koko päivän, kone oli auki lähes koko ajan, työnteko oli pääasiassa s-postia ja puheluita. Pöydillä ei ole esillä arkaluontoista materiaalia eikä salasanoja.

Havainnoitava aihealue	**Mitä havainnoitiin?**	**Havainnot 26.11.2021**
Työtiloihin saapuminen	Ovien lukitus, vastaanotto	Ulko-ovi avoinna, tiloissa yksi henkilö. Hän havaitsee minut heti ja alamme jutella.

Tilojen suunnittelu ja työpisteiden sijoittelu	pöydät, tietokoneet, muut verkkolaitteet, kansiot, tulostimelle pääsy	Pöytien ja koneiden sijoittelu kuten ensimmäisessä havainnoinnissa. Runsaasti kansioita hyllyissä, portaiden oikealla puolella toimihenkilöiden työpisteiden läheisyydessä.
Henkilöiden käyttäytyminen	koneiden ja laitteiden käyttö, läsnäolo työpisteellä	Toimihenkilöt käyttivät omia koneitaan, omilla työpisteillä, soittivat ja vastaanottivat puheluita, hetkellisiä poistumisia koneilta. Koneet jäivät lukitsematta.
Henkilöiden työskentely	millaisia tehtäviä, keskustelu kollegoiden kanssa, mahdolliset häiriöt ja reagointi niihin	Toimihenkilöiden työskentely oli normaalia toimistotyötä koneella ja puhelimitse, välillä keskustelua kollegoiden kanssa työasioista, häiriöitä ei havaittu.
Tiloissa sijaitseva fyysinen materiaali	mitä tulosteita, mitä materiaalia työpöydillä, onko arkaluontoista, onko salasanoja esillä, seinien ilmoitustaulujen materiaalit, kansioiden sisällöt	Pöydillä ei ole arkaluontoista materiaalia tai salasanoja. Tutustuin kansioiden materiaaleihin, ne sisälsivät piirustuksia, käyttöohjeita, myyntisaamisia, ei arkaluontoista.

Ulkopuolisten henkilöiden vierailu tiloissa	miten otetaan vastaan, miten saa kulkea tiloissa	Havainnoinnin aikana tiloissa ei käynyt ulkopuolisia henkilöitä. Tiloissa käy myös firman omia tuotannon työntekijöitä.
Tiloista poistuminen	ovien lukitus, koneilta uloskirjautuminen	Havainnoinnin aikana tiloista ei poistuttu siten, että ne olisivat jääneet tyhjiksi.

Taulukko 5 Kolmas havainnointi 26.11.2021

Kolmannella havainnointikerralla 26.11.2021 saavutettiin seuraavat tulokset. Paikalla oli päivän aikana vaihtelevasti 2-3 toimihenkilöä. He työskentelivät pääasiassa omilla työpisteillään, käyttäen omia laitteitaan. En huomannut, että tiloissa olisi päivän aikana vieraillut ulkopuolisia henkilöitä. Havainnointia suoritettiin myös toimihenkilöiden tiloissa olevaan fyysiseen materiaaliin. Ilmoitustauluilla ei ole näkyvissä arkaluontoista materiaalia. Tiloissa on myös paljon arkistohyllyjä, joissa on runsaasti kansioita. Tutustuin kansioiden sisältöön ja niihin sijoitetut materiaalit eivät ole arkaluontoisia, lähinnä käyttöohjeita, myyntisaamisia, piirustuksia. Pöydillä ei ole esillä arkaluontoista materiaalia eikä salasanoja.

4.3 Kybermittarin tulokset

Kybermittarilla selvitettiin opinnäytetyössä kohdeorganisaation, HNR-konepajan kyberturvallisuuden nykytilaa. Työkalu on excel-pohjainen ja tässä kuvataan sen avulla saadut tulokset.

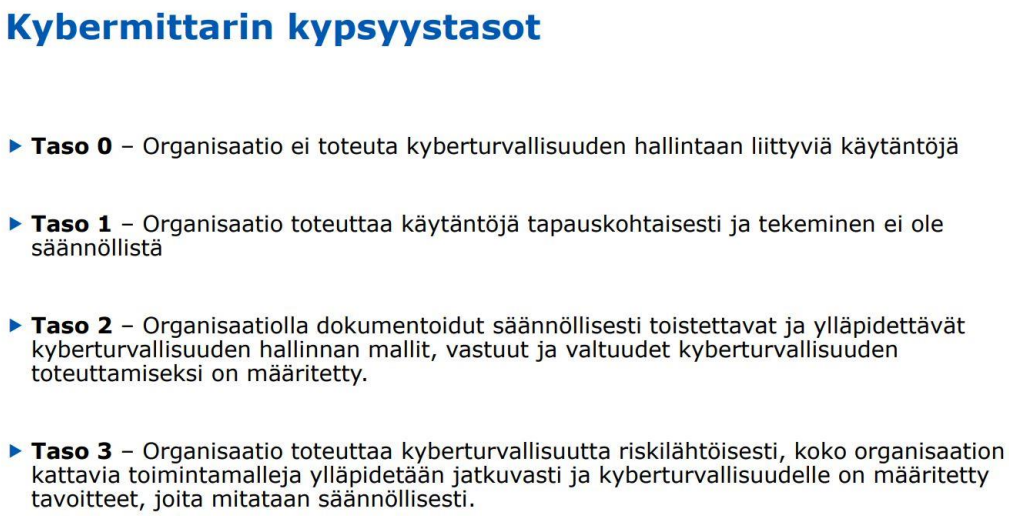
4.3.1 Tulosten esittäminen ja kypsyystasot

Kybermittari koostuu useasta välilehdestä, jotka arvioinnin tekijä täyttää. Vastausvaihtoehdot ovat:

1- Ei toteutettu
2- Osittain toteutettu
3- Enimmäkseen toteutettu
4- Täysin toteutettu

Osioiden ollessa täytetty, mittari laskee tuloksen organisaation kyberkyvykkyydestä asteikolla 0-3. (Kuvio 4). Traficomin järjestämässä Kybermittarin käyttökoulutuksessa 06/2021

kerrottiin, että tason 2 kypsyystason saavuttaminen on jo merkittävän hyvä taso ja sitä ei odoteta yrityksiltä, jotka eivät työskentele kyberturvallisuuden kannalta kriittisellä alalla.



Kuvio 4 Kyberkyvykkyyden tasot Kybermittarissa (Traficom)

4.3.2 Kypsyystasot välilehtien mukaan

Jokainen Kybermittari-työkalun osio käsitellään erikseen, työkalun avulla on määritetty kyberturvallisuuden kypsyystasot eri osioille. Oheisella taulukolla (taulukko 2) kuvataan Kybermittarin 11 eri osiota ja esitellään osion kypsyystaso. Kybermittarin excel-versiossa tulokset on saatavilla suoraan sen jokaiselta välilehdeltä, mutta excelin runsaan tietomäärän vuoksi tuloksien julkaisussa käytetään apuna tätä taulukkoa.

Osion kuvaus Kybermittarissa	**Kohdeyrityksen vastaus**	**Kypsyystaso Kybermittarilla**
CRITICAL. Kriittisten palveluiden suojaaminen- osio koostuu 27:stä arvioitavasta kohdasta. Osion tavoitteena on, että organisaatio tunnistaa oman roolinsa yhteiskunnan kannalta kriittisten palveluiden tuottamisessa ja osaa hallita riskejä sen mukaisesti.	*HNR-konepaja ei tuota yhteiskunnan kannalta kriittisiä palveluita, joten osion kaikkiin kohtiin vastattiin ei toteutettu.*	*Kypsyystaso 0.*

RISK. Riskienhallinnan osio koostuu 22:sta arvioitavasta kohdasta. Osion avulla arvioidaan organisaation kyberriskien hallintaa (Kyberturvallisuusriskien hallinta, strategia kyberriskien hallintaan, yleiset hallintatoimet).	*HNR-konepajalla ei ole kyberturvallisuusstrategiaa. Organisaatio tunnistaa ja dokumentoi poikkeavia tapahtumia ja tapahtumista tiedotetaan organisaation sisällä, myös ulkopuoliset palveluntarjoajat/kumppanit ovat tehneet osittaisia kartoituksia kyberriskeistä. Riskirekisteri on olemassa, mutta kyberriskejä sinne ei ole kirjattu. Yleisiä hallintatoimia on myös suoritettu ja vastuita on jaettu henkilöstölle. Tämä on toteutettu ISO9001 sertifioinnin yhteydessä.*	*Kypsyystaso 0.*
DEPENDENCIES. Toimitusketjun ja ulkoisten riippuvuuksien osio koostuu 28:sta kohdasta. Osion avulla arvioidaan organisaation kykyä tunnistaa ja hallita toimitusketjuihin ja kolmansiin osapuoliin liittyviä kyberriskejä.	*HNR-konepajalla on vakiintuneet analysoidut IT ja OT-toimittajat. Laatujärjestelmä ISO9001 määrittää myös kriteereitä toimittajan/asiakkaan valintaan. Organisaatio on myös tunnistanut riippuvuuksiin liittyviä riskejä ja toteuttaa osittain yleisiä riippuvuuksiin liittyviä toimenpiteitä.*	*Kypsyystaso 0.*
ASSET. Omaisuuden, muutoksen ja konfiguraation hallintaosio koostuu 31:stä kohdasta. Osiossa arvioidaan organisaation kykyä hallita toimintavarmuuden kannalta tärkeää omaisuutta (IT ja	*HNR-konepajalla ei ole IT ja OT- omaisuudelle rekisteriä, eikä myöskään tietovarantojen rekisteriä. Suojattavan omaisuuden konfiguraatiota ei myöskään toteuteta kybermittarin mukaisesti.*	*Kypsyystaso 0.*

OT- laitteet) ja siihen liittyviä muutoksia ja konfiguraatioita.	*Suojattavien kohteiden muutoksenhallintaa ei ole toteutettu. Yleisiä hallintatoimia, kuten resursseja ja vastuita on osittain toteutettu.*	
ACCESS. Identiteetin- ja pääsynhallinnan osio koostuu 22:sta kohdasta. Osiossa arvioidaan organisaation kykyä hallita ja rajoittaa pääsyä suojattaviin kohteisiin.	*HNR-konepajassa identiteettien hallinta on pääosin hyvin toteutettu, identiteettejä on luotu niitä tarvitseville ja vastuut esim. pääkäyttäjätunnuksien osalta on jaettu. Myös käyttöoikeuksien osalta hallintatoimet ovat pääasiassa hyvällä tasolla. Yleisiä hallintatoimia on osittain toteutettu.*	*Kypsyystaso 1.*
THREAT. Uhkien ja haavoittuvuuksien hallinta osio koostuu 32:sta kohdasta. Osiossa arvioidaan organisaation kykyä havaita ja hallita mahdollisia kyberuhkia ja haavoittuvuuksia.	*Uhkien tunnistaminen ja hallinta on HNR-konepajassa pääosin toteuttamatta. Samoin haavoittuvuuksien rajoittaminen. Yleisiä hallintatoimia on osittain toteutettu*	*Kypsyystaso 0.*
SITUATION. Tilannekuva osio koostuu 29:stä kohdasta. Osiossa arvioidaan organisaation kykyä määritellä ja ylläpitää kyberturvallisuuden tilannekuvaa.	*HNR-konepajassa lokitus on osittain toteutettu ja, monitorointi on pääasiassa toteuttamatta. Tietoa kerätään, mutta sitä ei hyödynnetä suoraan kyberturvallisuuden tilannekuvaan*	*Kypsyystaso 0.*
RESPONSE. Tapahtumien ja häiriötilanteiden hallinta osio koostuu 32:sta	*HNR-konepajassa ei ole keskitettyä kybermittarin määrittelemää*	*Kypsyystaso 0.*

kohdasta. Osiossa arvioidaan organisaation kykyä hallita, reagoida ja palautua kybertapahtumista ja -häiriöistä.	*raportointikanavaa tapahtumien havainnoinnille. Havaittuja poikkeavia tapahtumia käydään läpi viikkopalaverissa. Kybertapahtumia ei analysoida systemaattisesti ja koroteta niitä tarvittaessa häiriöiksi. Tapahtumia tunnistetaan, raportoidaan ja palautetaan tila normaaliksi ja selvitetään tapahtuman seurauksia, pääasiassa sisäisesti.*	
WORKFORCE. Henkilöstön hallinta osio koostuu 30:stä kohdasta. Osiossa arvioidaan organisaation kykyä kehittää ja ylläpitää henkilöstön kyberturvallisuusosaamista ja -valmiutta.	*HNR-konepajassa on osittain toteutettu monia kyberturvallisuuden vastuiden jakamiseen liittyviä tehtäviä. Kyberturvallisuushenkilöstön kehittämisen tehtäviä on myös hieman toteutettu. Henkilöstön yleisiä hallintatoimia, kuten taustatarkastukset, on osittain toteutettu. Organisaatio pyrkii tietoisesti lisäämään työntekijöiden kyberturvallisuusosaamista*	*Kypsyystaso 0.*
ARCHITECTURE. Kyberturvallisuusarkkitehtuuri osio koostuu 32:sta kohdasta. Osiossa arvioidaan organisaation kykyä hallita ja ylläpitää kyberturvallisuustoimintaansa	*HNR-konepaja on tunnistanut arkaluontoista tietoaan ja toteuttanut suojaustoimenpiteitä sille. Kyberarkkitehtuuria ei ole laajemmin toteutettu.*	*Kypsyystaso 0.*
PROGRAM. Kyberturvallisuusohjelma osio koostuu	*HNR-konepajalla ei ole kyberturvallisuusstrategiaa,*	*Kypsyystaso 0.*

40:stä kohdasta. Osiossa arvioidaan organisaation kykyä hallita ja ylläpitää organisaationlaajuista kyberturvallisuusohjelmaa.	*johdon tuki kyberturvallisuusohjelmalle on osittain toteutettu, kyberturvallisuutta ei ole huomioitu laajasti osana jatkuvuussuunnittelua ja yleisiä hallintatoimia on osittain toteutettu*	

Taulukko 6 Kybermittarin 11 osiota taulukkona ja kypsyystasot.

Critical-välilehti käsittelee kriittisten palveluiden ja niiden riippuvuuksien tunnistamista, palveluiden hallintaa ja kriittisten palveluiden kyberhäiriöiden minimointia. Critical osiossa käydään läpi 27 eri kohtaa, joiden perusteella organisaation roolia arvioidaan. Kohdeyritys ei liity yhteiskunnan kannalta kriittisten palveluiden piiriin, joten kaikkiin kohtiin vastattiin ei toteutettu ja osion kypsyystasoksi saatiin 0.

Risk-välilehdellä käsitellään organisaation kykyä tunnistaa ja hallita sen toimintaan kohdistuvia kyberturvallisuusriskejä. Osiossa käsitellään myös kyberturvallisuusriskien hallintastrategiaa ja yleisiä hallintatoimia (yhteensä 22 kohtaa). Osion vastausten perusteella kohdeorganisaatiossa tunnistetaan poikkeavia havaintoja ja tiedotetaan niistä sisäisesti, myös it-palveluja tarjoavat kumppaniyritykset ovat tuottaneet riskikartoituksia ja tarjonneet lisäturvaa. Riskienhallintaa yleisellä tasolla on kehitetty viimeisten vuosien runsaasti mm. laatusertifioinnin yhteydessä ja sertifikaatit vaativat myös säännöllistä tarkastusta ja auditointia. Kyberturvallisuusstrategiaa yrityksellä ei ole olemassa. Risk osion kypsyystasoksi saatiin 1.

Dependencies-välilehti käsittelee organisaation kykyä tunnistaa ja hallita toimitusketjuihin ja kolmansiin osapuoliin liittyviä riskejä. Osiossa käsitellään riippuvuuksien tunnistamista, riippuvuusriskien hallintaa ja yleisiä hallintatoimia (28 kohtaa). Kohdeorganisaatio tunnistaa riippuvuuksiaan ja on analysoinut ja vertaillut ulkoisia yhteistyökumppaneita. Myös laatujärjestelmän myötä tulee velvoitteita toimittajien valintaan. Kohdeorganisaatio on osittain tunnistanut myös riippuvuuksiin liittyviä riskejä ja työskentelee niiden riskienhallinnan parissa. Osa riskienhallinnan toimista on yrityksen päivittäistä riskienhallintaa, mutta niitä ei ole dokumentoitu. Dependencies osion kypsyystasoksi saatiin 0.

Asset-välilehdellä käsitellään omaisuuden, muutoksen ja konfiguraation hallintaa. Osio käsittelee IT ja OT- omaisuuden rekisterin hallintaa, tietovarantojen rekisterin hallintaa, suojattavan omaisuuden hallintaa, suojattavien kohteiden muutoksenhallintaa ja yleisiä hallintatoimia (31 kohtaa). Kohdeorganisaatio toteuttaa osittain yleisiä hallintatoimia, eli osa

käytännöistä on juurrutettu osaksi organisaation toimintaa. Muita osion toimia ei ole toteutettu. Asset osion kypsyystasoksi saatiin 0.

Access-välilehdellä käsitellään identiteetin ja käyttöoikeuksien hallintaa ja näihin liittyviä yleisiä hallintatoimia. Identiteetinhallinta on kohdeorganisaatiossa enimmäkseen toteutettu, samoin käyttöoikeuksien hallinta (22 kohtaa). Identiteetit ja käyttöoikeudet luodaan niitä tarvitseville ja ne poistetaan, jos niitä ei enää tarvita. Laajemmat käyttöoikeudet, kuten pääkäyttäjäoikeudet on vain niitä tarvitsevilla. Access osion kypsyystasoksi saatiin 1.

Threat-välilehti käsittelee organisaation kykyä havaita ja hallita kyberuhkia, rajoittaa haavoittuvuuksia sekä edellä mainittujen yleisiä hallintatoimia (32 kohtaa). Kohdeorganisaatiossa on osittain toteutettu uhkien tunnistamiseen ja hallintaan liittyviä toimia (analysointi, priorisointi, vastaaminen, tiedon jakaminen). Myös haavoittuvuuksien rajoittamiseen on reagoitu mm. vaihtamalla vanhoja koneita uusiin. Threat osion kypsyystasoksi saatiin 0.

Situation-väliehti arvioi organisaation kykyä määritellä ja ylläpitää kyberturvallisuuden tilannekuvaa. Osio arvoidaan lokituksen, monitoroinnin, tilannekuvan muodostamisen ja yleisten hallintatoimien perusteella (29 kohtaa). Kohdeorganisaatiossa suoritetaan lokitusta tietyille kohteille ja tietoja on saatavissa, jos organisaation koneet joutuisivat hyökkäyksen kohteeksi. Monitorointia ei suoriteta ja kyberturvallisuuden tilannekuvan edistämiseksi ei ole tehty toimenpiteitä. Situation osion kypsyystasoksi saatiin 0.

Response-välilehti käsittelee kybertapahtumien havainnointia, niiden analysointia ja häiriöksi korottamista, kybertapahtumiin ja häiriötilanteisiin regaointia ja näihin liittyviä yleisiä hallintatoimia (32 kohtaa). Kohdeorganisaatiossa on olemassa käytäntö havaittujen kybertapahtumien raportoinnille ja rekisteröinnille, mutta kriteereitä ei ole tarkemmin määritelty. Tapahtumia ei tarkemmin analysoida ja niiden tunnistamiseksi ei ole myöskään kriteeristöä. Häiriötilanteisiin liittyen ei ole määritelty selkeitä rooleja ja henkilöitä, eikä erillistä reagointisuunnitelmaa ole olemassa. Response osion kypsyystasoksi saatiin 0.

Workforce käsittelee organisaation kykyä kehittää ja arvioida henkilöstön kyberturvallisuusosaamista ja -valmiutta (vastuiden jakaminen, kyberhenkilöstön kehittäminen, henkilöstön hallintatoimet, kybertietoisuuden lisääminen, yleiset hallintatoimet, yhteensä 30 kohtaa). Kohdeorganisaatiossa vastuunjakoa on tunnistettu ja vastuita jaettu henkilöille ja eri toimijoille. Henkilöstö on saanut hieman kyberturvallisuuskoulutusta laatujärjestelmän ylläpidon yhteydessä ja siihen tullaan jatkossa panostamaan enemmän. Auditoinnin myötä mm. huumetestit on lisätty työhöntulotarkastukseen ja henkilöstön taustatarkastuksia on mahdollista tehdä rekrytointien yhteydessä. Myös muita henklöstön hallintatoimia kuten tunnuksien, avaimien ja tagien

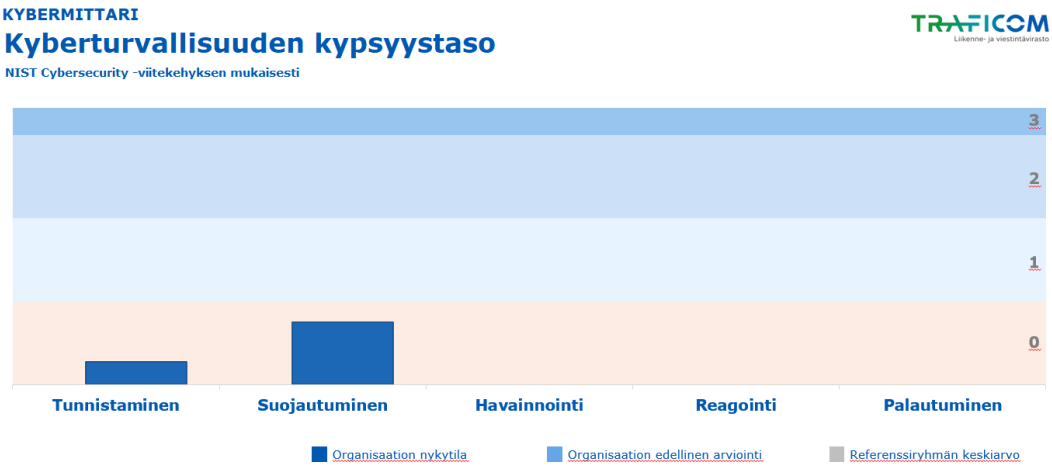
hallintaa suoritetaan. Kybertietoisuutta yrityksen toimihenkilöille lisätään tämän opinnäytetyön myötä. Workforce osion kypsyystasoksi saatiin 0.

Architecture-välilehti käsittelee kyberarkkitehtuuris- ja kehitysohjelmaa, verkkojen segmentointia osana kyberarkkitehtuuria, sovellusurvallisuutta osana kyberarkkitehtuuria, tietojensuojelua osana kyberarkkitehtuuria ja näihin liittyviä yleisiä hallintatoimia (32 kohtaa). Kohdeorganisaatiolla ei ole strategiaa kyberarkkitehtuurille, jolloin koko osion lähes kaikkiin kohtiin vastattiin ei toteutettu. Osiossa on myös muutamia yksittäisä tietojen suojaamista koskevia kohtia, joita organisaatiossa on osittain toteutettu. Näitä ovat esimerkiksi salattujen sähköpostien lähettäminen ja arkaluonteisten tietojen säilyttäminen lukitussa tilassa. Architecture osion kypsyystasoksi saatiin 0.

Program-välilehdellä arvioidaan organisaation kykyä hallita ja ylläpitää koko organisaationlaajuista kyberturvallisuusohjelmaa. Osio muodostuu kyberturvallisuusstrategiasta, johdon tuesta kyberturvallisuusohjelmalle, kyberturvallisuudesta osana jatkuvuussuunnittelua ja yleisistä hallintatoimista (40 kohtaa). Erillistä kyberturvallisuusstrategiaa kohdeorganisaatiolla ei ole. Johto tukee kyberturvallisuuden kehitystä ja resursseja on myös jonkin verran käytettävissä tähän, myös vastuunjako on selkeä. Organisaatiolla on saatavilla tarvitsemistaan tiedoista varmuuskopiot luotettavassa paikassa, mutta muuten erillistä jatkuvuudenhallintasuunnitelmaa ei ole laadittu. Program osion kypsyystasoksi saatiin 0.

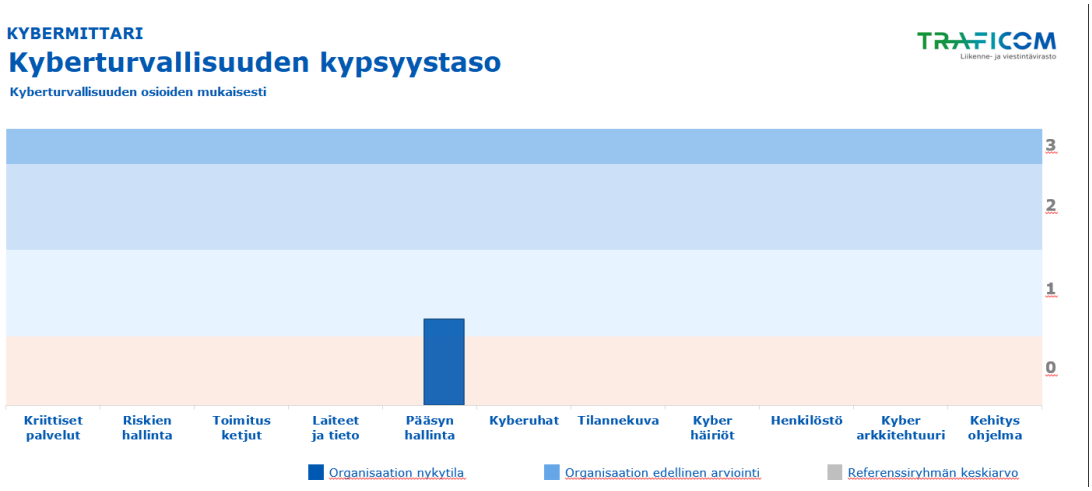
4.3.3 Raportit kypsyystasosta

Kybermittari-työkalusta on mahdollista saada tuloksia eri muodoissa, yksi raportti esittää tulokset NIST-viitekehyksen mukaisesti (kuvio 6). Tämän mallin mukaan kohdeorganisaatiossa kaikki kypsyystasot ovat tasolla 0. Tulokset esitetään tunnistamisen, suojautumisen, havainnoinnin, reagoinnin ja palautumisen alueilta.



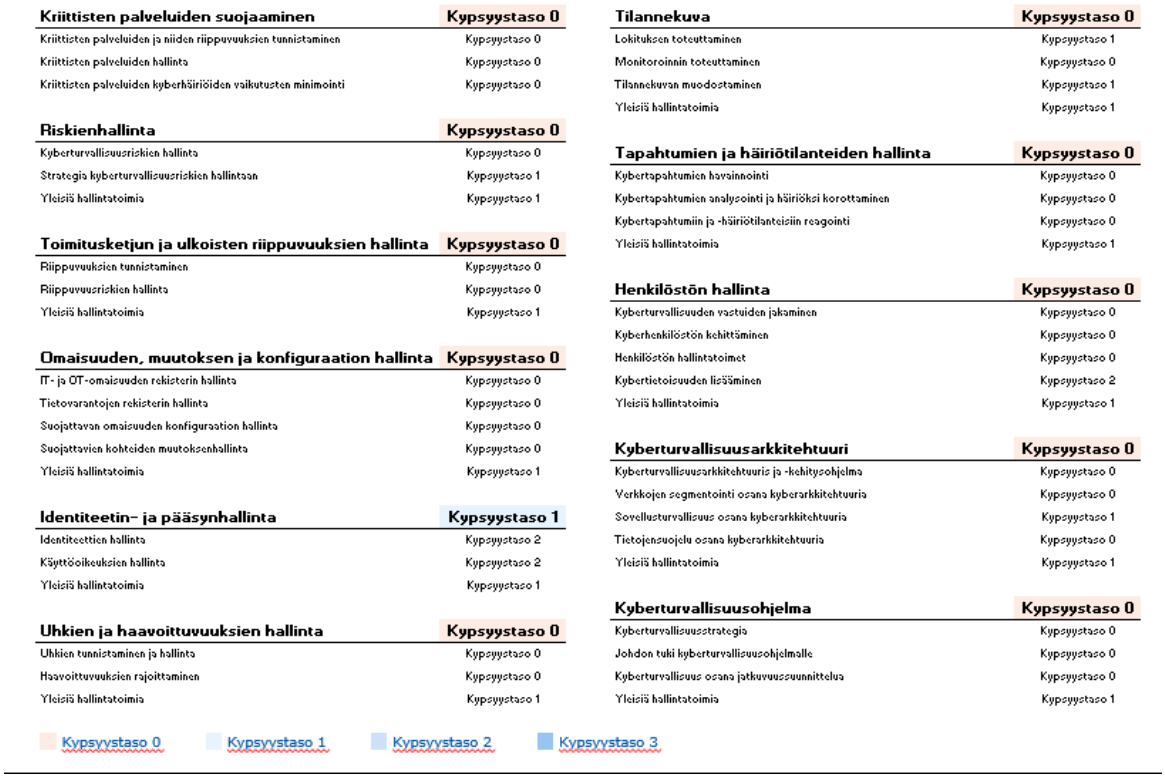
Kuvio 6 Kohdeorganisaation kyberturvallisuuden kypsyys NIST

Kybermittarin tulokset esitetään myös eri osioden mukaisesti (kuvio 7). Kohdeorganisaatiossa pääsyn hallinta oli tasolla 1, muut osa-alueet (Kriittiset palvelut, riskienhallinta, toimitusketjujen ja ulkoisten riippuvuuksien hallinta, laitteet ja tieto, kyberuhat, tilannekuva, kyberhäiriöt, henkilöstö, kyberarkkitehtuuri, kehitysohjelma) kypsyystasolla 0.



Kuvio 7 Kohdeorganisaation kyberturvallisuuden kypsyystaso osioiden mukaisesti

Kuviossa 8 esitetään kypsyystason osioiden lisäksi niiden alaosioita. Kuvion 8 kypsyystasot ovat vastaavat, kuin kuviossa 7, mutta alaosioiden mukaan tuominen hieman helpottaa yksityiskohtien tarkastelua. Tarkastelun perusteella kohdeyritys on saanut useammassa alaosion osassa pisteitä Kybermittarissa, mutta kypsyystason kokonaisuus jää osiossa silti tasolle 0.



Kuvio 8 Kohdeorganisaation kyberturvallisuuden kypsyystaso osiot ja alaosiot

5 Johtopäätökset

Kyberturvallisuuden lähtötilanteesta saatiin tietoa kehittämistyön aikana haastatteluilla, havainnoinnilla ja kybermittarilla. Haastatteluilla saatiin hyvää yleistietoa työntekijöiden työtehtävistä ja vastuista yrityksessä. Haastattelukysymyksillä saatiin selvitettyä myös työntekijöiden tietoisuutta ja kiinnostusta kyberturvallisuusasioista. Havainnoinnilla haettiin vahvistusta, toimivatko työntekijät tehtävissään kerrotulla tavalla ja millainen työympäristö on kyberturvallisuuden näkökulmasta. Kybermittarin avulla selvitettiin kohdeorganisaation kyberturvallisuuden nykytilaa.

Haastatteluiden tulosten perusteella henkilöstöllä on jo jonkin verran tietämystä kyberturvallisuuden yleisistä asioista ja osa on kohdannut yleisiä kyberturvallisuushäiriöitä työssä tai vapaa-ajalla. Tulosten perusteella henkilöstöllä ja yrityksen johdolla on myös halua kehittää osaamistaan kyberturvallisuusasioissa ja yleisesti keskustelua kyberturvallisuusasioista toivotaan enemmän. Kyberturvallisuuden tasoa voidaan nostaa lisäämällä keskustelua näistä asioista ja liittämällä kyberturvallisuusaihe myös säännöllisiin yrityksen henkilöstöpalavereihin.

Havainnointien yhteydessä kävi ilmi, että ulkopuolisella on helppo pääsy yrityksen tiloihin. Tämä ei kuitenkaan aiheuttanut kyber- tai tietoturvallisuuden kannalta ongelmia, koska

välittömästi tiloihin pääsyn jälkeen kohtasi yrityksen toimihenkilön. Haastatteluissa osa toimihenkilöistä kertoi säilyttävänsä salasanoja paperilapuilla työpisteellään, mutta havainnointien yhteydessä näitä lappuja ei näkynyt, jolloin kyberturvallisuus on korkeammalla tasolla.

Käytin kybermittaria ensimmäistä kertaa, eikä kohdeorganisaatiossakaan ollut siitä aiempaa kokemusta. Mittarin tulokset yleisellä tasolla antavat heikon kuvan kyberturvallisuuden hallinnasta, vaikka jotain torjuntatoimenpiteitä on toteutettu kohdeorganisaatiossa. Yritys toteuttaa monelta osin riskienhallintaa ja tekee kyberturvallisuuden kannalta ennalta estäviä toimia. Kybermittarin välilehtikohtaisessa tarkastelussa hallintatoimet vaikuttavat kattavilta, mutta Kybermittarin raportointiosio antaa kuitenkin kypsyystasoksi 0. Yrityksen kannattakin keskittyä tarkastelemaan Kybermittarin eri osioiden sisältöä raportoinnin tuloksen sijaan ja näin tunnistaa heille keskeisimmät kehityskohteet. Paras tieto kyberturvallisuuden nykytilasta saatiin haastatteluiden perusteella, kybermittarin ja havainnoinnin tukiessa tätä. Voidaan myös todeta, että kyseisen yrityksen kyberturvallisuuden nykytila kannattaa vastaisuudessa todeta jollakin muulla keinolla kuin kybermittarilla.

Kohdeyrityksen nykytilan selvityksen aikana selvisi, että kohdeorganisaatiolta puuttuu tietoturvaohjeistus. Tämän opinnäytetyön myötä HNR-Konepajalle laadittiin sellainen. Opinnäytetyön aikana kerätty ja työssä esitelty tieto toimivat pohjana ohjeistuksen laadinnassa. Toimitusjohtajan kanssa käydyn keskustelun perusteella ohjeesta haluttiin hyvin kompakti, helposti ymmärrettävä ja yrityksen tarpeet täyttävä.

Tietoturvaohjeistus määrittää kohdeorganisaation tavoitteen kyberturvallisuuden osalta. Yrityksessä tietoturvallisuus kuuluu kaikille työntekijöille ja sillä tavoitellaan tietojärjestelmien, tietoaineistojen ja palveluiden turvaamista, huomioiden luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit. Ohjeistus käsittelee yleisimpiä kyberuhkia (phishing, haittaohjelmat ja kiristyshaittaohjelmat) ja antaa suojautumiskeinoja niitä vastaan. Suojautumiskeinot on jaettu eri teemoihin lukemisen selkeyttämiseksi. Ohjeistuksen teemat suojautumiselle ovat: Tietokoneiden ja muiden päätelaitteiden turvallisuus, käyttäjätunnukset ja salasanat, toimitilojen turvallisuus ja tietoturvallinen työskentely. Perehtymällä ohjeistukseen ja noudattamalla siinä esitettyjä ehdotuksia, kohdeyrityksen työntekijöiden työskentely on jatkossa tietoturvallisempaa. Esittelin ohjeistuksen yrityksen toimihenkilöille 24.4.2023 yrityksen viikkopalaverissa ja se on toimitettu kohdeyritykselle sekä tämän opinnäytetyön liitteenä. (Liite 2)

6 Pohdinta

Aloitin työn tekemisen jo vuonna 2021 ja prosessin aikana oli pidempiä ajanjaksoja, jolloin en edistänyt työtä lainkaan. Tämä toi opinnäytetyöprosessille haasteita, koska aiemmalla

kerralla kirjoitetut asiat olivat jo poistuneet mielestä ja niiden muistamiseksi täytyi aina palata alkuun. Suurimmat haasteet kohtasin aikataulutuksen kanssa, koska tein opinnäytetyötä työni ohella. Yhteistyö toimeksiantajan kanssa oli mutkatonta koko opinnäytetyön tekemisen ajan ja vaikka alkuperäinen aikataulu venyi suunnitellusta aika paljonkin, yhteistyö oli helppoa. Tiedonhankinnan järjestäminen sujui suunnitelmien mukaan ja toimihenkilöiltä löytyi hyvin aikaa haastatteluja varten omien töidensä lomassa.

Opinnäytetyön tiedonhankintamenetelmät olivat pääasiassa onnistuneita, tosin Kybermittarin toteuttaminen vei varsin paljon aikaa ja kyberturvallisuuden nykytila jäi pelkästään sen avulla ilmaistuna epäselväksi. Kybermittarin käyttö oli hyvän ohjeistuksen takia aika helppoa, mutta osa kysymyksistä oli selkeästi suunnattu organisaatioille, jotka toimivat kyberturvallisuuden kannalta kriittisellä alalla. Tämän takia kaikkiin Kybermittarin kysymyksiin ei saatu vastausta ja tämä näkyi myös sen tulosraportoinnissa. Kaikki yrityksen toimihenkilöt saatiin haastateltua ja haastateltavat vastasivat hyvin ennalta määritettyihin kysymyksiin. Lisäksi haastateltavat osoittivat kiinnostusta kyberturvallisuutta kohtaan ja osa oli jo kohdannut yleisiä kyberuhkia työssään tai vapaa-aikana. Havainnoinnin tuottama lisäarvo opinnäytetyölle oli aika pieni. Havainnointikertoja oli kolme ja jälkikäteen tarkasteltuna niitä olisi voinut olla kaksinkertainen määrä. Kolmen havainnointikerran havainnot olivat keskenään aika samankaltaisia ja kyberturvallisuutta vaarantavia tapahtumia ei havaittu. Havainnointia olisi voinut myös tarkentaa hieman ja pyrkiä saamaan yksityiskohtaisempia havaintoja henkilöiden tietokoneiden ja päätelaitteiden käytöstä. Lisäämällä havainnointikertoja ja tarkentamalla havaintoja, olisi voitu saavuttaa enemmän toisistaan poikkeavia havaintoja.

Menetelmät sopivat tämän opinnäytetyön tiedonhankintamenetelmiksi hyvin, koska yhdessä ne antoivat tietoa yrityksen kyberturvallisuuden nykytilasta ja menetelmillä kerättyä tietoa voitiin ja voidaan käyttää kyberturvallisuuden tilan kehittämiseen tulevaisuudessa. Opinnäytetyöprosessi kokonaisuutena paransi kyber- ja tietoturvatasoa kohdeyrityksessä, koska nämä asiat nostettiin moneen kertaan esille tiedonhankintatapahtumien yhteydessä. Lisäksi valmiiseen opinnäytetyöhön ja opinnäytetyön osana syntyneeseen tietoturvaohjeistukseen perehtymällä yrityksen kyberturvallisuutta voidaan jatkossa huomioida paremmin päivittäisen liiketoiminnan yhteydessä.

Tietoturvaohjeistuksesta tuli kompakti, kuten oli tavoitteenakin. Ohjeistuksessa keskitytään tietoturvallisuuden perusasioihin, jotka ovat helposti ymmärrettäviä. Rajaamisen kanssa oli hieman haasteita, koska täysin tietoturvallinen työskentely vaatisi erittäin monta huomioitavaa asiaa ja niiden kirjaaminen kompaktiin ohjeistukseen ei ole mahdollista. Ohjeistusta on myös mahdollista päivittää tulevaisuudessa kohdeyrityksessä ja räätälöidä siitä vielä sopivampi.

Jatkossa vastaavan nykytilan selvityksen voisi tehdä huomattavasti kevennetyllä versiolla kybermittarista. Jatkotutkimuksen aiheena olisi sopivan menetelmän löytäminen pk-yrityksen kyberturvallisuuden auditoimiseksi tapauksessa, jossa yritys ei toimi kyberturvallisuuden näkökulmasta kriittisellä alalla.

Lähteet

Painetut

Hirsjärvi S., Remes, P., & Sajavaara, P. 2009. Tutki ja kirjoita. 15. painos. Jyväskylä: Tammi

Järvinen P. & Rousku K. 2017. Työpaikan tietoturvaopas. Liettua: Balto Print

Ojasalo, K. Moilanen, T. & Ritalahti, J. 2014. Kehittämistyön menetelmät: uudenlaista osaamista liiketoimintaan. 3. painos. Helsinki: Sanoma pro.

Rousku K. 2014. Kyberturvaopas. Tietoturvaa kotona ja työpaikalla. Viro: Print Best

Sähköiset

Department of Energy. 2021. Viitattu 1.11.2021 https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

European Union Agency for Cybersecurity. 2021. Viitattu 5.1.2022. https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape-2020

Helsingin seudun kauppakamari. Yrityksiin kohdistuvat kyberuhat 2019. https://helsinki.chamber.fi/wp-content/uploads/2020/01/yrityksiin-kohdistuvat-kyberuhat-2019.pdf . Viitattu 4.11.2021

Juvonen M., Koskensyrjä M., Kuhanen, L. Ojala V., Pentti A., Porvari P., Talala T. 2014. Yrityksen riskienhallinta. Helsinki. Finanssi- ja vakuutuskustannus Oy. E-kirja.

Järvinen P. 2022. Yrityksen tietoturvaopas. Viro: Meedia Zone OU. E-kirja.

Kauppakamari. Yritykset kokevat tietojenkalastelun ja haittaohjelmat suurimpina kyberuhkina. https://www.sttinfo.fi/tiedote/yritykset-kokevat-tietojenkalastelun-ja-haittaohjelmat-suurimpina-kyberuhkina?publisherId=26487429&releaseId=69957554 Viitattu 1.4.2023

Kyberturvallisuuden sanasto. 2018. Turvallisuuskomitea. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf. Viitattu 1.11.2021

Limnéll, J., Majewski, K. & Salminen M. 2014. Kyberturvallisuus. Jyväskylä:Docendo. E-kirja

SFS-EN-ISO/IEC 27001.2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Viitattu 8.12.2021

SFS-ISO 31000. 2018. Riskienhallinta. Ohjeet. Viitattu 8.12.2021.

SFS-EN 9001. 2015. Laadunhallintajärjestelmät. Vaatimukset. Viitattu 1.11.2021

Traficom. 2021. Pienyritysten kyberturvallisuusopas. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

Traficom. 2021. Kybermittari. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari

Traficom. 2021. Kybermittarin käyttöohje. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_K%C3%A4ytt%C3%B6ohje_V1.pdf

Traficom. 2023. Kybermittarin esittely. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_esittely_v1.pdf

Julkaisemattomat

Verkkokoulutus Kybermittarin käytöstä. Traficom Kyberturvallisuuskeskus. Kesäkuu 2021.

Kuviot

Taulukot

Liitteet

Liite 1: Haastattelukysymykset

Puolistrukturoidut haastattelut toteutettiin 11.10.-30.11.2021 vierailemalla sovitusti kohdeyrityksessä. Toimitusjohtaja haastateltiin kaksi kertaa, jossa ensimmäisellä kerralla kerättiin yleistietoa yrityksestä:

- liikevaihto ja historia
- työntekijöiden lukumäärä ja toimenkuvat
- tyypilliset työt ja asiakaskunta
- asiakkaiden hankinta
- toimitusjohtajan oma tausta (koulutus, kurssit)
- arvio omasta kyberturvallisuuden osaamisesta
- yrityksen tietotekniset laitteet ja niiden käyttö
- arvio henkilöstön kyberturvallisuuden osaamisesta
- henkilöstön koulutus ja perehtyminen kyberturva-asioihin
- kyberturvallisuuden uhkat ja poikkeamat historiasta

Toimitusjohtajan ensimmäisellä haastattelulla saatiin tietoa edellä listatuista asioista ja tätä tietoa käytettiin osaltaan luotaessa kysymyksiä toimihenkilöiden haastatteluihin.

Haastattelukysymykset toimihenkilöille:

Yleiset tiedot:

- Kuinka kauan olet työskennellyt yrityksessä?
  Työskentelyhistoria kertoo, miten hyvin henkilö tuntee tai hänen pitäisi tuntea yrityksen toimintakulttuuri ja muut työntekijät. Pitkä työhistoria voi kertoa ammattitaidosta, hyvästä tuntemuksesta, mutta se voi myös johtaa myös rutiineihin, joita on tehty jo hyvin pitkään ja tämän kautta asioita ei ajatella yhtä kriittisesti, joka voi johtaa huolimattomuuteen ja mahdollisesti turvallisuuden laiminlyöntiin.

- Mitkä ovat tyypilliset työtehtäväsi?
  Työtehtävät kertovat, millaista henkilön työ on ja millaisia laitteita hän käyttää. Puolistrukturoidussa haastattelussa tämä on oleellinen tieto jatkokysymysten kannalta. Jos henkilön työtehtäviin ei kuulu esim. palkanmaksu, ei tästä tarvitse kysellä lisää haastattelussa.

- Mikä on koulutuksesi?
  Koulutus ja sen suoritusajankohta kertoo paljon henkilön valmiuksista. Esimerkiksi viimeisen kymmenen vuoden sisällä suoritettu insinöörintutkinto antaa varmasti

valmiuksia tietoteknisten laitteiden käyttöön ja koulutuksessa on todennäköisesti käsitelty myös tietoturvaan liittyviä asioita.

- Oletko koulutuksen lisäksi suorittanut ammattitaitoa tukevia ja edistäviä kursseja?
  Muut kurssit ja koulutukset ovat hyödyksi ammattitaidolle, mutta myös yleissivistykselle. Hiljattain käydyillä kursseilla todennäköisesti on käytetty edelleen ajankohtaisia tietoteknisiä laitteita ja palveluita. Lisäksi kursseilla on voitu sivuta myös kyberturvallisuuteen tai riskienhallintaan liittyviä asioita.

- Aiemmat tehtävät muissa organisaatioissa?
  Selvitys aiemmista työtehtävistä muissa organisaatioissa kertovat mahdollisesta aiemmasta osaamisesta kyberturvallisuusasioista ja kokemuksista toisen organisaation tavasta työskennellä. Näitä taitoja voi hyödyntää nykyisessä työpaikassa.

- Mikä on oma arviosi kyberturvallisuusosaamisestasi? Asteikko 1-5, jossa on 1 on heikko ja 5 kiitettävä. Perustele vastaus lyhyesti. (laitteet, kirjautuminen palveluihin, tietoturva, virustorjunta, laitteiden käsittely, tietämys riskeistä)
  Oma arvio osaamisesta on tärkeä tieto kehittämisen kannalta. Lisäksi arviota voidaan verrata haastattelussa muuten saatuun materiaaliin ja katsoa kohtaavatko ne.

- Millaisia tietoteknisiä laitteita käytät työssäsi?
  Laitteiden käyttö määrittää, millaisia kyberriskejä työntekijään kohdistuu niiden välityksellä. Laitteiden käytön hyvä hallintaa pienentää riskejä merkittävästi.

- Onko laitteet päivitetty?
  Päivitykset ovat tärkeät kyberturvallisuuden kannalta. Käyttäjän tulee olla tietoinen laitteidensa päivityksen tilasta.

- Miten käytät laitteita toimistolla ja kotona (etätyö)? Onko jollain muulla mahdollista päästä käyttämään laitetta?
  Laitteiden oikea käyttö on olennaista tavoiteltaessa hyvää kyberturvallisuutta. Etätyössä ympäristö on erilainen ja riskit poikkeavat työpaikan olosuhteista. On tärkeää huolehtia, että varsinkin etätyössä muut mahdollisesti samassa tilassa olevat eivät pääse käyttämään laitteita.

- Miten käsittelet paperimateriaalia?
  Kriittistä, tärkeää ja salaista materiaalia esiintyy myös paperimuodossa monissa organisaatioissa. Myös tämän materiaalin oikea käsittely lisää kyberturvallisuutta. Materiaalin päätyminen ulkopuoliselle voi aiheuttaa ongelmia verkkomaailmassa.

Esimerkiksi salasanat ja käyttäjätunnukset paperilla ja asiakkaiden luottamukselliset tiedot.

- Onko salasanoja näkyvillä esim. paperilla?
  Salasanojen esillä pitäminen kertoo kyberturvallisuuden laiminlyönnistä. Salasanojen joutuessa toisen käsiin, hänellä voi olla pääsy luottamukselliseen tietoon tai hän voi aiheuttaa haittaa yrityksen toiminnalla.

Termit:

- Mitä kyberturvallisuus mielestäsi tarkoittaa?
  Halutaan selvittää haastateltavalta mitä keskeinen termi tarkoittaa. Termin tunnistaminen ja laaja kuvailu kertoo hyvästä perehtyneisyydestä. Jos koko sana on vieras, tietämys ei ole kovin korkealla tasolla.

- Phishing?
  Tärkeä termi. Kysymystä voidaan helpottaa kertomalla haastateltavalle termin suomenkielinen versio ”tietojenkalastelu”. Termin oikeaoppinen kuvailu kertoo, että haastateltava on tietoinen ilmiöstä.

- Haittaohjelma?
  Tärkeä termi. Yleinen kyberturvallisuuden riski. Termin oikeaoppinen kuvailu kertoo, että haastateltava on tietoinen ilmiöstä.

- Kiristyshaittaohjelma?
  Tärkeä termi. Yleinen kyberturvallisuuden riski. Termin oikeaoppinen kuvailu kertoo, että haastateltava on tietoinen ilmiöstä.

- Palvelunestohyökkäys?
  Tärkeä termi. Yleinen kyberturvallisuuden riski. Termin kuvailu kertoo, että haastateltava on tietoinen ilmiöstä.

- Toimitusjohtajapetos? CEO-fraud?
  Tärkeä termi. Yleinen kyberturvallisuuden riski. Termin kuvailu kertoo, että haastateltava on tietoinen ilmiöstä.

- Tunnistatko suojatun verkkoyhteyden?
  Suojattu verkkoyhteys on tärkeää tunnistaa hyvän kyberturvallisuuden kannalta. Jos haastateltava osaa kuvata, millainen suojattu verkkoyhteys on ja kertoa asiasta

enemmän, hän on keskimääräistä tietoisempi riskeistä ja selkeästi huolellinen käyttäessään eri verkkosivustoja.

Häiriöt:

- Onko työtehtävissäsi tullut vastaan kyberturvallisuutta uhkaavaa häiriöitä? Entä aiemmissa työpaikoissa?
  Aiemmat kokemukset kyberhäiriöistä auttavat muistamaan, miten tilanteessa toimittiin ja mitä siitä opittiin.

- Onko työasemallasi ollut viruksia tai muita haittaohjelmia? Jos on ollut, miten toimittiin?
  Virusten ja haittaohjelmien avulla rikollinen toimija haluaa saada vahinkoa aikaiseksi kohteelle. Tavoitteena on usein tiedostojen tuhoaminen tai koneen käyttäjän tietojen haltuun saaminen.

- Oletko saanut epämääräisiä sähköposteja?
  Monet phishing-viestejä jakavat tahot lähestyvät kohdetta sähköpostilla. Tavoitteena on saada kohde jakamaan arkaluonteista tietoja, kuten pankkitunnuksia.

- Oletko saanut puheluita ATK-tuesta? Onko joku halunnut tehdä etänä asennuksia koneellesi?
  ATK-tuen puhelut ovat yleinen huijaustapa, jossa rikollinen toimija haluaa tehdä asennuksia huijattavan koneelle ja saada koneella olevaa tietoa haltuunsa.

- Onko sosiaalisessa mediassa tullut epäilyttäviä lähestymisyrityksiä?
  Myös sosiaalisen median välityksellä liikkuu suuri määrä erilaisia huijauskampanjoita. *Suuri osa on ns. yleisiä phishing-tyyppisiä kampanjoita, joissa kohdetta yritetään houkutella antamaan tietoja ja myöhemmin rahaa. Myös kohdennettuja huijauksia tapahtuu, jos henkilön tiedetään olevan tietyssä yrityksessä ja tietyssä asemassa ja tätä huijaamalla rikollinen toimija voisi hyötyä henkilön tiedoista.*

- Oletko antanut salasanaasi tai käyttäjätunnusta muiden käyttöön?
  Pitämällä salasanan ja käyttäjätunnuksen vain omassa tiedossa, vältytään useimmiten tilanteelta, jossa toinen henkilö pääsee kirjautumaan palveluun ja mahdollisesti aiheuttaa vahinkoa siellä.

- Onko sinulla eri salasanat eri palveluihin?
  Eri salasanat eri palveluihin lisäävät merkittävästi kyberturvallisuutta. Vaikka jonkin palvelun salasana päätyisi esim. tietomurrossa rikollisen toimijan haltuun, ei sen avulla päästä kirjautumaan kyseisen käyttäjän muihin palveluihin.

- Puhutaanko kyberasioista töissä? Tietoturva-asioista?
  Keskustelu kyberturvallisuudesta ja tietoturvallisuudesta työyhteisössä lisää tietämystä näistä asioista ja auttaa toimimaan oikein uhkatilanteessa.

- Miten toimit, jos saat epämääräisen s-postin tai lähestymisyrityksen?
  Jonkinlaisen toimintamallin hahmottaminen erityisessä tilanteessa auttaa käsittelemään uhkatilannetta ja parantaa kyberturvallisuutta.

- Haluaisitko ymmärtää kyberturvallisuudesta nykyistä enemmän?
  Kysymyksellä selvitetään henkilön motivaatiota kyberturvallisuusasioihin. Opinnäytetyön tekijän tavoite on lisätä henkilöstön tietämystä kyberturvallisuudesta.

Liite 2: Tietoturvaohjeistus

Tietoturvaohjeistus, HNR-konepaja Oy

Tavoite

Tietoturvallisuus HNR-Konepaja Oy:ssä kuuluu kaikille työntekijöille. Tietoturvallisuus on osa yrityksen riskienhallintaa, kokonaisturvallisuutta ja toiminnan laatua. Viime kädessä tietoturvallisuudesta vastaa yrityksen johto. Tietoturvallisuudella pyritään varmistamaan tietojärjestelmien, tietoaineistojen ja palveluiden turvaaminen huomioiden luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvät riskit.

Tietoturvaohjeistukseen on koottu keskeisimmät tietoturvallisuuden perusasiat, joiden avulla yrityksen työntekijöiden työskentely on tietoturvallista. Ohjeistus antaa käytännön tason ohjeita turvalliseen työskentelyyn. Tietoturvaohjeistus on osa HNR- Konepaja Oy:n riskienhallintaa.

Yleisimmät kyberuhat

Tietojenkalastelu eli phishing on kyberrikollisuuden muoto, jossa kohdetta lähestytään esim. lähettämällä aidon näköinen sähköpostiviesti, mutta tarkoituksena on huijata kohteelta tietoa tai rahaa, tai pyrkiä saamaan pääsy tietojärjestelmään. Tyypillisiä tietojenkalastelurikoksia ovat toimitusjohtajapetokset ja tietojenkalastelurikokset, joissa pyritään saamaan haltuun pankkitunnuksia. Kyseisiä rikoksia toteutetaan suurina massoina ja kohteeksi voi valikoitua kuka tahansa.

Haittaohjelmilla pyritään aiheuttamaan kohteen tietojärjestelmiin tai niiden osiin ei toivottuja tapahtumia. Rikoksen tekijän tavoitteena on useimmiten taloudellinen hyöty ja ohjelmia pyritäänkin saamaan kohteiden koneille anastamaan sieltä tietoja, kuten salasanoja ja pankkitunnuksia tai seuraamaan koneen käyttäjän toimintaa. Haittaohjelmia ovat virukset, troijalaiset, madot ja vakoiluohjelmat. Haittaohjelmien kohteeksi voi joutua kuka tahansa, useimmiten onnistuneet haittaohjelma-asennukset suoritetaan huonosti suojatuille kohteille.

Kiristyshaittaohjelma on kyberrikos, jossa kohteen koneelle asennetaan haittaohjelma, joka lukitsee koneen ja vaatii lunnaita sen avaamiseksi. Rikollinen taho lupaa usein avata koneen ja tiedostojen lukituksen, kun rikollisille maksetaan tietty summa. Kiristyshaittaohjelmien asentajien motiivina on taloudellinen hyöty. Kuka tahansa voi joutua kiristyshaittaohjelmien kohteeksi. Helppo kohde rikollisille ovat käyttäjät, jotka eivät ole varautuneet kyberhyökkäyksiin.

Suojautuminen yleisimmiltä kyberuhkilta

Digitaalinen maailma muuttuu jatkuvasti ja sen myötä myös uusia uhkia nousee koko ajan esiin rikollisten muuttaessa toimintatapojaan. Valtaosaan uhkista voidaan varautua ja suojautua pitämällä huolen perusosaamisesta kyberturvallisuusasioissa. Uhkat voivat konkretisoitua tietoverkkojen välityksellä suoraan, tai esimerkiksi siten, että vihamielinen taho saa fyysisesti haltuunsa yrityksen luottamuksellista tietoa ja käyttää sitä myöhemmin hyväkseen verkkorikollisuudessa.

Yleisimmiltä kyberuhkilta suojautuminen vaatii huolehtimista seuraavista asioista:

Tietokoneet ja muut päätelaitteet

- päivitä käyttöjärjestelmät (automaattinen päivitys)
- päivitä ohjelmistot (automaattinen päivitys)

- ota tärkeimmistä tiedoista varmuuskopiot (automaattinen varmuuskopiointi)
- huolehdi, että koneille ja muille päätelaitteilla kirjaudutaan salasanalla

Käyttäjätunnukset ja salasanat

- luo jokaiselle käyttäjälle omat tilit järjestelmiin, ei yhteiskäyttötunnuksia palveluihin ja pääkäyttäjätunnus vain pääkäyttäjälle
- poista tunnukset käyttäjiltä, jotka eivät tarvitse pääsyä kyseiseen tietoon tai järjestelmään tai työntekijän työsuhde päättyy
- dokumentoi käyttöoikeudet ja päivitä dokumenttia säännöllisesti
- luo riittävän hyvät salasanat eri palveluihin
- älä luovuta salasanojasi muille
- vaihda salasana riittävän usein
- älä kirjoita salasanoja muistiin, jos kirjoitat, älä säilytä niitä paikassa, johon on helppo pääsy
- käytä töissä ja työn ulkopuolella eri salasanoja

Toimitilat

- huolehdi tilojen lukituksesta, kun ne jäävät tyhjilleen
- huolehdi hälytyksestä, jos poistut tiloista viimeisenä
- säilytä arkaluonteiset tiedot lukituissa kaapeissa
- hävitä arkaluonteinen materiaali, jota et tarvitse
- selvitä tiloissa liikkuvilta ulkopuolisilta, ketä he ovat ja miksi ovat tiloissa

Tietoturvallinen työskentely

- lukitse työasemasi, kun poistut sen luota
- älä lataa internetistä ohjelmia omalle koneellesi
- suhtaudu varauksella sähköposteihin, jotka sisältävät:
    1. pyyntöjä pikaisen tilisiirron tekemisestä
    2. pyyntöjä tai ohjeita tilitietojen päivittämisestä,
    3. pyyntöjä tai ohjeita tarkistaa jonkin palvelun kirjautumistiedot
    4. viesti tulee tuntemattomalta toimijalta ja sisältää liitteitä tai linkkejä
    5. viesti tulee ”tutulta” toimijalta, mutta rakenne tai kirjoitusasu poikkeaa aiemmista
- ilmoita tietoturvallisuutta koskevasta poikkeamasta viipymättä yrityksen johdolle