Tuukka Monto

EETTISEN HAKKEROINNIN VAIKUTUKSET TIETOJÄRJESTELMÄN TIETOTURVAN KEHITYKSESSÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Monto, Tuukka
Eettisen hakkeroinnin vaikutukset tietojärjestelmän tietoturvan kehityksessä
Jyväskylä: Jyväskylän yliopisto, 2023, 31 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Saastamoinen, Anna

Lähes kaikki liiketoiminta organisaatioissa tapahtuu käyttämällä erilaisia tietojärjestelmiä. Järjestelmiin on tallennettuna organisaatioon ja sen toimintaan liittyviä tietoja, joita pyritään suojelemaan hyvän tietoturvan avulla. Tässä tutkielmassa käsitellään eettisen hakkeroinnin hyödyntämistä organisaation tietojärjestelmän tietoturvan kehityksessä, ja mitä hyötyjä ja haasteita siihen liittyy. Eettinen hakkerointi on tietojärjestelmän omistajan luvalla tapahtuvaa tietojärjestelmään tunkeutumista, jonka tarkoituksena on parantaa kyseisen järjestelmän tietoturvaa tunkeutumisen aikana tehtyjen havaintojen ja niiden perusteella laaditun raportin avulla. Eettinen hakkerointi eroaa rikollisesta hakkeroinnista siten, että järjestelmään tunkeutumiseen on lupa ja tunkeutumisen tarkoitus on kehittää tietoturvaa. Oikein käytettynä eettinen hakkerointi on tehokas työkalu havaitsemaan organisaation tietojärjestelmien tietoturvan heikkoja kohtia järjestelmän teknisestä toteutuksesta, kuten myös sen käyttämisestä ja käyttäjien toimintatavoista. Havaittuihin tietoturvan heikkoihin kohtiin esitetään parannusehdotuksia eettisen hakkeroinnin lopuksi laadittavassa raportissa. Eettisen hakkeroinnin hyödyntämiseen liittyy myös haasteita, joista organisaatioiden tulisi olla tietoisia ennen eettisen hakkeroinnin hyödyntämistä prosesseissaan. Tutkielma on toteutettu kuvailevana kirjallisuuskatsauksena.

Asiasanat: eettinen hakkerointi, tietoturva, tietoturvan kehittäminen

ABSTRACT

Monto, Tuukka
Effects of ethical hacking on the development of information system security
Jyväskylä: University of Jyväskylä, 2023, 31 pp.
Information Systems, Bachelor's Thesis
Supervisor: Saastamoinen, Anna

Almost all business in organisations is done using different information systems. These systems store information about the organisation and its activities, which is protected by good information security. This bachelor's thesis discusses the use of ethical hacking in the development of information security in an organisation's information system, and the benefits and challenges involved. Ethical hacking is an intrusion into an information system, with the permission of the owner of the information system, with the aim of improving the security of that system through observations made during the intrusion and the resulting report based on these observations. Ethical hacking differs from criminal hacking in that the intrusion is authorised and the purpose of the intrusion is to improve security. When used correctly, ethical hacking is a powerful tool for identifying security weaknesses in an organisation's information systems, from the technical implementation of the system, as well as from the way it is used and how users operate. At the end of the ethical hacking process, suggestions for improvement will be made to address the security weaknesses identified. There are also challenges to using ethical hacking, which organisations should be aware of before utilising ethical hacking in their processes. This bachelor's thesis has been carried out as a descriptive literature review.

Keywords: ethical hacking, information security, development of information security

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Whitmanin ja Mattordin (2013) mukaan viimeisten vuosikymmenten aikana tapahtunut teknologian kehitys on johtanut siihen, että lähes kaikessa liiketoiminnassa hyödynnetään teknologiaa. Yrityksen ja sen liiketoimintaan liittyvät tiedot tallennetaan tietojärjestelmiin, ja nämä tiedot ovat usein yrityksen arvokkainta omaisuutta (Whitman & Mattord, 2013, s. 2). Thomas, Burmeister ja Low (2018) toteavat, että tietojärjestelmät, joiden kautta hallitaan arvokasta dataa tai reaalimaailman kohteita, voivat houkutella kyberrikollisia tekemään murto- tai kaappausyrityksiä. Rikolliset hakkerit murtautuvat tietojärjestelmään tai -verkkoon ja pyrkivät sitä kautta saavuttamaan hyötyä itselleen tai edustamalleen järjestölle (Thomas, Burmeister & Low, 2018).

Tietojärjestelmiin voidaan tunkeutua esimerkiksi järjestelmän teknisiä haavoittuvuuksia hyödyntämällä, tai varastamalla tai huijaamalla järjestelmän käyttäjiltä heidän tunnuksensa järjestelmän käyttöön (Applegate, 2009). Näitä tietomurtoja voidaan ehkäistä esimerkiksi korjaamalla tietojärjestelmien teknisiä haavoittuvuuksia, ja panostamalla käyttäjien tietoturvallisiin toimintatapoihin (Cabrera, Reyes & Lasco, 2020).

Verizonin (2022) suorittaman tutkimuksen mukaan vuonna 2021 heille raportoiduista 5212 tietomurroista 47 %:iin liittyi varastettujen tunnuksien hyödyntäminen, 18 % tapauksista puolestaan liittyi käyttäjän manipulaatiota, ja 10 % tapauksista liittyi järjestelmän teknisten haavoittuvuuksien hyödyntämistä. Huomioitavaa on myös se, että yksittäisen ihmisen toiminta vaikutti jollain tapaa 82 % tietomurroista (Verizon, 2022).

Thomas ja kumppanit (2018) toteavat, että panostamalla järjestelmien tietoturvaan pystytään ehkäisemään järjestelmässä liikkuvan tiedon vuotamista järjestelmän ulkopuolelle. Eettinen hakkerointi on järjestelmän omistajan kanssa yhteisymmärryksessä tapahtuvaa järjestelmään tunkeutumista (Thomas ym., 2018). Palmerin (2001) mukaan eettisen hakkeroinnin tarkoituksena on testata järjestelmän turvallisuutta käyttämällä samoja tunkeutumismenetelmiä kuin rikolliset hakkeritkin käyttävät. Erona toiminnassa on se, ettei eettisen hakkeroinnin aikana vahingoiteta järjestelmää tai varasteta tietoja, vaan pyritään havaintojen ja palautteen avulla parantamaan järjestelmän tietoturvaa (Palmer, 2001).

Tässä tutkielmassa käsitellään sitä, miten eettistä hakkerointia voidaan hyödyntää toimialasta riippumatta organisaation tietojärjestelmien tietoturvan parantamisessa, ja minkälaisia vaikutuksia eettisen hakkeroinnin menetelmillä on mahdollista saada organisaation tietojärjestelmien tietoturvaan. Tutkielmassa vastataan seuraavaan tutkimuskysymykseen:

- Miten eettisen hakkeroinnin avulla voidaan parantaa organisaation tietojärjestelmien tietoturvaa, ja mitä haasteita siihen liittyy?

Tutkielma on toteutettu kuvailevana kirjallisuuskatsauksena. Lähteitä on etsitty JYKDOK-tietokannan ja Google Scholar -palvelun kautta. Lähteiden etsinnässä käytettiin muun muassa seuraavia hakusanoja ja niiden yhdistelmiä: *ethical hacking, penetration testing, social engineering, information security* ja *information security development*. Lisäksi lähteiden etsinnässä on hyödynnetty keskeisten julkaisujen lähdeluetteloita. Lähteiksi on valittu ensisijaisesti vertaisarvioituja julkaisuja.

Tämä tutkielma koostuu viidestä luvusta, joista ensimmäinen on johdanto. Toinen luku käsittelee hakkerointia ja eettistä hakkerointia, ja luvussa käydään läpi, mikä tekee hakkeroinnista eettistä, sekä esitellään lyhyesti kirjallisuudessa esiintyviä eettisen hakkeroinnin menetelmiä. Kolmannessa luvussa käsitellään tietojärjestelmien tietoturvaa organisaatioissa. Luvussa määritellään lyhyesti tietojärjestelmä ja tietoturva, minkä jälkeen käsitellään tarkemmin eri osa-alueita, joista organisaation tietojärjestelmän tietoturva koostuu. Lisäksi tarkastellaan sitä, mistä eri osa-alueet koostuvat ja miten ne vaikuttavat organisaation tietoturvan kokonaisuuteen. Neljännessä luvussa tarkastellaan sitä, miten eettistä hakkerointia voidaan hyödyntää organisaation tietojärjestelmien tietoturvan kehityksessä, ja mitä vaikutuksia sillä voidaan saavuttaa. Luvussa käsitellään eettisen hakkeroinnin eri menetelmien avulla saatavia hyötyjä ja haasteita organisaation tietojärjestelmän tietoturvan eri osa-alueisiin, ja miten eettisen hakkeroinnin menetelmiä käytetään yhdessä muiden menetelmien kanssa tietoturvaa kehittäessä. Viimeinen luku on yhteenveto, jossa kerrataan tutkielman tavoitteet ja esitellään kirjallisuudesta löydetyt keskeisimmät tulokset.

Tutkielmassa havaittiin, että eettisen hakkeroinnin keinoilla on mahdollista havaita tietoturvan puutteita organisaation tietojärjestelmän teknisistä ratkaisuista, järjestelmän käyttämisestä organisaatiossa sekä käyttäjien toimintatavoista. Havaittuihin puutteisiin esitetään korjausehdotuksia, jotka voivat liittyä esimerkiksi teknisiin ratkaisuihin, järjestelmän asetusten määrittelyyn tai henkilöstön koulutuksessa huomioitaviin asioihin. Eettisen hakkeroinnin hyödyntämiseen liittyy myös haasteita, jotka on hyvä tiedostaa organisaatiossa. Haasteena voi olla esimerkiksi se, ettei organisaatiossa haluta päästää ulkopuolista testaamaan kriittisten tai arkaluonteisten järjestelmän osien tietoturvaa, jolloin kyseisistä osista ei löydetä ja korjata mahdollisia haavoittuvuuksia. Tällöin mahdolliset haavoittuvuudet jäävät rikollisten hakkereiden hyödynnettäviksi.

2 HAKKEROINTI JA EETTINEN HAKKEROINTI

Thomasin ja kumppaneiden (2018) mukaan termi "hakkeri" sai alkunsa 1960-luvulla, jolloin se tarkoitti taitavaa teknologian käyttäjää. Nykyään hakkerit jaetaan kolmeen kategoriaan heidän tarkoitusperiensä mukaan: musta-, harmaa- ja valkohattuhakkereihin. Hakkerit ovat edelleen taitavia teknologian käyttäjiä, mutta hakkerointiin kuuluu nykyään lisäksi myös ihmisten manipulointi, josta käytetään termiä sosiaalinen manipulaatio (Thomas ym., 2018). Tässä luvussa määritellään kategoriat, joihin hakkerit jaetaan, sekä esitellään lyhyesti hakkereiden käyttämiä menetelmiä. Musta- ja harmaahattuhakkereista käytetään tässä tutkielmassa nimitystä rikollinen hakkeri.

2.1 Mustahattuhakkerointi ja harmaahattuhakkerointi

Mustahattuhakkerit tunkeutuvat laittomasti järjestelmään ilman lupaa, tarkoituksenaan aiheuttaa haittaa kohdejärjestelmälle ja sen omistajalle, tai saada jonkinlaista henkilökohtaista hyötyä tunkeutumisen seurauksena, esimerkiksi informaatiota tai rahaa (Hatfield, 2019). Thomasin ja kumppaneiden (2018) mukaan mustahattuhakkereista käytetään myös nimitystä pahantahtoinen hakkeri. Mustahattuhakkerit ovat tunnetuin hakkereiden kategoria, sillä mediassa esiintyvät hakkerit ovat useimmiten mustahattuhakkereita (Thomas ym., 2018).

Harmaahattuhakkerit tunkeutuvat myös laittomasti järjestelmään, mutta heidän tarkoitusperänsä eivät ole täysin pahantahtoiset (Hatfield, 2019). Thomasin ja kumppaneiden (2018) mukaan harmaahattuhakkerit voivat etsiä haavoittuvuuksia kohdejärjestelmästä ilman lupaa järjestelmän omistajalta, ja sitten huomauttaa järjestelmän omistajaa löytämistään haavoittuvuuksista. Valtioiden palkkaamia hakkereita voidaan pitää harmaahattuhakkereina esimerkiksi niissä tilanteissa, kun hakkerit suorittavat laittomia tunkeutumisia toisen maan järjestelmiin, tarkoituksena toimeksiantajan maan turvallisuuden parantaminen. Aktivistitoimintana suoritetut tunkeutumiset, esimerkiksi kohdeorganisaation

kotisivujen muuttamiseksi, lasketaan myös harmaahattuhakkeroinniksi (Thomas ym., 2018).

Hakkerit voivat hankkia pääsyn tietojärjestelmään etsimällä ja hyödyntämällä järjestelmässä olevia haavoittuvuuksia, tai varastamalla kirjautumistiedot järjestelmän käyttäjältä (Palmer, 2001). Haavoittuvuuksia etsitään esimerkiksi kokeilemalla tunnettujen haavoittuvuuksien hyödyntämistä, tai analysoimalla järjestelmän lähdekoodia, mikäli hakkerilla on siihen pääsy (Mudiyanselage & Pan, 2020). Kirjautumistiedot ja informaatio järjestelmästä voidaan hankkia sosiaalisen manipulaation avulla (Applegate, 2009). Mouton, Malan, Kimppa ja Venter (2015) toteavat, että sosiaalisen manipulaation tarkoitus on järjestelmän käyttäjien kanssa käydyn vuorovaikutuksen avulla saada tietoa, jota hyödyntäen voisi tunkeutua järjestelmään. Sosiaalinen manipulaatio pyrkii hyödyntämään ihmisessä olevia psykologisia haavoittuvaisuuksia, esimerkiksi tunteisiin vetoamalla, ja sitä kautta saamaan haluttua informaatiota (Mouton, Malan, Kimppa & Venter, 2015).

2.2 Valkohattuhakkerointi eli eettinen hakkerointi

Valkohattuhakkerit, eli eettiset hakkerit, käyttävät samoja työkaluja ja keinoja kuin musta- ja harmaahattuhakkerit (Thomas ym., 2018). Hatfieldin (2019) mukaan eettisten hakkereiden tarkoitus kohdejärjestelmään tunkeutuessa on parantaa järjestelmän tietoturvaa. Toiminta tapahtuu yhteisymmärryksessä järjestelmän omistajan kanssa, ja siitä on sovittu ennen tunkeutumisen aloittamista. Taulukossa 1 on koottuna hakkeroinnin eri kategoriat ja niiden keskeisimmät erot (Hatfield, 2019).

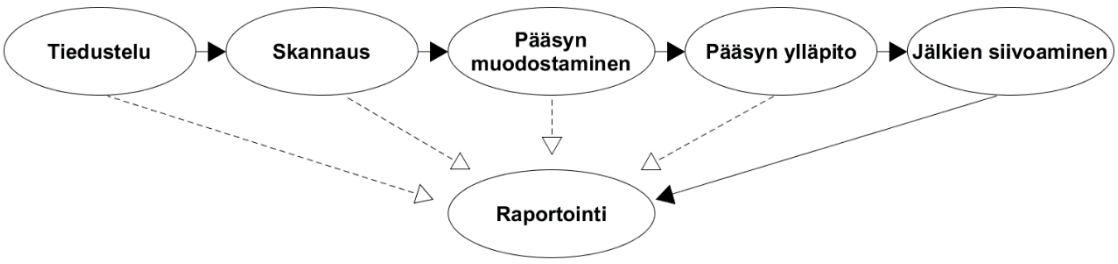
TAULUKKO 1 Hakkeroinnin kategoriat (Hatfield, 2019)

Hakkeroinnin kategoria	Lupa tunkeutumiseen	Pahantahtoiset tarkoitusperät
Mustahattuhakkerointi	Ei	Kyllä
Harmaahattuhakkerointi	Ei	Mahdollisesti
Valkohattuhakkerointi	Kyllä	Ei

Thomas ja kumppanit (2018) määrittelevät eettisen hakkeroinnin siten, että eettiset hakkerit testaavat tietojärjestelmien turvatoimia, ja varmistavat niiden tehokkuuden. Eettinen hakkeri etsii ja tunnistaa haavoittuvuuksia järjestelmästä, ja selvittää mitä vaikutuksia voisi seurata, jos rikollinen hakkeri hyödyntäisi näitä haavoittuvuuksia. Eettinen hakkeri kokoaa raportin löydetyistä haavoittuvuuksista, niiden vaikutuksista ja mahdollisista korjaustoimista, ja luovuttaa sen järjestelmän omistajalle. Eettinen hakkeri voi osoittaa luotettavuuttaan erilaisilla sertifikaateilla. Sertifikaatin hankkiminen ei ole vaatimus eettiselle hakkeroinnille, mutta se viestii asiakkaalle eettisen hakkerin luotettavuudesta. Sertifikaatit sisältävät toimintatapojen eettisiä ohjeistoja, mitkä sertifikaatin haltijan tulee hallita. Monet eri tietoturva-alan toimijat tarjoavat sertifikaatteja, mutta eri

toimijoiden tarjoamille sertifikaateille ei ole muodostunut täysin yhtenäistä linjaa sisällön ja vaatimusten suhteen (Thomas ym., 2018). Eettinen hakkerointi -termin alle kuuluvat kaikki hakkeroinnin keinot, jotka voivat esimerkiksi aiheuttaa jonkinasteista vahinkoa järjestelmään murtautuessa, mm. kaatamalla sivuston (Lorenzini, Shaw & Elger, 2022). Eettinen sosiaalinen manipulaatio on osa eettistä hakkerointia, ja sen avulla havaitaan tietoturvan heikkoja kohtia henkilöstöstä tai organisaation tietoturvakäytänteistä (Hatfield, 2019).

Lorenzinin ja kumppaneiden (2022) mukaan penetraatiotestaus on eettisen hakkeroinnin alakategoria, jossa käytetyt keinot ovat rajoitetumpia kuin eettisen hakkeroinnin keinot laajimmillaan. Se on tarkasti suunniteltu prosessi, jossa vaaditaan kaikki tarvittavat luvat järjestelmään tunkeutumisesta ja mahdollisista rajoituksista ennen testauksen aloittamista. (Lorenzini ym., 2022). Dalalana Bertoglion ja Zorzon (2017) mukaan penetraatiotestaus koostuu viidestä vaiheesta, joiden jälkeen muodostetaan raportti testauksen aikana tehdyistä havainnoista (kuvio 1). Ensimmäinen vaihe on tiedustelu, jonka aikana kohdejärjestelmästä hankitaan tietoa yleisellä tasolla ja mahdollisia haavoittuvuuksia kartoitetaan alustavasti. Toinen vaihe on skannaus, jonka aikana pyritään selvittämään järjestelmän etäkäyttömahdollisuuksia, käytössä olevia järjestelmiä, palomuurien sijainteja ja verkon rakennetta syvällisemmin kuin ensimmäisessä vaiheessa. Kolmas vaihe on tunkeutuminen eli pääsyn muodostaminen kohdejärjestelmään löydettyjen haavoittuvuuksien avulla. Neljäs vaihe on pääsyn ylläpito, jotta haavoittuvuuksien hyödyntämistä voidaan jatkaa tulevaisuudessa. Viimeinen vaihe on tunkeutumisen jättämien jälkien siivoaminen, jotta tunkeutumista ei havaittaisi. Penetraatiotestauksen tarkoitus on arvioida ja vähentää kohdejärjestelmän tietoturvariskejä. Penetraatiotestauksen aikana kohdejärjestelmään tunkeudutaan käyttäen samoja menetelmiä, joita rikolliset hakkerit käyttävät. Tällöin löydettyihin haavoittuvuuksiin voidaan kehittää asianmukaiset korjaustoimet, jotta hakkerit eivät pysty hyödyntämään kyseisiä haavoittuvuuksia (Dalalana Bertoglio & Zorzo, 2017).



KUVIO 1 Penetraatiotestauksen vaiheet (Dalalana Bertoglio & Zorzo, 2017)

Ding, De Jesus ja Janssen (2019), sekä Zhao, Laszka ja Grossklags (2017) toteavat, että haavoittuvuuspalkkio-ohjelma (engl. Bug Bounty Program), on yksi eettisen hakkeroinnin toteutustavoista. Organisaatio voi käynnistää haavoittuvuuspalkkio-ohjelman, jonka tarkoituksena on joukkoistaa tietoturvahaavoittuvuuksien löytäminen ja korjaaminen lukuisille (jopa tuhansille) organisaation ulkopuolisille eettisille hakkereille ja muille tietoturva-asiantuntijoille.

Haavoittuvuuspalkkio-ohjelma toimii siten, että eettinen hakkeri ilmoittaa organisaatiolle löytämistään haavoittuvuuksista, ja mahdollisesti myös korjausehdotuksista kyseiseen haavoittuvuuteen. Vahvistetuista raportoiduista haavoittuvuuksista ohjelman käynnistänyt organisaatio antaa palkkioksi rahaa tai mainetta. Palkkion saa se ilmoittaja, joka on ensimmäisenä löytänyt haavoittuvuuden ja esittänyt siihen toimivan korjausehdotuksen. Palkkiot riippuvat usein raportoidun haavoittuvuuden vakavuudesta, ja palkkion suuruuden määräytymisperusteet on kerrottu ohjelmassa (Ding, De Jesus & Janssen, 2019; Zhao, Laszka & Grossklags, 2017).

3 TIETOJÄRJESTELMÄN TIETOTURVA

Tässä luvussa käydään läpi tietojärjestelmän tietoturvaa, ja miten sitä toteutetaan organisaatioissa. Luku on jaettu kolmeen alalukuun, joista kahdessa ensimmäisessä käsitellään tietojärjestelmän ja tietoturvan määritelmiä. Kolmannessa alaluvussa käsitellään sitä, mitä eri osa-alueita organisaatioiden tietoturva sisältää, ja miten ne näkyvät organisaation toiminnassa.

3.1 Tietojärjestelmän määritelmä

Cabreran ja kumppaneiden (2020) mukaan tietojärjestelmä on tietotekniikan, ihmisten, ja liiketoiminnan prosesseja tukevien toimintojen yhdistelmä. Tietojärjestelmien tarkoitus on kerätä, tuottaa ja jakaa hyödyllistä dataa (Cabrera ym., 2020). Goyal ja Gupta (2020) lisäävät, että tietojärjestelmän tarkoitus on myös muodostaa käyttöliittymä ihmisten, prosessien, ja datan välille. Tietojärjestelmien avulla tuetaan liiketoiminnan prosesseja, johtamista ja päätöksentekoa jalostamalla ja hyödyntämällä dataa (Goyal & Gupta, 2020).

Goyalin ja Guptan (2020) mukaan tietojärjestelmä koostuu viidestä osasta: laitteistosta, ohjelmistosta, datasta, toimintaohjeista ja ihmisistä. Laitteisto käsittää tietotekniset laitteet, jotka ovat käsin kosketeltavissa tai nähtävissä. Ohjelmisto käsittää sen tietoteknisen osan, joka ohjaa laitteiston tai sovellusten toimintaa. Data käsittää merkkijonot, jotka ovat tallennettuina järjestelmään. Datasta tulee tietoa, kun se prosessoidaan ja esitetään muodossa, joka on esimerkiksi ihmisen luettavana tekstinä. Toimintaohjeet käsittävät sen, mitä toimintoja käyttäjät voivat suorittaa, ja miten he suorittavat ne. Ihmiset ovat tietojärjestelmän osa, jolle koko järjestelmä pyrkii tuottamaan hyödyllistä tietoa. Ihmiset ovat mukana myös tiedon tuottamisessa järjestelmän käytön kautta, sekä esimerkiksi järjestelmän huolto- ja kehitystoimenpiteissä (Goyal & Gupta, 2020).

3.2 Tietoturvan määritelmä

Lundgrenin ja Möllerin (2019) mukaan tietoturva voidaan määritellä kuvaamalla sitä, mitä tietoturvalla pyritään saavuttamaan. CIA-kolminaisuus (Confidentiality, Integrity, Availability), eli luottamuksellisuus, eheys, ja saatavuus ovat tiedon ominaisuuksia, jotka saavutetaan hyvän tietoturvan avulla. Luottamuksellisuus tarkoittaa sitä, että tieto on saatavilla vain niille toimijoille, joilla on lupa ja oikeus käsitellä sitä. Eheys tarkoittaa sitä, että tieto on paikkansapitävää ja kokonaista, eikä se saa muuttua tahattomasti, tai muutos pitää ainakin havaita. Saatavuus tarkoittaa sitä, että valtuutetut toimijat pääsevät tietoon käsiksi silloin kun sille on tarvetta (Lundgren & Möller, 2019).

Cabrera ja kumppanit (2020) puolestaan määrittelevät tietoturvan siten, että tietoturva on joukko käytänteitä, joiden avulla tietojärjestelmissä sijaitsevan tiedon luvaton käyttö, levitys, muuttaminen tai tuhoaminen estetään. CIA-kolminaisuus sisältää heidän määritelmässään tietoturvan ydinperiaatteet, mutta ydinperiaatteisiin voisi lisätä myös tiedon aidoksi todentamisen (engl. authenticity) ja kieltämättömyyden (engl. non-repudiation) (Cabrera ym., 2020).

Samonas & Coss (2014) puolestaan määrittelevät tietoturvan ydinperiaatteet siten, että tiedon aidoksi todentaminen ja kieltämättömyys ovat tärkeä osa tiedon eheyttä, mutta eivät erillisiä periaatteita. He nostavat eheyden ja saatavuuden yhteiseksi ominaisuudeksi järjestelmän tarkoituksenmukaisen määrittelyn, mikä liittyy tietoturvan sosiotekniseen näkökulmaan. Sosiotekninen näkökulma ottaa huomioon järjestelmien käyttäjät ja heidän muodostamansa potentiaaliset tietoturvariskit, tahalliset ja tahattomat. Järjestelmän tarkoituksenmukaisella määrittelyllä pyritään rajoittamaan käyttäjien ja järjestelmän eri osien oikeuksia siten, että CIA-kolminaisuutta ei pystyisi rikkomaan (Samonas & Coss, 2014).

3.3 Tietojärjestelmän tietoturva organisaatioissa

Cabreran ja kumppaneiden (2020) mukaan organisaatioissa tietoturvaa voidaan tarkastella neljältä eri näkökulmalta: tekniseltä, hallinnoinnin, kulttuurin ja talouden näkökulmalta.

- Tekninen näkökulma käsittää laitteistot ja ohjelmistot, joissa tieto on tallennettu, tai joilla tietoa käsitellään organisaatiossa.
- Hallinnoinnin näkökulma käsittää tiedon käsittelyyn liittyvät toiminnat ja toimintatavat organisaatiossa, sekä niiden valvomisen.
- Kulttuurin näkökulma käsittää inhimillisten ominaisuuksien vaikutukset organisaation tietoturvaan.
- Talouden näkökulma käsittää tietoturvaratkaisujen toteuttamisen vaikutukset organisaation talouteen (Cabrera ym., 2020).

Kalloniatis ja kumppanit (2014) toteavat, että organisaation tietojärjestelmien kokonaisuudella tulee olla tarkoituksenmukaiset turvatoimet riskien hallitsemiseksi ja järjestelmään tallennetun tiedon CIA-ominaisuuksien (luottamuksellisuus, eheys ja saatavuus) turvaamiseksi. Tyypilliset tietojärjestelmien tietoturvahuolet liittyvät datan turvaamiseen, luvattomaan pääsyyn järjestelmään ja palveluiden saatavuuteen (Kalloniatis ym., 2014). Organisaation teknisissä tietoturvakäytänteissä määritellään se, miten järjestelmän teknisellä tasolla vastataan näihin haasteisiin (Paananen, Lapke & Siponen, 2020). Teknisissä tietoturvakäytänteissä esimerkiksi määritellään, miten dataa luodaan, säilytetään, käytetään, arkistoidaan ja tuhotaan (Kalloniatis ym., 2014). Organisaation tietojärjestelmien käytössä oleva data on tallennettu fyysisille laitteille. Laitteet voivat olla organisaation itsensä omistamia ja hallinnoimia, tai ulkoisena palveluna hankittuja (Zhou, Varadharajan & Hitchens, 2013). Kalloniatis ja kumppanit (2014) toteavat, että datan turvallisuuden takaa verkon suojaus, datan yhtenäisyys, varmuuskopiointi, datan ja laitteiston salaus ja pääsynhallinta, sekä laitteiston kunnosta huolehtiminen. Puutteellisesti toteutetut rajapinnat, pahantahtoiset työntekijät, datavuoto ja datan menetys ovat merkittävimmät uhat datan turvallisuudelle. Sovellusten osalta turvallisuus tulee varmistaa sekä sisäisissä, että ulkoisissa toimintaympäristöissä mikäli sovelluksella on organisaation ulkopuolisia käyttäjiä. Käyttäjäntunnistus, oikeuksien rajaus, lokitiedot ja penetraatiotestaus ovat esimerkkejä toimista, joilla voidaan edistää ja tukea sovelluksen turvallisuutta. Jos organisaation palvelut eivät ole saatavilla, se voi johtaa siihen, että organisaation toimintaan syntyy häiriöitä, kun kaikkia toimintoja ei pystytä suorittamaan. Häiriötilanteista palautumista auttaa palautussuunnitelma, jonka avulla häiriötilanteen seurauksena tuhoutunut data tai kaatuneet palvelut saadaan palautettua ja organisaation toimintaa pystytään jatkamaan (Kalloniatis ym., 2014).

Organisaatioissa tietoturvaa hallinnoidaan tietoturvastrategian avulla (Rocha Flores, Antonsen & Ekstedt, 2014). Tietoturvastrategia on suunnitelma, jossa yhdistyy organisaation tavoitteet ja käytänteet tietoturvaan liittyen (Beebe & Rao, 2010). Rocha Flores ja kumppanit (2014) toteavat, että organisaation tietoturvastrategian tulee olla linjassa liiketoiminnan strategian kanssa, eli tietoturvastrategian tulee nojata liiketoiminnan tarpeisiin, eikä se saa haitata liiketoimintaan kuuluvien toimintojen suorittamista. Tietoturvasta vastaavien tahojen tulee täten ymmärtää liiketoiminnan ja loppukäyttäjien tarpeita, jotta he voivat kehittää organisaation tarpeisiin sopivan tietoturvastrategian (Rocha Flores ym., 2014).

Barton, Tejay, Lane ja Terrel (2016) sekä Calder ja Watkins (2010) totesivat, että tietoturvan hallinnassa tietoturvariskien hallinta on keskeisessä roolissa. Riskien hallinnassa on kaksi vaihetta, joista ensimmäinen on tietojärjestelmän turvallisuusriskien tunnistus ja arviointi. Toisessa vaiheessa tunnistettuihin riskeihin kehitetään kustannustehokkaita vastatoimia, joilla kyseisiä riskejä pyritään pienentämään rajoittamatta liiketoiminnallisia prosesseja liikaa (Barton, Tejay, Lane & Terrel, 2016; Calder & Watkins, 2010). Calder ja Watkins (2010) toteavat, että tietoturvariskien hallinta on kuitenkin käytännössä jatkuva prosessi, missä toistuu riskien hallinnan kaksi vaihetta. Tietoturvariskien tunnistuksessa keskitytään lähtökohtaisesti vain niihin riskeihin, joista voi koitua vain negatiivisia

vaikutuksia. Riskit, joista voi koitua negatiivisia tai positiivisia vaikutuksia käsitellään useimmiten liiketoiminnan riskejä arvioitaessa. Riskeihin vastatessa riskien todennäköisyyttä tai vaikutusta pyritään pienentämään siten, että ne laskevat organisaatiossa riskien hyväksytyn sietotason alle. Keinoina on riskiä aiheuttavan toiminnon välttäminen, toiminnon muokkaaminen siten, että riskin syntyminen estetään, ja riskitekijän seuranta. Sopiva keino riskiin vastaamiseen valitaan sen perusteella, miten merkittävä riski on (Calder & Watkins, 2010). Kalloniatis ja kumppanit (2014) toteavat, että toteutuessaan tietoturvariskistä tulee tietoturvaloukkaus. Riskien lisäksi myös loukkausten varalle tulisi olla suunniteltu vastatoimia ja selvityssuunnitelmia, jotta loukkaus ja sen vaikutukset saadaan korjattua ja sen uusiutuminen estettyä (Kalloniatis ym., 2014).

Toinen keskeinen osa tietoturvan hallintaa on tietoturvakäytänteet (Bulgurcu, Cavusoglu & Benbasat, 2010). Paanasen, Lapken ja Siposen (2020) mukaan tietoturvakäytänteille ei ole aiemmissa tutkimuksissa vakiintunut yhtä ainoaa oikeaa määritelmää, vaan määritelmiä on useita, jotka riippuvat näkökulmasta, josta tietoturvakäytänteitä käsitellään. He määrittelevät tietoturvakäytänteet siten, että ne ovat dokumentteja, jotka sääntelevät ihmisten toimintaa tietoturva-asioissa, ja ilmaisevat organisaation tavoitteet tietoturvan suhteen. Tämä määritelmä koskee hallinnollisia tietoturvakäytänteitä, jotka ovat eri asia kuin tekniset tietoturvakäytänteet, vaikkakin ne liittyvät toisiinsa. Tietoturvakäytänteet voidaan jakaa kolmeen kategoriaan niiden ominaisuuksien ja toimintojen perusteella. Kategoriat ovat: organisaation ohjaaminen, toimijoiden ja omaisuuksien määrittely, ja tietoturvaloukkauksiin varautuminen (Paananen ym., 2020).

Paanasen ja kumppaneiden (2020) mukaan organisaation ohjauksen kategoriaan kuuluvat käytänteet määrittelevät organisaation tietoturvan tavoitteet, kertovat miksi näihin tavoitteisiin pyritään ja miten tavoitteisiin päästään mahdollisista tietoturvaloukkauksista huolimatta. Samalla tietoturvatavoitteet tukevat organisaation liiketoiminnan tavoitteita. Käytänteisiin kuuluvat toimintaohjeet, joiden avulla työntekijöitä ohjataan tietoturvallisiin toimintatapoihin tiedonkäsittelyyn liittyvissä toiminnoissa. Käytänteisiin voi olla kirjattuna myös käytänteiden rikkomisesta seuraavat sanktiot. Tietoturvakäytänteiden noudattamista voidaan seurata mittaamalla käytänteisiin määriteltyjen tavoitteiden toteutumista, niissä tapauksissa, kun luotettava mittaaminen on mahdollista (Paananen ym., 2020).

Paanasen ja kumppaneiden (2020) mukaan toimijoiden ja omaisuuksien kategoriaan kuuluvat tietoturvakäytänteet auttavat toimijoita (organisaation henkilöstö) tekemään päätöksiä käsitellessään organisaation käytössä olevaa omaisuutta (informaatiota). Käytänteissä määritellään se, miten tiukkoja turvatoimia mihinkin organisaation omaisuuteen sovelletaan, kenellä henkilöstöstä on mitäkin oikeuksia omaisuuksien käyttöön tai muokkaamiseen liittyen, ja ketkä ovat vastuussa omaisuuksiin liittyvien päätöksien tekemisestä. Tämän kategorian tietoturvakäytänteet koskevat myös organisaation ulkopuolista henkilöstöä, joka käyttää organisaation omaisuutta (Paananen ym., 2020).

Paanasen ja kumppaneiden (2020) mukaan tietoturvakäytänteiden kolmas kategoria on tietoturvaloukkauksiin varautuminen. Tietoturvakäytänteet ovat

tärkeässä roolissa tietoturvaloukkausten havaitsemisessa, ehkäisyssä ja niihin vastaamisessa. Käytänteiden suunnitteluvaiheessa kiinnitetään huomiota siihen, että niiden avulla organisaation toimintatapoja ohjataan tietoturvalliseen suuntaan. Tämä pakottaa organisaatiot miettimään etukäteen niitä uhkia, jotka voivat kohdistua organisaation hallussa olevaan informaatioon. Käytänteet voidaan johtaa organisaation tietoturvariskien hallinnan linjauksista, minkä seurauksena organisaation eri yksiköiden toimintatavat ovat yhteneviä, mikä tukee riskien hallintaa. Tietoturvakäytänteissä on määritelty suunnitelma tietoturvaloukkauksista palautumisen varalle. Suunnitelma voi sisältää esimerkiksi ohjeistuksen siitä, miten loukkauksen syitä tutkitaan, dokumentoidaan ja miten loukkauksen vaikutukset rajoitetaan suuremman vahingon välttämiseksi. Tavoitteena on, että organisaation toiminta ei pysähtyisi tietoturvaloukkausten ilmetessä, vaan toimintaa pystyttäisiin jatkamaan samalla kun loukkausta selvitetään. Tietoturvakäytänteet toimivat usein todisteena siitä, että organisaation toimintatavat vastaavat yleisiä määräyksiä ja vaatimuksia informaation käsittelyyn liittyen. Osoitus siitä, että organisaatio on valmistautunut mahdollisten tietoturvaloukkausten varalle, voidaan nähdä positiivisena asiana esimerkiksi asiakkaan näkökulmasta (Paananen ym., 2020).

Bartonin ja kumppaneiden (2016) mukaan ylimmän johdon tuki tietoturva-asioissa on edellytys tehokkaalle tietoturvan hallinnalle. Ylimmän johdon ei tarvitse osallistua tietoturvan hallinnoinnin käytännön toteuttamiseen, mutta johdon selkeä ja näkyvä tuki viestii organisaatiossa tietoturvan tärkeydestä ja riittävä resursointi mahdollistaa tietoturvatoimien toteuttamisen. Useissa tutkimuksissa johdon tuella on osoitettu olevan yhteys tietoturvatoimien tehokkaaseen kehitykseen, käyttöönottoon ja myös niiden noudattamiseen. Ylimmän johdon huomio tietoturva-asioihin on voimakasta erityisesti organisaatioissa, jotka toimivat kriittisen infrastruktuurin aloilla tai jakavat informaatiota muiden organisaatioiden kanssa. Näiden organisaatioiden johdolla on ulkoinen paine huolehtia tietoturvasta, jolloin he todennäköisemmin huolehtivat siitä, että organisaatiossa panostetaan tietoturvaan (Barton ym., 2016).

Rocha Flores ja kumppanit (2014) ehdottavat, että tietoturvan hallintaan käytettyjen keinojen tehokkuutta tulisi seurata säännöllisesti. Tarpeen mukaan keinoja tulisi muokata tai korvata vastaamaan liiketoimintaympäristön muuttuvia tarpeita. Onnistunut tietoturvan hallinta yhdistää organisaation prosesseihin ja palveluihin tietoturvalliset toimintatavat ilman, että prosessien tai palveluiden tehokkuus kärsii (Rocha Flores ym., 2014).

Kulttuurin näkökulma käsittää organisaation työntekijöiden inhimilliset ominaisuudet, esimerkiksi käyttäytymisen, asenteet ja arvot, jotka sisäisesti tai ulkoisesti ohjaavat ihmisiä organisaation tiedon turvaamiseen (Cabrera ym., 2020). Barton ja kumppanit (2016) toteavat, että tietoturvakäytänteistä on hyötyä silloin, kun käyttäjät noudattavat niitä. Organisaatiokulttuuri vaikuttaa siihen, miten hyvin tietoturvakäytänteitä noudatetaan. Työntekijät noudattavat tietoturvakäytänteitä paremmin, jos he kokevat ne reiluiksi ja laadukkaiksi. Tietoturvakäytänteiden noudattamista voidaan parantaa muun muassa ylimmän johdon tuella, hyvällä viestinnällä, sanktioilla tietoturvakäytänteiden rikkomisesta, sekä

koulutuksilla, jotta käytänteet ymmärrettäisiin paremmin (Barton ym., 2016). Tietoturvakoulutuksen tarjoaminen työntekijöille on tärkeää, jotta he osaavat tehdä työssään kohtaamissaan tilanteissa asianmukaisia päätöksiä (Young & Windsor, 2010).

Talouden näkökulma käsittää organisaation tietoturvaratkaisujen taloudelliset vaikutukset (Cabrera ym., 2020). Palmerin (2001) mukaan suorat kustannukset tietoturvaan liittyen syntyvät esimerkiksi konsultoinnista, henkilöstön palkkauksesta, järjestelmän käyttöönotosta ja sen tietoturvallisuuden ylläpidosta. Epäsuoria kustannuksia syntyy järjestelmän käytettävyydestä ja sen vaikutuksesta käyttäjien työskentelyyn. Tietoturvallinen, mutta käytettävyydeltään huono järjestelmä heikentää käyttäjien tuottavuutta. Tietoturvallinen ja käytettävyydeltään sujuvampi järjestelmä puolestaan voi olla suorilta kustannuksiltaan suurempi (Palmer, 2001). Tietomurroista voi seurata organisaatiolle negatiivisia taloudellisia seurauksia (Lorenzini ym., 2022).

4 EETTINEN HAKKEROINTI TIETOJÄRJESTELMÄN TIETOTURVAN KEHITYKSESSÄ

Tässä luvussa käsitellään eettisen hakkeroinnin erilaisten menetelmien vaikutuksia tietojärjestelmän tietoturvaan, ja miten eettistä hakkerointia voidaan hyödyntää tietojärjestelmän tietoturvan kehityksessä. Luku on jaettu kahteen alalukuun, joista ensimmäisessä käsitellään eettisen hakkeroinnin hyödyntämistä tietoturvan kehityksessä, ja mitä hyötyjä sen avulla on mahdollista saavuttaa. Lisäksi demonstroidaan case-tutkimuksen avulla sitä, miten eettistä hakkerointia voidaan toteuttaa ja millainen rooli eettisellä hakkeroinnilla voi olla osana organisaation tietojärjestelmän tietoturvan kehittämistä. Toisessa alaluvussa käsitellään eettiseen hakkerointiin ja sen toteuttamiseen liittyviä haasteita.

4.1 Eettisen hakkeroinnin hyödyntäminen

Palmerin (2001) mukaan eettinen hakkerointi pyrkii vastaamaan kolmeen peruskysymykseen testaamalla järjestelmän tietoturvaa: Mitä tietoja murtautuja voi saada kohdejärjestelmästä? Mitä murtautuja voi tehdä saamallaan tiedolla? Huomataanko kohdejärjestelmään kohdistuvia murtautumisia tai niiden yrityksiä? Eettinen hakkerointi on tehokkaimmillaan silloin, kun kohdeorganisaatio ei rajoita heidän järjestelmänsä testaamiseen käytettäviä keinoja. Tällöin tilanne vastaa parhaiten rikollisen hakkerin suorittamaa murtautumisyritystä. Jos kohdeorganisaatiossa halutaan rajoittaa eettisessä hakkeroinnissa käytettäviä keinoja vetoamalla järjestelmän kriittisyyteen, olisi entistäkin tärkeämpää käyttää kaikkia eettisen hakkerin keksimiä keinoja, koska tällöin mahdollisia haavoittuvuuksia etsitään mahdollisimman perusteellisesti (Palmer, 2001).

Palmer (2001) totesi, että eettisen hakkeroinnin hyödyllisyyden maksimoimiseksi henkilöstöä ei tulisi etukäteen tiedottaa tulevasta testauksesta liian julkisesti. Tämä voisi aiheuttaa testauksen ajaksi tavanomaisesta poikkeavaa panostusta henkilöstön toimintatapoihin tietoturvan osalta, mikä puolestaan ei kuvastaisi normaalia tilannetta organisaatiossa. Tällöin testauksen aikana tehdyt

havainnot ja raportointi eivät vastaisi järjestelmän tietoturvan todellista tilaa (Palmer, 2001).

Palmerin (2001) mukaan paras ajankohta eettiselle hakkeroinnille olisi mahdollisimman aikaisessa vaiheessa ennen järjestelmän käyttöönottoa, jotta löydetyt haavoittuvuudet ehditään korjaamaan, ja korjausten seurauksena mahdollisesti syntyvät uudet haavoittuvuudet tai järjestelmän toiminnan ongelmat ehditään korjata ennen käyttöönottoa. Eettisen hakkeroinnin aikana löydetyt havainnot kirjataan loppuraporttiin, joka luovutetaan kohdeorganisaatiolle. Raportti sisältää vastaukset peruskysymyksiin, eli mitä tietoja murtautuja voi saada kohdejärjestelmästä, mitä niillä tiedoilla on mahdollista tehdä, ja huomattiinko kohdejärjestelmään kohdistuvia murtautumisia tai niiden yrityksiä. Raportissa on yksityiskohtaiset tiedot löydetyistä haavoittuvuuksista tai puutteista esimerkiksi murtautumisyritysten havaitsemisessa, ja ehdotuksia niiden korjaamiseksi tai niistä aiheutuvan uhan pienentämiseksi (Palmer, 2001).

Ding ja kumppanit (2019) totesivat tutkimuksessaan, että haavoittuvuuspalkkio-ohjelman (engl. Bug Bounty Program) avulla organisaatio voi ulkoistaa haavoittuvuuksien löytämisen ja korjaamisen, ja ohjelman merkittävimpänä hyötynä on haavoittuvuuksien hallintaan tarvittavan organisaation sisäisen resurssimäärän vähentäminen. Tällöin organisaation resursseja voi suunnata muille toiminnan osa-alueille. Haavoittuvuuspalkkio-ohjelman käynnistystä suositellaan aikaisintaan siinä vaiheessa ohjelmiston kehitystä, kun ensimmäiset tietoturva-auditoinnit on tehty (Ding ym., 2019), mutta kuitenkin hyvissä ajoin ennen ohjelman julkaisua, jotta haavoittuvuudet ehditään korjata (Malladi & Subramanian, 2020). Ding ja kumppanit (2019) totesivat myös, että käynnistämällä haavoittuvuuspalkkio-ohjelman ensimmäisten tietoturva-auditointien jälkeen voidaan olettaa, että merkittävä osa haavoittuvuuksista on jo löydetty ja korjattu. Haavoittuvuuspalkkio-ohjelman kautta lukuisten haavoittuvuuksien korjaus ja palkkioiden maksaminen kävisi organisaatiolle huomattavasti kalliimmaksi, kuin esimerkiksi penetraatiotestauksen kautta vastaavien haavoittuvuuksien korjaaminen (Ding ym., 2019).

Mudiyanselage ja Pan (2020) tekivät tutkimuksessaan penetraatiotestauksen avulla tietoturvatestin Moodle -verkko-oppimisalustalle, minkä tarkoituksena oli löytää alustalta haavoittuvuuksia. Alustan lähdekoodi analysoitiin manuaalisesti, ja lisäksi se skannattiin useilla automaattisilla työkaluilla, jotta haavoittuvuuksia löydettäisiin mahdollisimman kattavasti. Lähdekoodin analysoinnissa löytyneet potentiaaliset haavoittuvuudet arvioitiin manuaalisesti ihmisen toimesta niiden hyödyntämisten todennäköisyyden ja hyödyntämisestä johtuvien seurausten vakavuuden perusteella. Lisäksi haavoittuvuuksiin esitettiin korjausehdotuksia (Mudiyanselage & Pan, 2020). Kyseisessä tutkimuksessa käytetyt menetelmät ja saadut tulokset vastaavat tyypillisiä kirjallisuudessa esiintyviä penetraatiotestauksen menetelmiä ja odotettavissa olevia tuloksia kohdejärjestelmän tietoturvan teknisestä näkökulmasta (Dalalana Bertoglio & Zorzo, 2017; Kalloniatis ym., 2014; Palmer, 2001).

Kuten eettiseen hakkerointiin yleisesti, myös penetraatiotestaukseen kuuluu testauksen aikana havaittujen haavoittuvuuksien raportointi (Beran, 2012).

Usein raportin yhteydessä, tai ainakin sen pohjalta, suunnitellaan jatkotoimet havaittujen haavoittuvuuksien suhteen (Beran, 2012; Palmer, 2001). Riskien hallinta ja tietoturvakäytänteiden testaus ovat osa tietoturvakäytänteiden kehittämisen prosessia (Paananen ym., 2020). Penetraatiotestaus voi toimia argumenttina tai todisteena riskien hallinnan päätöksenteossa siitä, että panostamalla tietoturvaan organisaatio voi ehkäistä kassavirran menetystä, oikeustoimia tai maineellista haittaa mahdollisen tietomurron seurauksena (Lorenzini ym., 2022). Euroopassa valvontaviranomainen voi määrätä organisaatiolle hallinnollisia sakkoja tietoturvaloukkausten seurauksena tapahtuvista tietosuoja-asetusten rikkomisesta, mikäli organisaatio toimii rekisterinpitäjänä tai henkilötietojen käsittelijänä (Tietosuojavaltuutetun toimisto, 2017).

Sosiaalisen manipulaation hyökkäyksiltä suojaavien tietoturvakäytänteiden testaamiseen yksi tehokkaimmista työkaluista on eettinen sosiaalinen manipulaatio (Winkler & Dealy, 1995). Sosiaalisen manipulaation hyökkäyksien onnistumista ehkäisee myös henkilöstön hyvä tietoturvatietoisuuden taso, sekä kattavat tietoturvakäytänteet, joita henkilöstö noudattaa. Tietoturvatietoisuuden kehittämisessä tietoturvakoulutukset ovat tärkeässä roolissa (Applegate, 2009).

Bulgurcu ja kumppanit (2010) havaitsivat tutkimuksessaan, että työntekijät noudattivat tietoturvakäytänteitä todennäköisemmin silloin, kun käytänteen noudattamiseen vaadittavan vaivan ja siitä saatavan hyödyn suhde on suurempi kuin noudattamatta jättämisestä aiheutuva oletettu haitta itselle tai organisaatiolle. Tutkimuksessa havaittiin myös se, että työntekijän tietoisuus tietoturvasta vaikuttaa positiivisesti tietoturvakäytänteiden noudattamiseen. He ehdottavat, että henkilöstön tietoturvakoulutuksissa voitaisiin käyttää havainnollistavina esimerkkeinä sellaisia materiaaleja, joiden tarkoituksena on vaikuttaa työntekijöiden näkemyksiin tietoturvakäytänteiden noudattamisen ja noudattamattomuuden hyötyjen ja haittojen suhteesta, ja siten edistää käytäntöjen noudattamista organisaatiossa (Bulgurcu ym., 2010). Säännöllisten tietoturvakoulutusten on myös havaittu parantavan organisaation yleistä tietoturvakulttuuria (da Veiga & Martins, 2015).

Bulgurcu ja kumppanit (2010) eivät erikseen nimenneet eettistä hakkerointia keinoksi tuottaa havainnollistavia esimerkkejä, mutta myös Puhakainen ja Siponen (2010) mainitsivat omassa tutkimuksessaan käytännön esimerkkien tärkeyden henkilöstön tietoturvakoulutuksissa. Tutkimuksessa mainittiin esimerkkinä tapaus, jossa luottamuksellista informaatiota sisältävä sähköposti lähetettäisiin salaamattomana, ja sitten koulutuksessa näytettäisiin miten ulkoinen taho pääsisi tämän sähköpostin sisältöön käsiksi. Tämän demonstroinnin jälkeen henkilöstöä pyydettäisiin pohtimaan, mitä seurauksia vastaavan tahattoman tietovuodon tapahtuessa voisi aiheutua heidän työssään käsittelemiensä tietojen kohdalla (Puhakainen & Siponen, 2010). Puhakaisen ja Siposen (2010) esimerkki vastaa eettisen hakkeroinnin määrittelyä, koska siinä tapahtuva sähköpostin kaappaus tehdään yhteisymmärryksessä järjestelmän omistajan kanssa tarkoituksena parantaa tietoturvaa (Thomas ym., 2018; Palmer, 2001).

Winkler ja Dealy (1995) tarkastelivat tutkimuksessaan eettisen sosiaalisen manipulaation tapausta, joka kohdistui useisiin suuriin finanssialan

organisaatioihin. Tutkimuksessa havaittiin, että työntekijöiden tietoturvatietoisuuteen tulisi panostaa, sillä tutkimuksen aikana salasanoja luovutettiin puhelimessa soittajalle, joka esiintyi teknisen tuen henkilönä. Tietoturvakoulutuksella saataisiin huomattavia säästöjä aikaan koulutuksen ollessa verrattain halpaa saatuihin hyötyihin ja vältettyihin tappioihin verrattuna (Winkler & Dealy, 1995). Työntekijöiden tietoturvatietoisuuteen panostaminen on tärkeää, sillä heikko tietoturvatietoisuus on syynä suureen osaan tietomurroista (Verizon, 2022).

Lorenzini ja kumppanit (2022) käsittelivät tutkimuksessaan eettisen hakkeroinnin sovellusalueita terveydenhoidon alalla. Muille aloille yleistettäviä havaintoja tutkimuksessa oli, että IT-investointien pitkäaikaisen laiminlyönnin seurauksena organisaation käytössä voi olla valitettavan paljon tietoturvaltaan vanhentunutta ohjelmistoa. Esimerkiksi Windows XP -käyttöjärjestelmään pohjautuvia ratkaisuja oli käytössä useissa terveydenhuollon alan organisaatioissa. Toinen yleistettävä havainto oli, että terveydenhuollon alalla tai muilla kuin IT-alalla ei välttämättä pystytä tarjoamaan tietoturva-ammattilaiselle yhtä kilpailukykyistä palkkaa, kuin mitä he saisivat oman alan organisaatioissa. Tämä eri aloilla toimivien organisaatioiden välinen palkkaero ei houkuttele asiantuntijoita tehtäviin, joissa heille olisi tarvetta. Osaltaan palkkauksen ero johtuu pienemmistä resursseista, joita suunnataan IT-toimiin. Vanhentuneet ohjelmistot eivät saa tietoturvapäivityksiä, joissa paikataan ohjelmiston haavoittuvuuksia. Päivitysten puutteen takia vanhentuneisiin järjestelmiin murtautuminen on helpompaa kuin niihin, joiden haavoittuvuuksia paikataan aktiivisesti. Penetraatiotestauksen avulla näitä haavoittuvuuksia on mahdollista löytää ja korjata, ennen kuin pahantahtoiset tahot hyödyntävät niitä. Penetraatiotestausta on mahdollista hankkia ostopalveluna, jolloin organisaation omat investoinnit jäävät kertaluonteisiksi, mikä voi kannustaa menetelmien käyttöön (Lorenzini ym., 2022).

Eettisen hakkeroinnin hyödyt tietojärjestelmän tietoturvan kehityksessä ovat monipuolisia aiheen kirjallisuuden perusteella. Järjestelmän teknisen toteutuksen haavoittuvuuksia voidaan havaita ja korjata esimerkiksi penetraatiotestauksen tai haavoittuvuuspalkkio-ohjelman avulla. Löydettyjä haavoittuvuuksia voidaan myös käyttää argumentteina osana organisaation riskien hallintaa. Teknisen näkökulman lisäksi eettisen hakkeroinnin avulla voidaan havaita tietoturvan heikkoja kohtia henkilöstön toimintatavoista ja organisaation käytänteistä, jotka ohjaavat henkilöstön toimintatapoja. Tutkimuksissa havaittiin, että tietoturvakoulutuksilla voitaisiin ehkäistä merkittävää osaa henkilöstön toimintaan liittyvistä tietoturvauhista. Koulutusten todettiin myös olevan taloudellisesta näkökulmasta tehokas keino tietoturvan yleisen tason nostamiseen organisaatioissa. Koulutuksissa on myös mahdollista käyttää eettistä hakkerointia havainnollistavien ja todellisia tilanteita mukailevien esimerkkien luomiseen, minkä voi olettaa vahvistavan koulutuksen vaikutuksia. Eettiseen hakkerointiin liittyvät taloudelliset vaikutukset ovat näkyvimmillään siinä vaiheessa, kun eettistä hakkerointia toteutetaan ja siitä syntyy organisaatiolle kuluja. Toisaalta eettisen hakkeroinnin avulla parantuneen tietoturvan voidaan olettaa pitemmällä aikavälillä ehkäisevän mahdollisia rahallisia menetyksiä, joita voisi tapahtua heikomman tietoturvan takia.

4.1.1 Case: Using penetration testing feedback to cultivate an atmosphere of proactive security amongst end - users

Styles ja Tryfonas (2009) tutkivat eräälle elektroniikkateollisuuden alalla toimivalle yritykselle toteuttamansa projektin kautta sitä, miten eettisen hakkeroinnin keinoja hyödyntäen voitaisiin parantaa kyseisen yrityksen tietoturvaa, erityisesti yrityksen henkilöstön toimintatapojen osalta. Projekti toteutettiin sarjana erilaisia tehtäviä, jotka alkoivat henkilöstön yleisen tietoturvaosaamisen tason selvityksellä. Tämän jälkeen tietoturvaosaamisen tasoa pyrittiin nostamaan, ja henkilöstön tietoturvakäyttäytymistä pyrittiin viemään ennaltaehkäisevään suuntaan (Styles & Tryfonas, 2009).

Projektin alussa kohdeyrityksen henkilöstön tietoturvatietoisuuden kartoittamiseen käytettiin joukkoa erilaisia testejä. Ensin haluttiin selvittää, käyttävätkö käyttäjät jotakin yksinkertaista kaavaa keksiessään kuukausittain vaihtuvia salasanoja. Jos joidenkin käyttäjien havaittiin toistuvasti käyttävän turvattomia salasanoja, heidän tunnuksiinsa kohdistettiin säännöllisesti salasanan murtoyrityksiä. Salasanojen murtamistestin tuloksena oli, että 61,49 % testatuista salasanoista luokiteltiin korkean riskin omaaviksi. Monet yrityksen työntekijät käyttivät yksinkertaisia salasanoja vahvojen sijaan, ja valtaosa käytössä olleista salasanoista murrettiin alle minuutissa, ja monet vain sekunneissa. Salasanatestin jälkeen henkilöstölle lähetettiin yleisen tason kysely tietoturvasta ja tietoturvaongelmista. Tietoturvakyselyn jälkeen henkilöstöä testattiin phishing- eli tietojenkalastelutesteillä. Testit suunniteltiin yrityksen saamien oikeiden tietojenkalasteluyritysten pohjalta (Styles & Tryfonas, 2009).

Testien jälkeen yrityksen tietoturvaa lähdettiin parantamaan saatujen tulosten perusteella. Kyselyn ja testien tuloksista muodostettiin info-/koulutusmateriaalia, jota lähetettiin yrityksen työntekijöille. Materiaalissa käsiteltiin konkreettisella tasolla sitä, miten havaittuja ongelmakohtia voisi kehittää heidän päivittäisessä toiminnassaan. Henkilöstö arvosti oppimiaan asioita tietoturvasta, sillä he kokivat pystyvänsä hyödyntämään oppimaansa myös vapaa-ajalla. Yrityksen johdon mielestä tämä oli hyvä asia, sillä yritystä voitaisiin kiristää tai sitä kohti tehdä hyökkäyksiä esimerkiksi henkilöstön vapaa-ajalla internetissä tekemien julkaisujen avulla. Lisäksi uusien työntekijöiden perehdytysjaksoon lisättiin tietoturvan osuus. Projektin tuloksia esiteltiin yrityksen emoyhtiölle, minkä seurauksena kyseisessä konsernissa alettiin suhtautumaan tietoturvaan vakavammin. Johtotasolta alettiin luomaan painetta ja kannustimia osastojen tietoturvan jatkuvaan kehittämiseen niin tekniseltä kuin henkilöstön toimintatapojen osalta. (Styles & Tryfonas, 2009).

Projektin päätteeksi tutkijat nimesivät tärkeimmät havaitsemansa tekijät tietoturvan parantamisessa:

- Alttius ulkoiselle vaikuttamiselle. Salasanatesti sai henkilöstön pohtimaan uudestaan käyttämiensä salasanojen vahvuutta ja miten heidän käyttämänsä salasanat liittyvät myös yrityksen turvallisuuteen. Salasanatesti demonstroi myös johtoportaalle salasanakäytäntöjen tärkeyttä.

- Johdon osallistuminen. Henkilöstö suhtautui vakavammin tietoturvaan, kun johtoporras painotti sen tärkeyttä yrityksen kannalta.
- Interaktiiviset koulutukset. Monipuolisten ja interaktiivisten koulutusten avulla henkilöstön tietoturvaosaaminen kehittyi.
- Testeissä ja demonstraatioissa käytettyjen materiaalien pohjautuminen todellisiin yritykseen kohdistuneisiin tietoturvaloukkauksiin. Realististen ja samaistuttavien demonstraatioiden avulla henkilöstö sai konkreettisen käsityksen siitä, minkälaisia uhkia he voivat työssään kohdata ja miten niiden kanssa toimitaan.
- Tietoturvaosuuden lisääminen uusien työntekijöiden perehdytykseen. Tällä pyritään varmistamaan se, että uudet työntekijät noudattavat tietoturvakäytänteitä työsuhteen alusta alkaen samalla tasolla kuin muu henkilöstö (Styles & Tryfonas, 2009).

Tutkijat pohtivat tutkimuksen tuloksien perusteella, että yrityksissä olisi löydettävä tasapaino tiukkojen tietoturvatoimien ja sujuvan työskentelyn väliltä. Jos tietoturvaan liittyvät säännöt ovat liian tiukat, kaikki eivät välttämättä noudata niitä tai työn tehokkuus laskee merkittävästi. Yrityksen henkilöstö on keskeinen osa yrityksen tietoturvaa. Koulutuksella ja hyvillä toimintatavoilla yrityksen työympäristön turvallisuutta on mahdollista parantaa. Kun työntekijä ymmärsi roolinsa yrityksessä ja roolinsa mahdollisesta väärinkäytöstä johtuvat riskit, hänen asennoitumisensa tietoturvaan muuttui myönteisemmäksi (Styles & Tryfonas, 2009).

4.1.2 Havaintoja Case-tutkimuksesta

Stylesin ja Tryfonasin (2009) suorittamassa tutkimuksessa painotettiin kohdeyrityksen henkilöstön toimintatapojen roolia yrityksen tietoturvan kokonaisuuden parantamisessa. Eettisen hakkeroinnin menetelmien avulla saatiin selvitettyä henkilöstön tietoturvaosaamisen heikot osa-alueet, ja saatujen tietojen perusteella luotiin koulutusohjelmat, joilla näitä heikkoja osa-alueita saatiin tehokkaasti vahvistettua. Tutkimuksen aikana saadut tulokset vaikuttivat positiivisesti kohdeorganisaation tietoturvaan hallinnan ja kulttuurin näkökulmista. Kirjallisuudessa esiintyvän luokittelun mukaan tietoturvan hallinnan näkökulmaan liittyi johdon osallistuminen ja henkilöstön ohjeistettujen toimintatapojen eli käytänteiden muutos. Tietoturvan kulttuurin näkökulmaan liittyi henkilöstön asennoitumisen muutos tietoturvaan (Bulgurcu ym., 2010; Cabrera ym., 2020). Tutkimuksen aikana organisaation johto aloitti tutkimuksessa saatujen havaintojen perusteella panostuksen tietoturvaan myös teknisestä näkökulmasta, mutta sen vaikutukset eivät vielä näkyneet tutkimuksen aikana. Tutkimuksessa ei käsitelty tietoturvan parantamisen taloudellisia vaikutuksia, mutta aiheen kirjallisuuden perusteella kohdeorganisaatiossa tehdyt parannukset tietoturvassa voivat johtaa myös taloudellisiin hyötyihin, vähintään tietomurroista seuraavien taloudellisten haittojen oletetun vähenemisen myötä (Lorenzini ym., 2022).

4.2 Eettisen hakkeroinnin haasteet

Palmerin (2001) mukaan eettistä hakkerointia suoritettaessa on riskinä, että rikollinen hakkeri tarkkailee toimintaa, ja saa selville samoja asioita kuin eettinen hakkeri. Tällöin rikollinen hakkeri voisi hyödyntää löydettyjä haavoittuvuuksia ennen kuin ne ehditään korjata. Eettisen hakkeroinnin päätteeksi asiakasorganisaatiolle annettava raportti löydetyistä haavoittuvuuksista voisi vääriin käsiin joutuessaan olla erittäin vaarallinen. Organisaation kilpailija voisi suorittaa yritysvakoilua sen avulla, rikollinen hakkeri voisi murtautua organisaation järjestelmään ja aiheuttaa tuhoa, tai raportti voitaisiin julkaista internetissä. Eettisen hakkeroinnin kohteena oleva järjestelmä voi olla organisaation käytössä oleva tuotantoversio, jolloin riskinä voi ilmetä järjestelmän kaatumisia tai ongelmia suorituskyvyssä, palvelunestoja, henkilöstön hätääntymistä tai lokitietojen räjähdysmäistä kasvua (Palmer, 2001).

Palmerin (2001) mukaan eettisen hakkeroinnin haasteena on myös se, että kohdeorganisaation edustajat voivat olla sitä mieltä, että testaaminen tulisi lopettaa heti kun heidän järjestelmäänsä päästään sisälle. Tällöin on kuitenkin erittäin todennäköistä, että järjestelmään jäisi vielä haavoittuvuuksia, jotka löydettäisiin suorittamalla testaus loppuun. Keskeyttämällä testaus ensimmäisen löydetyn haavoittuvuuden kohdalla ja korjaamalla se, kohdeorganisaatiolle voi syntyä virheellinen käsitys heidän järjestelmänsä tietoturvasta (Palmer, 2001).

Dalalana Bertoglio ja Zorzo (2017) totesivat, että penetraatiotestauksen suurimpia haasteita on kaikkien haavoittuvuuksien löytäminen, sekä testauksessa käytettävien yleispätevien toimintamallien ja välineiden puute. Haavoittuvuuksien löytämiseen vaikuttavat testattavan järjestelmän tai järjestelmien monimutkaisuus, mahdollisissa hyökkäyksissä käytettävien tekniikoiden monimuotoisuus, sekä muutokset järjestelmäympäristössä testauksen aikana tai sen jälkeen. Penetraatiotestauksessa ei ole muodostunut yleisiä standardeja käytettävien toimintamallien ja välineiden suhteen, joten ne vaihtelevat testaajien ja kohdeympäristöjen mukaan. Tällöin testausten tuloksissa voi ilmetä merkittäviä eroja löydettyjen haavoittuvuuksien suhteen eri testaajien välillä. (Dalalana Bertoglio & Zorzo, 2017).

Väärään aikaan aloitettu tai huonosti testatun ohjelmiston haavoittuvuuspalkkio-ohjelma voi koitua organisaatiolle kalliiksi, sillä kaikkien ohjelmiston haavoittuvuuksien korjaaminen haavoittuvuuspalkkio-ohjelman kautta on erittäin kallista ja tehotonta (Ding ym., 2019). Ohjelmien suurien osallistujamäärien takia virheellisiä haavoittuvuusraportointeja voi olla jopa 50–70 % raporttien kokonaismäärästä. Raporttien läpi käyminen vie aikaa, ja mahdollisuus huonon ratkaisun hyväksymiseen on myös olemassa (Malladi & Subramanian, 2020).

Moutonin ja kumppaneiden (2015) mukaan hakkeroinnin eettisyys tulee siitä, että hakkeroinnin kohteena olevan järjestelmän omistaja on antanut luvan hakkerointiin. Eettisen hakkeroinnin aikana voidaan tehdä eettisen sosiaalisen manipulaation toimenpiteitä, mutta tarkoituksenmukaisten tulosten saamiseksi eettisen manipuloinnin kohde ei välttämättä tiedä etukäteen olevansa eettisen

sosiaalisen manipuloinnin kohteena, eikä siten ole voinut antaa suostumustaan toimiin. Tämä toimintamalli on ristiriidassa eettisen hakkeroinnin perusajatuksen kanssa. Tietoturvakäytänteiden testaamisessa on haasteena esimerkiksi se, kun työntekijä tekee työtään tietoturvakäytänteiden mukaan, mutta käytänteet on määritelty huonosti ja eettinen hakkeri saa kyseisen työntekijän kohdalla selville tietoturvahaavoittuvuuden. Työntekijästä voi tuntua siltä, että vika olisi hänessä, varsinkin jos eettisen hakkeroinnin loppuraportissa on yksilöllisesti mainittu kyseinen työntekijä, ja siitä koituu työntekijälle yksilöllisiä seurauksia. Eettisen hakkeroinnin ja eettisen sosiaalisen manipulaation tarkoitus ei ole etsiä yksittäisten henkilöiden toimintatavoista virheitä syyllistäen yksilöä, vaan organisaation toimintaa tarkastellaan kokonaisuutena (Mouton ym., 2015).

Thomasin ja kumppaneiden (2018) mukaan eettiseen hakkerointiin liittyy luottamus asiakkaan ja eettisen hakkerin välillä. Asiakas luottaa eettisen hakkerin käsiin organisaationsa hallussa olevaa mahdollisesti luottamuksellista ja arkaluontoista informaatiota. Mikäli eettinen hakkeri päättää hylätä eettisyytensä järjestelmään tunkeutumisen aikana, aiheutuu siitä merkittävää haittaa asiakkaalle. Jotta tämän riskin toteutumista voitaisiin välttää, tulisi asiakkaan varmistua siitä, että eettiseksi hakkeriksi itseään väittävä on oikeasti eettinen hakkeri (Thomas ym., 2018).

Eettisen hakkeroinnin haasteet liittyvät enimmäkseen ihmisten toimintaan eettisen hakkeroinnin yhteydessä. Asiakasorganisaation edustajat voivat esimerkiksi tahattomasti rajoittaa eettisen hakkeroinnin toteuttamista, jolloin saadut tulokset ovat merkittävästi suppeampia kuin tulokset ilman toiminnan rajoittamista. Haasteena voivat olla myös eettisen hakkerin valitsemat keinot ja välineet, mikäli ne eivät ole täysin tarkoituksenmukaisia asiakasorganisaation kontekstissa. Myös eettisen hakkerin toiminta ja toiminnan eettisyys riippuvat inhimillisistä ominaisuuksista, joita voi olla vaikea ennustaa etukäteen.

5 YHTEENVETO

Tämän tutkielman tarkoituksena oli selvittää, miten eettistä hakkerointia voidaan hyödyntää toimialasta riippumatta organisaatioiden tietojärjestelmien tietoturvan kehityksessä, ja mitä vaikutuksia sen avulla on mahdollista saada. Tämän perusteella muodostui tutkimuskysymys ”Miten eettisen hakkeroinnin avulla voidaan parantaa organisaation tietojärjestelmien tietoturvaa, ja mitä haasteita siihen liittyy?”.

Tutkielman alussa käytiin läpi erilaisia hakkeroinnin muotoja, ja miten eettinen hakkerointi eroaa muista hakkeroinnin muodoista. Hakkeroinnin eri muodoille on yhteistä hakkeroinnin kohteena olevaan järjestelmään tunkeutuminen, mutta vain eettisessä hakkeroinnissa tunkeutumiseen on lupa järjestelmän omistajalta. Tutkielmassa todettiin, että eettisen hakkeroinnin tarkoitus on parantaa hakkeroinnin kohteena olevan järjestelmän tietoturvaa palautteen avulla. Eettisen hakkeroinnin yhteydessä ei pyritä aiheuttamaan vahinkoa kohdejärjestelmälle, eikä eettinen hakkeri pyri saamaan henkilökohtaista hyötyä kohdejärjestelmässä olevan datan avulla. Eettisen hakkeroinnin menetelmistä esiteltiin penetraatiotestaus, haavoittuvuuspalkkio-ohjelma, sekä eettinen sosiaalinen manipulaatio.

Seuraavaksi tutkielmassa käsiteltiin tietojärjestelmän tietoturvaa, ja miten se näkyy organisaatioissa. Organisaatioiden tietojärjestelmien tietoturvaa tarkasteltiin Cabreran ja kumppaneiden (2020) mukaan teknisen, hallinnoinnin, kulttuurin ja talouden näkökulmista. Tekniseen näkökulmaan kuuluvat laitteistot ja ohjelmistot, jotka osallistuvat tiedon käsittelyyn organisaatiossa. Hallinnoinnin näkökulmaan kuuluu organisaatiossa määritellyt tiedon käsittelyyn liittyvät toiminnot ja toimintatavat, eli tietoturvakäytänteet, sekä niiden valvominen. Kulttuurin näkökulmaan kuuluu työntekijöistä itsestään lähtöisin olevat vaikutukset organisaation tietoturvaan, kuten tietoturvatietoisuus, asenteet ja arvot tietoturvaan ja organisaation määrittelemiin käytänteisiin liittyen. Talouden näkökulmaan kuuluu tietoturvaratkaisuista aiheutuvat taloudelliset vaikutukset organisaatiolle.

Viimeisessä luvussa käsiteltiin eettisen hakkeroinnin vaikutuksia organisaation tietojärjestelmien tietoturvaan, ja miten eettistä hakkerointia voidaan

hyödyntää organisaation tietojärjestelmien tietoturvan kehityksessä. Luvussa käsiteltiin erilaisten menetelmien avulla saavutettavia hyötyjä organisaation tietoturvan eri näkökulmista, sekä demonstroitiin case-tutkimuksen avulla, miten erään organisaation tapauksessa on käytännössä hyödynnetty eettistä hakkerointia osana tietoturvan kehitystä. Hyötyjen lisäksi käsiteltiin eettiseen hakkerointiin liittyviä haasteita, ja mitä riskejä näihin haasteisiin liittyy.

Tutkielmassa havaittiin, että eettisen hakkeroinnin avulla on mahdollista parantaa organisaation tietojärjestelmien tietoturvaa teknisen, hallinnoinnin, kulttuurin ja talouden näkökulmista. Teknisen näkökulman hyötyjä saavutetaan tunkeutumisen aikana havaittujen haavoittuvuuksien raportoinnilla ja korjausehdotuksilla, jotta rikolliset hakkerit eivät pysty hyödyntämään näitä haavoittuvuuksia. Hallinnoinnin näkökulmasta eettinen hakkerointi toimii keinona hankkia tietoa organisaation tietoturvan heikoista kohdista päätöksenteon tueksi. Organisaation johto voi saada konkreettisen kuvan siitä, mitä heihin kohdistuvasta tietoturvaloukkauksesta voisi seurata, tai miten organisaation tietoturvakäytänteitä kannattaisi kehittää vastaamaan paremmin organisaatioon kohdistuviin riskeihin.

Kulttuurin näkökulmasta eettisen hakkeroinnin avulla voidaan kehittää organisaation henkilöstön asenteita tietoturvaa kohtaan, sekä parantamaan henkilöstön tietoturvatietoisuutta ja tietoturvakäytänteiden noudattamista koulutusten avulla. Eettistä hakkerointia voidaan käyttää tietoturvakoulutusten sisällön suunnittelussa, ja myös osana tietoturvakoulutuksia demonstroimaan henkilöstölle sitä, miten tietoturvakäytänteet pyrkivät suojaamaan organisaation käsittelemää informaatiota. Talouden näkökulmasta eettisen hakkeroinnin avulla tietoturvaa kehittämällä voidaan ehkäistä tietoturvaloukkauksista aiheutuvia kuluja. Eettisen hakkeroinnin avulla voidaan havaita organisaation tietoturvasta sellaisia osa-alueita, joissa voidaan saada kustannustehokkaasti merkittäviä parannuksia organisaation tietoturvan kokonaisuuteen.

Eettisen hakkeroinnin yhtenä haasteena on hakkeroinnin eettisyys. Mikäli eettisen hakkeroinnin kohteena on henkilö, tältä ei voida pyytää selkeää lupaa olla eettisen hakkeroinnin kohteena, koska tällöin henkilö saattaa muuttaa toimintatapojaan ja tietoturvan todellista tilaa ei saada selville eettisen hakkeroinnin avulla. Eettinen hakkeri voi myös ryhtyä rikolliseksi hakkeriksi, mikä aiheuttaisi merkittävää haittaa hakkeroinnin kohteena olevan järjestelmän omistajalle. Rikollinen hakkeri voi myös tarkkailla eettistä hakkerointia, jolloin tämä voi saada tietoonsa löydetyt haavoittuvuudet. Lisäksi eettinen hakkerointi on useimmiten ihmisen suorittamaa, mikä jättää mahdollisuuden inhimillisille virheille.

Tutkielma toteutettiin kuvailevana kirjallisuuskatsauksena. Tutkielman rajoitteena oli yleistettävissä olevan lähdekirjallisuuden rajallisuus, sillä eettisen hakkeroinnin vaikutuksista on tehty paljon tutkimuksia spesifeistä aiheista, joiden tulosten ja havaintojen perusteella tähän kandidaatintutkielmaan soveltuvien referointien tai johtopäätösten tekeminen ei olisi tarkoituksenmukaista. Tästä syystä lähteiksi valikoitui joitakin lähteitä, jotka eivät täytä tavoiteltuja laatuvaatimuksia. Näiden lähteiden kohdalla on kuitenkin pyritty varmistamaan sisällön laadukkuus vertailemalla lähteen sisältöä aihepiirin laadukkaaksi

mielletyn kirjallisuuden kanssa. Lähdekirjallisuudessa esiintyneet tulokset ja johtopäätökset noudattivat useimmiten hyvin samanlaista kaavaa, ja niissä tuotiin esille samankaltaisia asioita. Lähdekirjallisuudessa sivuttiin sitä, että eettistä hakkerointia on päädytty käyttämään tietoturvakoulutuksissa tai niiden suunnittelussa. Aiheesta ei kuitenkaan löytynyt erillistä tutkimusta, joten tulevaisuudessa voisi olla hyvä tutkia tarkemmin esimerkiksi sitä, miten eettistä hakkerointia voitaisiin hyödyntää tietoturvakoulutuksissa tai niiden suunnittelussa.

LÄHTEET

Barton, K. A., Tejay, G., Lane, M. & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & security, 59*, 9-25.

Beebe, N. L. & Rao, V. S. (2010). Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process. *Communications of the Association for Information Systems, 26*, 17.

Beran, R. (2012). PENETRATION TESTING AS ACTIVE SECURITY CHECK ON. *Journal of Technology and Information Education, 4*(1), 89.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS quarterly, 34*(3), 523-548.

Cabrera, J. S., Reyes, A. R. L. & Lasco, C. A. (2020). Multicriteria Decision Analysis on Information Security Policy: A Prioritization Approach. *Advances in technology innovation, 6*(1), 31.

Calder, A. & Watkins, S. (2010). *Information Security Risk Management for ISO 27001/ISO 27002, third edition*. IT Governance Ltd.

Dalalana Bertoglio, D. & Zorzo, A. F. (2017). Overview and open issues on penetration test. *Journal of the Brazilian Computer Society, 23*(1), 1-16.

da Veiga, A. & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & security, 49*, 162-176.

Ding, A., De Jesus, G. & Janssen, M. (2019). Ethical hacking for boosting IoT vulnerability management: A first look into bug bounty programs and responsible disclosure. *In Proceedings of the Eighth International Conference on Telecommunications and Remote Sensing (ICTRS '19). Association for Computing Machinery*, New York, NY, USA, 49–55.

Goyal, K. K. & Gupta, C. P. *Cybersecurity : A Self-Teaching Introduction*, Mercury Learning & Information, 2020.

Hatfield, J. M. (2019). Virtuous human hacking: The ethics of social engineering in penetration-testing. *Computers & security, 83*, 354-366.

Kalloniatis, C., Mouratidis, H., Vassilis, M., Islam, S., Gritzalis, S. & Kavakli, E. (2014). Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. *Computer standards and interfaces, 36*(4), 759-775.

Lorenzini, G., Shaw, D. M. & Elger, B. S. (2022). It takes a pirate to know one: Ethical hackers for healthcare cybersecurity. *BMC medical ethics, 23*(1), 131.

Lundgren, B. & Möller, N. (2019). Defining Information Security. *Science and engineering ethics, 25*(2), 419-441.

Malladi, S. S. & Subramanian, H. C. (2020). Bug Bounty Programs for Cybersecurity: Practices, Issues, and Recommendations. *IEEE software, 37*(1), 31-39.

Mouton, F., Malan, M. M., Kimppa, K. K. & Venter, H. (2015). Necessity for ethics in social engineering research. *Computers & security, 55*, 114-127.

Mudiyanselage, A. K. & Pan, L. (2020). Security test MOODLE: A penetration testing case study. *International journal of computers & applications, 42*(4), 372-382.

Paananen, H., Lapke, M. & Siponen, M. (2020). State of the art in information security policy development. *Computers & security, 88*, 101608.

Palmer, C. (2001). Ethical hacking. *IBM systems journal, 40*(3), 769-780.

Puhakainen, P. & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS quarterly, 34*(4), 757-778.

Rocha Flores, W., Antonsen, E. & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & security, 43*, 90-110.

Samonas, S. & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security, 10*(3).

Styles, M. & Tryfonas, T. (2009). Using penetration testing feedback to cultivate an atmosphere of proactive security amongst end-users. *Information management & computer security, 17*(1), 44-52.

Thomas, G., Burmeister, O. & Low, G. (2018). Issues of Implied Trust in Ethical Hacking. *ORBIT Journal, 2*(1), 1-19.

Tietosuojavaltuutetun toimisto. (3.10.2017) Euroopan tietosuojaneuvoston ohjeet - hallinnolliset sakot https://tietosuoja.fi/euroopan-tietosuojaneuvoston-ohjeet

Verizon. (2022). "2022 Data Breach Investigations Report" https://www.verizon.com/business/resources/reports/dbir/

Whitman, M. E. & Mattord, H. J. (2013). *Management of information security*. Cengage Learning.

Winkler, I. S. & Dealy, B. (1995). Information Security Technology?...Don't Rely on It. A Case Study in Social Engineering. *Proceedings of the 5th conference on USENIX UNIX Security Symposium - Volume 5.*

Young, R. F. & Windsor, J. (2010). Empirical Evaluation of Information Security Planning and Integration. *Communications of the Association for Information Systems, 26*, 13.

Zhao, M., Laszka, A. & Grossklags, J. (2017). Devising Effective Policies for Bug-Bounty Platforms and Security Vulnerability Discovery. *Journal of information policy (University Park, Pa.)*, 7, 372-418.

Zhou, L., Varadharajan, V. & Hitchens, M. (2013). Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage. *IEEE transactions on information forensics and security, 8*(12), 1947-1960.