OULUN AMMATTIKORKEAKOULU

TIETOTURVAOSAAMISEN TARVE

Iikka Niemikorpi
Opinnäytetyö AMK
Kevät 2025
Tietojenkäsittelyn tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittelyn tutkinto-ohjelma

Tekijä: Iikka Niemikorpi
Opinnäytetyön otsikko: Tietoturvaosaamisen tarve
Työn ohjaaja: Markku Kekkonen
kevät 2025
Sivumäärä: 31 + 2 liitettä

Tämän opinnäytetyön tarkoituksena on avata lukijalle, mitä tietoturvaosaaminen on ja millainen tarve organisaatioilla on kyseiselle osaamiselle.

Tutkimustyön taustalla on yleinen ymmärryksen puute tietoturvaongelmista sekä osaajien riittämätön hyödyntäminen.

Tavoitteena on myös edistää kaltaisilleni osaajille tarjoutuvia mahdollisuuksia eri organisaatioissa sekä lisätä yhteistyöhalukkuutta.

Tietoperustassa selvennetään tutkimuksen seuraamisen kannalta keskeisiä käsitteitä. Tutkimusmenetelmänä käytetään määrällistä eli kvantitatiivista sisällönanalyysiä.

Työ etenee vastaamalla seuraaviin kysymyksiin: mitä tietoturvaosaaminen on, millaiselle osaamiselle on eniten tarvetta, ja onko organisaatioissa tärkeämpää hyödyntää ammattilaisia vai kouluttaa omaa henkilöstöä?

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Business Information Systems

Author: Iikka Niemikorpi
Title of thesis: The need for cybersecurity skills
Supervisor: Markku Kekkonen
Term and year when the thesis was submitted: Spring 2025
Number of pages: 31 + 2 appendices

The purpose of this thesis is to provide the reader with an understanding of what cybersecurity competence entails and to explore the demand for such expertise within organizations. The study is motivated by a general lack of awareness surrounding cybersecurity issues and the underutilization of skilled professionals in the field.

The research also aims to create more opportunities for professionals like myself by encouraging collaboration and increasing interest in cybersecurity competence across various organizations.

The theoretical framework clarifies key concepts necessary to follow the study. The research method employed is quantitative content analysis.

This thesis addresses the following core questions: What is cybersecurity competence? What types of cybersecurity skills are most in demand? And finally, is it more relevant for organizations to invest in utilizing external professionals or in training their existing staff?

SISÄLLYS

SANASTO

Pentestaus	Pentestaus eli penetraatiostestaus on systeemien tieturva-aukkojen etsimistä, jotta ne voitaisiin paikata
hakkeri	Hakkeri on henkilö, joka etsii ja käyttää jotain aukkoa tietoturvassa, laittomaan tarkoitukseen.
Haavoittuvuus	Tarkoittaa mitä tahansa heikkoutta, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamiseksi. (Kyberturvallisuuskeskus 2019)
Phishing	Tietojenkalastelu eli ”phishing” on verkko-rikollisuuden muoto, jossa uhri huijataan paljastamaan henkilö-kohtaisia tietoja, kuten henkilö-, talous- tai kirjautumis-tietoja. (F-secure)
Salasanaholvi	Salasanojen tallentamiseen käytettävä ohjelma, joka on usein pilvipalvelu.
Tietovuoto	Tietoa pääsee sellaisille tahoille, joille se ei ole tarkoitettu
Ransomware	On englantia ja tarkoittaa kiristysohjelmaa, joka kryptaa, eli salaa uhrin tiedostot käyttökelvottomiksi.
Palomuuri	Joko fyysinen tai tietokoneen sisällä oleva turvallisuus ohjelma, joka päättää, millaista tietoa päästetään läpi.
Bruteforce	Suomeksi väsytyshyökkäys on tapa arvata jokin asia, kokeilemalla jopa miljoonia eri vaihtoehtoja, kunnes arvaus menee oikein.

GitHub	Yhteistyöhön tarkoitettu pilvialusta, johon tallennetaan pääasiassa koodia.
Payload	Haittaohjelma, jonka hakkeri tahtoo saada uhrin koneelle.
Kryptaus	On tiedon salausta avaimella niin, ettei sitä voi lukea ilman avainta.

JOHDANTO

Valitsin tämän opinnäytetyön aiheen omasta kiinnostuksestani tietoturvaa kohtaan. Erityisesti minua motivoi halu tehdä tietoturvasta ymmärrettävämpää myös niille, joilla ei ole teknistä taustaa. Työtä tehdessäni haluan tuoda esiin havaintoni siitä, että monet vakavat tietomurrot johtuvat yllättävän usein yksinkertaisista, helposti vältettävissä olevista virheistä. Näiden virheiden ehkäiseminen vaatisi usein vain perustason ymmärrystä tietoturvasta tai hieman ammattilaisten hyödyntämistä.

Tietomurtojen määrä on ollut viime aikoina kasvussa. Esimerkiksi kiristysohjelmien (Ransomware) käyttö hyökkäyksissä kasvoi marraskuussa 2023 jopa 50 prosenttia verrattuna edellisvuoteen (Forbes, 2023). Myös kiristysohjelmista vaadittujen lunnasvaatimusten keskiarvo nousi merkittävästi: vuonna 2022 summa oli keskimäärin 812 380 dollaria, kun taas vuonna 2023 se oli jo 1 542 333 dollaria (SC Magazine, 2023).

Uskon, että vahva ja kestävällä pohjalla oleva tietoturva syntyy, kun yhdistetään asiantuntijoiden hyödyntäminen ja organisaation jäsenten yleinen tietoturvatietoisuus. Tämän työn tavoitteena on ennen kaikkea kannustaa vastuulliseen toimintaan ja hälventää tietoturvaan liittyvää mystiikkaa, sekä tehdä siitä koko organisaation yhteinen tavoite.

Opinnäytetyössäni tarkastelen yksittäisiä tietomurtotapauksia, jotka on julkaistu DataBreaches.net-sivustolla. Analysoin, mitkä tekijät ovat johtaneet näihin tapauksiin, ja kokoan yhteen toistuvimmat syyt. Tavoitteena on muodostaa kokonaiskuva siitä, millaiset henkilöstöön liittyvät sekä tekniset virheet ovat yleisimpiä, ja millaista osaamista tulevaisuudessa tarvitaan, jotta vastaavilta tilanteilta voitaisiin välttyä.

TIETOPOHJA

Jotta opinnäytetyöni vastaisi alkuperäistä suunnitelmaani, niin sen tulisi olla jokaiselle luettava, riippumatta teknisestä osaamisesta. Tämän vuoksi käymme läpi ensinnäkin mitä tietoturva on. Sen jälkeen yritän jakaa tietoturvaosaamisen edellä mainitulla tavalla yläkategorioihin. Ja lopulta jakaa nämä vielä alakategorioihin, kun kehittelemme koodausjärjestelmää. Tämän tietopohjan lopussa esittelen määrällisen, eli kvantitatiivisen sisällönanalyysin tutkimusmenetelmänä.

1.1 Tietoturva

Tietoturva on keskeinen osa laajempaa tietosuojan käsitettä. Sen tehtävänä on varmistaa tiedon luottamuksellisuus, eheys ja saavutettavuus (NIST Special Publication 1800-26A). Näillä kolmella peruskäsitteellä tarkoitetaan seuraavaa:

Luottamuksellisuus tarkoittaa, että tieto on luettavissa vain niille tahoille, joille se on tarkoitettu. Eheydellä viitataan siihen, että tiedon alkuperä on varma ja sitä ei ole muutettu luvattomasti. Saavutettavuus puolestaan merkitsee sitä, että tieto on saatavilla silloin, kun sitä tarvitaan.

Nämä kolme elementtiä muodostavat tietoturvan perustan. Vaikka kaikki osa-alueet ovat tietoturvan kannalta keskeisiä, julkisessa keskustelussa eniten huomiota saa usein luottamuksellisuus. Tämä korostuu erityisesti tilanteissa, joissa uutisoidaan tietomurroista ja yksityisten tietojen vuotamisesta.

Tietoturvaloukkaukset voivat johtua sekä teknisistä puutteista että ihmisen toiminnasta. Tekninen virhe tai inhimillinen virhe voi aiheuttaa sen, että jokin tietoturvan osa-alueista pettää. Tietoturva ei siten tarkoita pelkästään teknisiä ratkaisuja, kuten palomuureja tai virustorjuntaohjelmia, vaan se kattaa myös ihmisten toiminnan, ajattelutavat ja organisaation kulttuurin. Koko organisaation tulee toimia tietoturvallisesti, mikä tarkoittaa esimerkiksi sitä, että työntekijät osaavat

tunnistaa riskit, johto tukee turvallisuuskulttuuria, ja järjestelmät on suunniteltu kestämään erilaisia uhkia.

1.2 Tietoturvaosaaminen

Tietoturvaosaaminen on laaja ja moniulotteinen kokonaisuus, mutta tämän tutkimuksen yhteydessä jaottelen sen kahteen keskeiseen osa-alueeseen: henkilöstön yleiseen tietoturvaosaamiseen ja ammattilaisten tietoturvaosaamiseen.

Henkilöstön tietoturvaosaaminen tarkoittaa perustietoja ja -taitoja, jotka jokaisen organisaation jäsenen tulisi hallita. Näitä ovat esimerkiksi turvallinen salasanojen käyttö, huijausviestien tunnistaminen ja tietojen käsittely vastuullisesti. Näiden taitojen hallinta on koko henkilöstön yhteinen vastuu.

Ammattilaisten tietoturvaosaaminen puolestaan viittaa syvällisempään tekniseen asiantuntemukseen, jota tietoturva-ammattilaiset käyttävät suojatakseen organisaation infrastruktuuria. Tähän sisältyy esimerkiksi palomuurien ja tunkeutumisenestojärjestelmien ylläpito, haavoittuvuuksien arviointi ja teknisten hyökkäysten torjunta.

Kumpikaan näistä osa-alueista ei yksin riitä takaamaan tietoturvaa. Jos kaikki työntekijät ovat tietoturvatietoisia, mutta järjestelmät sisältävät teknisiä haavoittuvuuksia, on organisaatio silti altis hyökkäyksille. Vastaavasti, vaikka tekninen suojaus olisi huippuluokkaa, voi tietoturva vaarantua, jos työntekijä toimii huolimattomasti tai tulee huijatuksi sosiaalisen manipuloinnin keinoin. Siksi vahva tietoturva perustuu sekä tekniseen osaamiseen että koko henkilöstön tietoturvatietoisuuteen.

1.2.1 Henkilöstön tietoturvaosaaminen

Tietoturvaosaamista tulisi opettaa jokaiselle organisaation jäsenelle, sillä tietoturva on usein yhtä vahva kuin sen heikoin lenkki. Tämän ovat havainneet myös kyberrikolliset. Siksi yksittäiset työntekijät ovat usein heidän ensisijainen kohteensa.

Yksi yleisimmistä hyökkäysmenetelmistä on tietojenkalastelu (engl. phishing). Tässä määritelmä F-Securen artikkelista: Tietojenkalastelu eli ”phishing” on verkko-rikollisuuden muoto, jossa uhri huijataan paljastamaan henkilö-kohtaisia tietoja, kuten henkilö-, talous- tai kirjautumis-tietoja. Huijari tekeytyy yleensä joksikin luotettavaksi tahoksi. Tietojen urkkimiseen on useita erilaisia keinoja, kuten sähkö-postit, teksti-viestit, puhelut ja jopa QR-koodit, joiden avulla huijarit manipuloivat uhrinsa paljastamaan arvokkaita tietoja (F-Secure 2022).

IBM:n vuoden 2023 raportin mukaan tietojenkalastelu oli yleisin hyökkäyksen aloitusmuoto, ja se liittyi 41 %:iin tietoturvaloukkauksista (IBM, 2023). Tyypillisin kalastelumenetelmä on sähköposti, jossa esiintyjä tekeytyy organisaation sisäiseksi henkilöksi tai luotetuksi kumppaniksi. Tämänkaltaiset uhat voidaan torjua vain, jos jokainen työntekijä osaa tunnistaa huijausyritykset. Tämän takia koulutuksen tulisi olla koko organisaatiota koskevaa.

Toinen keskeinen osa-alue on käyttäjätunnusten ja salasanojen hallinta. Vaikka kehitys on menossa siihen suuntaan, että palvelut kuten Google tarjoavat salasanaholveja ja monivaiheista tunnistautumista, vahvojen salasanojen luominen ja suojaaminen on yhä kriittistä. Ihmisiä on edelleen tärkeä kouluttaa luomaan vaikeasti arvattavia salasanoja ja välttämään niiden uudelleenkäyttöä. GoodFirmsin vuoden 2021 kyselyn mukaan 30 prosenttia vastaajista (IT-asiantuntijoista, työntekijöistä sekä johtohenkilöistä) kertoi kokeneensa tietomurron heikkojen salasanojen vuoksi (GoodFirms, 2021). Lisäksi Keeper Securityn vuonna 2023 tekemän kyselyn mukaan 75 prosenttia vastaajista (yhteensä yli 8000 henkilöä Yhdysvalloista, Isosta-Britanniasta, Ranskasta ja Saksasta) ei noudata yleisesti hyväksyttyjä salasanakäytäntöjä (Keeper Security, 2023).

Vaikka työntekijä olisi koulutettu tunnistamaan kalasteluviestit ja hallitsemaan tunnuksiaan turvallisesti, riski ei koskaan poistu täysin. Mikäli hyökkääjä onnistuu saamaan pääsyn järjestelmään, syntyy usein poikkeavaa toimintaa, esimerkiksi epätavallisia kirjautumisia tai tiedonsiirtoja. Siksi on tärkeää, että työntekijöitä koulutetaan myös havainnoimaan ja reagoimaan epätyypilliseen käytökseen. Oikea toiminta oikeaan aikaan voi estää tietomurron etenemisen merkittävästi.

Yksi tietoturvaosaamisen tärkeimmistä osa-alueista on kyky ennaltaehkäistä tarpeettomia tietovuotoja. Sovelluskehityksen kontekstissa yksi yleisimmistä ja samalla helposti vältettävissä olevista virheistä on API-avainten tai muiden luottamuksellisten tunnistetietojen joutuminen vahingossa julkiseen lähdekoodiin. Tällainen tilanne voi syntyä esimerkiksi silloin, kun kehittäjä julkaisee koodia avoimeen lähdekoodivarastoon, kuten GitHubiin, ilman että tunnistetiedot on eriytetty tai suojattu asianmukaisesti.

Vaikka tällaiset virheet saattavat vaikuttaa yksittäistapauksilta, ne ovat yllättävän yleisiä ja voivat johtaa merkittäviin tietovuotoihin tai järjestelmien luvattomaan käyttöön. Tämän vuoksi kehitystyössä mukana olevien henkilöiden kouluttaminen tietoturvatietoisuuteen ja hyviin käytäntöihin, kuten salausavainten hallintaan ja konfiguraatiotiedostojen suojaamiseen, on keskeistä. Lisäksi tekniset valvontakeinot, kuten automaattiset tarkistustyökalut, voivat auttaa tunnistamaan ja ehkäisemään tällaisia virheitä jo kehityksen alkuvaiheessa.

1.2.2 Asiantuntijoiden rooli

Monella varmasti tulee ensimmäisenä mieleen haavoittuvuudet tähän kategoriaan. Haavoittuvuuden määritelmä Kyberturvallisuuskeskuksen mukaan on: Haavoittuvuus tarkoittaa mitä tahansa heikkoutta, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamiseksi. Haavoittuvuuksia voi olla esimerkiksi tietojärjestelmissä, sovelluksissa, laitteissa, prosesseissa, kotiautomaatiossa tai niitä voi aiheutua ihmisten toiminnan seurauksena. (Kyberturvallisuuskeskus 2020).

Olisi ideaalia, ettei haavoittuvuuksia tulisi, kun kehitetään uusia sovelluksia, mutta niitä vääjäämättä tulee kehittäjävirheiden johdosta. Koska haavoittuvuuksia tulee aina lisää, meidän on mietittävä, miten me löydämme ne ennen hakkereita.

Hakkerin määritelmä Tieteen termipankista (käännetty suomeksi): Henkilö, joka pyrkii murtautumaan tietojärjestelmien suojausten läpi tarkoituksenaan sabotoida ohjelmistoja tai päästä käsiksi suojattuun tietoon, hyödyntää sitä tai mahdollisesti

muokata sitä. Alun perin sanalla viitattiin taitavaan ohjelmoijaan, jolla oli laaja valikoima keinoja ja menetelmiä. (Tieteen termipankki)

Asiantuntijoiden rooli on pääasiassa pysyä hakkereita edellä ja tehdä hyökkäämisestä mahdollisimman vaikeaa. Tämä saavutetaan monesti tekemällä penetraatiotestauksia, eli “pentestejä”. Penetraatiotestauksen määritelmä NIST-raportista (käännetty suomeksi): Penetraatiotestaus eli tunkeutumistestaus on tietoturvatestausta, jossa testaajat jäljittelevät todellisen maailman hyökkäyksiä pyrkien tunnistamaan tapoja kiertää sovelluksen, järjestelmän tai verkon tietoturvaominaisuudet. Penetraatiotestauksessa käytetään usein oikeita hyökkäystapoja oikeita järjestelmiä ja tietoja vastaan, samoilla työkaluilla ja tekniikoilla kuin oikeat hyökkääjätkin käyttävät. Useimmissa penetraatiotesteissä pyritään löytämään useiden haavoittuvuuksien yhdistelmiä joko yksittäisessä järjestelmässä tai useammassa järjestelmässä, joiden avulla voidaan saavuttaa laajempi pääsy kuin mitä yksittäinen haavoittuvuus mahdollistaisi (NIST SP 800-115).

Ammattilaisten hyödyntäminen tulisi aloittaa jo siinä vaiheessa, kun uusia järjestelmiä suunnitellaan ja rakennetaan. Esimerkiksi toteutettaessa Microsoft Office 365 -ympäristöä organisaatiolle, asiantuntija suosittelisi monivaiheista tunnistautumista (MFA, Multi-Factor Authentication). Kyseessä on erittäin tehokas tapa estää luvaton pääsy käyttäjätunnuksilla. Monivaiheisella tunnistautumisella tarkoitetaan henkilöllisyyden varmistamista kahden tai useamman eri tunnistautumistavan avulla. Lähes kaikki käyttäjätilien kaappausyritykset voidaan estää monivaiheista tunnistautumista hyödyntämällä. Vaikka rikollinen saisikin haltuunsa käyttäjätunnuksen ja salasanan, palveluun ei pääse kirjautumaan ilman lisävahvistusta. Erityisesti palvelut, joissa käsitellään henkilö- tai maksutietoja, tulisi aina suojata monivaiheisella tunnistautumisella (Traficom, 2024).

Toinen keskeinen suojaustekniikka on salaus eli enkryptio. Salaus tarkoittaa tiedostojen muuntamista sellaiseen muotoon, että niitä ei voi lukea ilman oikeaa salausavainta. Esimerkiksi kiristysohjelmat käyttävät salausta tehdäkseen tiedostoista käyttökelvottomia, kunnes uhri maksaa lunnaat ja saa salausavaimen. Myös organisaatioiden tulisi huolehtia salauksen käyttöönotosta osana omaa

tietoturvapolitiikkaansa, mikäli sitä ei ole vielä toteutettu. Kuten tutkimuksen myöhemmissä osioissa havaitaan, salauksen puuttuminen on yksi yleisimmistä tekijöistä vakavissa tietomurroissa.

1.3 Kvantitatiivinen/määrällinen sisällönanalyysi

Kvantitatiivinen sisältöanalyysi on systemaattinen ja objektiivinen menetelmä viestinnän sisällön tutkimiseen, jossa aineistosta tunnistetaan toistuvia rakenteita ja piirteitä numeerisesti mitattavassa muodossa (Krippendorff, 2018). Se mahdollistaa suurtenkin aineistomäärien analysoinnin vertailevasti ja tilastollisesti, jolloin tutkija voi tunnistaa ilmiöitä, joita ei välttämättä laadullisin menetelmin havaittaisi. Sisältöanalyysi lähtee liikkeelle selkeästä tutkimuskysymyksestä ja operationalisoiduista luokista, joiden perusteella aineisto koodataan.

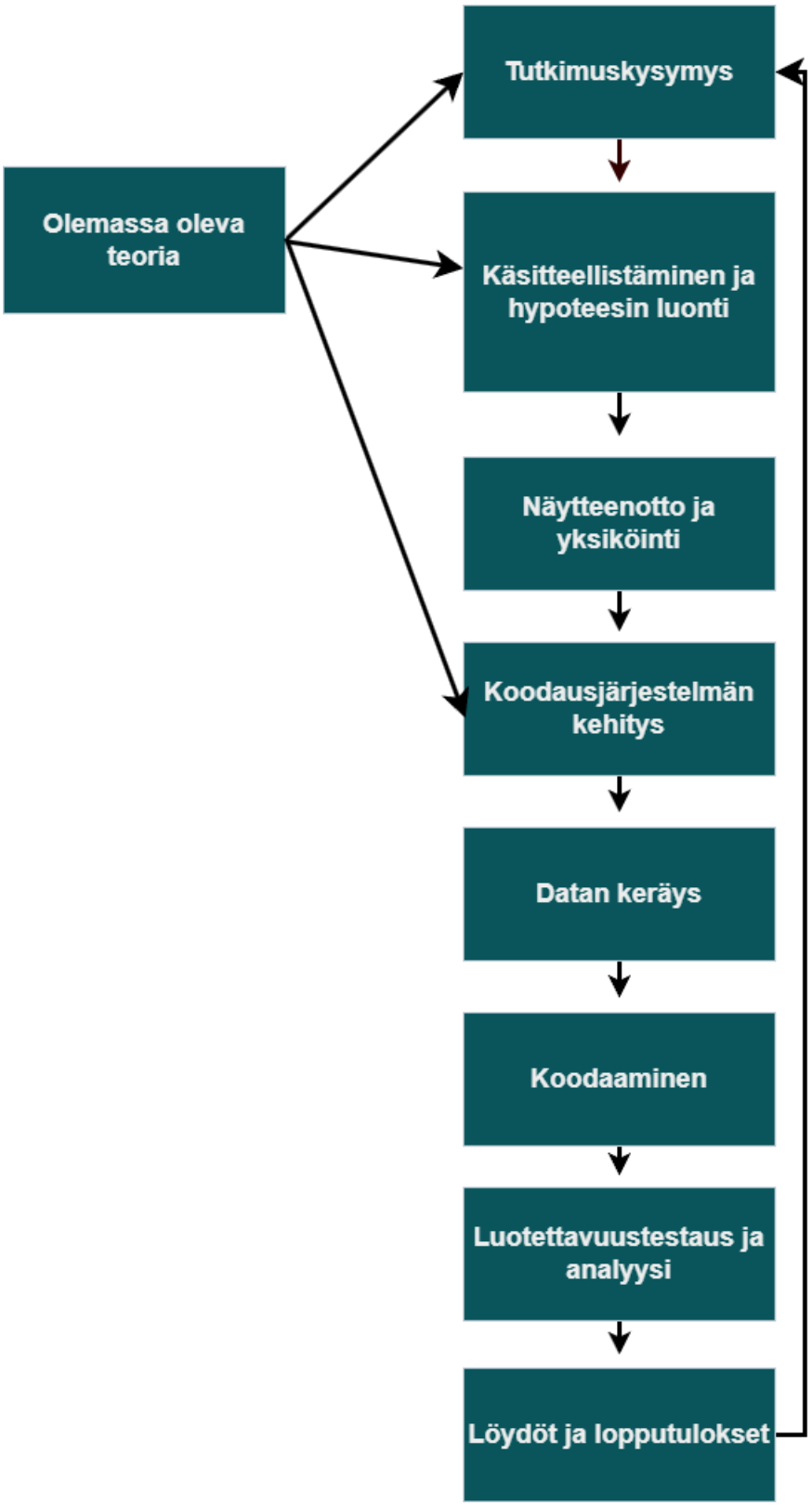
Tässä tutkimuksessa kvantitatiivista sisältöanalyysiä käytetään analysoimaan databreaches.net-sivustolla raportoituja tietomurtotapauksia, keskittyen siihen, minkälaisia tietoturvaosaamisen puutteita eri tapaukset sisältävät. Tavoitteena on luokitella tietomurrot esimerkiksi henkilöstövirheisiin, teknisiin haavoittuvuuksiin, puutteelliseen suojaukseen tai huonoon konfiguraatioon. Tällä tavalla voidaan tunnistaa, minkälaisessa osaamisessa näyttäisi olevan eniten puutteita organisaatioissa. Tutkimuksen avulla voidaan myös vertailla eri vuosien eroja sekä arvioida mahdollisia trendejä.

Analyysi edellyttää koodausluokitusten huolellista suunnittelua, jotta ne olisivat luotettavia ja toistettavia. Luokittelun pätevyyden varmistamiseksi voidaan käyttää esimerkiksi kahden koodaajan välistä reliabiliteettitarkastelua (Lombard, Snyder-Duch & Bracken, 2002). Tulokset esitetään tilastollisessa muodossa, esimerkiksi frekvensseinä ja prosenttiosuuksina, jolloin tutkimuskysymykseen voidaan vastata kvantitatiivisesti perustellusti.

TUTKIMUKSEN ETENEMINEN

Tässä opinnäytetyössä hyödynnetään sisällönanalyysia Databreaches.net-sivuston "Breach Incidents" -kategoriaan kuuluvista artikkeleista. Käyn läpi jokaisen artikkelin yksitellen ja tarkastelen, onko artikkelissa esitetty tietoa siitä, miten tietomurto onnistui. Mikäli artikkelista käy ilmi, että tapahtumaan vaikutti esimerkiksi henkilökunnan toiminta tai osaamisen puute, merkitsen sen havaintona ylös. Lisäksi kartoitan, minkälaista osaamista tai toimintatapaa olisi tarvittu murtautumisen estämiseksi, mikäli tämä käy tekstistä ilmi. Artikkelit, joissa syytä tai olosuhteita ei kuvata riittävän selkeästi, jätetään analyysin ulkopuolelle.

Menetelmä tuottaa numeerista aineistoa, joka voi olla hyödyllistä esimerkiksi organisaatioiden johdon suuntaan viestittäessä, kun arvioidaan tietoturvatoimien ja koulutuksen tarpeellisuutta sekä niihin suunnattavaa budjettia. Kvantifioidut tulokset tukevat myös jatkotutkimusta sekä tiedon jäsentämistä eri viestintäkanaviin, kuten artikkeleihin tai sosiaalisen median julkaisuihin. Mitä enemmän tietoturvasta keskustellaan ja jaetaan ymmärrettävää tietoa, sitä vahvemmaksi koko yhteiskunnan kyberturva kehittyy.



.

KUVA 1. Määrällisen sisällönanalyysin eri vaiheet (Rose, Spinks & Canhoto, 2015)

1.4 Tutkimuskysymys

Tutkimuksen lähtökohtana on tavoite muodostaa mahdollisimman tarkoituksenmukainen tutkimuskysymys, joka vastaa opinnäytetyön tavoitteisiin. Tutkimuksen taustalla oleva ongelma on se, että julkisesti saatavilla oleva tieto organisaatioiden tietoturvaosaamistarpeista on vähäistä. On epäselvää, millaista osaamista organisaatioilta konkreettisesti puuttuu, ja mihin osa-alueisiin tietoturvakehityksessä tulisi erityisesti panostaa.

Alkuperäiseksi tutkimuskysymykseksi muotoutui: Millaisia tietoturvaosaamistarpeita organisaatioilla on? Koska tutkimusaineisto koostuu uutisartikkeleista, jotka käsittelevät todellisia tietomurtoja, tutkimuskysymystä tarkennettiin vastaamaan paremmin aineiston luonnetta. Tämän opinnäytetyön varsinaiset tutkimuskysymykset ovat: Millaisia osaamistarpeita nousee esiin todellisista tietomurroista? Sekä: Onko henkilöstön koulutuksella vai tietoturva-ammattilaisten hyödyntämisellä suurempi merkitys tietomurtojen ennaltaehkäisyssä?

Tutkimuskysymykset ohjaavat sisällönanalyysia, jossa pyritään tunnistamaan, millaisia osaamispuutteita tai toimintavirheitä tietomurtoihin on liittynyt, ja mitä osaamista niiden ehkäisy olisi mahdollisesti edellyttänyt.

1.5 Käsitteellistäminen ja hypoteesin luonti

Tutkimuksen keskeiset käsitteet ovat henkilöstön tietoturvaosaaminen ja ammattilaisten tietoturvaosaaminen. Nämä kaksi käsitettä toimivat tutkimuksessa toisensa poissulkevina pääluokkina, joiden avulla pyritään tarkentamaan, minkälaista osaamista tietomurtojen ehkäisy olisi edellyttänyt. Kategorisointi mahdollistaa sen, että tutkimuksen analyysi vastaa mahdollisimman täsmällisesti tutkimuskysymykseen osaamistarpeiden luonteesta.

Pääkategorioiden alle muodostetaan lisäksi alakategorioita, jotka kuvaavat tarkemmin havaittuja osaamistarpeita. Alakategorioiden tarkka erottelu ei kuitenkaan ole tutkimuksessa poissulkevaa; toisin sanoen, mikäli jokin alakategoria ei ole suoraan tunnistettavissa, mutta osaaminen voidaan selkeästi sijoittaa

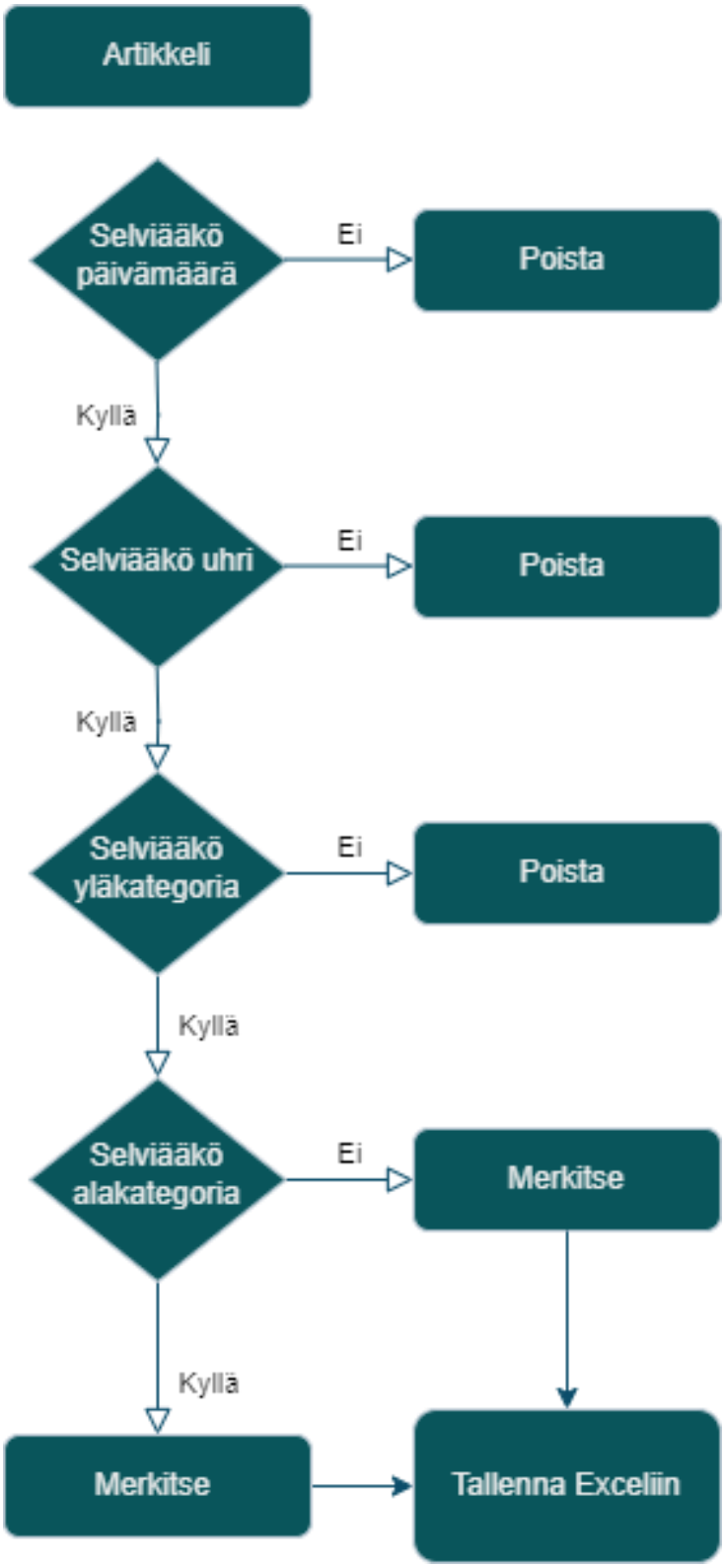
jommankumman pääluokan alle (henkilöstön tai ammattilaisten osaaminen), se otetaan analyysissä mukaan.

Tutkimuksen hypoteesi on, että ammattilaisten osaamisella on merkittävämpi rooli tietoturvan varmistamisessa kuin usein ymmärretään. Tämä on kuitenkin investointikysymys, sillä asiantuntijapalveluiden hyödyntäminen on monesti sekä kallista että pitkäjänteistä. Vaikka henkilöstön kouluttaminen on tärkeää ja tietoturvakoulutukset ovat tehokkaita, pelkästään koulutuksen varassa toimiva organisaatio ei saavuta riittävää suojaustasoa. Ammattilaisten osaaminen tuo syvempää teknistä ymmärrystä ja valmiuksia, joita tarvitaan monimutkaisten uhkien torjumiseen.

1.6 Näytteenotto ja yksiköinti

Tutkimusaineistosta otin analyysin näytteeksi kymmenen ensimmäistä artikkelia. Tämä valinta perustui oletukseen, että näiden pohjalta saadaan hyvä kokonaiskuva siitä, millaista lajittelujärjestelmää tutkimuksessa tulisi käyttää. Ensimmäiset kaksi lajitteluvaihetta varmistavat, ettei samaa tapausta käsitellä aineistossa kahteen kertaan. Kolmas vaihe kuvaa analyysin yksikköä, jota laskemme tarkasti tutkimustamme varten. Tämä muodostuu artikkelin käsittelemän tietomurron mahdollisesta henkilöstön osaamistarpeesta tai ammattilaisten osaamistarpeesta.

Osaamistarpeen määrittäminen perustuu siihen, mikä tietomurron taustalla oleva syy on ollut: onko kyseessä henkilöstön puutteellinen koulutus vai tekninen haavoittuvuus. Henkilöstön osaamiseen liittyviä tekijöitä ovat muun muassa kalasteluhyökkäykset (engl. phishing), heikot salasanat, tietovuodot sekä organisaation sisäisten käytäntöjen rikkominen. Teknisen osaamisen osa-alueisiin puolestaan kuuluvat esimerkiksi haavoittuvuudet, virheelliset järjestelmäkonfiguraatiot, puuttuvat suojaustoimenpiteet sekä vanhentuneen teknologian käyttö. Jos jokin näistä alakategorioista selviää lisäämme sen myös mukaan. Ja kuten aikaisemmin jo kerroin, jos mitään osaamistarvetta ei ole selkeästi havaittavissa jätämme artikkelin poissa tutkimuksesta. Jos aineistossa mainitaan sama puute useaan kertaan, laskemme sen vain kerran mukaan. Tämä sen takia, ettei tulokset vääristy, kun artikkelissa ilmaistaan sama osaamistarve useasti.



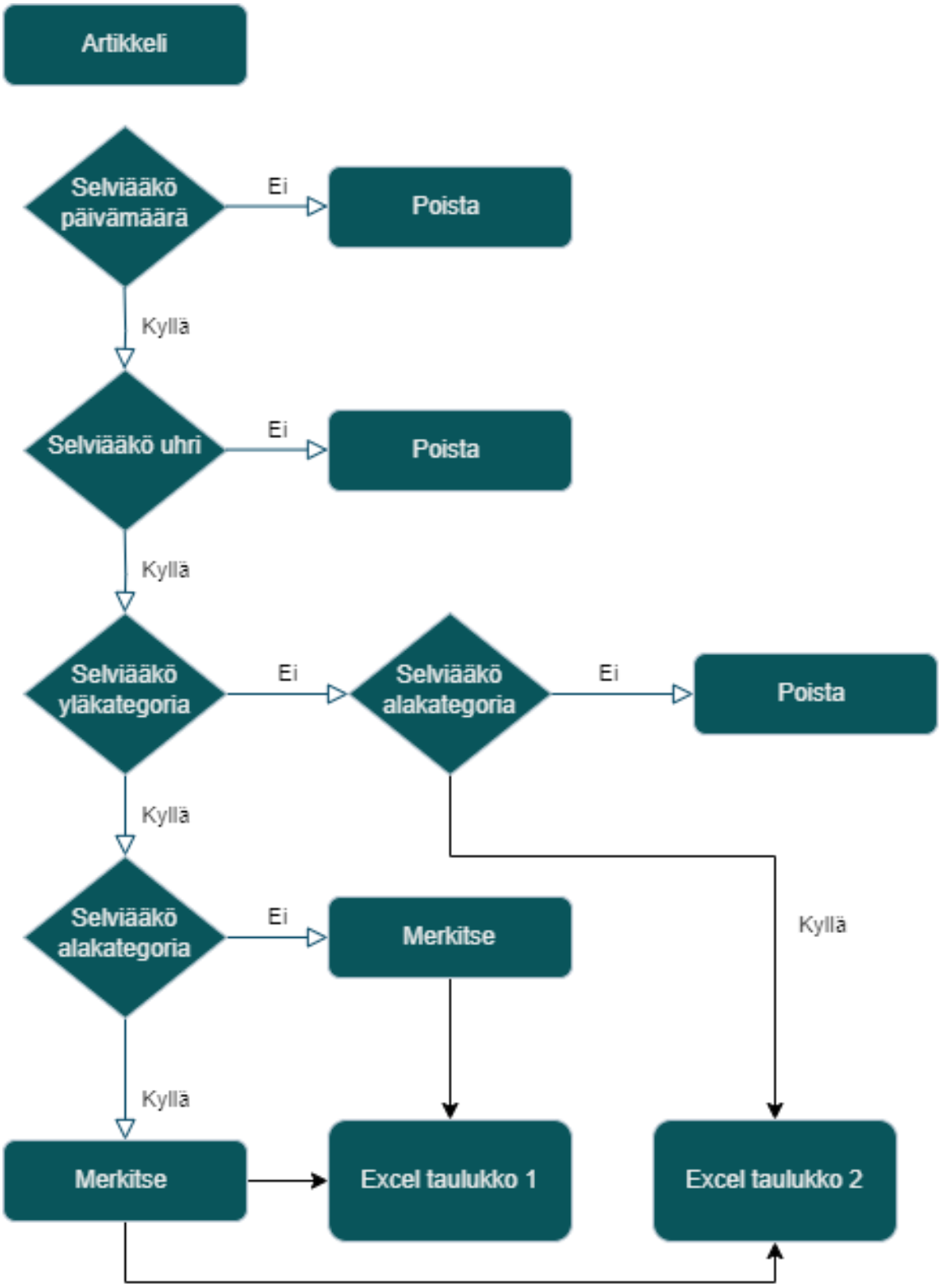
KUVA 2. Ensimmäinen versio artikkeleiden lajittelujärjestelmästä

1.7 Koodausjärjestelmän kehitys

Ensimmäinen kehitysideani syntyi jo ensimmäisen artikkelin analyysin yhteydessä. Kyseessä oli tietoturvaloukkaus, jossa uhri oli lasten hyväntekeväisyysjärjestö. Vaikka organisaation nimeä ei suoraan mainittu, sen tunnistaminen oli mahdollista sen harvinaisen luonteen vuoksi sekä alkuperäisen lähdeaineiston kautta. Tästä opin, että myös vastaavissa tapauksissa nimeämättömät organisaatiot voidaan ottaa huomioon analyysissa, mikäli tunnistettavuus on varmistettavissa.

Toinen kehitysidea liittyi siihen, kuinka monissa tapauksissa hyökkäyksen sisäänpääsyn keino jää epäselväksi. Tämä havainto muutti olennaisesti analyysin rakennetta, minkä vuoksi haluan tässä selventää uuden rakenteen perusteet. Aineisto jaetaan kahteen erilliseen taulukkoon: Ensimmäiseen taulukkoon kirjataan tapaukset, joissa hyökkäyksen mahdollistanut tekijä on selkeästi tunnistettavissa. Toiseen taulukkoon puolestaan sijoitetaan tapaukset, joissa hyökkäyksen keinoa ei ole voitu määritellä, mutta joissa ilmenee jokin tietty osaamistarve alakategorioista.

Tällä menetelmällä pyrimme tuottamaan luotettavaa tietoa erityisesti kahteen keskeiseen tutkimuskysymykseen: Onko henkilöstön koulutus vai ammattilaisten hyödyntäminen relevantimpaa (Taulukko 1) sekä millaisia osaamistarpeita todelliset tietomurrot paljastavat (Taulukko 2).



KUVA 3. Uusi versio artikkeleiden lajittelujärjestelmästä

1.8 Datan keräys

Tässä tutkimuksessa tarkastelen, kuinka usein eri tietoturvaosaamisen tarpeet nousevat esiin julkisesti saatavilla olevassa aineistossa. Tutkimusaineistona käytän DatBreaches.net -sivuston tietoturvaloukkauksia käsitteleviä artikkeleita.

Aineisto koostuu DatBreaches.net -sivuston Breach Reports -kategoriassa julkaistuista artikkeleista. Datan keruun aikaväli on 24.4.2024–24.4.2025. Valittu ajanjakso takaa aineiston ajantasaisuuden ja riittävän määrän tilastollisesti merkittävien johtopäätösten tekemiseksi.

Aineistoa voi itse tutkia osoitteessa: https://databreaches.net/category/breach-reports/

1.9 Koodaaminen

Seuraavassa käydään tarkemmin läpi tutkimuksen koodausjärjestelmää sekä selvennetään, mitä eri alakategoriat sisältävät.

Tutkimuksessa henkilökunnan osaaminen jaetaan neljään alakategoriaan. Ensimmäisenä on tietojenkalastelu (engl. phishing), jossa hyökkääjä esiintyy luotettavana tahona ja pyrkii saamaan uhrilta esimerkiksi arkaluonteista tietoa tai saamaan tämän lataamaan haittaohjelman. Toisena alakategoriana on heikko salasana, joka usein mahdollistaa järjestelmään pääsyn esimerkiksi väsytyshyökkäyksen (engl. bruteforce) avulla. Kolmantena on tietovuoto, joka ei välttämättä johda välittömään hyökkäykseen, mutta jonka kautta hakkerit voivat löytää herkkiä tietoja julkisista lähteistä, kuten pilvipalveluista (esimerkiksi GitHubista ja GitLabista). Neljäntenä on käytäntöjen rikkominen, joka ei yleensä ole suora syy tietomurtoon, mutta voi mahdollistaa hyökkäyksen jatkumisen esimerkiksi silloin, kun haittaohjelman asennustiedosto (engl. payload) jää poistamatta uhrin tietokoneelta.

Tekninen osaaminen koostuu myös neljästä alakategoriasta. Haavoittuvuus tarkoittaa teknistä heikkoutta ohjelmistossa, kuten SQL-injektiohyökkäystä, jonka avulla hyökkääjä voi manipuloida tietokantaa omiin tarkoituksiinsa. Huono

konfiguraatio viittaa järjestelmän virheellisiin asetuksiin. Esimerkiksi Windows-ympäristössä salasanojen lukituksen puuttuminen väsytyshyökkäyksiä vastaan on tyypillinen esimerkki. Puuttuva suojauskerros on tutkimuksen yleisin kategoria ja kattaa esimerkiksi salauksen puuttumisen sekä yksivaiheisen tunnistautumisen käytön. Lopuksi vanhentunut teknologia on jatkuvasti ajankohtainen ongelma, sillä vanhentuneiden järjestelmien käyttö altistaa aina erilaisille riskeille ja haavoittuvuuksille.

1.10 Luotettavuustestaus ja analyysi

Koodaustyöni luotettavuuden varmistamiseksi kävin läpi kymmenen ensimmäistä artikkelia uudelleen ja vertasin uusia havaintoja aiempiin tuloksiini. Toisen tutkijan perehdyttäminen koodausprosessiin osoittautui haastavaksi, joten tein uudelleenkoodauksen itse noin kolmen viikon kuluttua alkuperäisestä analyysista.

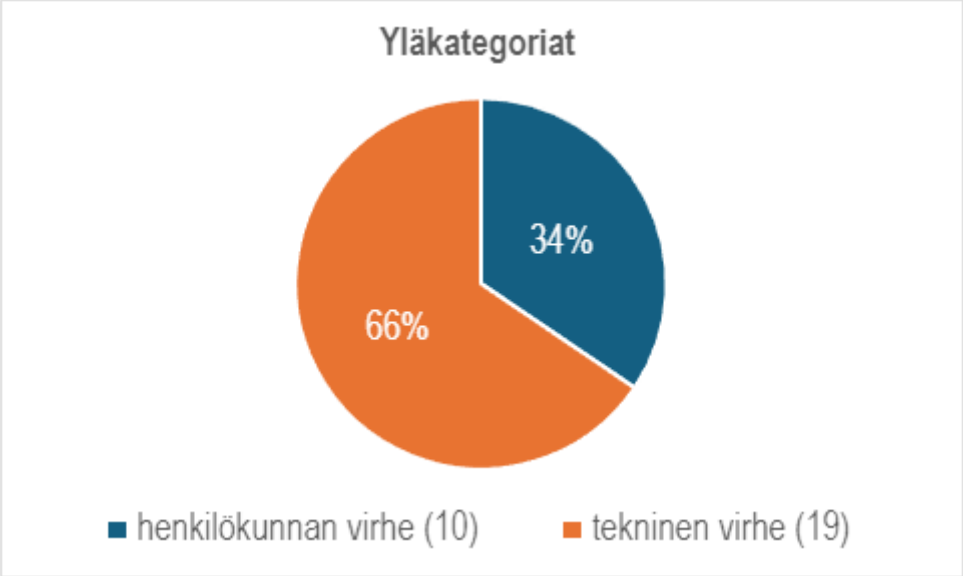
luotettavuustestaus		ihmis	tekninen
Change healthcare	tietovuoto, puuttuva suojauskerros	x	
blackbaud	haavoittuvuus,puuttuva suojauskerros, käyt	-	x
snowflake	puuttuva suojauskerros		x
consulting radiologists	puuttuva suojauskerros, huono konfiguraatio	-	-
Florida CHC	haavoittuvuus,		x
healthed	haavoittuvuus		x
MLCB	haavoittuvuus		x
Tabb Inc	huono konfiguraatio, puuttuva suojaus		x
CFIUS	käytäntöjen rikkominen	-	-
NPD			x

KUVA 4. Luotettavuustestaus

Luotettavuustestauksen tuloksena havaitsin, että kaikki yläkategoriat olivat identtisiä aiempaan koodaukseen verrattuna. Alakategorioissa esiintyi yksi uusi merkintä Blackbaudin tapausta käsittelevässä artikkelissa. Ottaen huomioon aineiston luonteen sekä koodausjärjestelmän laaja-alaisuuden, tulosta voidaan pitää varsin hyvänä.

1.11 Löydöt ja lopputulokset

Ensimmäisen taulukon mukaan analysoiduissa tapauksissa tunnistettiin yhteensä 10 henkilöstöön liittyvää virhettä ja 19 teknistä virhettä, jotka johtivat tietomurtoon. Aineistossa oli yhteensä 34 uniikkia artikkelia.



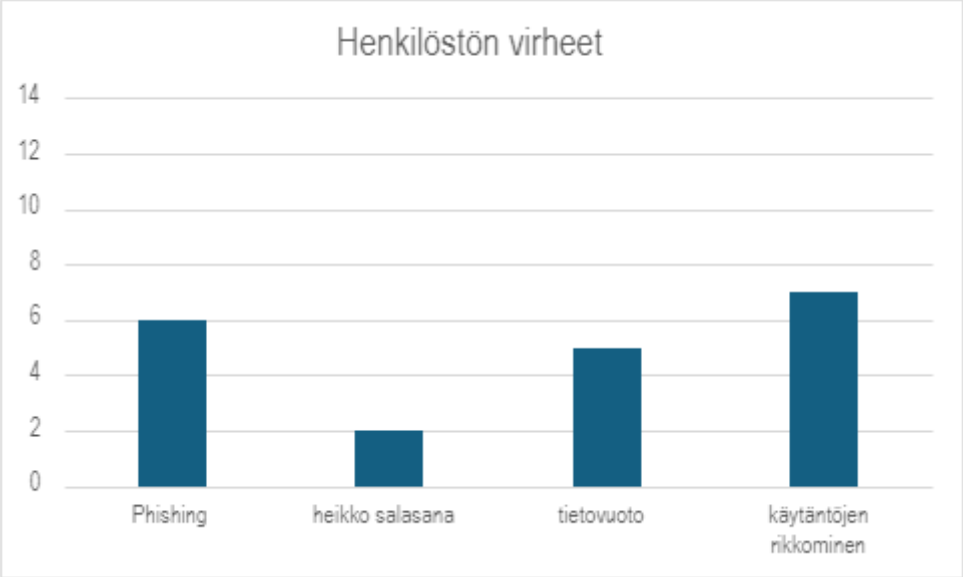
KUVA 5. Yläkategoriat

Tutkimustulokset vahvistavat alkuperäisen hypoteesini, sillä teknisten virheiden määrä ylitti henkilöstön virheiden määrän. Tämä tulos on merkittävä, sillä se viittaa siihen, että suurten tietomurtojen ennaltaehkäisyssä tarvittaisiin erityisesti ammattilaisten asiantuntemusta.

On kuitenkin tärkeää huomioida, että tässä tutkimuksessa henkilöstön virheillä tarkoitetaan nimenomaan henkilöstön tekemistä virheistä aiheutuneita murtoja, ei kaikkia ihmisperäisiä virheitä yleisesti. Esimerkiksi tekninen haavoittuvuus saattaa olla ihmisen aiheuttama, mutta sitä ei tässä tutkimuksessa luokitella henkilöstön virheeksi. Tämä rajaus on tehty, jotta tutkimus voisi tarkemmin vastata keskeiseen tutkimuskysymykseen: onko henkilöstön koulutus vai ammattilaisten hyödyntäminen relevantimpaa?

Toisen taulukon tulokset kuvaavat havaittuja osaamistarpeita tietoturvaloukkauksissa. Henkilöstön osaamisen puutteita olivat tietojenkalastelu (6 tapausta),

heikot salasanat (2 tapausta), tietovuodot (5 tapausta) sekä käytäntöjen rikkominen (7 tapausta).



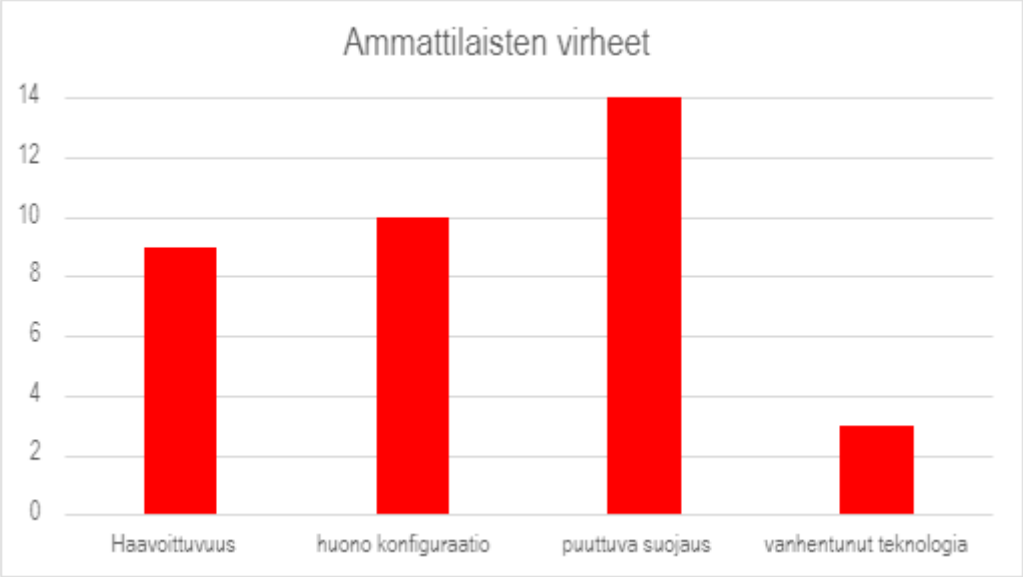
KUVA 6. Henkilöstön virheet

Hieman yllättävästi käytäntöjen rikkominen oli yleisin henkilöstön virhe. Tämä esiintyi useimmiten joko välinpitämättömyytenä tai kyvyttömyytenä toimia oikein, kun on havaittu tietomurto tai jokin tietoturvaongelma. Henkilöstölle tulisi ohjeistaa, että näitä havaintoja saa ja pitää nostaa esiin, kun niitä tulee vastaan.

Tietojenkalastelu (engl. phishing) oli kanssa iso kategoria ilman yllätyksiä. kalastelusta kirjoitin jo aikaisemmin paljon ja se tulee varmasti olemaan suuri ongelma myös jatkossa.

Tietovuoto oli myös suuri tekijä ja tämän luvun laskeminen onnistuu vain henkilöstön tietoisuutta kasvattamalla. Suuri osa henkilökunnan jäsenistä, jotka aiheuttavat tietovuodon eivät itse ole edes tietoisia asiasta. Tämä aiheuttaa taas sen, että tietovuodon löytää luultavimmin jokin henkilö, joka saattaa käyttää tietoa väärin.

Ammattilaisten osaamisen puutteita olivat haavoittuvuudet (9 tapausta), huono konfiguraatio (10 tapausta), puuttuva suojaus (14 tapausta) ja vanhentunut teknologia (3 tapausta).



KUVA 7. Ammattilaisten virheet (tai puutteellinen hyödyntäminen)

Ammattilaisten virheistä suurin oli puutuva suojauskerros. Puuttuva suojauskerros on hieman laajahko käsite ja ehkäpä yksivaiheinen todistus olisi voinut olla oma kategoriansakin. Tämä kategoria on näin suuri yksivaiheisen todistuksen ja puutuvan salauksen takia.

Huono konfiguraatio tulee heti perässä. Tässä kategoriassa yleisin tapaus on jonkinlainen organisaation toimintaa auttava sovellus, jota hakkeri pääsee hyödyntämään.

Haavoittuvuus oli kategoria, jota itse oletin suurimmaksi, se ei kuitenkaan pitänyt paikkaansa. Tietenkin kaikkia näitä voitaisiin kutsua haavoittuvuuksiksi, mutta tämän tutkimuksen kontekstissa tarkoitan haavoittuvuudella ohjelmistossa olevalla haavoittuvuudella.

Vanhentunut teknologia oli yllättävän pieni tulos ja se selittyy varmaankin sillä, että yritykset eivät välttämättä halua kertoa julkisesti, että päivityksiä ei ole hoidettu. Voi myös olla mahdollista, että tämän kaltainen hyökkäysvektori alkaa hiljalleen pienentyä, sillä ihmiset alkavat olla tästä ongelmasta jo yleisesti tietoisia.

POHDINTA

Tuloksiemme perusteella organisaatioilla on erityisesti tarvetta erilaisten suojauskerrosten lisäämiseen ohjelmistoissa. Erityisesti monivaihetunnistus ja salaus eli kryptaus tulisi lisätä jokaisen organisaation tietoturvaan. Teknisellä puolella taas ammattilaisten osaamista tarvitaan, sillä haavoittuvuuksista ja huonosta konfiguraatiosta johtuneita murtoja tapahtui paljon. Tietojenkalastelun vastaista koulutusta tulee jatkaa, sillä se on edelleen hyvin relevantti uhka. Oikeaoppisia käytäntöjä tulee opettaa vielä enemmän ja tämä on yksi kiinnostavimmista tutkimustuloksista. Monesti keskitymme estämään tietomurrot, mutta unohdammeko opettaa henkilöstölle, kuinka jo alkaneiden tietomurtojen tuhot voidaan minimoida?

Tutkimuksen keskeinen havainto on, että suuri osa tietomurroista olisi ollut estettävissä oikeanlaisen osaamisen avulla. Tämä pätee sekä henkilöstön että asiantuntijoiden tasolla. Käytännön osaamisen ja tietoisuuden puutteet aiheuttavat merkittävän osan murroista ja juuri siksi osaamisen kehittäminen on olennaista.

Oikein kohdennettu henkilöstökoulutus voisi estää merkittävän määrän tietojenkalasteluhyökkäyksiä, tietovuotoja ja käytäntöjen rikkomisia. Samalla ammattilaisten asiantuntemuksella olisi ollut ratkaiseva vaikutus monien teknisten virheiden, kuten suojausten puutteiden ja konfiguraatiovirheiden, ennaltaehkäisyssä.

Kysymys ei siis ole siitä, onko koulutus vai asiantuntijuus tärkeämpää, vaan siitä, miten molemmat voidaan integroida organisaatioiden tietoturvatoimintaan saumattomasti. Suurin hyöty saadaan aikaan, kun kaikki tietävät roolinsa ja heillä on valmiudet toimia oikein tietoturvan vaarantuessa. Tämä on koko tutkimuksen keskeisin johtopäätös ja viesti: Osaaminen on avain tietomurtojen ennaltaehkäisyyn sekä teknisellä, että inhimillisellä tasolla.

LÄHTEET

Wikipedia 2024. Penetraatiotestaus. Luettavissa: https://fi.wikipedia.org/Wiki/Penetraatiotestaus. Luettu: 13.3.2025.

Kyberturvallisuuskeskus 2019. Kyberturvallisuuskeskus. Haavoittuvuudet – miten niistä ilmoitetaan oikein? Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-miten-niista-ilmoitetaan-oikein?. Luettu: 13.3.2025.

Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J. & Sweetnam, J. 2020. NIST special publication 1800-26A. Luettavissa: https://doi.org/10.6028/NIST.SP.1800-26. Luettu: 29.5.2025.

Sobers, R. 2024. 157 Cybersecurity Statistics and Trends. Luettavissa: https://www.varonis.com/blog/cybersecurity-statistics. Luettu: 29.5.2025.

Rose, S., Spinks, N. & Canhoto, A. 2015. Stages of Quantitative Content Analysis. Luettavissa: https://www.researchgate.net/profile/David-Morgan-43/post/How-can-I-measure-learners-collaboration-skills-quantitatively-or-qualitatively/attachment/59d64cfe79197b80779a6a72/AS%3A486422697254912%401492983616025/download/Quantitative+content+analysis.pdf. Luettu: 29.5.2025.

Krippendorff, K. 2018. Content analysis: An introduction to its methodology. Luettavissa: https://books.google.fi/books?id=nE1aDwAAQBAJ&lpg=PP1&ots=y_bmZndQbz&dq=Content%20analysis%3A%20An%20introduction%20to%20its%20methodology&lr&hl=fi&pg=PP1#v=onepage&q=Content%20analysis:%20An%20introduction%20to%20its%20methodology&f=false. Luettu: 29.5.2025.

Lombard, M., Snyder-Duch, J. & Bracken, CC. 2002. Content Analysis in Mass Communication: Assessment and Reporting of Intercoder Reliability. Luettavissa: https://doi.org/10.1111/j.1468-2958.2002.tb00826.x. Luettu: 29.5.2025.

Forbes 2023. Cybersecurity Trends & Statistics; More Sophisticated And Persistent Threats So Far In 2023. Luettavissa: https://www.forbes.com/sites/chuckbrooks/2023/05/05/cybersecurity-trends--statistics-more-sophisticated-and-persistent-threats-so-far-in-2023/?sh=76b968e37cb6. Luettu 27.5.2025.

SC Magazine 2023. Report: Ransomware payouts and recovery costs went way up in 2023. Luettavissa: https://www.scworld.com/resource/report-ransomware-payouts-and-recovery-costs-went-way-up-in-2023. Luettu 27.5.2025.

Tieteen termipankki 2025. Hakkeri. Luettavissa: https://tieteentermipankki.fi/wiki/Tietojenk%C3%A4sittelytiede:hakkeri. Luettu: 27.5.2025.

F-Secure 2022. Mitä on tietojen-kalastelu eli phishing? Näin verkko-urkinta toimii. Luettavissa: https://www.f-secure.com/fi/articles/what-is-phishing. Luettu: 27.5.2025.

GoodFirms 2021. Top Password Strengths and Vulnerabilities: Threats, Preventive Measures, and Recoveries. Luettavissa: https://www.goodfirms.co/resources/top-password-strengths-and-vulnerabilities. Luettu: 28.5.2025.

Keeper Security 2023. Password Management Report. Luettavissa: https://www.keeper.io/hubfs/5481240/Reports/Password-Management-Report-Unifying-Perception-with-Reality-English.pdf. Luettu: 28.5.2025

LIITTEET

Liite 1 Yläkategorioiden tulokset

Liite 2 Alakategorioiden tulokset

LIITE 1

	pvm	org	virhe	ihmisvirhe	tekninen virhe	henkilökur tekninen virhe (19)
1	01.05.2024	Change healthcare	ihmis	x		
2	21.05.2024	Blackbaud	tekninen		x	10
3	12.06.2024	Snowflake	tekninen		x	
5	03.07.2024	Florida Community H	tekninen		x	19
6	16.07.2024	Healthed	tekninen		x	
7	24.07.2024	MLCB	tekninen		x	
10	19.08.2024	NPD	tekninen		x	
11	02.09.2024	Verkada	tekninen		x	
13	20.09.2024	Barbados Revenue Au	tekninen		x	
14	01.10.2024	Epsilon	ihmis	x		
15	03.10.2024	PSNI	ihmis	x		
16	04.10.2024	Alaska DOC	tekninen		x	
17	05.10.2024	Center for Orthopaed	ihmis	x		
18	09.10.2024	Marriott and Starwoo	tekninen		x	
19	03.11.2024	Chelan Douglas H	ihmis	x		
20	20.11.2024	Central Group	tekninen		x	
21	25.11.2024	Geico and Travelers	tekninen		x	
22	25.11.2024	Inmediata Health Group			x	
23	19.12.2024	Noblr			x	
24	21.12.2024	IDHS	ihmis	x		
25	14.01.2025	Robinhood	ihmis	x		
26	17.01.2025	MedSave	tekninen		x	
27	10.02.2025	Humboldt IPA		x		
28	07.03.2025	Chicago Public Schoc	tekninen		x	
29	21.03.2025	OrthoMinds	tekninen		x	
30	31.03.2025	GCHQ	ihmis	x		
31	31.03.2025	ImagineX	tekninen		x	
32	01.04.2025	Vitenas Cosmetic	tekninen		x	
34	24.04.2024	PIH Health	ihmis	x		

ID	pvm	org	alakategoria(t)	lisätietoja	Phishing	heikko salasana	tietovuoto	käytäntöjen rikkominen
1	01.05.202	Change he	tietovuoto, puuttuva suojaus		6	2	5	7
2	21.05.202	Blackbaud	haavoittuvuus,puuttuva suojaus					
3	12.06.202	Snowflake	puuttuva suojaus		Haavoittuv	huono kon	puuttuva s	vanhentunut teknologia
4	27.06.202	Consulting	huono konfiguraatio, puuttuva suojaus		9	10	14	3
5	03.07.202	Florida Co	haavoittuvuus					
6	16.07.202	Healthed	haavoittuvuus					
7	27.07.202	MLCB	haavoittuvuus					
8	15.08.202	Tabb inc	huono konfiguraatio, puuttuva suojaus					
9	16.5.2024	CFIUS	käytäntöjen rikkominen					
11	02.09.202	Verkada	heikko salasana, puuttuva suojauskerros					
12	21.09.202	MCC911	puuttuva suojaus					
13	20.09.202	Barbados I	haavoittuvuus					
14	01.10.202	Epsilon	tietovuoto					
15	03.10.202	PSNI	tietovuoto					
16	04.10.202	Alaska DO	tietovuoto, huono konfiguraation					
17	05.10.202	Center for	phishing, heikko salasana, huono konfiguraatio, puuttuva suojaus, vanhentunut teknologia					
18	09.10.202	Marriott ar	huono konfiguraatio, puuttuva suojaus, vanhentunut teknologia,					
19	03.11.202	Chelan C	Phishing					
20	20.11.202	Central Gr	käytäntöjen rikkominen, Haavoittuvuus, huono konfiguraatio					
21	25.11.202	Geico and	käytäntöjen rikkominen, Haavoittuvuus, huono konfiguraatio, puuttuva suojaus					
22	10.12.202	Inmediata	huono konfiguraatio, käytäntöjen rikkominen,					
23	19.12.202	Noblr	Huono konfiguraatio, puuttuva suojaus					
24	21.12.202	IDHS	Phishing					
25	14.01.202	Robinhooc	Phishing					
26	17.01.202	MedSave	käytäntöjen rikkominen, Haavoittuvuus, puuttuva suojaus					
27	15.02.202	Humboldt	Phishing					
28	07.03.202	Chicago Pi	Haavoittuvuus					
29	21.03.202	OrthoMinc	puuttuva suojaus					
30	31.03.202	GCHQ	tietovuoto					
31	31.03.202	ImagineX	käytäntöjen rikkominen, vanhentunut teknologia					
32	01.04.202	Vitenas Cc	huono konfiguraatio					
33	19.04.202	Baltimore (	puuttuva suojaus					
34	24.04.202	PIH Health	Phishing, käytäntöjen rikkominen					