jamk

Kriittisen poikkeaman jälkeinen purku-keskustelu

Karri von Schalien

Opinnäytetyö, AMK
Helmikuu 2024
Tieto- ja Viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

von Schalien Karri

Kriittisen poikkeaman jälkeinen purkukeskustelu

Jyväskylä: Jyväskylän ammattikorkeakoulu. **Helmikuu 2024**, 32 sivua

Tieto- ja Viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Security Operations Centerin (SOC) toimintaan keskittyvä opinnäytetyö tarkasteli kognitiivisen kuormituksen ja poikkeamatilanteiden vaikutusta työntekijöiden hyvinvointiin. Työn päätavoitteena oli kehittää purkukeskustelumalli, joka voisi toimia ratkaisuna näihin haasteisiin SOC-ympäristössä. Tutkimus lähti liikkeelle vankasta teoreettisesta viitekehyksestä, ja sen tulokset tuovat esiin purkukeskustelun keskeisen roolin työntekijöiden hyvinvoinnin ylläpitämisessä erityisesti korkean kognitiivisen kuormituksen tilanteissa.

Kehitetty purkukeskustelumalli koostuu useasta olennaisesta osa-alueesta, kuten valmistelusta, luottamuksellisen ilmapiirin luomisesta, keskusteluraken teesta, itsetuntemuksen edistämisestä ja jälkihoidosta. Nämä elementit tarjoavat organisaatioille tehokkaan ja systemaattisen tavan käsitellä stressaavia tilanteita ja tarjota tukea työntekijöilleen. Tulokset antavat vankan pohjan jatkotutkimukselle ja käytännön sovelluksille, erityisesti teknologiapainotteisella alalla, kuten SOC-ympäristössä, missä kognitiivinen kuormitus voi olla erityisen korkea.

Opinnäytetyön purkukeskustelumalli on suunniteltu joustavaksi ja sovellettavaksi erilaisten organisaatioiden tarpeisiin. Tutkimuksen myötä saadut tulokset viittaavat siihen, että purkukeskustelu voi toimia avaintekijänä sekä kognitiivisen kuormituksen hallinnassa että työntekijöiden hyvinvoinnin tukemisessa SOC-ympäristössä. Tämä lähestymistapa tarjoaa mahdollisuuksia laajempaan käyttöönottoon ja sovelluksiin työelämässä, jossa työntekijöiden henkisen hyvinvoinnin merkitys korostuu entisestään

Avainsanat (asiasanat)

Security Operations Center (SOC), Hybridi työskentely, Työhyvinvointi, Kognitiivinen kuormitus, Purkukeskustelu

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

von Schalien Karri

Defusing after a critical incident

Jyväskylä: JAMK University of Applied Sciences, February 2024, 32 Pages.

Degree Programme in Information and Communications Technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

The thesis focusing on the operations of the Security Operations Center (SOC) examined the impact of cognitive load and exceptional situations on the well-being of employees. The main objective of the study was to develop a debriefing model that could serve as a solution to these challenges in the SOC environment. The research started with a solid theoretical framework, and its results highlight the central role of debriefing in maintaining the well-being of employees, especially in situations with high cognitive load.

The developed debriefing model consists of several essential components, such as preparation, creating a confidential atmosphere, conversation structure, promoting self-awareness, and aftercare. These elements provide organizations with an effective and systematic way to manage stressful situations and offer support to their employees. The results provide a solid foundation for further research and practical applications, especially in technology-focused fields like the SOC environment, where cognitive load can be particularly high.

The debriefing model presented in the thesis is designed to be flexible and applicable to various organizational needs. The results obtained through the research indicate that debriefing can function as a key factor in both managing cognitive load and supporting employee well-being in the SOC environment. This approach provides opportunities for broader adoption and applications in the workplace, where the importance of employee’s mental well-being is increasingly emphasized.

Keywords/tags (subjects)

Security Operations Center (SOC), Cognitive load, Debriefing discussion, Employee well-being, hybrid work

Miscellaneous (Confidential information)

Sisältö

Kuviot

1 Työn lähtökohdat

1.1 Aiheen esittely

Tämän opinnäytetyön tavoitteena oli tutkia kriittisen poikkeaman jälkeistä purkukeskustelua IT-alalla. Kriittinen poikkeama viittaa tilanteeseen, jossa organisaation tietoturva tai palveluiden saatavuus on vaarantunut merkittävästi, ja sen selvittämiseen tarvitaan nopeaa ja tehokasta toimintaa. Keskityimme erityisesti siihen, miten poikkeamaan osallistuminen vaikuttaa henkilöiden henkiseen kuormaan, stressiin, vastuuntuntoon ja tunnetiloihin.

Tutkimukseni kohdistuu Security Operations Center (SOC) -ympäristöön, jossa organisaation tietoturvaa ja palveluiden saatavuutta turvataan poikkeamienhallinnan avulla. SOC on valittu tutkimuskohteeksi sen keskeisen roolin vuoksi poikkeamien havaitsemisessa ja käsittelyssä. SOC varmistaa, että poikkeamat havaitaan, analysoidaan ja niihin reagoidaan mahdollisimman nopeasti. Tämä ympäristö on merkittävä poikkeamienhallinnassa, ja sen ymmärtäminen auttaa kehittämään tehokkaita strategioita ja prosesseja kriittisten tilanteiden hallitsemiseksi IT-alalla. Nykypäivänä, kun tietoturvapoikkeamien ja palveluiden määrä kasvaa, SOC:n rooli korostuu, asettaen organisaatiot ja niiden työntekijät entistä suurempien paineiden ja haasteiden eteen poikkeamiin reagoitaessa ja niitä selvittäessä.

Security Operations Centerin (SOC) toiminnassa on ratkaisevaa varmistaa, että poikkeamat havaitaan, analysoidaan ja niihin reagoidaan mahdollisimman nopeasti ja tehokkaasti. Poikkeamien käsittely voi sisältää monenlaisia tilanteita, kuten haitallisten sähköpostien tunnistamista, haittaohjelmien havaitsemista, torjuntaa ja ympäri vuorokauden toimivien palveluiden saatavuuden varmistamista. On tärkeää ymmärtää, että poikkeamaan osallistumisella voi olla merkittäviä vaikutuksia sekä organisaation että yksittäisen työntekijän näkökulmasta (Toimivien palveluiden ja turvallisuuden eturintama, 2022).

1.2 Aikaisemmat tutkimukset

Aikaisempien tutkimusten kentällä on huomattava, että vaikka purkukeskustelun merkitystä on tutkittu perusteellisesti työympäristöissä, joissa kriittisten tapahtumien kohtaaminen on osa päivittäistä rutiinia, vastaavia tutkimuksia purkukeskustelun vaikutuksista poikkeamien hallintaan IT-

alalla ei ole juurikaan tehty. Tämä avaa mielenkiintoisen tutkimuskentän, jossa voimme syventyä purkukeskusteluiden merkitykseen ja niiden vaikutuksiin poikkeamatilanteiden hallinnassa ja yrityksen turvallisuudessa IT-alalla.

IT-alan erityispiirteet, kuten jatkuvasti kehittyvät uhkakuvat ja teknologiset haasteet, tekevät poikkeamienhallinnasta yhä tärkeämmän näkökohdan organisaatioiden toiminnassa. Tällä hetkellä tarvitaan syvällisempää ymmärrystä siitä, miten poikkeamiin osallistuminen vaikuttaa työntekijöiden hyvinvointiin ja organisaation kykyyn hallita poikkeamatilanteita IT-ympäristössä. Koska organisaatiot joutuvat kohtaamaan entistä monimutkaisempia tietoturvauhkia, tämä tutkimus täyttää merkittävän aukon nykyisessä kirjallisuudessa tarjoamalla ainutlaatuista tietoa ja ymmärrystä kriittisten poikkeamien jälkeisestä purkukeskustelusta tarpeesta IT-alalla.

1.3 Opinnäytetyön tavoitteet

Yksi keskeinen näkökulma oli pohtia, miten poikkeamaan osallistuminen mahdollisesti aiheuttaisi työntekijöille henkistä kuormaa ja stressiä. Epävarmuus, paineet ja vastuu poikkeamien hallinnassa saattaisivat luoda merkittävää stressiä, erityisesti tilanteissa, jotka edellyttävät nopeita päätöksiä ja toimenpiteitä. Lisäksi poikkeamaan osallistuminen saattaisi vaikuttaa työntekijöiden itsetuntoon ja ammatilliseen luottamukseen, mikä puolestaan heijastuisi heidän työhyvinvointiinsa.

Kaiken kaikkiaan tässä opinnäytetyössä pyrittiin saavuttamaan syvempää ymmärrystä siitä, kuinka kriittisen poikkeaman käsittely vaikuttaisi työntekijöiden henkiseen kuormaan, stressiin, vastuuseen ja tilannekuormaan. Näitä näkökulmia tutkimalla voitiin luoda arvokasta tietoa siitä, miten organisaatiot voisivat paremmin tukea työntekijöidensä hyvinvointia ja tehokkuutta tällaisissa haastavissa tilanteissa. Samalla pyrittiin avaamaan ovia jatkotutkimuksille, keskustelulle sekä prosessin kehittämiselle. Keskeisenä pääkysymyksenä oli tarkastella, mitä käytännön toimenpiteitä organisaatiot voivat toteuttaa parantaakseen työntekijöidensä hyvinvointia kriittisen poikkeamienhallinan jälkeen.

2 Kirjallisuuskatsaus ja aiheen käsittely

Ennen kuin syvennämme aiheen eri näkökulmiin, on tärkeää hahmottaa kokonaiskuva kirjallisuudesta ja käsiteltävästä aiheesta. Tämä kappale toimii koko opinnäytetyön viitekehyksen rakentajana, tarjoten pohjan ymmärtää aiheen monimutkaisuutta ja relevanssia. Kattava kirjallisuuskatsaus auttaa luomaan vankkaa perustaa tutkimuksen ymmärtämiselle ja siihen liittyvälle kontekstille. Se mahdollistaa aikaisempien tutkimusten ja teorioiden tarkastelun aiheesta, tunnistaa mahdolliset aukot nykyisessä tiedossa ja hahmottaa keskeiset kysymykset, joihin tämä opinnäytetyö pyrkii vastaamaan.

Aiheen käsittelyssä tarkastellaan valitun aiheen eri osa-alueita syvällisesti. Kyse ei ole pelkästään tiedon kertaamisesta vaan myös oman panoksen tuomisesta aiheen ymmärtämiseen. Käsittelemällä aiheen eri näkökulmia voimme paitsi tunnistaa nykyiset haasteet ja mahdollisuudet myös hahmottavat tulevaisuuden suuntauksia. Tämä luo perustan sille, miksi poikkeamienhallinnassa kiinnitetään erityistä huomiota organisaatioiden toiminnan sujuvuuteen ja samalla työntekijöiden hyvinvointiin. Työtekijöiden hyvinvoinnin turvaamiseksi esimerkiksi poikkeaman jälkeinen purkukeskustelu tarjoaa mahdollisuuden käsitellä kohtaamiaan haasteita ja edistää työyhteisön kokonaisvaltaista hyvinvointia.

Opinnäytetyöni toteutuksessa käytin kuvailevaa kirjallisuuskatsausta, joka on tutkimusmenetelmä, jossa tarkastellaan aikaisempia tutkimuksia. Kirjallisuuskatsauksen avulla tavoitteenani oli edistää tieteenalan teoreettista käsitteistöä ja syventää ymmärrystäni valitusta teemasta. Valitsin kuvailevan kirjallisuuskatsauksen sen laajan aineistonkäsittelymahdollisuuksien vuoksi, ja sen suorittamisprosessi sisälsi neljä vaihetta: Tutkimuskysymyksen laatiminen, aineiston valinta, kuvailevan rakenteen muodostaminen ja tuotetun tuloksen tarkastelu (Kangasniemi, Pietilä, Utriainen, Jääskeläinen, Ahonen, & Liikanen 2013, 292). Näiden vaiheiden avulla pyrin järjestelmällisesti hahmottamaan valittua aihetta ja luomaan vankkaa perustaa työni viitekehykselle.

2.1 Kyberturvallisuus

Vaikka käsite kyberturvallisuudesta saattaa kuulostaa helposti ymmärrettävältä, käytännössä se kattaa monenlaisia tilanteita ja on eri ihmisille hyvin erilainen kokemus. Tämä monimuotoisuus

johtaa hyvin erilaisiin sääntöihin, protokolliin ja toimintatapoihin eri yhteyksissä. Esimerkiksi henkilö, joka haluaa suojata sosiaalisen median tilinsä hakkeroinnilta, ei todennäköisesti käytä samoja menetelmiä ja teknologioita kuin Pentagonin työntekijät, jotka suojaavat salaisia verkkoyhteyksiään. Teknisesti ottaen kyberturvallisuus on tietoturvan osa-alue, joka käsittelee tietoa ja tietojärjestelmiä, jotka tallentavat ja käsittelevät dataa sähköisessä muodossa. Toisaalta tietoturva kattaa kaikenlaisen datan suojauksen. (Steinberg 2020.)

Kybertoimintaympäristö viittaa ihmisen luomaan digitaaliseen ympäristöön, joka yhdistää maailmanlaajuisesti informaatioteknologian, automatisoidut ohjausjärjestelmät, internetin ja sosiaalisen median, ylittäen valtioiden rajat. Yhteiskunnan elintärkeät toiminnot, kuten teollisuus, vesi- ja energiaverkot, pankkijärjestelmät, terveydenhuolto ja liikenne, ovat riippuvaisia digitaalisista verkostoista, jotka ovat osa päivittäistä elämäämme. Tietotekniikan nopea kehitys ja globaalit digitaaliset verkostot, kuten internet ja sosiaalinen media, ovat avanneet uusia mahdollisuuksia taloudelliselle kasvulle, innovaatioille, yritysten perustamiselle ja laajentumiselle. Ne ovat myös edistäneet sosiaalista osallistumista ja demokraattista kehitystä yhteiskunnassa. Digitaaliset verkostot ovat kuitenkin haavoittuvia, ja niiden myötä on syntynyt uusia uhkia, kuten kyberrikollisuus, kybervakoilu ja kyberhyökkäykset. Nämä uhkat muodostavat merkittäviä haasteita turvallisuudelle ja vaativat jatkuvaa valppautta ja suojaustoimenpiteitä. (Kyberturvallisuus ja kybertoimintaympäristö n.d.)

2.2 Euroopan unionin kyberstrategia

Joulukuussa 2020 Euroopan komissio yhdessä EU:n ulko- ja turvallisuuspolitiikan kanssa esitteli uuden kyberturvallisuusstrategian. Tämän strategian päämääränä on vahvistaa Euroopan kykyä torjua kyberuhkia varmistaen, että kaikki kansalaiset sekä yritykset voivat täysipainoisesti hyödyntää turvallisia palveluita ja digitaalisia välineitä. (kyberturvallisuus: miten EU torjuu kyberuhkia 2023).

Yhteiskunnan digitaalinen muutos, jota COVID-19-kriisi on voimistanut, on laajentanut uhkanäkymää ja tuonut mukanaan uusia haasteita, jotka vaativat sopeutettuja ja innovatiivisia vastauksia. Kyberhyökkäysten määrä jatkaa kasvuaan, ja entistä monimutkaisempia hyökkäyksiä tulee laajalta joukolta lähteitä sekä EU:n sisältä että ulkopuolelta. EU:n tulisi näin ollen johtaa ponnisteluja turvallisen digitalisaation puolesta. Sen tulisi edistää normeja maailmanluokan ratkaisuille ja kyber-

turvallisuuden standardeja olennaisille palveluille ja kriittisille infrastruktuureille sekä edistää uusien teknologioiden kehittämistä ja soveltamista. Hallitusten, yritysten ja kansalaisten on jaettava vastuu varmistaakseen kyberturvallisen digitaalisen muutoksen. (The cybersecurity strategy 2022).

Strategia kuvaa, miten EU voi hyödyntää ja vahvistaa kaikkia työkalujaan ja resurssejaan ollakseen teknologisesti suvereeni. Se myös esittää, miten EU voi tehostaa yhteistyötään maailmanlaajuisesti sellaisten kumppaneiden kanssa, jotka jakavat arvomme demokratian, oikeusvaltion ja ihmisoikeuksien suhteen. EU:n teknologinen suvereniteetti on perustuttava kaikkien liitettyjen palveluiden ja tuotteiden sietokykyyn. Kaikkien neljän kyberyhteisön – sisämarkkinoihin, lainvalvontaan, diplomaattisiin ja puolustuksellisiin liittyvien – on tehtävä tiiviimpää yhteistyötä yhteisen uhkanäkymän tietoisuuden saavuttamiseksi. Ne tulisi olla valmiita vastaamaan yhdessä, kun hyökkäys konkretisoituu, jotta EU voi olla yhdessä vahvempi. (The cybersecurity strategy 2022).

Uusi strategia pyrkii varmistamaan maailmanlaajuisen ja avoimen internetin vahvoilla suojatoimenpiteillä, kun riskit turvallisuudelle ja ihmisoikeuksille Euroopassa ovat olemassa. Edellisten strategioiden saavutusten pohjalta siinä on konkreettisia ehdotuksia kolmen pääinstrumentin käyttöönotosta. Nämä kolme instrumenttia ovat sääntely-, investointi- ja politiikkatoimenpiteet. EU sitoutuu tukemaan tätä strategiaa ennennäkemättömällä investointitasolla EU:n digitaalisessa siirtymisessä seuraavan seitsemän vuoden aikana. Tämä nelinkertaistaisi aiemmat investointitasot. Se osoittaa EU:n sitoutumista uuteen teknologiseen ja teollisuuspolitiikkaan sekä elpymisohjelmaan. (The cybersecurity strategy 2022).

2.3 Kyberuhat

ENISA, Euroopan unionin kyberturvallisuusvirasto julkaisi 2023 Threat Landscape raportin. Raportti on perusteellinen analyysi kyberuhista heinäkuusta 2022 kesäkuuhun 2023. Se kattaa eri toimialat, teknologiat ja tilanteet, pyrkien olemaan riippumaton ja puolueeton. (ENISA Threat Landscape 2023). Kyberturvallisuuden uhat voidaan jakaa kahdeksaan pääryhmään, joista alla purettu seitsemän.

2.3.1 Kiristysohjelmat

Tietojen kaappaamisesta ja niiden palauttamiseksi vaadittavista lunnaista tuli merkittävä uhka vuonna 2022. Kiristysohjelma tarkoittaa sitä, kun hakkerit saavat yrityksen tietojärjestelmät hallintaan ja vaativat maksua niiden palauttamiseksi. Kiristysohjelmahyökkäykset pysyivät edelleen yhtenä suurimmista kyberuhkista mainittuna vuonna. Niiden monimutkaisuus lisääntyi myös huomattavasti. ENISA:n raportti viittasi vuoden 2021 loppuun ja vuoden 2022 aikana suoritettuihin kyselytutkimuksiin, joista kävi ilmi, että yli puolet vastaajista tai heidän työntekijöistään joutui kiristysohjelmahyökkäyksen kohteeksi. (Kyberturvallisuus: nykyiset ja tulevat uhat 2023.)

Vaikka suurin lunnasvaatimus hakkereilta oli vuonna 2019 13 miljoonaa euroa, vuonna 2021 summa nousi jo 62 miljoonaan euroon. Keskimääräinen maksettu lunnasraha kaksinkertaistui vuosien 2019 ja 2020 välillä, nousi 71 000 eurosta 150 000 euroon. Arvioiden mukaan kiristysohjelmat aiheuttivat maailmanlaajuisesti 18 miljardin euron tappiot vuonna 2021, mikä on 57 kertaa enemmän kuin vuonna 2015. (Kyberturvallisuus: nykyiset ja tulevat uhat 2023.)

2.3.2 Haittaohjelmat

Madot, virukset, troijan hevoset ja vakoiluohjelmat ovat esimerkkejä haittaohjelmista. Vaikka haittaohjelmien määrä väheni maailmanlaajuisesti vuonna 2020 ja vuoden 2021 alussa pandemian vaikutuksesta, ne kokivat voimakkaan kasvun vuoden 2021 loppupuolella, kun ihmiset palasivat takaisin toimistoihin etätyöjakson jälkeen. Haittaohjelmien lisääntymiseen vaikutti myös kryptokaappaukset, joissa uhrin tietokonetta käytetään salaa kryptovaluutan laittomaan luomiseen, sekä esineiden internetin haittaohjelmat, jotka kohdistuvat internetiin liitettyihin laitteisiin, kuten reitittimiin tai kameroihin. ENISA:n mukaan ensimmäisen puoliskon aikana vuonna 2022 tehtiin enemmän hyökkäyksiä esineiden internetin laitteisiin kuin neljän edellisen vuoden aikana. (Kyberturvallisuus: nykyiset ja tulevat uhat 2023.)

2.3.3 Käyttäjän manipulointi

Käyttäjän manipulointi tarkoittaa tietojen tai palvelujen hankkimista hyödyntämällä inhimillisiä virheitä. Uhria huijataan avaamaan haitallisia asiakirjoja, tiedostoja tai sähköpostiviestejä, tai vierailemaan haitallisilla verkkosivustoilla, jolloin hän antaa luvan päästä järjestelmiin tai palveluihin. Yleisin tämäntyyppinen hyökkäys tapahtuu tietojen kalastelun tai tekstiviestihuijauksen kautta.

ENISA:n mainitsemien tutkimusten mukaan käyttäjän manipulointi liittyy lähes 60 prosenttiin Euroopassa, Lähi-idässä ja Afrikassa tapahtuneista tietoturvaloukkauksista. Tietojen kalastajat esiintyvät yleisimmin rahoitus- tai teknologia-alojen organisaatioiden edustajina, ja rikolliset suuntaavat toimintaansa entistä enemmän myös kryptopörsseihin ja kryptovaluuttojen omistajiin. (Kyberturvallisuus: nykyiset ja tulevat uhat 2023.)

2.3.4 Dataan kohdistuvat uhat

Datan uhkia ilmenee, kun hyökkäyksillä pyritään luvattomaan tietojen käyttöön ja paljastamiseen datalähteissä. Elämme aikakaudella, jossa syntyy massiivisia datamääriä, jotka ovat äärimmäisen tärkeitä erityisesti yrityksille ja tekoälylle. Tästä syystä ne ovat keskeisiä kohteita kyberrikollisille. Dataan kohdistuvat uhat voidaan pääasiassa jakaa kahteen ryhmään: tietoturvaloukkauksiin, jotka ovat kyberrikollisten tahallisesti suorittamia hyökkäyksiä, ja tietovuotoihin, joissa tapahtuu tahatonta tietojen leviämistä. Näiden hyökkäysten yleisin motiivi on edelleen taloudellinen hyöty, kun taas vain kymmenessä prosentissa tapauksista kyseessä on vakoilu. (Kyberturvallisuus: nykyiset ja tulevat uhat 2023.)

2.3.5 Käytettävyyteen kohdistuvat uhat

Uhkat käytettävyydelle liittyvät palvelunestohyökkäyksiin, jotka estävät tietojen tai palvelujen normaalin käytön. Nämä hyökkäykset ovat tietotekniikkajärjestelmille erittäin kriittisiä uhkia, ja ne kasvavat sekä laajuudessa että monimutkaisuudessa. Yksi yleinen hyökkäystyyppi on verkkoinfrastruktuurin ylikuormittaminen niin, että järjestelmää ei voi enää käyttää. Palvelunestohyökkäykset kohdistuvat yhä enemmän mobiiliverkkoihin ja niiden liitettyihin laitteisiin, ja niitä käytetään runsaasti Venäjän ja Ukrainan välisessä kybersodankäynnissä. Hyökkäyskohteina ovat olleet myös verkkosivustot, jotka liittyvät koronaviruspandemiaan ja rokotuksiin. (Kyberturvallisuus: nykyiset ja tulevat uhat 2023.)

2.3.6 Disinformaatio ja misinformaatio

Disinformaatio ja misinformaatio tarkoittaa uhkatekijöiden pyrkimystä levittää harhaanjohtavaa informaatiota. Sosiaalisen median alustojen ja verkkomedian käytön yleistyminen on johtanut disinformaation (tietoisesti väärennettyjen tietojen) ja misinformaation (virheellisten tietojen) leviä-

misen kampanjoihin. Niiden päämääränä on synnyttää pelkoa ja epävarmuutta. Venäjä on hyödyntänyt näitä teknologioita vaikuttaakseen ihmisten käsityksiin sodasta. Deepfake- eli syväväärennösteknologian avulla on nykyään mahdollista luoda väärennettyä ääni-, video- ja kuvamateriaalia, jota on lähes mahdotonta erottaa aidoista. Todellisina ihmisinä esiintyvät botit voivat aiheuttaa häiriötä verkkoyhteisöille lähettämällä valtavia määriä kommentteja. (Kyberturvallisuus: nykyiset ja tulevat uhat 2023.)

2.3.7 Toimitusketjuhyökkäykset

Toimitusketjun hyökkäykset kohdistuvat organisaatioiden ja toimittajien välisiin suhteisiin. Nämä hyökkäykset vaikuttavat sekä toimittajiin että asiakkaisiin. Organisaatiot ovat nykyään entistä alttiimpia tällaisille hyökkäyksille, koska niiden järjestelmät ovat monimutkaisempia ja toimittajia on yhä enemmän, mikä vaikeuttaa niiden valvontaa. (Kyberturvallisuus: nykyiset ja tulevat uhat 2023.)

Kuvio 1. Suurimmat kyberturvallisuusuhat (Euroopan unionin kyberturvallisuuskeskus 2022).

2.4 Palveluiden saatavuus

Laki digitaalisten palvelujen tarjoamisesta, voimaan tullessaan, pyrkii edistämään digitaalisten palvelujen yleistä saavutettavuutta ja laatua. Säännösten tavoitteena on parantaa tietoturvallisuutta, sisällön helppoa saavutettavuutta ja näin varmistaa tasapuolinen käyttömahdollisuus kaikille. Lain taustalla on Euroopan parlamentin ja neuvoston saavutettavuusdirektiivi (EU) 2016/2102. Määritelmien osalta laki selventää verkkosivuston ja mobiilisovelluksen käsitteet sekä digitaalisen palvelun laajemman määritelmän. Saavutettavuus kattaa periaatteet ja tekniikat, joiden avulla digitaaliset palvelut, erityisesti vammaisten henkilöiden, ovat helpommin saavutettavissa. Viranomaisen käsitteeseen sisältyvät erilaiset julkishallinnolliset tahot, ja lain soveltamisala ulottuu myös ortodoksiseen kirkkoon, yliopistoihin, ja ammattikorkeakouluihin. Julkisoikeudellinen laitos määritellään oikeushenkilöksi, joka on perustettu yleisen edun mukaisia tarpeita varten, kun taas palveluntarjoaja kattaa viranomaiset, julkisoikeudelliset laitokset, yritykset, säätiöt, yhdistykset ja muut yhteisöt, joiden digitaalisiin palveluihin lakia sovelletaan. Lisäksi määritellään yhdenmukaistettu standardi ja aikasidonnainen media. (Laki digitaalisten palvelujen tarjoamisesta 306/2019).

Lain tuoma selkeys ja määritelmät, kuten verkkosivuston ja mobiilisovelluksen käsitteet, auttavat hahmottamaan sen soveltamisalaa. Saavutettavuusperiaatteiden huomioiminen suunnittelussa, kehityksessä, ylläpidossa ja päivityksissä on avainasemassa varmistaessa, että palvelut ovat helposti saavutettavissa kaikille käyttäjille.

Toinen olennainen näkökulma on häiriöhallinta ja sen johtaminen. Digitaalisten palvelujen lisääntyessä ja monimutkaistuessa on tärkeää kehittää tehokkaita mekanismeja, joilla voidaan hallita ja minimoida häiriöitä. Digitaalisten palvelujen tarjoajilla on vastuu varmistaa jatkuvuus ja tehokas toiminta myös häiriötilanteissa. Häiriötilanteisiin varautuminen ja niiden hallinta edellyttävät tehokasta johtamista ja resurssien oikea-aikaista mobilisointia.

Häiriötilanteiden johtaminen on moniulotteinen tehtävä, joka käsittää tekniset, organisatoriset ja viestinnälliset näkökulmat. Teknisten ongelmien ratkaisemisen lisäksi on tärkeää viestiä avoimesti ja läpinäkyvästi asiakkaille ja käyttäjille, jotta heidät voidaan pitää ajan tasalla tilanteen kehittymisestä. Myös sidosryhmien välillä tapahtuva yhteistyö on kriittisen tärkeää, erityisesti kun häiriöt voivat vaikuttaa laajemmin kuin yhden palveluntarjoajan toimintaan.

2.5 Poikkeamanhallinta

Poikkeamanhallinnan ymmärtämiseksi on olennaista ensin hahmottaa, mikä tarkoittaa poikkeamaa. Tietotekniikassa incident tai poikkeama kuvaa tapahtumaa, joka eroaa normaalista toiminnasta ja vaikuttaa haitallisesti yrityksen toimintaprosessiin tai jopa keskeyttää sen. Tällainen poikkeama voi liittyä esimerkiksi palvelun häiriöihin tai sen epäonnistumisiin. Tietoturvapoikkeamat puolestaan ovat tapahtumia, jotka viittaavat siihen, että yrityksen järjestelmät tai tieto ovat vaarassa. Poikkeamat voivat ilmetä monissa muodoissa, kattaen niin pienemmät häiriöt, kuten kiintolevytilan täyttymisen, kuin suuremmat häiriöt, kuten tietomurrot, joissa arkaluontoinen tieto on uhattuna. (Shacklett 2021).

Poikkeamanhallinta, eli Incident Response (IR), viittaa toimintaprosessiin, joka käynnistyy, kun organisaatio kohtaa tietomurron, kyberhyökkäyksen tai häiriön palveluiden saatavuudessa. Tavoitteena on rajoittaa poikkeaman vaikutuksia mahdollisimman tehokkaasti. Päämääränä on hallita poikkeamaa siten, että vahingot jäävät minimiin. Pyrkimyksenä rajoittamaan sekä toipumisaikaa että kustannuksia samalla säilyttäen yrityksen maineen. (Lord 2023).

Organisaatiolla olisi suositeltavaa olla selkeä Incident Response Plan (IRP) eli poikkeamanhallintasuunnitelma. Tässä suunnitelmassa on tärkeää määritellä, miten yrityksessä ymmärretään poikkeama. Suunnitelmassa tulee myös olla ohjeistettu prosessi siitä, miten toimitaan havaitun poikkeaman tapahtuessa. Lisäksi organisaatiossa olisi hyvä olla poikkeamanhallintatiimi (Computer Incident Response Team, CIRT), joka koostuu yleensä tietoturva- ja IT-henkilöstöstä sekä jäsenistä laki-, henkilöstö- ja PR-osastoilta. CIRT vastaa tietomurtoihin, viruksiin, palveluiden saatavuuteen ja muihin poikkeamiin reagoimisesta. Sen jäsenten tulisi olla teknisten asiantuntijoiden lisäksi myös viestinnän ammattilaisia, jotka voivat ohjata yrityksen johdon oikeanlaisessa viestinnässä poikkeamatilanteissa. (Lord 2023).

2.6 Hybridityöskentely

Määrittelemme hybridityön joustavaksi tasapainoksi, jossa työaika jaetaan yrityksen sijainnin ja muun paikan, yleensä kotitoimiston, välillä. Sen kestävyys tuli ilmi kahden vuoden aikana, jona tutkimme markkinoiden johtavia maailmanlaajuisia yrityksiä, jotka olivat ottaneet mallin käyttöön COVID-19-pandemian aikana. Kaikki tutkimuksemme johtajat sanoivat, että heidän yrityksillään oli

tarkoitus luoda pitkäaikaisia hybridistrategioita tai ne olivat jo tehneet niin. Hybridityön tukemisen imperatiivi on suurelta osin työvoiman kysyntää. Työntekijät – osoittaen vahvaa suorituskykyään työskennellessään kotoa pahimman pandemian aikana – vaativat perustellusti suurempaa joustavuutta työskennelläkseen missä ja milloin haluavat. Johtajat tietävät niiden täytyvän tarjota joustavia työjärjestelyjä houkutellakseen, pitääkseen ja motivoidakseen huippuosaajia. (trewor & Holweg 2023).

Kun yritykset ja päivittäinen elämä ovat palanneet pre-pandemisiin aktiviteetteihin, yksi asia käy selväksi: kotitoimiston sulkeminen ei ole tapahtumassa. Nicholas Bloomin tekemän tutkimuksen mukaan ja keskusteluissaan satojen johtajien kanssa eri toimialoilla hän huomasi, että noin 70 prosenttia yrityksistä – pienistä yrityksistä massiivisiin monikansallisiin kuten Apple, Google, Citi ja HSBC – aikoo ottaa käyttöön jonkinlaisen hybridi työskentelyjärjestelyn, jotta heidän työntekijänsä voivat jakaa aikansa yhteistyöhön kollegoiden kanssa paikan päällä ja työskentelyyn kotoa käsin. (Bloom 2021).

2.7 Mitä ovat CSIRT, CIRT, CERT SIRT ja SOC

Edellisessä kappaleessa hieman avattiin jo käsitettä CIRT (Computer Incident Response Team.)

Käsite CSIRT eli Computer Security Incident Response Team luotiin 1990 luvulla. CSIRT kutsuttiin myös nimillä CIRT eli Computer Incident Response Team, CERT eli Computer Emergency Response Team, SIRT eli Security Incident Response Team. Kansallisia tiimejä voidaan kutsua myös kansallisiksi kyberturvakeskuksiksi, jotka ovat yleensä lailla määrätty hoitamaan CSIRT-roolia sekä tarjoamaan lisäpalveluita maalle. Jokainen yritys, organisaatio, tiimi valitsee nimensä mieltymyksen perusteella. CSIRT on muuttunut yleiseksi nimeksi tiimeille, joka tarjoaa joukon palveluita: tieto- ja tietoturvaongelmien käsittely, turvallisuusvalvonta, haavoittuvuuksien hallinta ja palveluiden hallinta. (How to setup CSIRT and SOC 2020).

SOC eli Security Operation Center tarjoaa tapahtumien havaitsemispalvelua tarkkailemalla teknisiä tapahtumia verkostoissa ja järjestelmissä, ja se voi myös olla vastuussa tapahtumaan reagoimisesta ja käsittelystä. Suurissa yrityksissä SOC:it keskittyvät joskus vain valvontaan ja havainnointiin ja siirtävät sitten tapahtumakäsittelyn erilliselle CSIRT tiimille. Pienemmissä yrityksissä CSIRT ka

SOC katsotaan usein synonyymeiksi. Yleensä SOC-tiimit toimivat SOC-huoneista käsin, jossa analyytikot istuvat työasemillaan videoseinän äärellä, joka heijastaa nykytilanteen ja luo nopean visuaalisen tilannekuvan. (How to setup CSIRT and SOC 2020).

Tehokas SOC on avainasemassa auttaessaan yrityksiä, hallituksia ja muita organisaatioita pysymään askeleen edellä kehittyvässä kyberuhkien maisemassa. Sekä hyökkääjät että puolustusyhteisö kehittävät jatkuvasti uusia teknologioita ja strategioita, ja kaiken muutoksen hallitseminen vaatii aikaa ja keskittymistä. Hyödyntäen tietämystään laajemmasta kyberturvallisuuden ympäristöstä sekä ymmärrystään sisäisistä haavoittuvuuksista ja liiketoiminnan painopisteistä, SOC auttaa organisaatiota laatimaan turvallisuussuunnitelman, joka on linjassa liiketoiminnan pitkän aikavälin tarpeiden kanssa. SOC:it voivat myös minimoida liiketoiminnan vaikutukset, kun hyökkäys sattuu. Koska ne tarkkailevat verkkoa jatkuvasti ja analysoivat hälytysdataa, ne todennäköisesti havaitsevat uhkat aikaisemmin kuin tiimi, joka jakautuu useiden muiden painopisteiden kesken. Säännöllisen koulutuksen ja hyvin dokumentoitujen prosessien avulla SOC voi käsitellä nykyisen tapahtuman nopeasti - jopa äärimmäisen stressaavissa olosuhteissa. (What is security operations center (SOC) n.d.).

3 Työhyvinvointi ja psyykkinen kuormitus työympäristössä

3.1 Työhyvinvointi

Sosiaali- ja terveysministeriö määrittelee työhyvinvoinnin laajaksi kokonaisuudeksi, joka käsittää työn merkityksellisyyden, terveyden, turvallisuuden ja yleisen hyvinvoinnin. Hyvä työhyvinvointi ei ole pelkästään poissaoloa sairauksista, vaan se heijastaa työntekijöiden kykyä kohdata haasteet työssään ja selviytyä niistä tehokkaasti. Työntekijöiden hyvinvointi on suoraan yhteydessä työssä jaksamiseen; hyvinvoiva työntekijä on sitoutuneempi ja tuottavampi työssään, mikä vähentää sairauspoissaoloja ja parantaa työn laatua. (Sosiaali- ja terveysministeriö, 2023).

Työturvallisuuslaki (738/2002) toimii perustana työympäristön turvallisuuden ja työntekijöiden terveyden ylläpitämiselle. Lain tavoitteena on parantaa työympäristöä, ennaltaehkäistä työtapaturmia ja muita terveyshaittoja sekä turvata ja ylläpitää työntekijöiden työkykyä. Lain avulla työnantajat voivat luoda turvallisen ja terveellisen työympäristön, jossa työntekijät voivat kukoistaa. (Työturvallisuuslaki 738/2002).

Toisaalta, vaikka lait ja säännökset ovat tärkeitä työhyvinvoinnin kannalta, ne eivät yksinään riitä takaamaan työntekijöiden hyvinvointia. Työntekijän näkökulmasta työhyvinvointi voi horjua, kun joutuu kohtaamaan työssään haastavia tilanteita. Esimerkiksi virheen aiheuttama syyllisyys ja jatkuva epävarmuus omista kyvyistä voivat aiheuttaa stressiä ja vaarantaa pitkäaikaisen hyvinvoinnin. Tämä korostaa tarvetta ymmärtää työntekijöiden kokemuksia ja tunteita, jotta voidaan luoda työympäristö, joka tukee heidän henkistä ja emotionaalista hyvinvointiaan.

Työhyvinvoinnin näkökulmasta tarkasteltuna kriittisten poikkeamien sekä tietoturvapoikkeamien hallinta vaikuttaa merkittävästi työntekijöiden hyvinvointiin. Työntekijöiden jatkuvasti kohtaamat poikkeamat ja niiden käsittely voivat aiheuttaa stressiä ja henkistä kuormaa, erityisesti tilanteissa, joissa nopeita päätöksiä ja toimenpiteitä vaaditaan. Tällaiset tilanteet voivat johtaa työntekijöiden uupumiseen, lisääntyneeseen stressiin ja jopa työmotivaation laskuun.

Työntekijä, joka vahingossa aiheutti kriittisen tietoturvapoikkeaman klikkaamalla sähköpostilinkkiä, voi tuntee syvää syyllisyyttä tapahtuneesta. Tämä syyllisyys lepää raskaana hänen harteillaan, varjostaen päivittäistä työskentelyä. Jatkuvasti pohdinnassa oleva virhe aiheuttaa epävarmuutta omiin kykyihin ja päätöksentekoon. Tämä taakka syyllisyydestä ja pelosta tekee työstä ahdistavaa ja vaikeaa.

Tämä tunnekuorma ei vain vaikuta hetkellisesti työtehtäviin tarttumiseen, vaan vaarantaa myös työntekijän pitkäaikaisen hyvinvoinnin. Syyllisyyden tunne syö motivaatiota ja luottamusta omiin kykyihin, mikä voi johtaa vakavaan stressiin ja lopulta uupumukseen. Tällainen henkinen kuorma voi johtaa jatkuviin sairaspoissaoloihin, kun työntekijä ei kykene käsittelemään tunteitaan ja ahdistustaan tehokkaasti.

3.2 purkukeskustelu

Duodecim Terveyskirjaston (2023) mukaan defusing tarkoittaa stressin pikapurkua lääketieteen sanaston käsitteellä.

Defusing-niminen psykologinen keskustelutekniikka sai alkunsa 1980-luvulla Jeffrey Mitchellin toimesta, joka on amerikkalainen psykologi. Hän loi tämän menetelmän erityisesti niille ryhmille,

jotka kohtaavat työssään traumaattisia tilanteita. Tällaisiin ryhmiin lukeutuvat esimerkiksi ensihoitajat, poliisit, pelastusviranomainset sekä terveydenhuollon ammattilaiset. (Saari 2003).

Defusing, eli purkukeskustelu, on henkistä ensiapua, joka toteutetaan purkukokouksena. Kun yksilö kohtaa puhuttelevan tilanteen, hän voi reagoida fyysisesti tai psyykkisesti. Silloin, kun tilanne ylittää normaalit työrutiinit, on tärkeää järjestää purkutilaisuus. Esimerkkejä tällaisista tilanteista voisi olla kriittinen poikkeama palveluiden saatavuudessa tai yrityksen tietoturvallisuudessa. Defusing-istunto on aiheellinen, kun osallinen itse kokee tilanteen voimakkaasti. Ei ole yksiselitteistä vastausta siihen, milloin defusing-istuntoa tarvitaan (Kuisma, Holmström, Nurmi, Porthan, Taskinen, Ahlskog-Karhu 2017, 796–798).

Defusing-istunto tulisi järjestää rauhallisessa ympäristössä mahdollisimman nopeasti tapahtuman jälkeen ja kestää yleensä noin 20–45 minuuttia. Ennen istunnon alkua henkilöstön tulisi irrottautua muista tehtävistä istunnon ajaksi, ja istunnon vetäjäksi voi valita esimerkiksi kollegan omasta organisaatiosta. Useissa työyhteisöissä on koulutettuja työntekijöitä, jotka voivat vetää purkukokouksia. Ensisijainen vastuu defusing-toiminnasta on työterveyshuollolla (Kuisma ym. 2017, 796, 736.) Tämä keskustelu keskittyy käymään läpi tapahtuman ja jakamaan päällimmäiset tuntemukset. Keskustelun aikana arvioidaan tarvetta jälkipuintiin, ja lopuksi annetaan ohjeita jatkotoimenpiteistä. Keskustelun päämääränä on varmistaa, että kaikki tapahtumaan osallistuneet saavat yhtenäistä tietoa tapahtumasta. Keskustelun osallistujat voivat löytää omista kokemuksistaan yhtäläisyyksiä, mikä vahvistaa vertaistukea. Purkukeskustelussa työntekijät voivat purkaa stressiä ja antaa arvostavaa palautetta toistensa toiminnasta. (Nurmi 2006).

3.3 Kognitiivinen kuormitus ja suorituskyky

Ihminen kokee kuormitusta, kun hänen aivojensa tiedonkäsittelykykyä haastetaan. Tähän voivat vaikuttaa esimerkiksi suuri määrä informaatiota sekä erilaiset häiriötekijät ja kiire. Jokapäiväisessä arjessa ihmisen on käsiteltävä suurta tietomäärää, joiden erottaminen olennaisimmista seikoista, tiedon yhdistäminen ja päätelmien tekeminen on välttämätöntä. Aivojen on oltava valmiita ratkaisemaan ongelmia, kestämään stressiä, olemaan itsenäisiä ja sopeutumaan muutoksiin tässä yhteydessä. (Rantanen & Ståhlberg 2022).

Kognitiivinen rasitus tarkoittaa tiedon määrää, jonka yksilö tarvitsee säilyttää mielessään ja käsitellä työmuistissaan samaan aikaan suorittaessaan tehtävää (Collins 2020). Kognitiivinen tietotaakka liittyy uusiin havaintoihin, jotka yksilö joutuu integroimaan aiemmin omaksumiinsa tietoihin. Aiempi käytännön kokemus ja omaksutut tiedot ja taidot auttavat uusien havaintojen oikeassa tulkinnassa. Kognitiivisen tiedonkäsittelyn yhtenä rajoituksena on työmuistin rajallinen kapasiteetti: siihen mahtuu vain muutama asia kerrallaan. Kokemus voi auttaa kiertämään tätä rajoitetta jossain määrin, sillä kokemuksen myötä käsiteltävät asiat voivat laajentua. Kuitenkin kahden vaativan ratkaisun, valinnan tai päätöksen tekeminen samanaikaisesti ei ole mahdollista kognitiivisen tiedonkäsittelyn rajoitteiden vuoksi. Työmuisti on myös herkkä häiriöille, kuten keskeytyksille, jotka voivat helposti pyyhkiä pois aktiivisessa ajattelussa työmuistiin tallennetut asiat (Kuikka, Paajanen 2015, 36–37).

3.4 Kognitiivisen kuormituksen oireet ja vaikutukset

Aivotyön kuormittavuus voi johtaa uupumukseen. Epäselvät ohjeistukset, keskeytykset, häiriöt ja suuri työmäärä korreloivat työuupumuksen ja tiedonkäsittelyn oireiden kanssa. (Kalakoski, Lahti, Paajanen, Valtonen, Ahtinen, Kauppi, Turunen, Ojajärvi, Luokkala 2022, 36.) Työntekijöiden stressitasot kasvoivat sitä enemmän, kun he kokevat aivotyöhön liittyviä vaatimuksia, kuten keskittymistä. Monitehtävyyden, epäselvien ohjeiden ja häiriöiden havaittiin lisäävän painetta (Kalakoski ym. 2022, 38–40).

Työterveyslaitos teki tutkimuksen vuonna 2016 jossa havaittiin kytkös keskeytysten lukumäärän, stressitasojen ja palautumiskyvyn välillä. Kuinka monta keskeytystä ilmeni, sitä suurempi oli koettu stressi ja sitä heikompana koettiin palautuminen. Niiden joukossa, jotka olivat jatkuvien keskeytysten kohteena, 47 % koki melko tai erittäin korkeaa stressiä, kun taas niistä, joille keskeytykset olivat harvinaisia, vain 4 % ja 5 % koki voimakasta stressiä. Lisäksi 19 % ja 28 % niistä, joilla oli jatkuvia keskeytyksiä, ilmoitti työkyvyn palautumisen heikentyneen, kun taas niiden joukossa, joille keskeytyksiä oli harvoin. (Kalliomäki-Levanto ym. 2016, 22–24).

Häpeä on hämmennyksen tai nöyryytyksen tunne, joka syntyy käsityksestä, että on tehnyt jotain arvotonta, epäeettistä tai epäsopivaa. Ne, jotka kokevat häpeää, pyrkivät yleensä piilottamaan sen, mistä he tuntevat häpeää. Kun häpeä on pysyvää, se voi liittyä tunteeseen siitä, että olet perustavanlaatuisesti virheellinen. Häpeä voi olla usein vaikea tunnistaa itsessään. Vaikka häpeä on

negatiivinen tunne, sen alkuperällä on rooli lajimme selviytymisessä. Ilman häpeää meillä ei ehkä olisi tarvetta noudattaa kulttuurisia normeja, seurata lakeja tai käyttäytyä tavalla, joka mahdollistaa olemisemme sosiaalisina olentoina. (Cuncic 2023).

Häpeä ja syyllisyys ovat läheisiä käsitteitä, ja niiden erottaminen toisistaan voi olla haastavaa, sillä molemmilla on rooli yksilön tunne-elämän moraalisen käyttäytymisen säätelyssä. Niiden välillä on kuitenkin eroja: syyllisyys liittyy tekoon ja ilmoittaa meille, kun olemme toimineet väärin. Häpeä puolestaan kohdistuu itseen laajemmin; se leimaa itsensä huonoksi teosta riippumatta, ja sen taustalla olevien syiden tunnistaminen voi olla vaikeampaa. Häpeää ja syyllisyyttä koetaan usein samanaikaisesti. Syyllisyys nousee ensin näistä tunteista, kun henkilö kokee tehneensä väärin. Tunne muuttuu helposti häpeäksi, kun henkilö ei voi vaikuttaa tilanteeseen, jolloin hän leimaa itsensä kokonaisvaltaisesti epäonnistuneeksi ja riittämättömäksi. (Flemming, Ojamaa 2023, 9–10).

Kun tarkastellaan kriittisen poikkeaman jälkeistä tilannetta, on tärkeää huomata, että häpeä ja syyllisyys voivat nousta pintaan niin yksilöllisellä tasolla kuin organisaationkin näkökulmasta. Kriittinen poikkeama, olipa se sitten tietoturvaan liittyvä virhe tai väärinkäytös, voi laukaista voimakkaita tunteita työntekijöissä, erityisesti jos he kokevat osallisuutta tapahtuneeseen.

Häpeä, tässä kontekstissa, voi kietoutua tuntemukseen siitä, että yksilö on ollut osallisena toiminnassa, joka on vahingoittanut organisaation turvallisuutta. Tämä saattaa liittyä siihen, että yksilö kokee tehneensä jotain arvotonta tai epäeettistä, vaikka hän olisi toiminut organisaation asettamissa puitteissa. Tunteen voimakkuus voi kasvaa, kun yksilö ei kykene vaikuttamaan tilanteeseen tai korjaamaan tehtyä virhettä.

Häpeä ja syyllisyys ovat kuitenkin monimutkaisia tunteita, ja niiden erottaminen toisistaan voi olla vaikeaa. Organisaation jäsenet saattavat kokea nämä tunteet samanaikaisesti, ja tilanteen dynamiikka voi johtaa siihen, että aluksi koettu syyllisyys muuttuu häpeäksi. Tässä vaiheessa yksilö voi leimata itsensä laajemmin epäonnistuneeksi ja kyvyttömäksi, mikä voi vaikuttaa merkittävästi henkiseen hyvinvointiin ja jopa työtehoon.

Kun henkilöt kokevat häpeää tai syyllisyyttä, erilaiset tukitoimet voivat auttaa heitä käsittelemään näitä tunteita ja edistämään hyvinvointiaan. Yksi tehokas toimenpide on purkukeskustelu, joka tarjoaa turvallisen tilan avoimelle ja rehelliselle vuoropuhelulle. Purkukeskustelu, kun se toteutetaan rakentavasti ja kunnioittavasti, voi olla arvokas väline häpeän ja syyllisyyden käsittelyssä. Se ei ainoastaan auta yksilöitä selviytymään vaikeista tunteista, vaan myös edistää avoimuutta, vuorovaikutusta ja organisaation oppimista kohtaamistaan haasteista.

4 Keskeiset havainnot ja pohdinta

Työssä, joka liittyy Security Operations Centerin (SOC) toimintaan, kognitiivinen kuormitus nousee esiin monitahoisena haasteena. Erityisesti tilanteissa, joissa analyytikot joutuvat käsittelemään samanaikaisesti useita tietoturvatapahtumia ja häiriötilanteita palveluissa, kuormitus voi saavuttaa korkean tason. Esimerkiksi laajamittaisen uhkaavan haittaohjelmaepidemian keskellä analyytikoiden on tehtävä nopeita päätöksiä, arvioitava uhkien vakavuutta, määritettävä leviämisen laajuus ja toteutettava tehokkaat torjuntatoimenpiteet. Tämä monimutkainen päätöksentekoprosessi yhdistettynä ajallisesti herkkään ympäristöön luo merkittävän kognitiivisen kuormituksen analyytikoille.

Poikkeamatilanteissa, kuten tietoturvaloukkauksissa, tunteet kuten häpeä ja syyllisyys voivat nousta pintaan. Kuvitellaan tilanne, jossa organisaatio on kokenut tietoturvaloukkauksen, ja sen juurisyyksi paljastuu inhimillinen virhe. Henkilö, joka teki virheen, saattaa kokea voimakasta syyllisyyttä peläten seurauksia oman maineensa ja organisaation maineen kannalta. Samalla organisaation jäsenet voivat tuntea yleistä häpeää siitä, että sisäiset valvontamekanismit eivät riittäneet estämään tällaista tapahtumaa. Nämä tunteet voivat vaikuttaa merkittävästi henkilöstön hyvinvointiin, korostaen tarvetta ymmärtää ja käsitellä niitä asianmukaisesti.

Työhyvinvoinnin näkökulmasta purkukeskustelu nousee tärkeäksi työkaluksi näiden haasteiden hallinnassa. Keskustelutilaisuudet voivat tarjota turvallisen tilan, jossa työntekijät voivat avoimesti jakaa kokemuksiaan, tunteitaan ja huoliaan. Kognitiivisen kuormituksen vähentämiseksi purkukeskustelumalli SOC-ympäristöön voi tarjota rakenteen, joka auttaa analysoimaan ja käsittelemään tapahtumia tehokkaammin. Lisäksi se mahdollistaa häpeän ja syyllisyyden tunteiden purkamisen, edistäen siten henkilöstön kokonaisvaltaista hyvinvointia.

On olennaista huomata, että poikkeamatilanteiden käsittelyyn liittyvissä strategioissa on tärkeää ottaa huomioon kaikki osalliset, mukaan lukien tavalliset käyttäjät, jotka voivat olla mahdollisesti olleet aiheuttajina eivätkä vain tekniset analyytikot, jotka ovat olleet korjaamassa tilannetta. Tämä laaja näkökulma mahdollistaa kokonaisvaltaisen ymmärryksen poikkeamatilanteiden monitahoisista haasteista ja niiden vaikutuksista koko organisaatioon.

Kyberrikollisuuden aiheuttamien vahinkojen taloudellinen ulottuvuus on merkittävä. Vuosittain liikkuva valtava rahamäärä korostaa kyberuhkien vakavuutta. Rahalliset menetykset voivat kohdistua suoraan organisaatioihin, ja niiden vaikutukset voivat ulottua laajemmalle koko yhteiskuntaan. Kyberturvallisuuteen sijoitetut varat muodostavat olennaisen osan organisaatioiden toimintakustannuksista, ja tehokkaat kyberpuolustusratkaisut ovat olennainen osa liiketoimintastrategioita.

Huomioimalla kyberturvallisuuden taloudellinen ulottuvuus, organisaatiot voivat osoittaa, että panostukset kyberpuolustukseen eivät ole vain turvallisuuskysymys vaan myös liiketoiminnan jatkuvuuden ja taloudellisen vakauden kysymys. Kyberturvallisuuden laiminlyöminen voi altistaa organisaation merkittäville riskeille, jotka voivat heijastua suoraan liiketoiminnan tulokseen. Tämän vuoksi on tärkeää hahmottaa kyberuhkien taloudellinen merkitys ja varmistaa, että siihen varataan riittävät resurssit ja huomio organisaation tasolla.

4.1 Hybridi työskentelyn haasteet

Hybridi työskentelymalli on organisaation toimintatapa, jossa työntekijöille tarjotaan mahdollisuus työskennellä sekä fyysisessä työympäristössä että etänä. Tämä lähestymistapa yhdistää perinteisen toimiston ja etätyön parhaat puolet, tarjoten joustavuutta työntekijöille ja samalla mahdollistaen tehokkaan toiminnan.

Yhä useammat organisaatiot ovat siirtymässä kohti hybridiä työskentelymallia, jossa työntekijät voivat työskennellä sekä etänä että fyysisessä työympäristössä. Tämä muutos on tuonut mukanaan uusia haasteita, erityisesti tilanteissa, joissa poikkeamat vaativat nopeaa ja tehokasta reagointia. Kun suoranaista ihmiskontaktia ei ole, kommunikaatio- ja yhteistyöhaasteet voivat korostua. Poikkeamatilanteissa, kuten tietoturvaloukkauksissa tai kriittisissä häiriötilanteissa, tehokas ja nopea viestintä on elintärkeää. Hybridi työskentely voi kuitenkin tuoda mukanaan viestinnällisiä

esteitä, kun työntekijät eivät ole fyysisesti läsnä samassa tilassa. Tämä voi vaikeuttaa tilanteen nopeaa ymmärtämistä ja päätöksentekoa. Lisäksi hybridi työskentely voi lisätä kognitiivista kuormitusta, kun työntekijöiden on sopeuduttava erilaisiin työympäristöihin ja -tapoihin. Tämä voi vaikuttaa heidän kykyynsä käsitellä poikkeavat tilanteet tehokkaasti ja säilyttää työhyvinvointinsa.

Tässä yhteydessä on olennaista tarkastella, miten hybridi työskentely vaikuttaa organisaation valmiuteen käsitellä poikkeamatilanteita ja miten mahdolliset puutteet voitaisiin tunnistaa ja korjata. Tämä seikka nousee esiin tärkeänä näkökulmana työntekijöiden ja organisaation resilienssin kannalta.

Hybridi työmalli pyrkii vastaamaan nykyajan työelämän haasteisiin tarjoamalla joustavuutta ja työn tekemisen mahdollisuuksia erilaisissa tilanteissa. Se antaa työntekijöille vapauden valita, missä ympäristössä he voivat olla kaikkein tuottavimpia, olipa se sitten perinteisessä toimistossa, omassa kodissa tai vaikkapa coworking-tilassa. Tämä malli edellyttää kuitenkin myös vahvaa viestintää ja teknologian tehokasta käyttöä varmistaakseen sujuvan yhteistyön tiimin jäsenten välillä, jotka saattavat sijaita eri paikoissa. Etätyön ja fyysisen työskentelyn yhdistelmä asettaa korkeat vaatimukset infrastruktuurille, työkaluille ja organisaation kulttuurille. Hybridi työskentely voi tuoda mukanaan etätyöhön liittyviä etuja, kuten paremman työn ja perhe-elämän tasapainon sekä laajemman mahdollisuuden houkutella lahjakkaita työntekijöitä, jotka eivät välttämättä sijaitse fyysisesti lähellä toimistoa. Toisaalta se vaatii myös tiettyjä sopeutumisia ja strategisia päätöksiä varmistaakseen, että tiimit pysyvät yhteydessä ja että työntekijät voivat ylläpitää tehokasta yhteistyötä.

Hybridi työskentelymallin ymmärtäminen ja sen tehokas käyttöönotto voivat olla kriittisiä organisaation menestyksen kannalta, erityisesti nykypäivän muuttuvassa työympäristössä.

4.2 Case-esimerkki: Ensihoito ja purkukeskustelumalli

Aiemman 15-vuotisen työskentelyni perusteella pelastuslaitoksella ensihoitajana voin tuoda esiin konkreettisen esimerkin purkukeskustelun vakiintuneesta käytöstä ensihoitoalalla. Ensihoidossa purkukeskustelu on muodostunut välttämättömäksi työkaluksi, joka auttaa käsittelemään henkistä kuormitusta tilanteissa, joissa työntekijöitä rasittavat odottamattomat tai poikkeuksellisen vaativat tilanteet.

Tarve purkukeskustelulle voi syntyä erilaisista tilanteista, ei pelkästään monipotilastilanteista tai poikkeustilanteista. Ensihoitoalan henkilöstölle voi kertyä normaalia suurempaa henkistä kuormitusta, ja purkukeskustelu onkin tullut vakiintuneeksi käytännöksi tilanteissa, joissa työntekijät kokevat tarvetta jakaa kokemuksiaan ja tunteitaan.

Ensihoitoalan purkukeskustelun aloite voi tulla kenttäjohtajalta tai muulta työyhteisön jäseneltä, joka havaitsee, että henkilöstöllä voi olla tarve purkaa kokemuksiaan. Tilanne voi liittyä esimerkiksi vakavaan työturvallisuusuhkaan, joka kohdistuu oman tai työtoverin henkeen tai terveyteen. Lisäksi huoli työparista tai itse työntekijän ilmaisema tarve voivat olla riittäviä perusteita järjestää purkukeskustelu.

Purkukeskustelun rooli ensihoitoalalla on merkittävä, sillä se tarjoaa turvallisen ympäristön, jossa työntekijät voivat avoimesti ilmaista tunteitaan ja jakaa kokemuksiaan. Työskennellessäni ensihoitajana olen havainnut, että nämä keskustelut mahdollistavat työyhteisön jäsenille mahdollisuuden käsitellä stressaavia tilanteita ja purkaa henkistä painetta, edistäen näin työntekijöiden kokonaisvaltaista hyvinvointia. Tämä esimerkki korostaa purkukeskustelun tärkeyttä erityisesti ammateissa, joissa työntekijät kohtaavat säännöllisesti poikkeuksellisen haastavia tilanteita.

4.3 Eettisyys ja luotettavuus

Tutkimuseettisten periaatteiden tunteminen ja noudattaminen on jokaisen tutkimuksen tekijän velvollisuus, toteavat Hirsjärvi ym. (2009, 23.) Tutkimuksen toteutuksessa pyrittiin noudattamaan hyväksyttyjä tieteellisiä standardeja varmistaakseen tulosten uskottavuuden ja luotettavuuden. Rehellisyyttä, huolellisuutta ja tarkkuutta korostettiin koko tutkimusprosessin ajan. Opinnäytetyön keskeiset huomiot liittyvät kiinteästi tutkimuksen eettisiin periaatteisiin ja luotettavuuteen. Tässä osuudessa tarkastellaan, kuinka nämä tekijät vaikuttavat opinnäytetyön tuloksiin ja millaisia eettisiä näkökohtia on otettu huomioon tutkimuksen eri vaiheissa.

Kun tarkastellaan opinnäytetyön eettisyyttä ja luotettavuutta, keskitytään kirjallisuuskatsauksen näkökulmaan, jossa kyselyitä ja osallistujia ei ole mukana. Tässä yhteydessä korostetaan, kuinka eettiset periaatteet ja luotettavuusvaatimukset liittyvät kirjallisuuskatsauksen eri vaiheisiin. Opinnäytetyön suunnitteluvaiheessa on tärkeää harkita eettisiä näkökohtia, kuten alkuperäislähteiden oikeudenmukainen käyttö ja kunnioittava viittaaminen. Varovaisuus ja huolellisuus ovat keskeisiä,

jotta vältetään epäeettinen tietojen käyttö ja varmistetaan, että lähteet valitaan puolueettomasti ja asianmukaisesti.

Kirjallisuuskatsauksen toteutusvaiheessa eettiset huomiot voivat liittyä tekijänoikeuksiin, erityisesti jos käytetään suojaamatonta aineistoa. On tärkeää noudattaa eettisiä normeja kriittisen ajattelun ja tietolähteiden tarkastelun yhteydessä. Lisäksi luotettavuus vaatii, että kirjallisuuskatsauksen menetelmät ja rajaukset ovat selkeät ja systemaattiset.

Tulosten analysoinnissa eettisyys korostuu tulosten rehellisessä ja tasapuolisessa tulkinnassa. Kirjallisuuskatsauksessa tulokset koostuvat muiden tutkijoiden tuottamista tiedoista, joten tulee välttää tulosten vääristelyä tai selektiivistä raportointia. Luotettavuuden kannalta on olennaista arvioida valittujen lähteiden laatu ja merkitys tutkimuskysymyksen kannalta.

Lopulta, raportointivaiheessa eettiset harkinnat näkyvät siinä, miten viitataan ja kunnioitetaan alkuperäislähteitä. Luotettavuus edellyttää, että kirjallisuuskatsauksen tekeminen on avointa ja selkeää, jotta muut tutkijat voivat toistaa saman prosessin ja arvioida tuloksia itsenäisesti.

Yhteenvetona voidaan todeta, että kirjallisuuskatsauksen eettinen ja luotettava toteuttaminen edellyttää tarkkaa huolellisuutta ja avoimuutta kaikissa vaiheissa. Oikeudenmukainen ja asianmukainen viittaaminen sekä tietolähteiden huolellinen valinta ovat keskeisiä tekijöitä eettisessä ja luotettavassa kirjallisuuskatsauksessa.

5 Johtopäätökset ja jatkokehitys

Opinnäytetyön tulokset viittaavat siihen, että purkukeskustelu voi olla tehokas työkalu kognitiivisen kuormituksen ja häpeän ja syyllisyyden tunteiden käsittelyyn kriittisten poikkeamatilanteiden yhteydessä. Kappaleessa 5.1 on ehdotettu toimintamalli tarjoamalla rakenteen, joka mahdollistaa avoimen vuoropuhelun ja auttaa työntekijöitä käsittelemään stressiä, haasteita, häpeää ja syyllisyyden tunteitaan. Malli on suunniteltu huomioimaan SOC-ympäristön erityispiirteet, kuten työntekijöiden kokemuksen, työtehtävien vaativuuden ja organisaation kulttuurin.

Opinnäytetyön jatkokehityksessä olisi hyödyllistä tutkia seuraavia asioita:

- Purkukeskustelun vaikutusta työntekijöiden työhyvinvointiin pidemmällä aikavälillä. Tutkimuksessa voisi tarkastella, miten purkukeskustelu vaikuttaa työntekijöiden fyysiseen ja psyykkiseen hyvinvointiin, työtyytyväisyyteen ja työuupumuksen riskiin.

- Purkukeskustelun vaikutusta työntekijöiden päätöksentekoon ja suorituskykyyn kriittisten poikkeamatilanteiden yhteydessä. Tutkimuksessa voisi tarkastella, miten purkukeskustelu auttaa työntekijöitä tekemään parempia päätöksiä kriittisissä tilanteissa ja parantamaan suorituskykyään.

- Purkukeskustelun vaikutusta tiimityöhön ja yhteisöllisyyteen. Tutkimuksessa voisi tarkastella, miten purkukeskustelu vahvistaa tiimihenkeä ja luottamusta tiimin jäsenten välillä.

Näiden tutkimusten avulla saadaan lisää tietoa purkukeskustelun hyödyistä ja siitä, miten sitä voidaan tehokkaimmin hyödyntää.

5.1 Purkukeskustelumalli SOC-ympäristöön

Purkukeskustelumallin kehittäminen SOC-ympäristössä työskenteleville työntekijöille vaatii huomioon ottamista alan erityispiirteistä ja sen vaatimuksista. Seuraavassa on ehdotus mallista, joka voi soveltua tähän ympäristöön:

1. Valmistelu
2. Luottamuksellinen ilmapiiri
3. Keskustelun rakenne
4. Itsetuntemuksen Edistäminen
5. Jälkihoito ja seuranta

Tämä malli tarjoaa rakenteen, joka mahdollistaa avoimen vuoropuhelun ja auttaa työntekijöitä käsittelemään stressiä, haasteita, häpeää ja syyllisyyden tunteitaan. On tärkeää, että malli muokataan organisaation tarpeiden mukaiseksi ja että se joustaa työntekijöiden tarpeiden mukaan. Tämä voisi toimia jatkokehityksen pohjana.

Oletetaan, että Security Operations Center (SOC) -tiimi joutuu kohtaamaan kriittisen poikkeaman, joka herättää valtakunnallista mediahuomiota ja ulkopuolista painetta. Tilanteessa tarvitaan välit-

tömiä ja stressaavia päätöksiä, ja tiimi kokee valtavaa julkista ja kansallista painetta. Tämä korostaa entisestään tiimin stressitasoa ja vaatii erityistä huomioita henkisen hyvinvoinnin ylläpitämiseksi.

Tiimin toimintaa seurataan tiiviisti mediassa, ja ulkopuoliset odotukset ja arviot voivat vaikuttaa voimakkaasti tiimin jäsenten mielialaan ja suorituskykyyn. Tässä yhteydessä psykologinen purkukeskustelu nousee entistäkin tärkeämmäksi, tarjoten tiimin jäsenille tilaisuuden jakaa kokemuksiaan, käsitellä tuntemuksiaan ja löytää yhteinen näkökulma tilanteeseen. Tämä auttaa tiimiä käsittelemään ulkopuolista painetta ja säilyttämään henkisen tasapainonsa, mikä on olennaista tehokkaan päätöksenteon ja toiminnan kannalta.

Valmistelu:
Tiimin johtaja tunnistaa tarpeen purkukeskustelulle ja ilmoittaa siitä etukäteen tiimille. Valitaan sopiva aika, jolloin kaikki tiimin jäsenet voivat osallistua keskeytyksettä.

Luottamuksellinen ilmapiiri:
Kokoushuone varataan hiljaiseksi paikaksi, jossa keskustelu voidaan käydä luottamuksellisesti. Tiimin johtaja korostaa keskustelun luottamuksellisuutta ja kannustaa avoimeen ilmaisuun.

Keskustelun rakenne:
Keskustelu aloitetaan kertomalla tapahtumista objektiivisesti. Jokaiselle tiimin jäsenelle annetaan mahdollisuus jakaa omat kokemuksensa ja tuntemuksensa tilanteesta. Tiimin johtaja pitää keskustelun rakenteessa kiinni varmistaakseen, että kaikki pääsevät ääneen.

Itsetuntemuksen edistäminen:
Jokainen tiimin jäsen ilmaisee omat tuntemuksensa ja reaktionsa tapahtumaan. Tiimin jäsenet voivat tunnistaa yhteisiä tuntemuksia ja jakaa kokemuksiaan, mikä vahvistaa tiimihenkeä.

Jälkihoito ja seuranta:
Keskustelun päätteeksi sovitaan jatkotoimenpiteistä ja siitä, miten vastaavaa tilannetta käsitellään

tulevaisuudessa. Tarjotaan mahdollisuus yksilölliseen keskusteluun tarvittaessa, esimerkiksi työterveyshuollon kanssa. Tiimin johtaja seuraa tilannetta varmistaakseen, että tiimin jäsenet toipuvat tapahtuneesta.

Tämä purkukeskustelun malli pyrkii tarjoamaan turvallisen tilan tiimin jäsenille ilmaista tunteitaan ja purkaa stressiä, edistäen samalla avoimuutta ja tiimityöskentelyä. Keskustelun avulla tiimi voi oppia tapahtuneesta ja vahvistua vastaaviin tilanteisiin varautuessaan. Lisäksi on huomioitava, että tätä mallia voidaan soveltaa paitsi kansallisesti kriittisiin poikkeamiin myös matalammalla kynnyksellä oleviin tilanteisiin, korostaen sen joustavuutta erilaisten organisaatioiden tarpeisiin.

Purkukeskustelumalli tarjoaa perustan jatkokehitykselle ja sovelluksille. Se voidaan sovittaa eri organisaatioiden tarpeisiin ja tarjoaa tehokkaan tavan käsitellä stressaavia tilanteita. Tämän mallin avulla voidaan rakentaa kestävä ja tukemalla työympäristö, joka ei ainoastaan reagoi poikkeamatilanteisiin vaan myös ennaltaehkäisee niiden vaikutukset työntekijöiden hyvinvointiin.

Kokonaisuudessaan purkukeskustelumalli on suunniteltu vastaamaan SOC-ympäristön erityispiirteisiin, ja sen avulla pyritään varmistamaan, että työntekijöiden henkinen hyvinvointi säilyy myös vaativissa tilanteissa. Mallin jatkuva kehittäminen ja soveltaminen tarjoavat mahdollisuuden luoda entistä vahvempia ja turvallisempia työympäristöjä SOC-ammattilaisille.

Lähteet

Bloom, N. 2021. Hybrid is the future of work. Stanford University. Institute for Economic policy Research. Viitattu 11.1.2024. https://siepr.stanford.edu/publications/policy-brief/hybrid-future-work

Collins, R. 2020. Clinician Cognitive Overload and Its Implications for Nurse Leaders. Nurse Leader. Viitattu 5.11.2023. https://www.nurseleader.com/article/S1541-4612(19)30355-6/pdf .

Cuncic, A. 2023. The Psychology of Shame. Verywell mind. Viitattu 15.11.2023. https://www.verywellmind.com/what-is-shame-5115076 .

Duodecim Terveyskirjasto 2023. Lääketieteen sanasto. Viitattu 2.10.2023. https://www.terveyskirjasto.fi/ltt00502 .

ENISA Threat Landscape 2023. 19.10.2023. Euroopan parlamentin verkkosivu. Viitattu 6.1.2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 .

Flemming, L & Ojamaa, I. 2023. Lapsuudessa ja nuoruudessa syntyneet häpeän tunteet suhde yksilön elämänvalintoihin aikuisuudessa. Pro-gradu tutkielma. Jyväskylän yliopisto, ohjausalan maisteriohjelma.

Hirsjärvi, S., Remes, P., Sajavaara, P. 2009. Tutki ja kirjoita. 15. p. Helsinki: kustannusosakeyhtiö Tammi.

How to set up CSIRT and SOC. 10.12.2020. Euroopan parlamentin verkkosivu. Viitattu 6.1.2024. https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc .

Kalakoski, V., Lahti, H., Paajanen, T., Valtonen, T., Ahtinen, S. Kauppi, M. Turunen, J. Ojajärvi, A & Luokkala, K. 2022. Viisi avausta aivotyöhön – Viisikko. Tutkimushankkeen loppuraportti. Työterveyslaitos. Viitattu 4.10.2023. https://www.julkari.fi/bitstream/handle/10024/145177/TTL-978-952-391-044-7.pdf?sequence=1&isAllowed=y

Kalliomäki-Levanto, T. Ukkonen & A. Kalakoski, V. 2016. Ratkaisuehdotuksia keskeytyvään työhön. Keskeyttävien työolomuutosten ennakointimalli tietointensiivisen työskentelyn parantamiseksi. Työterveyslaitos. Viitattu 4.10.2023. https://www.julkari.fi/bitstream/handle/10024/131523/Ratkaisuehdotuksia%20keskeytyv%C3%A4%C3%A4n%20ty%C3%B6h%C3%B6n.pdf?sequence=2&isAllowed=y

Kangasniemi, M., Pietilä, A-M., Utriainen, K., Jääskeläinen, P., Ahonen, S., Liikanen, E. 2013. Kuvaileva kirjallisuuskatsaus. Hoitotiede 25, 291–301.

Kuikka, P. & Paajanen, T. 2015. Työstä ja tarkkaavaisuudesta. Työterveyslaitos. Viitattu 4.10.2023. https://www.julkari.fi/bitstream/handle/10024/129591/Tarkkaavaisuus_net-tiin%20%28002%29.pdf?sequence=3&isAllowed=y

Kuisma, M., Holmström, P., Nurmi, J., Porthan, K., Taskinen, T. & Ahlskog-Karhu, M. 2017. Ensi-hoito. 6. uud. p. Helsinki: Sanoma Pro Oy.

Kyberturvallisuus ja kybertoimintaympäristö. n.d. Ulkoministeriön verkkosivu. Viitattu 5.10.2023. https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto

Kyberturvallisuus: miten EU torjuu kyberuhkia. 25.7.2023. Eurooppa-neuvoston verkkosivu. Vii-tattu 8.1.2024. https://www.consilium.europa.eu/fi/policies/cybersecurity/ .

Kyberturvallisuus: nykyiset ja tulevat uhat. 20.4.2023. Euroopan parlamentin verkkosivu. Viitattu 6.1.2024 https://www.europarl.europa.eu/news/fi/headlines/so-ciety/20220120STO21428/kyberturvallisuus-nykyiset-ja-tulevat-uhat .

L 306/2019. Laki digitaalisten palvelujen tarjoamisesta. Viitattu 8.1.2024. https://www.fin-lex.fi/fi/laki/alkup/2019/20190306 .

L 738/2002. Työturvallisuuslaki. Viitattu 3.10.2023. https://www.finlex.fi/fi/laki/al-kup/2002/20020738 .

Leino-Kilpi, H & Välimäki, M. 2014. Etiikka hoitotyössä. 8, uud. p. Helsinki: Sanoma Pro.

Lord, N. 2023. What is incident response. Viitattu 2.1.2024. https://www.digitalguar-dian.com/blog/what-incident-response .

Nurmi, L. 2006. Kriisi, pelko, pakokauhu. Helsinki: Edita.

Rantanen, J. & Ståhlberg, A. 2022. Kognitiivinen kuormitus akuutilla osastolla. Opinnäytetyö, AMK. Turun ammattikorkeakoulu, sairaanhoitajakoulutus. Viitattu 5.10.2023. https://urn.fi/URN:NBN:fi:amk-2022121328494 .

Saari, S. 2003. Kuin salama kirkkaalta taivaalta: Kriisit ja niistä selviytyminen. 3. uud. laitos. Hel-singissä: Otava

Shacklett, M. 2021. What is security incident. Viitattu 2.1.2024. https://www.techtarget.com/wha-tis/definition/security-incident .

Sosiaali- ja terveysministeriö 2023. Työhyvinvointi. Sosiaali- ja terveysministeriön verkkosivu. Viitattu 3.10.2023. https://stm.fi/tyohyvinvointi

Steinberg, J. 2020. Cybersecurity for Dummies. Hoboken: John Wiley & Sons. Viitattu 5.10.2023. https://janet.finna.fi , Skillsoft Books.

The cybersecurity strategy. 7.7.2022. Euroopan unionin verkkosivu. Viitattu 8.1.2024. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy .

Toimivien palveluiden ja turvallisuuden eturintama. 2022. Artikkeli Elisa Oyj verkkosivuilla 27.10.2022. Viitattu 7.11.2023. https://elisa.fi/ideat/elisa-csoc/.

Trevor, J., Holweg, M. 2023. Managing the new tensions of hybrid work. MIT Sloan Management Review, 64, 2, 35-39,

What is security operations center. n.d. Microsoft security verkkosivu. Viitattu 6.1.2024. https://www.microsoft.com/en-us/security/business/security-101/what-is-a-security-operations-center-soc .