# Kyberturvallisuus kaupan ja jakelun alalla

## -käsikirja kyberpoikkeamien hallintaan

ELINA SUNI (TOIM.)

Jyväskylän ammattikorkeakoulun Elintarviketuotannon ja -jakelun kyberpoikkeamanhallinnan julkaisut, osa 3/3

jamk | Jyväskylän ammattikorkeakoulu

Maa- ja metsätalous-ministeriö

# Sisältö



Tekijät:

Vesa Vertainen
Jyväskylän ammattikorkeakoulu

Reijo Lähteenmäki
Jyväskylän ammattikorkeakoulu

Sampo Kotikoski
Jyväskylän ammattikorkeakoulu

Paavo Nelimarkka
Jyväskylän ammattikorkeakoulu

Jaana Brandt
Jyväskylän ammattikorkeakoulu

Elina Suni
Jyväskylän ammattikorkeakoulu

Kustantaja: Jyväskylän ammattikorkeakoulu

ISBN 978-951-830-680-4 (PDF)

Jyväskylä 2023

# 1 Johdanto

**Elina Suni**

Tämän käsikirjan päätavoitteena on tuottaa kaupan ja jakelun toimialan yrityksille kyberpoikkeamatilanteissa tarvittavia toimintaohjeita. Käsikirjan kohderyhmänä ovat kaikki kaupan ja jakelun alalla työskentelevät, mutta erityisesti erikokoisten kaupan ja jakelun yritysten kyberturvallisuuden johtamisesta sekä teknisestä ja hallinnollisesta toteutuksesta vastaavat henkilöt. Käsikirjan tarkoituksena on varmistaa yhteiskunnan kannalta kriittisten kaupan ja jakelun yritysten toimintojen jatkuvuutta myös kyberpoikkeamatilanteissa. Elintarviketuotannon ja -jakelun arvoketju on monitasoinen, ja keskinäiset riippuvuussuhteet voivat olla monitahoisia ja ennalta-arvaamattomia. Jos esimerkiksi alkutuotantoon, logistiikkaan, kylmälaitteisiin ja keskusvarastoihin vaikutetaan samanaikaisesti, voi sillä olla merkittävät vaikutukset kansalliseen ruokaturvaan ja kyberresilienssiin. On tärkeää, että kauppa ja jakelu osana elintarvikearvoketjua toimii mahdollisimman häiriöttömästi.

Käsikirja on syntynyt Kyberpoikkeamanhallinnan prosessit ja toimintaohjeet elintarviketuotannossa ja –jakelussa –projektin tuloksena ja on yksi kolmesta projektissa toteutetuista julkaisuista. Muut kaksi julkaisua ovat:

- Kyberturvallisuus alkutuotannossa – käsikirja kyberpoikkeamien hallintaan (Elintarviketuotannon ja -jakelun kyberpoikkeamanhallinnan julkaisut Jamk, osa 1/3)

- Kyberturvallisuus elintarviketeollisuudessa – käsikirja kyberpoikkeamien hallintaan (Elintarviketuotannon ja -jakelun kyberpoikkeamanhallinnan julkaisut Jamk, osa 2/3)

Projektin on rahoittanut maa- ja metsätalousministeriö ja toteuttanut Jyväskylän ammattikorkeakoulun IT-instituutti. Julkaisussa käsitellyt aiheet ovat nousseet projektin toteuttamasta alkukartoituksesta, jossa selvitettiin toimijoiden tämänhetkisiä ohjeita ja prosesseja kyberpoikkeamatilanteisiin, niiden puutteita sekä ajankohtaisia alaan kohdistuvia uhkia. Alkukartoitus toteutettiin haastattelemalla alan toimijoita, viranomaisia ja yrityksiä (9 haastattelua). Lisäksi toteutettiin Webropol-kysely, joka lähetettiin joukolle alkutuotannon, elintarviketeollisuuden sekä kaupan ja jakelun yrityksiä (vastaajamäärä 233). Lisäksi alkukartoituksessa perehdyttiin ajankohtaisiin aiheesta tehtyihin julkaisuihin ja tutkimuksiin.

Luku 2

# Kyberturvallisuus kaupan ja jakelun yrityksissä

**Luku kaksi keskittyy kyberturvallisuuden perusteisiin ja sen erityispiirteisiin kaupan ja jakelun alalla. Lisäksi esitellään merkittävimpiä kyberuhkia kaupan ja jakelun IT- ja OT-ympäristöissä sekä kyberhyökkäyksiä, joita ala on kohdannut viime vuosina.**

# 2 Kyberturvallisuus kaupan ja jakelun yrityksissä

**Vesa Vertainen, Reijo Lähteenmäki**

## Mitä on kyberturvallisuus ja miksi siihen pitäisi kiinnittää huomiota?

Yhteiskunnan digitalisoituminen aiheuttaa uusia turvallisuuteen liittyviä haasteita ja uhkia. Kun digitaalisia tietojärjestelmiä sisältävä toimintaympäristö eli kybertoimintaympäristö on luotettava ja sen toiminta turvattua, voidaan puhua **kyberturvallisuudesta.**

**Kybertoimintaympäristö** eli digitaalisista tietojärjestelmistä muodostuva toimintaympäristö koostuu sen käyttäjistä käyttöoikeuksineen, päätelaitteista (tietokoneista, matkapuhelimista, erilaisista ajoneuvopäätteistä jne.), joko fyysisistä tai virtuaalisista palvelimista, niitä yhdistävistä tietoverkkojen laitteista, ohjelmistoista sekä tallennusvälineistä tai järjestelmistä, joihin tieto tallennetaan. Tallennusjärjestelmät voivat vaihdella USB-muistitikusta pilvipohjaisiin ratkaisuihin. Perinteisen toimisto-IT-ympäristön lisäksi on huomioitava tuotannon-, varastoinnin- ja logistiikan ohjaus- sekä valvontajärjestelmät, eli niin sanotut ICS- tai OT-järjestelmät.

**Kyberuhkilla** tarkoitetaan sellaisia tapahtumia, jotka voivat häiritä järjestelmiä, ohjelmistoja, laitteita ja tietoliikenneyhteyksiä ja vaikuttaa haitallisesti yrityksen toimintaan, talouteen, tietoon ja liiketoiminnan jatkuvuuteen (Kyberturvallisuus ja hallituksen vastuu -opas 2020, 4).

***Tietoturvallisuuden tavoitteena on nimensä mukaisesti turvata nimenomaan tiedon luottamuksellisuus, eheys sekä saatavuus.***

Kyberturvallisuuden yhteydessä puhutaan usein myös **tietoturvasta**. Tietoturvallisuuden tavoitteena on nimensä mukaisesti turvata nimenomaan tiedon luottamuksellisuus, eheys sekä saatavuus. Tiedon luottamuksellisuudella tarkoitetaan sitä, että tietoon eivät pääse käsiksi tahot tai henkilöt, joilla kyseisen tiedon käsittelyoikeutta ei ole. Eheydellä tarkoitetaan tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa. Saatavuudella puolestaan tarkoitetaan sitä, että tieto on käytettävissä haluttuna aikana. Näin ollen käsitteinä kyber- ja tietoturvallisuus eivät ole ristiriidassa keskenään, vaan ne täydentävät toisiaan.

**Uhkatoimijat** voidaan jakaa kolmeen ryhmään: verkkorikolliset, vilpilliset työntekijät ja valtiolliset ryhmittymät. Verkkorikollisten motivaationa on taloudellisen edun tavoittelu. He hyökkäävät kohteisiinsa internetin välityksellä etsien järjestelmistä haavoittuvuuksia ja niitä hyödyntäen tunkeutuvat järjestelmiin asentaen haitallista koodia tai varastavat tietoa. Kohteet valikoituvat useimmiten satunnaisesti; mistä vain automatisoitu skannaus sattuu löytämään aukkoja. Vilpilliset työntekijät puolestaan ovat usein tyytymättömiä työnantajaansa ja taloudellista etua tavoitellessaan suorittavat yritykselle haitallisia toimenpiteitä. Heidän käyttämänsä menetelmät eivät välttämättä ole niin kehittyneitä kuin verkkorikollisten. On myös mahdollista, että he esimerkiksi myyvät hallussaan olevia järjestelmätietoja verkkorikollisille, jotka puolestaan hyödyntävät niitä varsinaisen tunkeutumisen yhteydessä. Valtiollisten toimijoiden vihamielisen toiminnan motivaationa voivat olla joko taloudelliset tai poliittiset syyt. Tällaisilla ryhmittymillä on tyypillisesti merkittävät resurssit käytettävissään, joten niiden toteuttamat operaatiot voivat olla hyvinkin pitkäkestoisia ja niissä käytettävät haittaohjelmat erittäin kehittyneitä.

***Uhkatoimijoita ovat verkkorikolliset, vilpilliset työntekijät ja valtiolliset ryhmittymät.***

## Kaupan ja jakelun toimialan erityispiirteet

Kaupan ja jakelun toimijatkaan eivät ole suojassa kyberturvallisuuteen kohdistuvilta häiriöiltä tai uhkilta. Huoltovarmuuskeskuksen mukaan kauppa ja jakelu on elintarvikeketjun aloista herkin häiriöille, yhdessä ravintola- ja suurkeittiötoimijoiden kanssa (Sektori ja poolit - Huoltovarmuuskeskus n.d). Toimiala on monen muun toimialan tapaan riippuvainen digitaalisista järjestelmistä. Erityispiirteenä on materiaalivirtojen automatisoitu ohjaus, seuranta ja raportointi. Isot logistiikkakeskukset ovat pitkälti automatisoituja, eikä robotiikkaan ja automaatiojärjestelmiin ole käytettävissä manuaalista varajärjestelmää. Näin ollen kyberturvallisuuden voidaan nähdä olevan oleellinen osa liiketoiminnan jatkuvuudenhallintaa. Toimialalla käsitellään kaikille tärkeitä elintarvikkeita ja siksi mahdolliset poikkeamat kiinnostavat suurta yleisöä. Alan yrityksillä on myös yhteiskunnallisesti merkittävä rooli kansallisen ruokaturvan kannalta.

Kyberturvallisuuden avulla voidaan nähdä turvattavan osaltaan myös elintarviketurvallisuutta varmistamalla esimerkiksi myymälöiden jäähdytysjärjestelmien toimivuus. Sen avulla tuetaan myös yritysten maineenhallintaa suojaamalla liiketoiminnan kriittinen tieto. Esimerkkinä tällaisesta kriittisestä tiedosta voidaan mainita asiakkaiden ja henkilöstön henkilö- ja maksuvälinetiedot, ostostiedot sekä muu liiketoimintaan liittyvä suojattava tieto.

Myös liikekumppanit edellyttävät tietojensa salassa pysymistä. Hyvä kyberturvallisuuskyvykkyys ja sen osoittaminen laatujärjestelmän kautta on kilpailuetu. Samaa kyvykkyyttä on syytä edellyttää myös alihankkijoilta ja toimittajilta. Viranomaisetkin voivat vaatia yritykseltä turvallisuusasioiden asianmukaista hallintaa. (Tieto- ja kyberturvallisuus n.d.) Kyberturvallisuuteen panostaminen voi vaikuttaa positiivisesti myös asiakkaiden käyttäytymiseen. Asiakas ostaa todennäköisemmin sellaisesta verkkokaupasta, jonka kokee turvalliseksi. (Mattila, Ali-Yrkkö & Seppälä 2020, 9.)

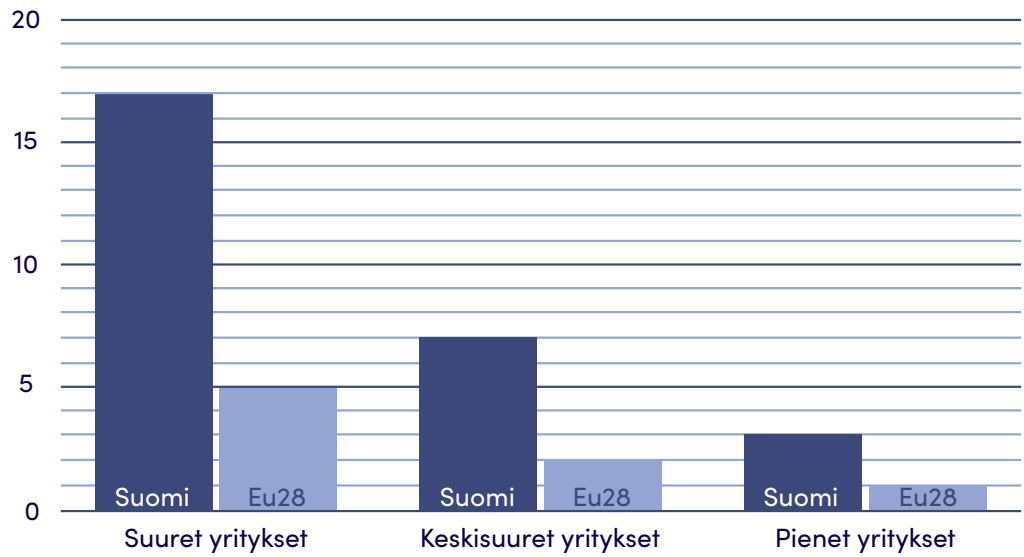
## Kyberhyökkäyksiä maailmalla

Kesällä 2021 ruotsalainen elintarvikeketju Coop joutui sulkemaan ovensa kyberhyökkäyksen takia. Tilanne aiheutui, kun ketjun käyttämä kassajärjestelmä lakkasi toimimasta palveluntarjoajaan, ohjelmistoyhtiö Kaseyaan, kohdistuneen hyökkäyksen johdosta. Kaseyan etävalvonta- ja hallintapalvelimelle (VSA-palvelimelle) saatiin ladattua erittäin korkealaatuinen valepäivitys, josta haittaohjelma levisi asiakkaina toimiville palveluntarjoajille ja edelleen varsinaisille kassajärjestelmien käyttäjille. Hyökkääjänä pidetään REvil ryhmittymää, joka omien kiristyskampanjoidensa lisäksi tarjoaa kiristyshaittaohjelmia palveluna. (Abrams 2021.)

Kansainvälinen maatalousalan yritys Danish Agro joutui kiristyshaittaohjelman kohteeksi keväällä 2020. Hyökkäyksessä hyödynnettiin tavarantoimittajan nimissä lähetettyä tietojenkalastelusähköpostia, jonka avulla tunkeutujat saivat pääsyn uhrin palvelimelle. (The Cyber Threat from Phishing Mails, 2020.) Keväällä 2022 myös Portugalin suurinta elintarvikkeiden vähittäismyyjää Modelo Continentea kohtasi hyökkäys, joka kaatoi sen verkkokaupan vaikuttaen samalla joihinkin sen myymälöiden palve-

luihin (The Biggest Supermarket In Portugal Attacked By Hackers, The Site Is Down, Stocks Plummeted As The Result 2022). Myös brittiläinen maatalousalan yritys NWF Group ilmoitti vuoden 2020 lopulla, että sen tietojärjestelmiin oli murtauduttu. Sen kahden toimialan, rehut ja polttoaineet, tietojärjestelmiin oli tunkeuduttu, ja järjestelmät jouduttiin ottamaan tutkinnan ajaksi pois käytöstä. Tapahtuman selvittely kesti viikon ja maksoi yhtiölle 500 000 puntaa. (Houghton 2020.)

Vuonna 2019 tehdyssä tutkimuksessa suomalaiset yli 250 työntekijän suuryritykset sijoittuivat kyberturvallisuuteen liittyvien ongelmien esiintyvyydessä selkeästi EU:n keskitasoa huonommin. **Tietovuotoihin liittyviä ongelmia oli Suomen suuryrityksissä jopa kolminkertaisesti verrattuna EU-maiden keskitasoon** (Kuvio 1.). (Mattila, Ali-Yrkkö & Seppälä 2020, 5.) Suomalaisyritysten on siis syytä panostaa kyberturvallisuuden kehittämiseen. Viime aikoina on myös uutisoitu useista suomalaisiin organisaatioihin kohdistuneista kyberhyökkäyksistä. Hyökkäyksiin on jouduttu osallisiksi sekä suoranaisina kohteina että välillisesti esimerkiksi emoyhtiöön kohdistuneen hyökkäyksen kautta.




*Kuvio 1. Tietovuodon kohteeksi joutuneet yritykset 2019 (mukaillen Mattila, Ali-Yrkkö & Seppälä 2020, 6).*

# Kaupan ja jakelun kyberuhkia

Kaupan ja jakelun toimialalla kybertoimintaympäristö voidaan jakaa kahteen eri ympäristöön, perinteiseen toimistoverkkoon eli IT-ympäristöön ja operatiiviseen tuotantoympäristöön, OT-ympäristöön. Toimialan erityispiirteenä on materiaalivirtojen automatisoitu ohjaus, seuranta ja raportointi. OT-ympäristö kaupan ja jakelun alalla tarkoittaa käytännössä logistiikkakeskuksia, joita voidaan kutsua myös keskusvarastoiksi. Huoltovarmuuskeskuksen tekemän kartoituksen perusteella IT- ja OT-ympäristöjen järjestelmiä ohjataan ja hallitaan usein täysin erillisesti. Tämä voi aiheuttaa eroja näiden ympäristöjen kyberturvallisuuden kypsyydessä yrityksen sisällä. Kuvaajasta (Kuvio 2.) voidaan nähdä, että merkittävimmät erot ovat pääsyn-, identiteettien- ja käyttövaltuuksien hallinnan, tapahtumien ja poikkeamien hallinnan, toiminnan jatkuvuuden sekä suojattavien kohteiden, muutosten ja konfiguraatioiden hallinnan osa-alueilla. (Kyberturvallisuuden nykytila eri toimialoilla 2020.) On syytä huomata, että OT-ympäristöt ovat erittäin harvoin täysin eristettyjä muista tietoverkoista tai järjestelmistä. Näin ollen, IT- ja OT-verkot saattavat muodostaa hyökkäysvektorin ympäristöjen välillä.


*Kuvio 2. IT- ja OT-ympäristöjen kypsyysarviot (mukaillen Kyberturvallisuuden nykytila eri toimialoilla 2020, 18).*

## OT-ympäristö

Nykyaikaisissa keskusvarastoissa on useita järjestelmiä, jotka ovat alttiita kyberuhkille. Automaatio, kuten kuormalava-automaatit ja pientavara-automaatio, lisääntyy kaiken aikaa. Erityisesti verkkokaupassa lyhyet toimitusajat ovat tärkeitä, ja toimintaa tehostetaan automaatiolla. Nykyiset toiminnanohjaus- ja varastonhallintajärjestelmät saattavat tehdä täydennystilauksia itsenäisesti tai ehdottaa tilausten tekemistä, kun havaitsevat sen tarpeelliseksi. Ruokalogistiikkaan kuuluvat myös lämpötilavyöhykkeet ja lämpötilahallitut kuljetukset. Myös erilaiset energiaa säästävät ratkaisut, kuten aurinkopaneelit, maalämpö- ja maakylmäjärjestelmät, LED-valaisimet, IoT-laitteet ja älykkäät kiinteistönohjausjärjestelmät yleistyvät kaiken aikaa. (Mononen n.d.)

Kyberhyökkäys järjestelmiin voi aiheuttaa logistiikan keskeytymisen ja sitä kautta suuriakin kustannuksia. Raha ei liiku, kun tavara loppuu kaupoista tai tuotteet pilaantuvat kylmäketjun katkettua. OT-ympäristö on usein integroitu IT-ympäristöön ja liiketoiminnan kannalta kriittiseen toiminnanohjausjärjestelmään, ERP:iin. ERP-järjestelmällä hoidetaan muun muassa myynti- ja ostoreskontraa, kirjanpitoa ja asiakkuuksienhallintaa (Hakkarainen 2017, 12). Myös esimerkiksi varastojen keräily- ja tilausjärjestelmät ovat kriittisellä tavalla riippuvaisia ERP-järjestelmästä. Liiketoiminnan kannalta kriittisiä voivat olla kassajärjestelmät, ja myös tilaus- ja toimitussanomien välityspalvelu, EDI (Electronic Data Interchange). Mikäli EDI-sanomat eivät välitä tietoa siitä, mitä tavaraa pitää toimittaa tai kassajärjestelmän kautta ei saada maksettua tavarantoimittajille, kuljetusketju voi pysähtyä. Monessa yrityksessä vielä edellä mainittuja järjestelmiä kriittisempi voi olla Microsoftin Azure AD -identiteetinhallintapalvelu, koska moniin järjestelmiin kirjaudutaan AD-palvelun tunnistautumisen kautta.

Teollisuuden ohjausjärjestelmien (ICS, Industrial Control Systems) elinkaari on tyypillisesti hyvin pitkä. Päivityksiä järjestelmiin tehdään harvoin, ja elinkaaren lopulla tietoturvapäivityksiä ei enää ehkä saada ollenkaan, jolloin järjestelmät ovat haavoittuvampia. Riskiä nostaa entisestään se, että järjestelmä- ja laitekantaa ei ole OT-ympäristössä välttämättä kartoitettu, jolloin ei ehkä tarkalleen edes tiedetä mitkä kaikki järjestelmät ovat verkossa, onko päivityksiä tehty tai saatavilla ja mitkä ovat järjestelmien haavoittuvuudet.

**Hyviä käytänteitä koskien teollisuuden ohjausjärjestelmiä:**

- Tarkista, priorisoi, testaa ja toteuta tietoturvapäivitykset ja ota käyttöön konfiguraatioiden hallinta.
    - › Lataa aina päivitykset valmistajan sivuilta, ja varmista niiden aitous.
- Tee varmuuskopiot järjestelmien datasta ja konfiguraatioista.
- Tunnista, minimoi ja varmista kaikki verkkoyhteydet. Pienennä hyökkäyspinta-alaa poistamalla tarpeettomat verkkoyhteydet, palvelut, portit ja protokollat käytöstä.
    - › Salli vain välttämättömät etäyhteydet. Käytä samoja yhteysreittejä ja toimintatapoja niin järjestelmätoimittajien kuin työntekijöidenkin osalta.
    - › Jos yhteys on välttämätön, mutta yksisuuntainen tiedonvälitys riittää, käytä datadiodeja. Salli kokoaikaiset yhteydet internetiin vain, jos se on aivan välttämätöntä.
    - › Eristä verkot segmentteihin. Käytä datadiodeja myös eri turvatason alueiden väliseen tiedonsiirtoon mahdollisuuksien mukaan.
- Panosta luotettavaan prosessiin käyttäjän tunnistamisessa ja käyttöoikeuksien hallinnassa.
    - › Toteuta monivaiheinen tunnistautuminen aina kun mahdollista.
    - › Anna käyttöoikeudet vain niille henkilöille, joille se on välttämätöntä, ja poista oikeudet työsuhteen päättyessä.
    - › Ota käyttöön vahvat salasanat, joita vaihdetaan vähintään 3kk välein.
- Ota käyttöön virustorjuntaohjelmistot sekä sovellusten ”allowlisting”.
    - › Uusi haittaohjelma voi jäädä torjuntaohjelmalta huomaamatta, mutta ”allowlisting” (eli sallittujen ohjelmien, toimintojen ja käyttäjien luettelointi) voi estää sen, koska sovellus ei kuulu sallittujen listalle.
- Seuraa ja arvioi järjestelmien, verkkojen ja yhteyksien turvallisuutta jatkuvasti.
    - › Tunnista verkkoliikenteestä haitallinen sisältö sekä epäilyttävä ja epänormaali liikenne.
    - › Käytä kirjautumisanalytiikkaa tunnistamaan tunnuksien väärinkäyttö, esimerkiksi epätavalliseen aikaan tai epätavallisesta osoitteesta tullut kirjautuminen kriittiseen järjestelmään.

- Hallinnoi fyysistä ympäristöä, estä pääsy asiattomilta henkilöiltä.
- Toteuta kyberturvallisuuskoulutus kaikille työntekijöille.
- Toteuta ja testaa poikkeamienhallintasuunnitelma.

(Cybersecurity Best Practices for Industrial Control Systems, 2020; Seven Steps to Effectively Defend Industrial Control Systems, Nd.)

## IT-ympäristö

Syyskuussa 2022 Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus totesi kyberympäristön uhkatason nousseen maailmanlaajuisesti. Myös aktiviteettien Suomea kohtaan todettiin lisääntyneen, erityisesti haittaohjelmien, tietojenkalastelun ja palvelunestohyökkäysten muodossa. (Kyberturvallisuuskeskuksen viikkokatsaus - 37/2022 2022.) Helsingin kauppakamarin vuonna 2019 tekemän selvityksen mukaan valtaosa yrityksistä, 61 %, piti tietojenkalastelu- tai haittaohjelmahyökkäyksiä suurimpana uhkana suomalaisille yrityksille. Toiseksi suurimpana uhkana vastaajayritykset pitivät yrityksen luottamuksellisen tiedon vuotamista. (Yrityksiin kohdistuvat kyberuhat 2019, 2019.)

**Tietojenkalastelussa** rikollisten päämääränä on huijata kohde kertomaan pankkitunnuksensa, luottokorttinsa numeron ja tunnusluvun, Microsoft Office 365 -tunnuksensa tai jotain muuta luottamuksellista tietoa, jotta rikolliset voivat sitä kautta saada rahallista hyötyä. Käytännössä kalastelu tapahtuu lähettämällä sähköposti- tai tekstiviestejä, jotka saadaan näyttämään jonkin viranomaisen tahon lähettämiltä ja siten uskottavilta. Viestien lähettäjäksi saatetaan väittää esimerkiksi veroviranomaista, pankkia, poliisia, postia tai teleoperaattoria. Viestit sisältävät linkin, jota klikkaamalla käyttäjälle avautuu aidolta näyttävä sivusto, johon syötetyt tiedot kuitenkin päätyvät rikollisten käsiin. Huijauksissa hyödynnetään ajankohtaisia aiheita, luvataan esimerkiksi ilmaista sähköä tai pelotellaan seuraamuksilla, jos viestiin ei reagoida riittävän nopeasti. Jos et ole varma, onko viesti aito, **kirjaudu linkin sijasta palveluun suoraan palvelun-tarjoajan osoitteesta**. (Kyberturvallisuuskeskuksen viikkokatsaus - 37/2022 2022; Pienyritysten kyberturvallisuusopas 2020, 4–5.)

Usein Microsoft Office 365 -tunnusten kaappaamisen tavoitteena on löytää yrityksen laskutukseen liittyviä tietoja ja sitä kautta laatia uskottavia **valelaskuja** (Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta, 2019). Valelaskuilla laskutetaan olemattomia palveluita ja toivotaan, ettei vastaanottaja kiireessä huomaa, että lasku ei ole aito ja maksetut rahat menevät rikollisen tilille. Lasku voi tulla sähköpostiviestinä tai paperilaskuna, ja laskun maksamista saatetaan hoputtaa jopa puhelinsoitolla. Laskun sisältävät sähköpostiviestit saattavat näyttää aidoilta ja tulevan yhteistyökumppanilta tai jopa oman yrityksen sisältä. Epäselvät tapaukset kannattaa varmistaa puhelimitse ja laskuja maksaessa käyttää alkuperäisiä yhteystietoja. Katso Kyberturvallisuuskeskuksen ohjeet laskutushuijausten tunnistamiseen sekä miten suojautua Microsoft Office 365 tunnusten kalastelulta ja tietomurroilta (pdf).

**Toimitusjohtajahuijauksessa** rikollinen lähettää hyvin aidon näköisen viestin yrityksen rahaliikenteestä vastaavalle henkilölle esiintyen yrityksen toimitusjohtajana. Viestissä pyydetään suorittamaan yleensä kiireellinen palkanmaksu tai tilisiirto tai maksamaan lasku, josta rahat päätyvät rikollisille. Jos viesti epäilyttää, varmista viestin aitous puhelimitse. (Pienyritysten kyberturvallisuusopas 2020, 4.)

**Lisää linkkejä avuksi huijausten tunnistamiseen ja niiltä suojautumiseen:**

- Näin suojaudut nettihuijaukselta
- Pienyritysten kyberturvallisuusopas (pdf)
- CYBERDI Tietopankki

**Kiristyshaittaohjelmat** ovat kyberrikollisten yleisesti käyttämä keino ansaita rahaa. Hyökkäyksessä kohdeyrityksen laitteilla olevat tiedot salataan, ja sen jälkeen vaaditaan lunnaita tietojen vapauttamista vastaan. Salatut tiedot sijaitsevat edelleen laitteissa, mutta niitä ei pystytä lukemaan ilman salausavainta. Lunnaita ei kuitenkaan pidä maksaa missään tapauksessa, sillä ei ole mitään takeita, että rikolliset toimisivat niin kuin lupaavat. On myös täysin mahdollista, että tiedot on jo tuhottu, eikä niiden palauttaminen ole alun perinkään ollut vaihtoehto. Rikolliset voivat kiristää myös tietojen vuotamisella internetiin. Kehittyneemmät kiristyshaittaohjelmat saattavat lisäksi sabotoida yrityksen verkkoinfrastruktuuria tai tuhota myös tärkeiden tietojen varmuuskopiot, mikäli niihin on pääsy.

## *Kyberturvallisuuskeskuksen mukaan pienyritykset ovat helppo kyberhyökkäyksien kohde.*

Pienillä yrityksillä ei välttämättä ole resursseja tietoturvatoimenpiteiden toteuttamiseen tai yhtä laajaa tietoisuutta tietoturvasta kuin suuremmilla. (Pienyritysten kyberturvallisuusopas 2020, 8.)

**Kiristyshaittaohjelmahyökkäyksestä kertovia merkkejä voivat olla:**

- ruudulle ilmestyvä tai muulla tavoin toimitettu kiristysviesti
- palveluntarjoajan tai tietoturvatuotteen hälytys
- tiedostot eivät aukea
- laitteet eivät tuntemattomasta syystä toimi
- yhteistyökumppani, viranomainen, asiakas tms. ilmoittaa hyökkäyksestä

(Toimintaohje - Kiristyshaittaohjelma 2022, 6.)

Kyberturvallisuuskeskus on julkaissut ohjeen Toimintaohje – Kiristyshaittaohjelma (pdf) avuksi tilanteisiin, joissa epäillään kiristyshaittaohjelmahyökkäystä tai sitä, että hyökkäys estää normaalin toiminnan. Julkaisusta löytyy ohjeet varautumisen hallinnollisiin ja teknisiin toimiin sekä harjoitteluun, poikkeamien havaitsemiseen ja toimintaan, kun tietoturvaloukkaus on tapahtunut. Myös organisaatioiden johdolle on julkaistu oma ohje, Toiminta kiristyshaittaohjelmatilanteessa - johdon ohje (pdf).

**Palvelunestohyökkäysten** tavoite on jonkin palvelun lamauttaminen kohdistamalla siihen suuret määrät tietoliikennettä. Yleensä kohteena on jokin julkinen sivusto tai yleisesti hyödynnetty palvelu. Yritykselle tämä voi aiheuttaa esimerkiksi seuraavanlaisia ongelmia:

- Kuluttajat eivät pääse yrityksen verkkosivustolle tekemään tilauksia.
  - › Yrityksen omaa palvelinta vastaan on hyökätty tai yritys joutuu hyökkäyksen kärsijäksi välillisesti, kun hyökkäys kohdistuu palvelinhotelliin, jota yritys käyttää. (Kyberturvallisuus ja hallituksen vastuu -opas 2020, 8.)
- Yritys ei pääse hoitamaan normaalia verkkoasiointiaan.
  - › Yrityksen käyttämää tärkeää palvelua vastaan on hyökätty estäen sen käyttö tai hidastaen sen toimintaa. Esimerkiksi tilauksia ei voi tehdä tai ottaa vastaan tai laskujen maksu ei onnistu.
- Yrityksen laitteet toimivat normaalia hitaammin.
  - › Yrityksen laitteet on kaapattu osaksi hyökkääjän käyttämää useiden laitteiden verkostoa, ns. bottiverkkoa, jota käyttäen hyökätään kohteisiin muualla internetissä. Bottiverkko koostuu hyökkääjän eri puolilta internetiä hallintaansa ottamista laitteista. Jos laitteesi on kaapattu, sitä ei todennäköisesti ole helppo havaita, mutta se saattaa ilmetä laitteen hidastumisena ja suurentuneena resurssien käyttönä.

Esimerkiksi Valtioneuvoston ja useampien ministeriöiden verkkosivustoihin kohdistui huhtikuussa 2022 palvelunestohyökkäys, jolloin osa sivuista toimi huonosti tai ei ollenkaan. Hyökkäys kesti joitakin tunteja. (Valtioneuvoston ja ministeriöiden verkkosivuihin kohdistunut palvelunestohyökkäys on ohi 2022.)

***Kyberturvallisuuskeskuksen viikkokatsauksen 37/2022 mukaan palvelunestohyökkäysten määrät ovat nousussa.***

Hyökkäyksistä on aiheutunut hetkellisiä palvelukatkoksia erilaisiin verkkosivustoihin ja yritysten sisäisiin palveluihin. (Kyberturvallisuuskeskuksen viikkokatsaus - 37/2022 2022.)

**Kyberturvallisuuskeskus on laatinut ohjeen palvelunestohyökkäystilanteisiin:** Toimintaohje – Palvelunestohyökkäys (pdf)

**Informaatiovaikuttaminen** on järjestelmällistä toimintaa, jonka tarkoitus on vaikuttaa yleiseen mielipiteeseen, ihmisten käyttäytymiseen, päätöksentekijöihin ja sitä kautta yhteiskunnan toimintakykyyn. Vaikuttamista voidaan tehdä muun muassa levittämällä vääriä tai harhaanjohtavia tietoja, painostamalla tai käyttämällä sinänsä oikeaa tietoa, mutta tarkoitushakuisesti. (Valtionhallinnon viestintäsuositus 2016, 13.) Supo arvioi, että Suomeen suuntautuva vaikuttaminen tulee tiedustelun ohella todennäköisesti lisääntymään entisestään (Tiedustelu ja vaikuttaminen, 2022).

Informaatiovaikuttaminen voi kohdistua myös yksittäiseen yritykseen. Hyökkääjä, joka voi olla esimerkiksi suurempi valtiollinen toimija tai haktivisti, voi haluta mustata yrityksen mainetta. Informaatiovaikuttamisen rinnalla voidaan käyttää myös muita keinoja jolloin puhutaan hybridivaikuttamisesta. Esimerkiksi jumitetaan yrityksen palvelut palvelunestohyökkäyksellä, ja sen jälkeen lietsotaan epäluottamusta yritystä kohtaan. Kyberhyökkäyksen varsinainen päämäärä voi siis olla yritykseen kohdistuva mainehaitta. (Informaatiovaikuttaminen on kyberympäristössä arkipäivää 2021.) Henkilöstön on syytä olla tietoinen, että yritys saattaa joutua informaatiovaikuttamisen kohteeksi ja osata myös ilmoittaa siihen liittyvistä havainnoista. Muun muassa yrityksen viranomaisyhteydet, omistajapohja, toimiala tai asiakassuhteet voivat olla syy vaikuttamisen kohteeksi joutumiselle. (Hybridivaikuttaminen voi romahduttaa yrityksen toimintakyvyn 2022.)

***Henkilöstön on syytä olla tietoinen, että yritys saattaa joutua informaatiovaikuttamisen kohteeksi, ja osata myös ilmoittaa siihen liittyvistä havainnoista.***

Lisätietoa informaatiovaikuttamisen tunnistamiseen ja analysointiin sekä siihen reagoimiseen löytyy Valtioneuvoston kanslian oppaasta Informaatiovaikuttamiseen vastaaminen: Opas viestijöille.

Myös Kyberturvallisuuskeskus tarjoaa Vinkkejä informaatiovaikuttamisen tunnistamiseksi.

Koronapandemian alussa huhu siitä, että perustuotteet loppuisivat, aiheutti ostopaniikin, jonka vuoksi vessapaperi- ja pastahyllyt tyhjenivät joissakin kaupoissa. Äkillinen piikki kysynnässä sekoitti toimitusketjua. Valheellisten tietojen tahallinen levittäminen voisi aiheuttaa vastaavanlaista hamstrausta, joka hankaloittaisi ja häiritsisi elintarviketeollisuutta, tavarantoimittajia ja kauppoja. (Hamstraus taklataan tiedolla 2022.) Huoltovarmuusorganisaatio onkin laatinut Viestintäoppaan hamstrauksen torjuntaan päivittäistavarahuollon toimijoille.

# Lähteet


Abrams, L. 2021. Coop supermarket closes 500 stores after Kaseya ransomware attack. BleepingComputer. Viitattu 8/2022. https://www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/

Cybersecurity Best Practices for Industrial Control Systems. 2020. CISA. Viitattu 10/2022. https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf

Hakkarainen, S. 2017. Pk-yrityksen liiketoiminnan tehostaminen toiminnanohjaus- järjestelmällä. 99. Viitattu 10/2022. https://www.theseus.fi/bitstream/handle/10024/140281/Hakkarainen_Seija.pdf

Hamstraus taklataan tiedolla. 2022. Huoltovarmuuskeskus. Viitattu 9/2022. https://www.varmuudenvuoksi.fi/artikkeli/hamstraus-taklataan-tiedolla/

Houghton, T. 2022. Hacking incident costs agricultural firm £500,000 as trading in shares restarts. Viitattu 10/2022. https://www.business-live.co.uk/economic-development/hacking-incident-costs-nwf-group-19266076

Hybridivaikuttaminen voi romahduttaa yrityksen toimintakyvyn. 2022. Keskuskauppakamari. Viitattu 9/2022. https://kauppakamari.fi/tiedote/hybridivaikuttaminen-voi-romahduttaa-yrityksen-toimintakyvyn-nailla-keinoilla-yritykset-voivat-ehkaista-hybridivaikuttamista/

Informaatiovaikuttaminen on kyberympäristössä arkipäivää. 2021. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 9/2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/informaatiovaikuttaminen-kyberymparistossa-arkipaivaa

Kyberturvallisuuden nykytila eri toimialoilla. 2020. Huoltovarmuuskeskus. Viitattu 8/2022. https://www.huoltovarmuuskeskus.fi/files/b3671ecb5d0b5b431174fec9350e0251b75227ba/kyberturvallisuuden-nykytila-eri-toimialoilla2-verkkosivuille.pdf

Kyberturvallisuus ja hallituksen vastuu -opas. 2020. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 8/2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Kyberturvallisuuskeskuksen viikkokatsaus—37/2022. 2022. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 9/2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-372022

Mattila, J., Ali-Yrkkö, J., & Seppälä, T. 2020. Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät? ETLA. Viitattu 8/2022. https://pub.etla.fi/ETLA-Muistio-Brief-93.pdf

Mononen, A. N.d. Automaatio lisääntyy logistiikkakeskuksissa. Viitattu 10/2022. https://www.prologistiikka.fi/natiivi/3212/automaatio-lisaantyy-logistiikkakeskuksissa

Pienyritysten kyberturvallisuusopas. (2020). Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 9/2022. https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pienyritysten-kyberturvallisuusopas

Sektorit ja poolit. N.d. Huoltovarmuuskeskus. Viitattu 8/2022. https://www.huoltovarmuuskeskus.fi/toimialat/elintarvikehuolto/elintarvikehuoltosektori/

Seven Steps to Effectively Defend Industrial Control Systems. N.d. CISA. Viitattu 10/2022. https://www.cisa.gov/uscert/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa 2019. 2019. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 10/2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Suojaamattomia_automaatioj%C3%A4rjestelmi%C3%A4_suomalaisissa_verkoissa_2019.pdf

Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta. 2019. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 9/2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Suojautuminen%20Microsoft%20Office%20365%20-tunnusten%20kalastelulta%20ja%20tietomurroilta%20web.pdf

The Biggest Supermarket in Portugal Attacked By Hackers, The Site Is Down, Stocks Plummeted As The Result. 2022. Viitattu 10/2022. https://voi.id/en/technology/151816/the-biggest-supermarket-in-portugal-attacked-by-hackers-the-site-is-down-stocks-plummeted-as-the-result

The Cyber Threat from Phishing Mails. 2020. Centre for Cybersecurity. Viitattu 8/2022. https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/treat-assessment---cyber-threat-from-phishing-mails.pdf

Tiedustelu ja vaikuttaminen. N.d. Suojelupoliisi. Viitattu 9/2022. https://supo.fi/tiedustelu-ja-vaikuttaminen

Tieto- ja kyberturvallisuus. N.d. Teknologiateollisuus ry. Viitattu 8/2022.https://teknologiateollisuus.fi/sites/default/files/inline-files/T-Tieto-ja-kyberturvallisuus.pdf

Toimintaohje—Kiristyshaittaohjelma. 2022. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 9/2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/KiristyshaittaohjelmaToimintaohje.pdf

Valtioneuvoston ja ministeriöiden verkkosivuihin kohdistunut palvelunestohyökkäys on ohi. 2022. Yle Uutiset. Viitattu 9/2022. https://yle.fi/uutiset/3-12396843

Valtionhallinnon viestintäsuositus 2016. 2016. Valtioneuvoston kanslia. Viitattu 9/2022. https://vnk.fi/viestintasuositus

Yrityksiin kohdistuvat kyberuhat 2019. 2019. Helsingin seudun kauppakamari. Viitattu 8/2022. https://rihykauppakamari.fi/files/yrityksiin-kohdistuvat-kyberuhat-2019.pdf

Luku 3

# Kyberpoikkeamien hallinta kaupan ja jakelun yrityksissä

**Luvun kolme aiheina ovat kyberpoikkeamien hallinta, erityisesti varautumisen näkökulmasta, kriisi- ja häiriöviestintä sekä olennaiset viranomaisyhteydet kyberpoikkeamatilanteissa.**

# 3 Kyberpoikkeamien hallinta kaupan ja jakelun yrityksissä

**Vesa Vertainen, Reijo Lähteenmäki, Sampo Kotikoski, Paavo Nelimarkka, Jaana Brandt, Elina Suni**

## Kyberuhkiin varautuminen

Varautumisen keskiössä ovat muun muassa havainnointikyvykkyyden kehittäminen ja toipumisen suunnittelu. Myös poikkeaman selvittämiseen ja tutkinnan edesauttamiseen sekä mahdolliseen viranomaisyhteistyöhön on varauduttava.

### Yhteinen operatiivinen kuva

On tärkeää luoda yhteistä operatiivista kuvaa toimialan sisällä. Jos yksittäisessä organisaatiossa tapahtuu kyberturvallisuuden poikkeama, on siitä syytä raportoida myös muille alan organisaatioille, ettei tilanne pääse leviämään laajemmin toimialalla. Luomalla yhdessä kattavaa tilannekuvaa, organisaatiot voivat kohdistaa kyberturvallisuuden resurssejaan oikeisiin asioihin. Tähän toimialan sisäiseen tiedonjakoon on erilaisia tapoja ja kanavia.

Tietoa jaettaessa on luonnollisesti syytä olla tarkkana siitä, mitä tietoa kannattaa tai voi lain nojalla jakaa, ja poistaa salassa pidettävät osuudet. On syytä käydä ennakkoon läpi, missä menee luottamuksellisen tiedon rajat tiedon jakamista ajatellen. Tietoa voidaan myös anonymisoida niin, että tiedosta käy ilmi vain oleellinen tekninen osuus. (Ilkka, Sahlman, Mäntylä, Hartikainen, Janhunen, Grönroos, Raappana, Kinnunen, Heikkinen, Niinikorpi, Lehtinen, Törmälä & Pajunen 2017, 21.)

ISAC (Information Sharing and Analysis Center) -ryhmät ovat toimialan sisäisiä tiedonvaihdon yhteistyökanavia. Ryhmissä käsitellään tietoa luottamuksellisesti. Organisaatiot kehittävät toimialan sisäistä tietoutta ja käytänteitä sekä auttavat organisaatioita varautumaan poikkeamiin. Ryhmät tukevat hyvin oppimista, sillä organisaatio pystyy jakamaan poikkeamatilanteen käsittelyssä syntyneet opit muillekin organisaatiolle.

Kyberturvallisuuskeskuksen ISAC-tiedonvaihtoryhmät löydät täältä. Lisää ISAC-ryhmistä myös kappaleessa: Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus.

VAHTI 2017 Tietoturvapoikkeamatilanteiden hallinta -julkaisun kappaleessa Kriisi- ja häiriöviestintä kyberpoikkeamatilanteessa kerrotaan tiedon jakamisesta ja viestinnästä poikkeamatilanteissa. Lisää aiheesta myös kappaleessa: Kriisi- ja häiriöviestintä kyberpoikkeamatilanteessa.

**Teknisesti uhkatiedon jakamisen** formaattina käytetään laajalti STIX-kuvauskieltä kyberuhkia käsittelevien organisaatioiden kesken. STIXin avulla voidaan luoda jäsenneltyjä ja johdonmukaisia uhkatietokuvauksia. STIX-formaattiin muotoiltua uhkatietoa voidaan kuvailla esimerkiksi seuraavien kysymysten kautta:

- Mitä tulisi etsiä? (Observable)
- Miksi siitä pitäisi välittää? (Indicator)
- Missä se nähtiin? (Incident)
- Mitä tapahtuu? (Tactics, techniques, and procedures, TTP)
- Mitä heikkoutta hyödynnetään? (Exploit target)
- Miksi se tehtiin? (Campaign)
- Kuka sen on toteuttanut? (Threat actors)
- Mitä asialle pitäisi tehdä? (Course of Action)

(Vertainen, Suni, Vatanen, Hautamäki, Laava, & Piispanen 2021, 32–33.)

Organisaatioiden väliseen formaaliin uhkatiedon jakamiseen on olemassa erilaisia uhkatiedon jakomalleja ja alustoja, kuten TAXII-protokolla ja MISP-tiedonjakoalusta. (Vertainen ym. 2021, 34–35.) Tarkemmin uhkatiedon jakamisesta voit lukea Kyberhäiriöiden hallinta – Käsikirja terveydenhuollon toimijoille (pdf) -julkaisun kappaleesta Kyberturvallisuuteen liittyvän tilannetiedon jakaminen.

## Tekninen jäljitettävyys

Lokitiedot ovat tapahtumatietoja, joita tallentuu automaattisesti tietojärjestelmistä tai laitteista. Tällaisia ovat esimerkiksi ulos- tai sisäänkirjautumiset, tiedon käsittely, kuten katselu, lisäys, poisto tai muutos tai erilaiset palomuurin suorittamat toimenpiteet. Lokitietoja voidaan tarvita normaalitilanteissa muun muassa käytönvalvontaan ja tilastointiin, mutta niiden avulla voidaan myös havaita tunkeutumisyrityksiä tai muita poikkeamia. (Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta 2020, 37.)

Huoltovarmuuskeskuksen kartoituksen mukaan lokitietojen seurannan kehittäminen on yksi merkittävimmistä kehityskohteista kaupan ja jakelun kyberturvallisuudessa. Lokitiedoilla on olennainen merkitys poikkeamien korjaustoimenpiteissä ja palautumisessa. Kun lokitus on järjestetty kattavasti ja hyvien käytäntöjen mukaisesti, auttaa se ajantasaisen tilannekuvan muodostamisessa, erityisesti suojattavien kohteiden hallinnoimiseen yhdistettynä. (Kyberturvallisuuden nykytila eri toimialoilla 2020, 11–12.)

On syytä määritellä tarkkaan, mitä tapahtumista tallennetaan, keillä on oikeus tietojen tarkasteluun, ja kuinka kauan lokitiedot säilytetään. Esimerkiksi yritykseen kohdistunut tietomurto saattaa tulla ilmi vasta pitkän ajan kuluttua. Tällaisen poikkeaman selvittämisessä voi auttaa huomattavasti, jos tiedot ovat vielä tallessa ja on tallennet-

tu oikeanlaista tietoa. Myös havaitun poikkeaman aikana lokitietojen keräämisestä ja analysoinnista on apua tilannekuvan muodostamiseen ja toipumisen suunnitteluun. Lokitieto toimii myös eräänlaisena allekirjoituksena, kun jokainen käyttäjä ohjeistetaan kirjautumaan järjestelmiin aina omilla tunnuksillaan, eikä tunnuksia luovuteta muille missään tilanteissa. Tätä onkin syytä korostaa henkilöstön ohjeistuksissa.

Jo palvelun hankintavaiheessa kannattaa määritellä, millä tavalla omaan toimintaan liittyviin tietoihin päästään poikkeamatilanteessa käsiksi. Esimerkiksi keskitetyissä palomuureissa ja palvelinympäristöissä myös lokitietojen keräys saattaa olla keskitetty niin, että palveluntarjoajan on vaikea eritellä tietyn asiakkaan lokit muista. On myös mahdollista, että lokijärjestelmää ylläpitää eri toimija kuin muita järjestelmiä, jolloin näiden väliset pääsyoikeudet on syytä olla selvillä. (Kyberhäiriötilanteet - Varautuminen ja toiminta 2019, 12.)

Kyberturvallisuuskeskus on laatinut ohjeistuksen yrityksille, joilla on omaa osaamista lokien hallintaan: Näin kerää ja käytät lokitietoja. Ohjeita lokienhallinnan suunnitteluun ja sitä ohjaavan dokumentaation laatimiseen löytyy myös valtionvarainministeriön suosituskokoelmasta tiettyjen tietoturvallisuussäännösten soveltamisesta (pdf).

## Riskienhallinta

Riskien tunnistaminen on Huoltovarmuusorganisaation Digipoolin mukaan lähtökohta muiden toimenpiteiden suunnittelulle. On tärkeämpää arvioida riskit ensin sen sijaan, että vain hankitaan erilaisia tietoturva- ja suojausratkaisuja. (Kyberhäiriötilanteet - Varautuminen ja toiminta, 2019). Mikäli riskienhallintaa ei aktiivisesti toteuteta, organisaation ei ole helppo tunnistaa tavoitteitaan uhkaavia riskejä tai saada niitä hallintaan. Organisaatio määrittää itse riskienhallintansa tason. Mitä korkeampi hallinnan taso, sitä korkeammat kustannukset. Riskienhallintaan panostaminen aiheuttaa aina kustannuksia. Riskienhallinta tulisi mitoittaa niin, että siitä aiheutuvat kustannukset eivät ole suuremmat kuin toteutuneiden riskien kustannukset.

**Riskienhallinnan prosessia voidaan kuvata seuraavasti:**

**1.** Määritetään toimintaympäristö.

**2.** Tunnistetaan keskeiset riskit.

**3.** Tehdään riskianalyysi (laadullinen tai määrällinen analyysi).

**4.** Arvioidaan riskien seuraukset.

**5.** Käsitellään riskit.

**6.** Hyväksytään riskit.

Prosessi aloitetaan uudestaan alusta, kun tuloksia on havainnoitu. Toistoperiaate mahdollistaa vaiheittaisen etenemisen. Korjataan aluksi pahimmat puutteet ja edetään pienempiin riskeihin tarvittaessa.

### Toimintaympäristön määrittäminen

Toimintaympäristö jaetaan yrityksen sisäiseen ja ulkoiseen osaan. Määritys pohjautuu yrityksen tietoturvapolitiikassa määriteltyihin asioihin, kuten esimerkiksi tietoturvan laajuus ja merkitys yrityksen toiminnassa. Toimintaympäristön määrittelyssä tulee punnita muun muassa liiketoimintaprosessien arvo, niihin liittyvien tietojen kriittisyys ja tietoturvan merkitys liiketoiminnan kannalta. Myös yrityksen maineeseen mahdollisesti aiheutuva haitta tulee punnita. Tieto on keskeisin suojattava kohde, ja keskeinen tieto luokitellaan vähintään tyyliin julkinen, luottamuksellinen, salainen.

### Riskien tunnistaminen

Määritellään ensin suojattavat kohteet ja niiden suhteellinen arvo. Suhteellinen arvo tarkoittaa tässä karkeaa asteikkoa esimerkiksi 1–5. Asiakasdata voitaisiin luokitella tässä asteikossa arvolle 5. Suojattavat kohteet tulee myös luetteloida. Suojattavia kohteita ovat esimerkiksi keskeiset tietojärjestelmät, data, tietoverkot ja toimintaprosessit. Kullekin kohteelle on syytä määritellä omistaja, jolla on vastuu kohteen toimivuudesta. Kun suojattavat kohteet on määritelty ja luetteloitu, aloitetaan uhkien tunnistaminen. Valmiit uhkaluettelot auttavat uhkien tunnistamisessa ja määrittämisessä. Esimerkiksi VAHTI-ohjeen 22/2017 liitteestä 5 (pdf) löytyy esimerkkejä riskien luokittelusta.

### Riskianalyysi

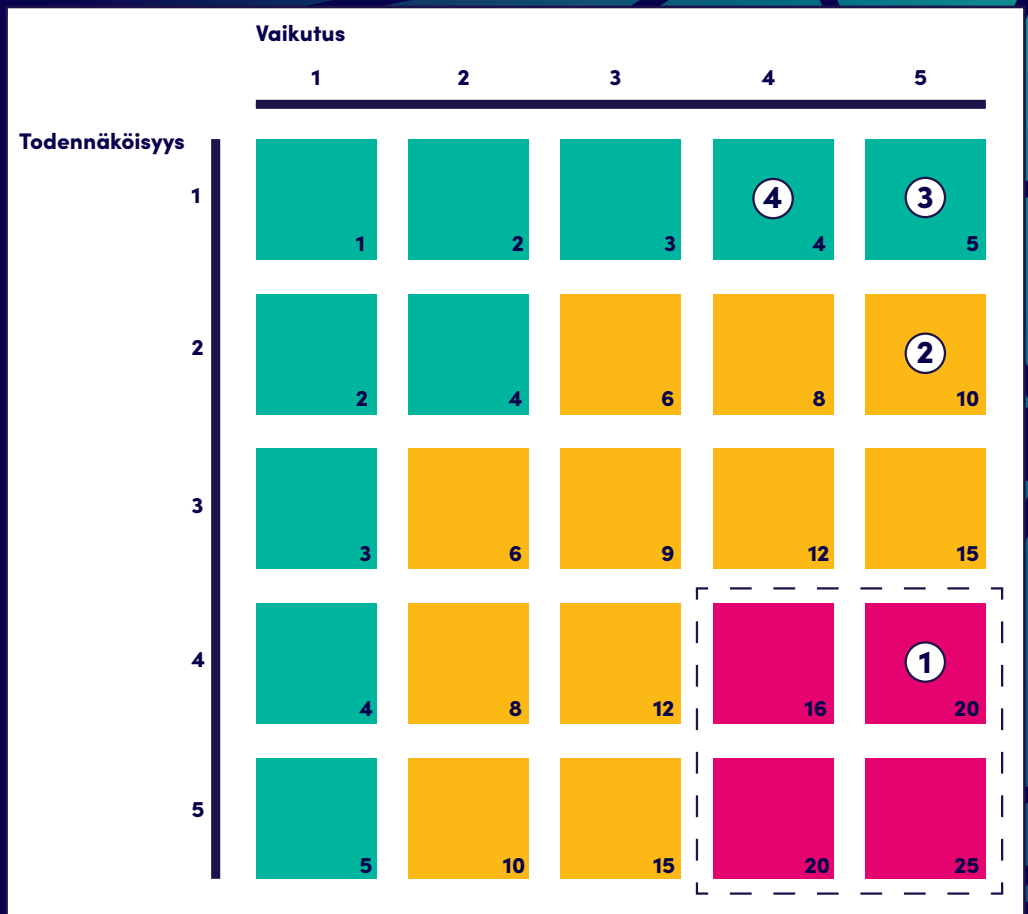
Analyysin tarkkuus ja syvyys voi vaihdella tarpeen mukaan. Epätarkemmalla analyysilla saadaan yleensä nopeammin tuloksia ja sitä voidaan soveltaa vähemmän kriittisiin kohteisiin ja uhkiin. Menetelmänä käytetään laadullista tai määrällistä analyysiä. Määrällinen analyysi soveltuu tilanteisiin, joissa on käytettävissä tarkkaa dataa kohteista, uhkista ja riskeistä (yrityksissä tällainen tilanne on harvinainen). Vakuutusyhtiöillä on melko hyvin dataa asiakkaista, mutta joskus nekin erehtyvät. Yrityksellä voi olla tapahtumatietoa kerättynä tietojärjestelmillä, esimerkiksi palomuureilla ja IDS-järjestelmillä (Intrusion Detection System, tunkeutumisenhavaitsemisjärjestelmä).

Laadullisessa analyysissä yksinkertaistetaan kohteiden arvoa, uhkien todennäköisyyksiä ja aiheutuneita riskejä. Yksinkertainen taulukkomenetelmä on kertoa uhkan vaikutus (1–5) sen todennäköisyydellä (1–5) ja näistä saadaan riskiä kuvaava arvo (1–25). Järjestämällä riskit laskevaan järjestykseen saadaan taulukon alkuun pahimmat riskit. Riskitaulukkoesimerkkiin (Taulukko 1.) on listattuna neljä eri riskiä ja laskettu niiden riskiarvo kertomalla uhkan vaikutus sen todennäköisyydellä. Taulukon uhkat on järjestetty siten, että riskiarvon mukaan luokiteltuna pahin uhka on ylimmäisenä.

Riskiarvotaulukon (Taulukko 1.) riskit sijoitetaan riskimatriisiin (Kuvio 3.) ja täten riskimatriisista voidaan havainnollisesti nähdä, mitkä riskit kannattaa ottaa jatkotarkasteluun (kuviossa katkoviivojen sisäpuolella).

TAULUKKO 1. Riskiarvotaulukko

| Nro | Tyyppi | Uhka | Vaikutus | Todennäköisyys | Riskiarvo |
|---|---|---|---|---|---|
| ① | Välttämättömien palveluiden menettäminen | Sähkökatkos | 5 | 4 | **20** |
| ② | Välttämättömien palveluiden menettäminen | Tietoliikennehäiriö | 5 | 2 | **10** |
| ③ | Fyysinen vaurio | Vesivahinko | 5 | 1 | **5** |
| ④ | Fyysinen vaurio | Jäätyminen | 4 | 1 | **4** |




*Kuvio 3. Riskimatriisi*

Riskin arvioinnissa on usein vähintään kaksi toistokertaa (karkea ja tarkempi). Arvioinnissa määritetään:

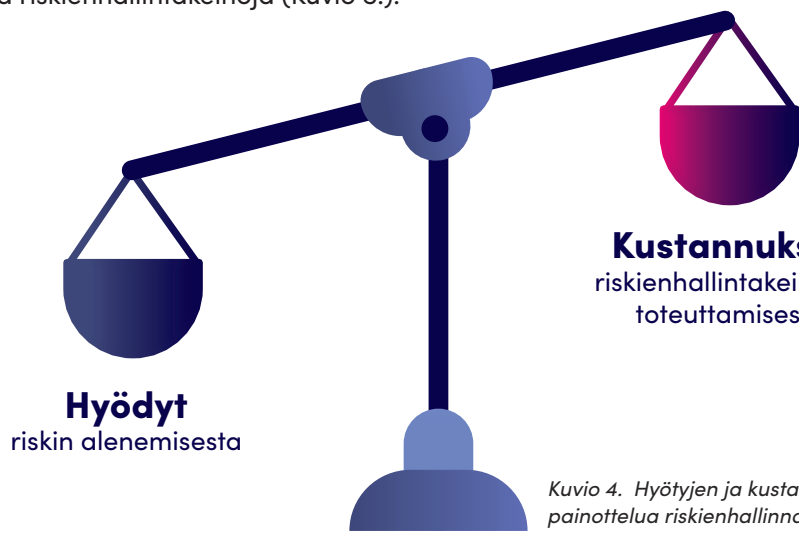
- Suojattavien kohteiden arvo.
- Yksilöidään niihin kohdistuvat uhkat ja olemassa olevat (tai mahdolliset) haavoittuvuudet.
- Yksilöidään käytössä olevat hallintakeinot ja niiden vaikutus tunnistettuihin riskeihin.
- Määritetään mahdolliset seuraukset ja asetetaan näistä tiedoista johdetut riskit tärkeysjärjestykseen toimintaympäristön määrittämisen yhteydessä määritettyjen riskien merkityksen arviointikriteerien mukaisesti.

### Riskien seurausten arviointi

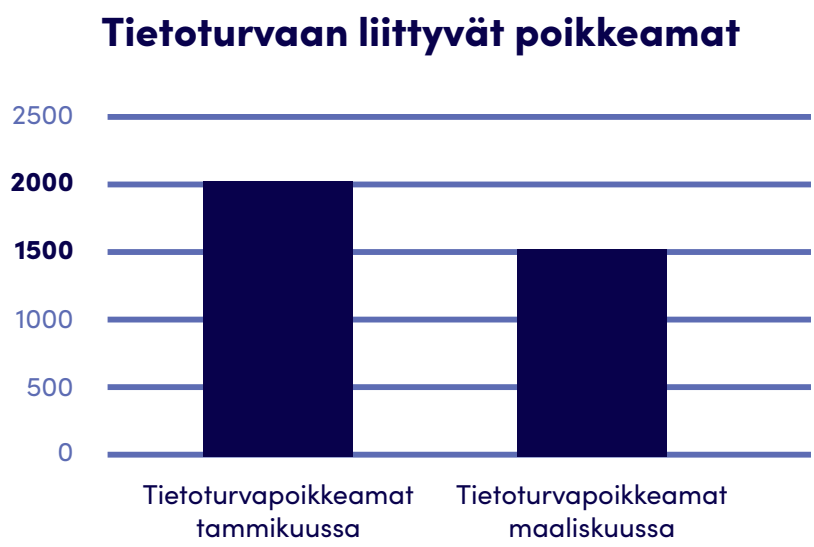
Riskien seurausten arviointi voi lähteä riskianalyysin tuloksista. Tulosten perusteella arvioidaan riskien aiheuttamia liiketoimintavaikutuksia.

### Riskien käsittely

Tutkitaan, onko jo jotain hallintakeinoja käytössä riskin alentamiseksi (control mechanisms, esim. SFS/ISO 27002 tietoturvastandardissa on luetteloitu hallintakeinoja). On myös tärkeää tutkia, onko olemassa tietoturvahaavoittuvuuksia, jotka lisäävät riskiä. Haavoittuvuudet johtuvat yleensä puutteellisesti toteutetuista hallintakeinoista. Jotkut hallintakeinot voivat pienentää useiden riskien vaikuttavuutta. Esimerkiksi henkilöstön kouluttaminen auttaa yleensä laaja-alaisesti. Liiketoiminnan jatkuvuuden kannalta kriittiset riskit tulisi punnita erikseen yrityksen johtotasolla, vaikka riskien todennäköisyys olisikin matala. Toteutuessaan ne voivat uhata liiketoiminnan jatkuvuutta. Esimerkkejä liiketoiminnan jatkuvuuden kannalta kriittisistä riskeistä ovat keskeisen tiedon vuotaminen, tiedon hallitsematon muuttuminen tai vakava tulipalo. Hallintakeinoja miettiessä tulee puntaroida niiden hyötyjä suhteessa kustannuksiin (Kuvio 4.). Parhaassa tapauksessa tietoturvapoikkeamien määrä laskee, kun käyttöönotetaan erilaisia riskienhallintakeinoja (Kuvio 5.).




*Kuvio 4. Hyötyjen ja kustannusten tasapainottelua riskienhallinnassa*




*Kuvio 5. Tietoturvaan liittyvien tietoturvapoikkeamien määrä ennen ja jälkeen riskienhallintakeinojen käyttöönottoa*

### Riskin hyväksyminen

Kun riskin käsittelyssä on saatu jäännösriski hyväksyttävälle tasolle, se voidaan johdon toimesta hyväksyä. Joskus korkea jäännösriski voidaan hyväksyä, vaikka sitä ei ole saatu alenemaan määritellylle tasolle. Tällöin voidaan turvautua esimerkiksi vakuutukseen, joka korvaa harvinaisen vahingon aiheuttamat kustannukset.

Riskienhallinnasta syntyy hyvä runko myös organisaation kyberturvallisuuden kehittämiseen, ja sen avulla pystytään kartoittamaan ne toiminnan alueet, missä kyberturvallisuuden kehittäminen on kriittisintä.

Lue lisää VAHTI 2017 ohjeistuksen (pdf) mukaisesta riskienhallinnan toteuttamisesta.

### Työkaluja riskien hallintaan

Valtionhallinto on laatinut VAHTI 22/2017 materiaalin riskienhallinnan tueksi. Materiaali sisältää ohjeita ja esimerkkejä ISO 31000 riskienhallintastandardiin pohjautuvan prosessin kuvaamiseen ja toteuttamiseen, mutta myös Excel-pohjaisen työkalun organisaation riskien arviointiin.

Kyberturvallisuuskeskuksen Kybermittari -arviointityökalu sisältää kyberturvallisuuden riskienhallinnan ja auttaa siten organisaatioita arvioimaan kyberturvallisuutensa nykytilaa ja tunnistamaan kehityskohteita. Työkalua voidaan käyttää sekä yhteiskunnalle kriittisten toimintojen että liiketoiminnan jatkuvuuden arvioinnissa.

Kybermittarista julkaistiin lokakuussa 2022 uusi, helpommin käytettävä versio, jossa myös raportointia ja arvioinnin toistettavuutta on kehitetty eteenpäin (Kybermittarin uusi versio saatavilla, 2022).

Yksi keino kyberturvallisuuden toimenpiteiden hallitsemiseen on laatia vuosikello. Kaikilla yrityksillä on omat sesonkikautensa, ja kybersuojaustoimenpiteet voidaan monelta osin sijoittaa näiden sesonkien ulkopuolelle. Ensimmäiseksi toimenpiteet listataan ja järjestetään loogiseen järjestykseen, ja sen jälkeen merkitään ne kalenterivuodelle sopiviin ajankohtiin. Toimenpiteet sijoitetaan mahdollisuuksien mukaan sesonkien ulkopuolelle, mutta on huomioitava, että osa tehtävistä jatkuu läpi vuoden, myös sesonkien aikana. Osa tehtävistä voi olla myös useamman kerran vuodessa toistuvia. (10 kohtaa kyberturvallisuuden parantamiseksi matkailualalla, 2021.)

Hyvä esimerkki kyberturvallisuuden vuosikellosta löytyy oppaasta 10 kohtaa kyberturvallisuuden parantamiseksi matkailualalla (pdf).

Riskienhallinnan vuosikellon esimerkkejä myös VAHTI-ohjeen 22/2017 Ohje riskienhallintaan liitteestä 4 (pdf).

## Haavoittuvuuksien hallinta

Haavoittuvuudet eli sovellusten tai palveluiden sisältämät heikkoudet voivat mahdollistaa rikollisille pääsyn ulkopuolisilta estettyyn tietoon tai haitallisten toimenpiteiden suorittamiseen (Muona 2021, 7). Haavoittuvuuksia hyödynnetään useissa eri hyökkäystyypeissä. Ohjelmistohaavoittuvuuksia voi olla esimerkiksi käyttöjärjestelmissä, palvelinsovelluksissa, ajureissa, BIOSissa, hallintaliittymissä, laiteohjelmistotasolla (firmware) tai loppukäyttäjän sovelluksissa. Haavoittuvuuksia aiheutuu myös muun muassa konfiguraatiovirheistä ja vanhentuneista algoritmeista tai protokollista. Haavoittuvuuksien hallintaan tulisi kuulua jatkuvaa ohjelmisto- ja järjestelmäympäristön seurantaa ja kehittämistä sekä uusimpien ohjelmistoversioiden ja päivitysten asentamista välittömästi. Tähän tarvitaan päämäärätietoista toimintamallia sekä yhteistyötä sidosryhmien kanssa. (Katakri – tietoturvallisuuden auditointityökalu viranomaisille 2020, 102).

Kansallisen turvallisuusauditointikriteeristö Katakri 2020:n mukaan haavoittuvuuksien hallintaan liittyy muun muassa seuraavia toimenpiteitä:

- CERT-toimijoiden ja valmistajien tiedotukset tilataan sähköpostiin ja niistä poimitaan säännöllisesti oman yrityksen järjestelmiin liittyvät toimenpiteet. Käytössä olevista ohjelmistoista ja järjestelmistä ylläpidetään tätä varten ajantasaista listausta.
- Päivitykset testataan vähintään kuukausittain, jotta tiedetään ovatko ne asentuneet onnistuneesti.
- Verkkoon kytketyt työasemat, palvelimet, tulostimet, mobiililaitteet ja muut tarkastetaan säännöllisesti sekä aina merkittävien muutosten jälkeen, esimerkiksi haavoittuvuusskannauksen avulla.

- Skannausohjelmisto sekä laite- ja ohjelmistokirjanpito pidetään ajan tasalla ja tietoturvasta huolehditaan. Skannausohjelmistot saattavat vaatia laajoja pääsyoikeuksia ja siksi niiden suojaaminen on pidettävä hyvällä tasolla.
- Haavoittuvuudet ja päivitysmenettelyjen puutteet käsitellään niin, että heikkoudet poistetaan, korjataan tai rajoitetaan vaarantamatta kriittisten tietojen käsittelyä. Esimerkiksi CVE-luokittelua voidaan hyödyntää haavoittuvuuksien vakavuutta arvioitaessa.

(Katakri – tietoturvallisuuden auditointityökalu viranomaisille 2020, 102–103.)

Haavoittuvuus- ja murtotestauksella voidaan selvittää omien järjestelmien haavoittuvuuden tilaa joko itse tai siihen palkatun ulkopuolisen tahon toimesta. On syytä analysoida myös, kuinka erilaiset häiriöt potentiaalisesti vaikuttavat suojattaviin kohteisiin ja mikä kohteiden merkitys on tuotettavalle palvelulle. Vinkkejä haavoittuvuusskannauksiin löytyy Kyberturvallisuuskeskuksen ohjeesta Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa 2019.

**Ajankohtaista haavoittuvuustietoa voi seurata muun muassa seuraavilta sivuilta:**

- Kyberturvallisuuskeskus - Haavoittuvuudet (ajankohtaista tietoa ohjelmistohaavoittuvuuksista).
- CISA - ICS-CERT Alerts (automaatioympäristöihin liittyviä hälytyksiä).
- NIST – National Vulnerability Database (haavoittuvuuksien hallinnan tietokanta Security Content Automation Protocol/ SCAP-formaatissa).

Haavoittuvuustietoa jaetaan myös aiemmin mainittujen ISAC-tiedonvaihtoryhmien tiedotteissa. Osa haavoittuvuuksien hallintaa on myös henkilökunnan kyvykkyys tunnistaa uhkia ja haavoittuvuuksia, josta lisää luvussa Henkilöstön osaamisen kehittäminen. Seuraavassa luvussa esiteltävät kansainväliset standardit ISO/IEC 27000 ja NIST sisältävät viitekehyksiä haavoittuvuuksien hallintaan.

## Tietoturvastandardit ja ohjeistukset

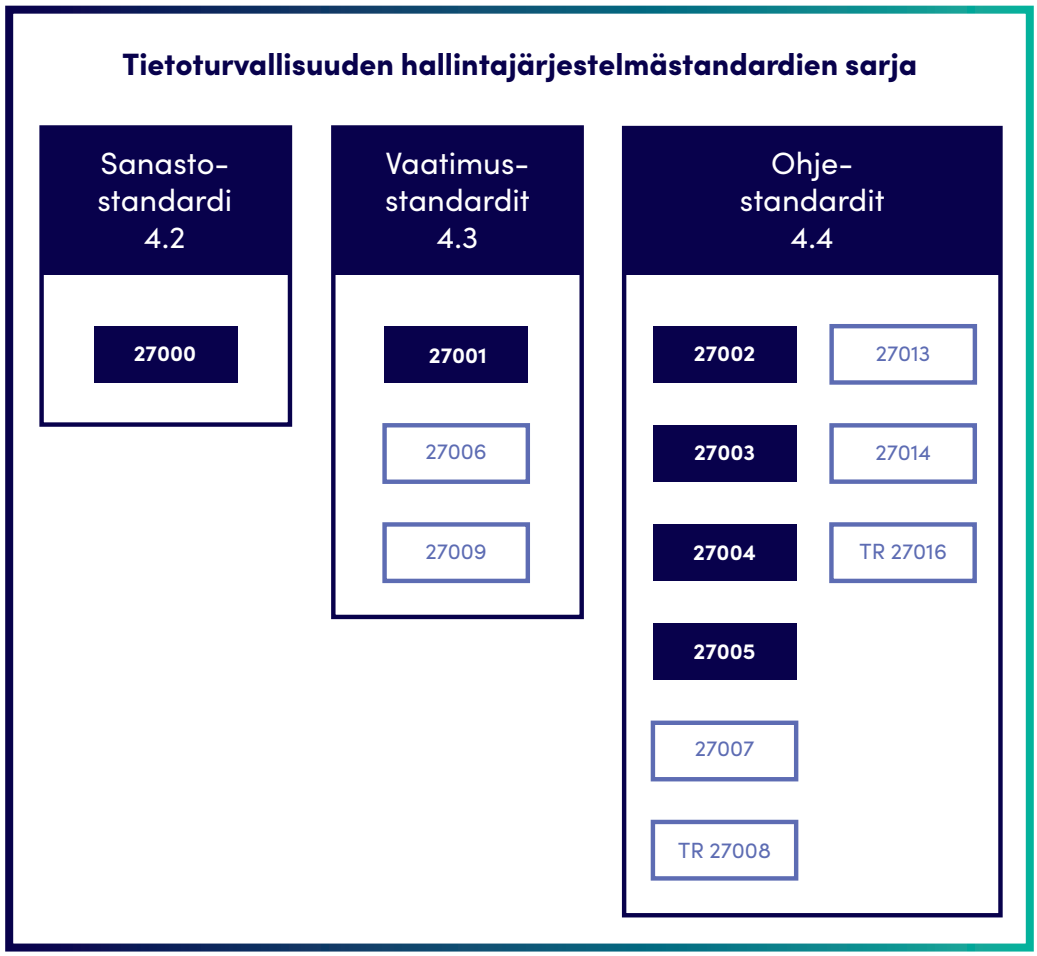
Tietoturvastandardit ja ohjeistukset voidaan jakaa karkeasti kahteen ryhmään: kansainvälisiin standardeihin ja kotimaisiin ohjeistuksiin, jotka perustuvat vahvasti kansainvälisiin ohjeistuksiin.

### NIST Cybersecurity Framework (NCF)

NCF pohjautuu USA:n NIST:n tekemään standardistoon, jonka tarkoituksena on ohjeistaa julkishallintoa, yrityksiä ja yksilöitä tietoturvalliseen toimintaan. NCF pohjautuu vahvasti dokumenttiin NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. NIST:n dokumentit ovat maksuttomia. Tarkoituksena ja vaatimuksena ei ole sertifioida toteutusta. Voisi ajatella, että NIST NCF sopii pienemmille ja aloitteleville yrityksille paremmin kuin ISO 27000. Molemmat lähtevät riskianalyysin pohjalta ja molemmissa on lueteltu suuri määrä hallintakeinoja, joilla tietoturva saadaan yrityksessä toteutettua.

### ISO/IEC 27000

ISO/IEC 27000 -sarja on laaja, kansainvälisesti käytetty standardi. Se on lähtöisin Euroopasta, tarkemmin Britanniasta, jossa laadittiin alkujaan ohjeistusta julkishallinnolle ja yrityksille. Myöhemmin ohjeistusta laajennettiin ja tarkennettiin kansainväliseksi ohjeistukseksi yrityksille. Standardi mahdollistaa yrityksen ISMS-järjestelmän (Information Security Management System eli tietoturvallisuuden hallintajärjestelmä) auditoinnin ja sertifioinnin. Dokumentit ovat maksullisia ja sertifiointi on melko raskas ja kallis prosessi. Isommat ja kypsemmät yritykset sertifioivat yleensä mielellään järjestelmänsä, koska siitä saadaan maine- ja markkinointietua. Standardia voi myös soveltaa valikoivasti ilman sertifiointia, mikä sopii paremmin pienemmille ja nuoremmille yrityksille.




*Kuvio 6. Keskeisimmät ISO/IEC 27000 -standardisarjan dokumentit yrityksen tietoturvan kannalta*

**ISO/IEC 27000:2020** on lyhyt yleiskatsaus ja sanasto.

**ISO/IEC 27001:2017** avulla määritellään vaatimukset yrityksen ISMS-järjestelmälle (tietoturvallisuuden hallintajärjestelmälle). Tämä dokumentti on pohjana yrityksen vaatimuksenmukaisuuden sertifioinnissa.

**ISO/IEC27002:2017** on tietoturvallisuuden hallintaa koskeva menettelyohje, jossa luetellaan tietoturvan hallintakeinot, joilla riskianalyysin esille tuomia riskejä voidaan hallita.

**ISO/IEC27003:2017** sisältää ISO/IEC 27001:2017 mukaisen ISMS-järjestelmän toteuttamisohjeita.

**ISO/IEC 27004:2016** sisältää ohjeita mittausten käyttöön ja kehittämiseen. Ohjeilla voidaan arvioida standardin ISO/IEC 27001 mukaisesti toteutetun ISMS-järjestelmän sekä turvamekanismien/ turvamekanismiyhdistelmien vaikuttavuutta.

**ISO/IEC 27005:2018** sisältää ohjeita organisaation tietoturvariskien hallintaan.

## Kotimaiset ohjeistukset

### VAHTI-ohjeet

VAHTI-ohjeet on laadittu alun perin valtion toiminnan tueksi. Ohjeet on myöhemmin otettu käyttöön laajemmin julkishallinnon ja yksityisten toimijoiden osalta. VAHTI-julkaisut on laadittu valtiovarainministeriössä toimineen Valtionhallinnon tietoturvallisuuden johtoryhmän (1992–2013), Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (2014–2016) sekä Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (2017–2019) toimesta. Yritykset voivat vapaasti käyttää ohjeita tietoturvansa parantamiseen. VAHTI-ohjeet nojautuvat kansainvälisiin ohjeistuksiin, mutta niissä on myös huomioitu paikalliset erityispiirteet. Koska dokumentteja on julkaistu pitkällä aikavälillä ja hyvin erilaisista aiheista, ne eivät ole tiivis kehys vaan joukko itsenäisiä ohjeistuksia. Ohjeet ovat vapaasti saatavissa ja käytettävissä. VAHTI-ohjeet löydät täältä.

### Katakri – tietoturvallisuuden auditointityökalu viranomaisille

Katakri 2020 -tietoturvallisuuden auditointityökalua (pdf) käyttäen voidaan arvioida yrityksen kyvykkyyttä salassa pidettävän tiedon suojaamiseen. Katakrin ensisijainen tarkoitus on auttaa varmistamaan, että organisaation turvallisuusjärjestelyt ovat riittävät viranomaisen salassa pidettävien tietojen paljastumisen ehkäisemiseen, mutta sitä voidaan käyttää myös muun turvallisuustyön kehittämisessä. (Katakri – tietoturvallisuuden auditointityökalu viranomaisille 2020.)

### Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)

Myös pilvipalveluiden osalta on varmistettava, että tietoturvakontrollit ovat riittävät. Esimerkiksi oletusasetukset eivät välttämättä ole parhaat mahdolliset omaan tarpeeseen. Vaikka ulkoistetuissa palveluissa toimittaja vastaa tyypillisesti infrastruktuurista, on loppuasiakkaan itse määriteltävä ja ohjeistettava tiedon suojaamisen, käsittelyn ja tietoturvakontrollien taso. (Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa - Ohje johdolle ja asiantuntijoille 2022.) Pilvipalveluissa sijaitsevan salassa pidettävän tiedon turvallisuuden edistämiseen on Kyberturvallisuuskeskus kehittänyt PiTuKri – pilvipalveluiden turvallisuuden arviointikriteeristön. Palvelu sisältää myös arviointityökalun.

## Toimitusketjun suojaaminen

Helsingin kauppakamarin selvityksessä Yrityksiin kohdistuvat kyberuhat 2019 kysyttiin yritysten kyberturvallisuuden toimenpiteitä neljän kuluneen vuoden aikana. Selvityksessä 36 % vastaajayrityksistä, joista suurin osa oli pien- tai mikroyrityksiä, ei ollut tehnyt mitään kyberturvallisuuden eteen. **Osa näistäkin yrityksistä toimii todennäköisesti alihankkijoina suuremmille yrityksille ja voivat siten olla väylinä hyökkäyksissä suurempia yrityksiä kohtaan.** (Yrityksiin kohdistuvat kyberuhat 2019 2019, 9.)

Niin kutsutuissa toimitusketjuhyökkäyksissä kohdeyritykseen hyökätään käyttäen reittinä alihankkijaa tai yhteistyökumppania. Esimerkiksi vuonna 2014 Target-vähittäiskauppaketjuun hyökättiin hyödyntäen verkkotunnuksia, jotka oli varastettu yrityksen yhteistyökumppanina toimineelta LVI-yritykseltä (Target Hackers Broke in Via HVAC Company 2014). Myös ruotsalainen Coop-elintarvikeketju joutui keskeyttämään toimintansa haittaohjelman vuoksi, joka levisi kassajärjestelmiin ohjelmistoyhtiön välityksellä. Kyseessä oli toimitusketjuhyökkäys, jossa uhkatoimija hyödynsi palveluntarjoajaa kiristysohjelmansa levittämiseen. (Abrams 2021.)

Sen lisäksi, että on tunnettava omat järjestelmät ja palvelut, on hyvä tietää yhteistyökumppaneista vastaavat asiat. Toimitusketjun toiminta edellyttää usein myös arkaluontoisten tietojen jakamista eri yritysten kesken. Asiantuntemus tietojen suojaamisessa voi kuitenkin vaihdella huomattavastikin toimitusketjun eri toimijoiden välillä. Olisikin tärkeää edellyttää alihankkijoilta kyberturvallisuuteen panostamista.

**Toimitusketjuhyökkäysten varalta voidaan tehdä muun muassa seuraavia toimenpiteitä:**

- Kartoitetaan toimitusketju.
  - Kartoitetaan, keillä yhteistyökumppaneilla on pääsy yrityksen järjestelmiin tai tiloihin.
  - Toimitusketjun ymmärtäminen auttaa riskien tunnistamisessa ja käsittelyssä, häiriöihin ja keskeytyksiin varautumisessa sekä ketjun heikkojen lenkkien havaitsemisessa.
- Sovelletaan kyberturvallisuusvaatimuksiin yhteisiä standardeja tai kehyksiä.
- Selvitetään potentiaalisen yhteistyökumppanin kyberturvallisuuskäytänteet ennen sopimusten tekoa.
  - Kumppanin valinta on tehtävä huolellisesti, selvittäen luotettavuus tietoturvan näkökulmasta.
- Varaudutaan poikkeamatilanteisiin ja harjoitellaan toimenpiteitä.

- Käydään yhteistyökumppanien kanssa läpi heidän toiminnoissaan käytössä olevat turvallisuusprosessit, kuten muun muassa:
  - jaettavan tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistaminen,
  - käyttöoikeuksien ajan tasalla pitäminen ja myöntäminen vain niille työntekijöille, joille se on työn kannalta välttämätöntä,
  - käytössä olevien laitteiden ja järjestelmien kartoittaminen ja luokittelu kriittisiin/ei-kriittisiin,
  - lokitietojen kerääminen ja tallentaminen.
- Huomioidaan sopimuksissa kyber- ja tietoturvallisuus. Sovittavia asioita ovat muun muassa:
  - palveluntuottajan velvollisuudet ja vastuut,
  - onko määritetty palvelu mahdollista auditoida,
  - tietosuojaan (GDPR) liittyvät asiat,
  - onko alihankintaketjuttaminen sallittua,
  - kuka tiedon omistaa,
  - miten ja millaisella aikataululla tiedon omistaja saa omat tietonsa itselleen sopimuksen päättyessä,
  - kuka vastaa kyberpoikkeamien selvittämisestä ja niiden aiheuttamista kustannuksista,
  - ilmoitusvelvollisuus ja menettelyt poikkeamatilanteissa,
  - mahdolliset rahalliset sanktiot poikkeamatilanteissa.

(Onko organisaatiosi suojautunut toimitusketjuhyökkäykseltä? 2021; Nyman 2021; Davis 2015.)

Kyberturvallisuuskeskus on laatinut ohjeen toimitusketjuhyökkäyksiin (pdf). Ohje esittelee tämän poikkeamatyypin erityispiirteitä ja opastaa poikkeamatilanteessa toimimisessa ja siitä toipumisessa. Kybermittari-arviointityökalua voi myös käyttää toimitusketjun ja ulkoisten riippuvuuksien hallinnan kypsyystason määrittelyssä.

Hyvä työkalu eri osapuolten roolien ja vastuiden määrittelyyn ja dokumentointiin on RACI-vastuumatriisi. Vastuumatriisi on hyvä laatia jo sopimusta tehdessä ja sopimuksessa edellyttää sen ulottamista myös mahdollisia alihankkijoita koskevaksi. RACI-matriisilla määritetään eri tehtävien vastuuhenkilöt. Jokaista tehtävää kohti on yksi tai useampi tehtävän suorittamisesta vastuullinen (R), yksi päätöksen tekemisestä ja tehtävän valmistumisesta vastaava (A) sekä valinnainen määrä konsultoijia (C) ja tiedotettavia (I). (Kyberturva ICT-sopimuksissa 2021, 23–24.) Kuvassa 1. on esimerkki vastuunjaosta RACI-matriisissa. Aiheesta lisää ja esimerkkejä löytyy Huoltovarmuuskeskuksen oppaasta Kyberturva ICT-sopimuksissa (pdf).

| TEHTÄVÄ | Asiakas | SOC-palvelujen toimittaja | Palomuuripalvelujen toimittaja | Työasemapalvelun toimittaja | Tietoliikennepalvelujen toimittaja | Käyttö- ja kapasiteettipalvelujen toimittaja | |
|---|---|---|---|---|---|---|---|
| **Prosessivastuut, Tietoturvan valvonta (SOC)** | | | | | | | |
| Toimintatapojen määritys | A,R | C,I | I | I | I | I | |
| Tietoturvatapahtumien tunnistaminen ja käsittely | I | A,R | | | | | |
| Tietoturvatapahtuman kirjaaminen | I | A,R | | | | | |
| Tietoturvatapahtumien validointi | I | A,R | | | | | |
| Tietoturvatapahtuman ratkaisuvastaavien määrittäminen ja eskalointi | C | A,R | R | R | I | I | |
| Tiedottaminen sovittujen viestintäkäytäntöjen mukaisesti | I | A,R | R | R | I | I | |
| Tietoturvatapahtuman ratkaisu - juurisyyn etsintä | C | A,R | R | R | R | R | Tuotevastuiden mukaisesti |

*Kuva 1. Ote Kyberturva ICT-sopimuksissa-oppaan RACI-vastuumatriisiesimerkistä (Kyberturva ICT-sopimuksissa 2021, 25).*

## Henkilöstön osaamisen kehittäminen

Helsingin kauppakamarin selvityksestä vuodelta 2019 käy ilmi, että suurimpia esteitä tehokkaan kyberturvallisuuden toteuttamiseen ovat vastaajayritysten mielestä riittämätön tieto ja piittaamattomuus kyberuhkista (Yrityksiin kohdistuvat kyberuhat 2019 2019, 7). Piittaamattomuudenkin taustalla osaltaan vaikuttaa tiedon puute; ei ehkä ymmärretä omien tekojen vaikutusta turvallisuuteen tai sitä, että uhkat ovat todellisia. Organisaation ihmiset, prosessit ja käytettävät teknologiat muodostavat kyberturvallisuuden kyvykkyyden (Pöyhönen 2020, 184). Näin ollen henkilöstö on keskeisessä osassa kyberuhkien torjunnassa.

Henkilöstön kouluttaminen toimimaan turvallisesti sekä havaitsemaan ja tunnistamaan uhkia on tehokas tapa ennaltaehkäistä häiriöitä. Kouluttamisen lisäksi yrityksen toimintakulttuuriin on hyvä kuulua jatkuva kyberturvallisuusasioiden esillä pitäminen, jolloin siitä tulee henkilöstölle osa arkipäivän rutiinia. Koko henkilöstön on oltava tietoinen tyypillisimmistä uhista, kuten tietojenkalasteluista ja muista huijauksista samoin kuin turvallisista käytänteistä esimerkiksi salasanojen suhteen.

On tärkeää, että yrityksellä on olemassa käytänteet tietoturvapoikkeamien raportoimiseen; henkilöstöä kannustetaan ilmoittamaan havaitsemansa poikkeamat ja myös palkitaan tehdyistä havainnoista (Pienyritysten kyberturvallisuusopas 2020, 16). Henkilöstön poikkeamientunnistustaitoa voidaan harjoittaa myös siihen tarkoitetuilla ohjelmilla kuten esimerkiksi Hoxhunt. Ohjelmat muun muassa lähettävät aika ajoin epäilyttävän oloisia sähköposteja, jotka vastaanottajan on tarkoitus oppia tunnistamaan epäilyttäviksi.

Arkipäivän kyberturvallisuuden lisäksi on hyvä järjestää säännöllisesti myös siihen liittyviä harjoituksia. Jyväskylän ammattikorkeakoulun IT-instituutin kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus JYVSECTEC – Jyväskylä Security Technology tarjoaa yrityksille räätälöityjä kyberharjoituksia, koulutusta, sertifiointia sekä muita kyberturvallisuuteen liittyviä palveluita. JYVSECTEC kehittää ja toteuttaa myös eri toimialojen kansallisia teknistoiminnallisia KYHA-harjoituksia (osana turvallisuusstrategian toimeenpano-ohjelmia ja kehittämissuunnitelmia). Johtavana ajatuksena on testata ja kehittää osallistujaorganisaatioiden kybersuorituskykyä ja yhteistoimintaa vakavissa kyberturvallisuuden häiriötilanteissa realistisessa teknisessä harjoitusympäristössä Realistic Global Cyber Environment (RGCE).

Huoltovarmuusorganisaation Digipooli yhteistyössä Kyberturvallisuuskeskuksen kanssa järjestää TIETO-harjoituksia joka toinen vuosi. Viimeisin eli TIETO22-harjoitus järjestettiin vuonna 2022. Harjoituksen tavoitteena oli harjoitella yhteiskunnalle keskeisiä palveluita tuottavien yritysten selviämistä kyberpoikkeamatilanteista. Lisäksi harjoiteltiin viranomaisten tukitoimia yritysten toimintakyvyn palauttamiseksi. Harjoitus oli skenaariopohjainen strateginen harjoitus, joka järjestettiin kolmiosaisena. (TIETO22 2021.)

Digi- ja väestötietovirasto järjestää digiturva-aiheisia webinaareja kuukausittain sekä organisaatioiden asiantuntijoille että koko henkilöstölle ja joka toinen kuukausi digiturvakatsauksen johdolle. Erilaisiin kaupallisiin tietoturvakoulutuksiin voit tutustua täältä.

Pienyritysten kyberturvallisuusoppaaseen (pdf) on kerätty yleisimpiä yritysten kohtaamia uhkia ja keinoja niiltä suojautumiseen, mukaan lukien harjoitus- ja koulutustoiminta. Kyberturvallisuuskeskus on julkaissut myös ohjeen Kyberharjoitusohje – Käsikirja harjoituksen järjestäjälle (pdf) organisaatioiden varautumistyön tueksi. Harjoitustoiminnasta voit lukea lisää myös Kyberturvallisuuskeskuksen sivuilta.

Yrityksen kyberturvallisuuden tasoa voi kartoittaa myös sertifioinneilla. Yksi tällainen on Jyväskylän ammattikorkeakoulun yhteistyössä elinkeinoelämän ja julkishallinnon kanssa kehittämä FINCSC-kyberturvallisuussertifikaatti. Sertifiointi kattaa organisaation henkilöstön, prosessit, toimitilat ja käytetyt teknologiat.

## Salasanat ja monivaiheinen tunnistautuminen

Kaikissa verkkoon liitetyissä laitteissa ja järjestelmissä on syytä kiinnittää huomiota salasanojen hyviin käytänteisiin. On tärkeää, että jokaisessa palvelussa ja järjestelmässä käytetään omaa, yksilöllistä salasanaa. Myös laitteiden oletussalasanat on muistettava vaihtaa vahvempiin. Henkilöstö tulee kouluttaa hyviin käytänteisiin, esimerkiksi omia tunnuksia ei luovuteta muiden käyttöön. On myös syytä muistaa, että huijarit voivat udella tunnuksia esiintyen viranomaisina, vaikka viranomaiset (pankit tai muut tahot) eivät koskaan tunnuksia kysele. Hyvä käytänne on myös poistaa tunnukset käytöstä työsuhteen päättyessä ja muutenkin ajoittain tarkistaa tarpeelliset käyttöoikeudet.

**Kyberturvallisuuskeskus opastaa ohjeessaan Pidempi parempi - Näin teet hyvän salasanan:**

- Mitä pidempi, sen turvallisempi.
- Helppo muistaa, mutta vaikea arvata.
- Kokonainen lause on hyvä salasana.
- Käytä sekä isoja että pieniä kirjaimia sekä erikoismerkkejä.
- Kirjoitusvirheet, murre, puhekielen ilmaisut ja muut perusmuodoista poikkeavat sanat vahventavat salasanaa.

(Pidempi parempi - Näin teet hyvän salasanan 2022.)

**Hyvien salasanojen lisäksi on erittäin tärkeää ottaa käyttöön monivaiheinen tunnistautuminen** kaikkiin yrityksen kirjautumista vaativiin palveluihin, joihin on pääsy julkisen verkon kautta sekä yrityksen omissa että kumppanien vastuulla olevissa palveluissa. Jos monivaiheinen tunnistautuminen ei ole mahdollista, järjestelmän suora käyttö julkisen verkon kautta on estettävä. (Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa - Ohje johdolle ja asiantuntijoille 2022.)

Office 365 -palveluissa saattaa kuitenkin olla käytössä niin sanottu legacy-tuki, joka mahdollistaa tunnistautumisen myös laitteilla, jotka eivät tue kaksivaiheista tunnistautumista. Rikolliset ovat hyödyntäneet tätä ominaisuutta tietojenkalastelussa, joten se kannattaa poistaa käytöstä. Toinen rikollisten tapa kiertää tunnistautuminen on kysyä kalastelusivullaan tunnuksen ja salasanan lisäksi uhrin tekstiviestinä saamaa aitoa vahvistusviestiä. Yritys voi pienentää kalastelun onnistumisen riskiä muun muassa parantamalla kirjautumisen vastaanottavan Azure AD:n suojausta. (Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta 2019.) Tarkempaa tietoa aiheesta löytyy Kyberturvallisuuskeskuksen ohjeesta Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta (pdf).

Lisää vinkkejä suojautumiseen ja ohjeita mitä tehdä, jos tili kaapataan, voit lukea Kyberturvallisuuskeskuksen sivulta Nasevia neuvoja tiliesi turvaamiseksi.

## Varajärjestelmät

### Varavoima

Päivittäistavarakauppa ry:n ja huoltovarmuusorganisaation PTH-hanke eli Päivittäistavarahuollon varautumisen kehittämisprojekti (2017–2020) testasi myymälöiden valmiutta toimia sähkökatkotilanteessa varavoiman avulla. Hankkeessa todettiin, että ulkoisen varavoiman avulla liiketoimintaa voidaan jatkaa tavallisissa myymälöissä, kunhan tietoliikenneyhteydet toimivat edes rajoitetusti. Hyväksi vaihtoehdoksi arvioitiin tarpeen tullen paikalle siirrettävä varavoimageneraattori. Paras tulos saatiin yhdistämällä aurinkopaneeli, suurtehoakku ja varavoimalaite. Akkujen käyttö myymälöissä onkin jo tuttua tietoliikenne- ja maksujärjestelmien UPS-virransyöttöjärjestelmien osalta. Varavoiman käyttöönoton suunnittelussa on syytä huomioida, että ne on yleensä räätälöitävä erikseen kuhunkin käyttöpaikkaan johtuen niiden erilaisista teknisistä ominaisuuksista ja esimerkiksi polttoaineen varastointimahdollisuuksista. (Kohti toimintavarmaa myymäläverkkoa - Varmuuden Vuoksi 2021.) Lisää aiheesta löytyy hankkeessa tuotetusta ohjeesta päivittäistavarakaupan myymälöille Toimintaohje sähkökatkostilanteessa (pdf).

### Tietoliikenneyhteydet

Tietoliikenneyhteyksien varmistamiseksi voidaan kiinteän liittymän lisäksi hankkia mobiili varayhteys. Useamman eri operaattorin liittymien käyttö on hyvä varokeino. Oman verkon palomuurilaitteisiin voidaan myös asettaa varayhteys niin, että ensisijaisen yhteyden katketessa laite ottaa automaattisesti varayhteyden käyttöön.

## Varmuuskopiointi

Yrityksen liiketoimintaan liittyvistä tärkeistä tiedoista on syytä ottaa säännöllisesti varmuuskopiot (mieluiten automatisoituna toimintona). Näin toimintaa pystytään jatkamaan varmuuskopioista palautettujen tietojen avulla, vaikka alkuperäiset katoaisivat esimerkiksi laiterikon tai kiristyshaittaohjelman vaikutuksesta. Esimerkiksi eräässä keminmaalaisessa autovaraosaliikkeessä menetettiin kiristyshaittaohjelman takia asiakas- ja varastotiedot, eikä kassaa voitu käyttää. Varsinaista varmuuskopiota ei ollut, mutta kaksi päivää myöhemmin toimintaa päästiin jatkamaan jo käytöstä poistetulle tietokoneelle jääneiden tietojen avulla. (Verkkohyökkäys lukitsi autotarvikeliikkeen kassat, salasi tiedot ja sulki ovet – Tiedätkö miten varautua, sillä voit olla rikollisen seuraava kohde? 2020.)

***Varmuuskopioinnin 3–2–1-sääntö: tee kolme kopiota, kahdelle eri medialle ja ainakin yksi kopioista fyysisesti eri sijaintiin kuin alkuperäinen.***

Erityisen tärkeää on kriittisen tiedon varmuuskopiointi. Kuten aiemmin mainittiin, kriittistä tietoa ovat esimerkiksi asiakkaiden ja henkilökunnan henkilö- ja maksuvälinetiedot, ostostiedot ja muu liiketoimintaan liittyvä suojattava tieto. Varmuuskopiointiin on olemassa ns. 3–2–1-sääntö; tee kolme kopiota, kahdelle eri medialle ja ainakin yksi kopioista fyysisesti eri sijaintiin kuin alkuperäinen. Kopiot voivat olla fyysisiä, kuten ulkoinen kovalevy tai DVD-levy, taikka sijaita pilvipalvelussa, mieluiten sekä että.

Tietojen varmuuskopiointi on hyvä aikatauluttaa tehtäväksi riittävän taajaan, jotta viimeisin kopio on tarpeen tullen käyttökelpoinen. Tietojen palauttamista kannattaa myös harjoitella, ettei sen opetteluun mene tositilanteessa aikaa. Samalla on hyvä varmistaa, että tiedot ovat tallentuneet tarkoituksenmukaisina ja säilyneet eheinä. (Elliott, 2021.) Yritys saattaa olla myös velvoitettu säilyttämään joitakin tietoja tietyn aikaa, esimerkiksi laskutukseen ja verotukseen liittyen, ja myös näiden osalta on varmistettava riittävä varmuuskopiointi (Pienyritysten kyberturvallisuusopas 2020).

## Tietosuoja

Liiketoiminnassa tiedon eheys ja jäljitettävyys ovat kriittisiä arvoja. Esimerkiksi asiakastietoja, asiakkaiden ostohistoriaa ja muuta luottamuksellista tietoa on käsiteltävä asianmukaisesti. Henkilötietoja käsiteltäessä on aina noudatettava tietosuojaperiaatteita ja pystyttävä myös osoittamaan, että periaatteet toteutuvat henkilötietojen käsittelyssä. Tietosuoja.fi -sivuston mukaan tietosuojaperiaatteisiin kuuluu muun muassa, että henkilötietoja saa kerätä ja käsitellä vain tiettyä, nimenomaista ja laillista tarkoitusta varten. Henkilötietoja saa kerätä vain tarpeellisen määrän ja vain niin kauan kuin se on tarpeen. Henkilötietoja on muutenkin käsiteltävä asianmukaisesti, lainmukaisesti, läpinäkyvästi, luottamuksellisesti ja turvallisesti. Tietoja on säilytettävä sellaisessa muodossa, josta rekisteröity voidaan tunnistaa. Virheelliset ja epätarkat henkilötiedot on poistettava tai oikaistava välittömästi, kun siihen ilmenee tarvetta. (Tietosuojaperiaatteet Nd.)

Yrityksen velvollisuus tietosuojaperiaatteiden noudattamiseen on myös kilpailutekijä. Se, että asiakkaat ja yhteistyökumppanit voivat luottaa yrityksen huolehtivan tietosuojasta, luo perustaa menestykselle. (Aalto-Setälä & Viitala 2018, 5.)

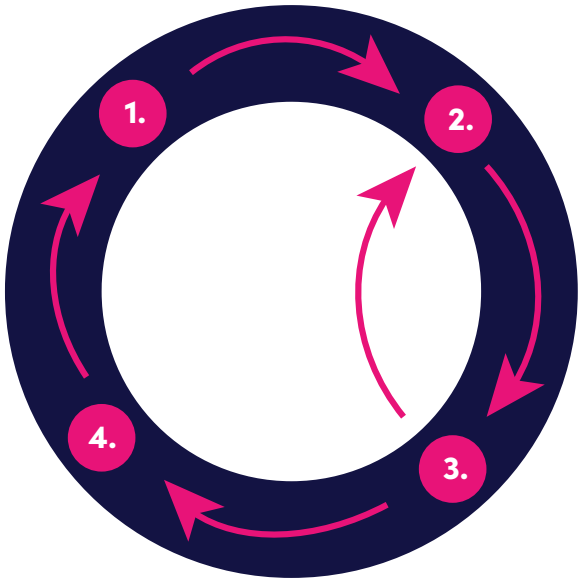
**Tietosuoja-asioita voidaan pitää ajan tasalla seuraavasti:**

- Kartoita, mitä henkilötietoja organisaatio pitää hallussaan ja missä niitä säilytetään.
- Hallitse, millä tavoin henkilötietoja käytetään ja miten käyttöoikeudet on toteutettu.
- Suojaa tietoa toteuttamalla tietoturvakontrolleja, jotta haavoittuvuudet ja tietoturvaloukkaukset estetään, havaitaan ja niihin reagoidaan.
- Raportoi tapahtuneista tietoturvaloukkauksista, säilytä dokumentaatio ja reagoi tietopyyntöihin. (Aalto-Setälä & Viitala 2018, 41.)

Lue aiheesta lisää Keskuskauppakamarin oppaasta Tietosuoja pähkinänkuoressa – tietosuojaopas yrityksille (pdf).

## Tietoturvapoikkeamatilanteiden hallinta, VAHTI 2017 -ohjeet

VAHTI 2017 -ohjeista löytyy ohjeistus tietoturvapoikkeamatilanteiden hallintaan. Ohjeistus on kattava, ja siihen kannattaa tutustua perusteellisesti. Tässä kappaleessa on vain suppea tiivistelmä prosessista. Ohjeistuksessa käydään läpi tietoturvapoikkeamien hallintaprosessi, käsittelykyvyn muodostaminen, tietoturvapoikkeamien hallitseminen ja analysointi, poikkeamatilanteisiin reagointi sekä toipuminen tietoturvapoikkeamatilanteista.




**Tietoturvapoikkeaman hallintaprosessi**
Ohjeistuksessa tietoturvapoikkeamien hallintaprosessi tiivistetään neljään osaan:

**1.** Käsittelykyvyn muodostaminen

**2.** Havaitseminen ja analysointi

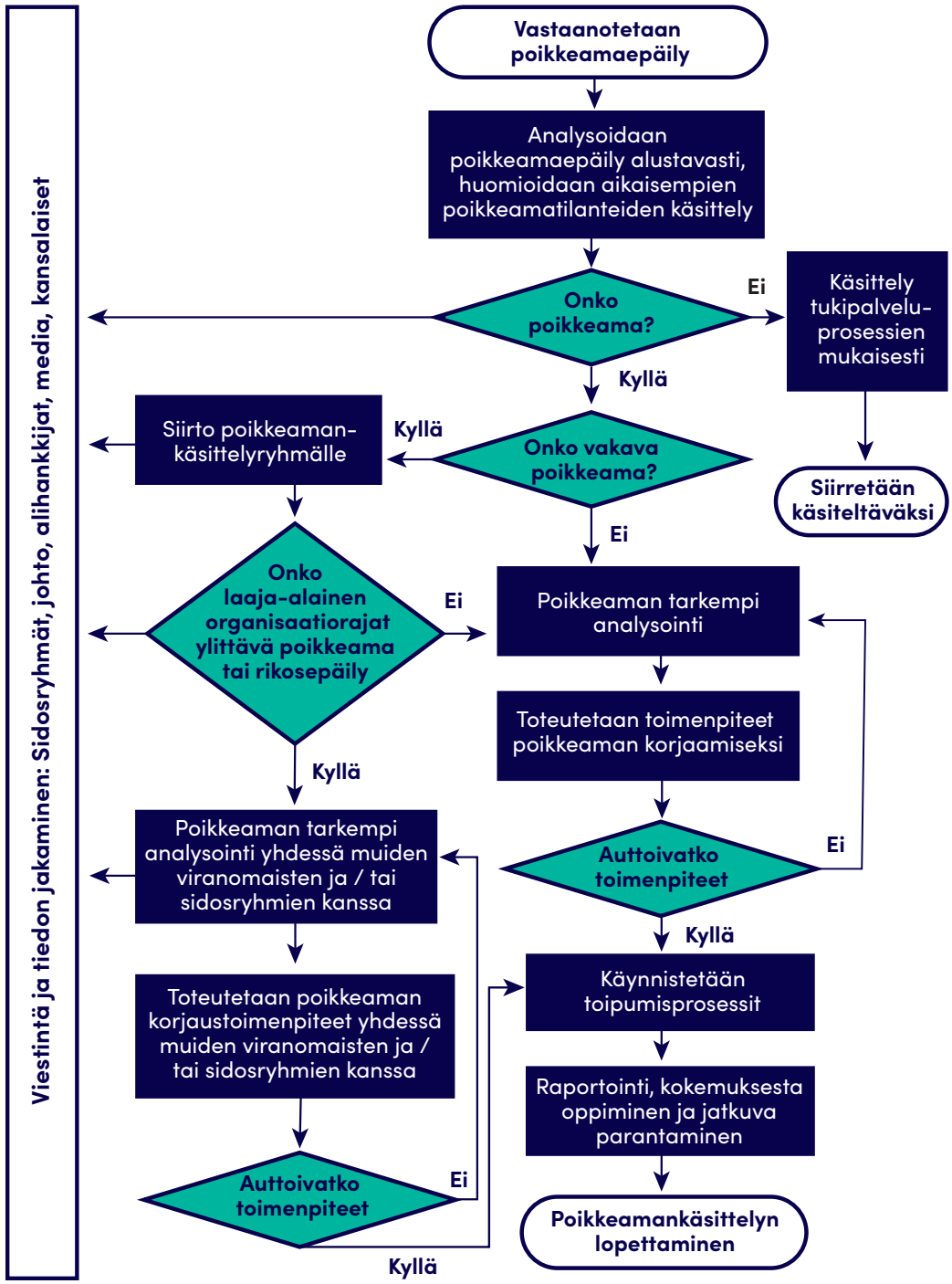
**3.** Reagointi

**4.** Toipuminen

*(Ilkka ym. 2017, 13).*

Ensimmäinen (1.) osa sisältää erilaisia varautumistoimia, joiden avulla poikkeamatilanteissa voidaan toimia. Toinen (2.) osa kattaa poikkeaman havaitsemisen ja analysoinnin. Tavoitteena on selvittää mitä on tapahtunut ja miksi. Tähän on syytä kouluttaa koko henkilöstö. Analyysin perusteella voidaan erotella poikkeamatilanne normaalista ICT-toimintahäiriöstä. Kolmas (3.) osa sisältää toimenpiteitä, jotka tulee vastuuttaa ja aikatauluttaa, jotta mahdolliset vahingot voidaan minimoida. Tähän sisältyy myös sidosryhmien ja viranomaisten informointi. Neljäs (4.) osa kattaa toipumisvaiheen, jossa organisaation ja palveluiden toiminta palautetaan takaisin normaaliin tilaan. Poikkeamasta tehdään raportti, jota käytetään poikkeamanhallinnan jatkokehityksessä. (Ilkka ym. 2017, 13.)

Yleiskuvan tietoturvapoikkeaman käsittelyprosessista näet kuviosta 7 (seuraava sivu).




*Kuvio 7. Tietoturvapoikkeaman käsittelyprosessi (mukaillen Ilkka ym. 2017, 15).*

### Tietoturvapoikkeamien käsittelykyvyn muodostaminen

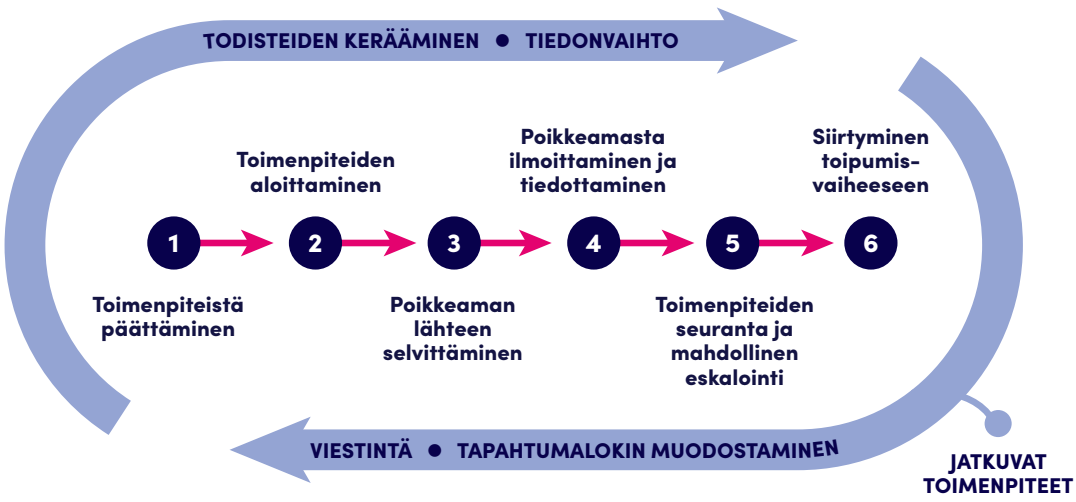
Tietoturvapoikkeamien käsittelykyvyn turvaamiseksi on hyvä muodostaa poikkeamaryhmä, joka käsittelee poikkeamat ryhmässä sovituin käytäntein. On syytä määritellä tietoturvapoikkeamien luokitteluperiaatteet, sekä suunnitella turvakontrollimekanismeja. Vastuita tulee jakaa poikkeamatilanteissa toimimisen, tiedon jakamisen ja viestinnän osalta. On myös tarpeen suunnitella käytänteet koulutukselle, harjoittelulle sekä poikkeamatilanteista oppimiselle. (Ilkka ym. 2017, 16–31.)

### Tietoturvapoikkeaman havaitseminen ja analysointi

Jotta poikkeamat pystytään havaitsemaan, on tunnettava verkkojen ja järjestelmien normaali toiminta. Tietokantojen sisältö ja käyttötavat tulee myös olla tuttuja. Henkilöstöä tulee ohjeistaa ja kannustaa ilmoittamaan poikkeuksista matalalla kynnyksellä. Poikkeaman tunnistus tehdään vertaamalla mahdollista häiriötilannetta normaalitilaan. Normaalitilan tunnistaminen vaatii laajempaa ja paikoin teknistäkin kartoitusta. Esimerkkejä hyvistä poikkeamatiedon lähteistä ovat järjestelmälokitiedostot, haittaohjelmien ja roskapostin suodatusjärjestelmät, tietoverkon laitteet ja erilaiset muiden organisaatioiden avoimet tietolähteet. Poikkeamatilanteiden tunnistus ei ole ainoastaan oman talon sisäistä työtä, vaan yhteistyö- ja ulkoistuskumppaneiltakin tulee odottaa kyberpoikkeamien havaitsemista. (Ilkka ym. 2017, 33–35.)

### Tietoturvapoikkeamaan reagointi

Poikkeamiin tulee reagoida nopeasti, etteivät mahdolliset negatiiviset vaikutukset pääse eskaloitumaan. Alla on tiivistettynä tietoturvapoikkeamaan reagointiprosessin päävaiheet (Kuvio 8.).




*Kuvio 8. Tietoturvapoikkeamaan reagoiminen (mukaillen Ilkka ym. 2017, 39).*

Reagointivaiheessa poikkeamanhallintaryhmä voidaan laajentaa kriisiryhmäksi, jolla on valtuudet tehdä päätöksiä kriisin aikana. Kriisin aikana tapahtuvat toimenpiteet ja tapahtumat tulee kirjata ylös ja kirjausten tulee olla kaikkien saatavilla. On myös viestittävä tapahtumasta selkeästi sidosryhmille ja asiakkaille. Poikkeamanhallintaryhmä päättää miten poikkeamaan reagoidaan ja pitää yllä ryhmän kokoonpanoa. Poikkeamatilanteessa on laitettava alulle toimenpiteet poikkeaman ja sen haittojen laajenemisen estämiseksi. Usein toimenpiteenä voi olla esimerkiksi sen järjestelmän tai tietoverkon eristäminen, jossa poikkeama tapahtui. Toimenpiteistä on hyvä pitää tapahtumapäiväkirjaa. Todistusaineiston turvaaminen on tärkeää siltä varalta, että poikkeama osoittautuu rikokseksi. Todistusaineistona voivat toimia esimerkiksi erilaiset lokitiedostot ja vedokset järjestelmien tilanteista sekä niiden muutoksista. Mikäli poikkeamatilanteeseen liittyy fyysinen pääsy tiloihin, kulun- ja kameravalvonnan tallenteet ovat myös mahdollista todistusaineistoa. (Ilkka ym. 2017, 39–41.)

### Tietoturvapoikkeamasta toipuminen

Kun kriisi on ohi, tulee varmistaa, että toimenpiteet ovat tehonneet. Tämän jälkeen voidaan siirtyä toipumisvaiheeseen, jonka aikana pyritään palaamaan takaisin normaalitilanteeseen. Toipumista varten tarvitaan esimerkiksi dokumentointi, josta käy ilmi, miten järjestelmät pystytetään uudelleen. Toipumisvaiheeseen tarvitaan toipumissuunnitelmat sekä riittävä henkilöstö. Sidosryhmiäkin on hyvä sitouttaa mukaan toipumiseen. Toipumisvaiheen teknisiin toimenpiteisiin voi kuulua esimerkiksi tietojen palautus varmuuskopioista, haavoittuvuuksien korjaaminen tai salasanojen muuttaminen. Joskus toimintatapoja on myös tarpeellista muuttaa. Viestinnällä on tärkeä rooli myös toipumisvaiheessa. (Ilkka ym. 2017, 51–53.)

Tietoturvapoikkeamatilanteiden hallinta, VAHTI 2017 ohjeistuksen löydät täältä (pdf).

# Kriisi- ja häiriöviestintä kyberpoikkeamatilanteessa

Tämä ohjeistus koskee normaaliolojen häiriö- ja kriisiviestintää, poikkeusoloissa tulee ensisijaisesti huomioida ko. poikkeusolojen erityispiirteet ja vaatimukset. Tätä ohjeistusta voi soveltuvin osin hyödyntää myös poikkeusoloissa. Ohjeistus soveltuu parhaiten keskisuurten/ suurten kaupan ja jakelun alan yritysten käyttöön. Pienet yritykset voivat soveltaa ohjeistusta käytössä olevat resurssit huomioiden.

**Häiriö** tarkoittaa tilapäistä poikkeamaa normaalista prosessinmukaisesta toiminnasta. Häiriö näkyy tai koskettaa organisaation tai yrityksen toimintaa, esimerkiksi palvelua. Häiriö näyttäytyy sidosryhmille, esimerkiksi asiakkaille, hetkellisenä palvelualenemana tai käyttökatkona. Organisaatio tai yritys toipuu häiriöstä nopeasti ja pystyy palauttamaan toimintansa häiriötä edeltävälle tasolle.

***Häiriö- tai kriisitilanne vaatii välitöntä reagointia. Häiriö-/kriisiryhmä johtaa tilanteen hoitoa ja viestii tilanteen vaatimalla tavalla. Viestinnän tulee olla suunniteltua ja tavoitteellista.***

**Kriisi** on äkillinen tai pitkäkestoinen vakava poikkeama normaalista prosessinmukaisesta toiminnasta. Se uhkaa organisaation aineellisia tai aineettomia arvoja kuten ihmisiä, materiaalista omaisuutta tai mainetta. Se voi uhata organisaation tuottamien palveluiden kautta organisaation sidosryhmiä tai näiden toimintaa.

Häiriö- tai kriisitilanne vaatii välitöntä reagointia. Häiriö-/kriisiryhmä johtaa tilanteen hoitoa ja viestii tilanteen vaikuttamalla tavalla. Viestinnän tulee olla suunniteltua ja tavoitteellista.

Tässä osiossa tarkastellaan kaupan ja jakelun alan yritysten kyberpoikkeamien hallintaa häiriö- ja kriisiviestinnän keinoin. Kyberpoikkeamat erotetaan normaaleista virtuaalisten palveluiden/tietojärjestelmien häiriöistä/kriiseistä. Kyberpoikkeamissa ulkopuolinen taho kohdistaa organisaation/yrityksen palveluihin/tietojärjestelmiin toimia haittatarkoituksissa. Kyberpoikkeaman aiheuttama häiriö-/kriisiviestintä päätetään tapauskohtaisesti.

## Kriisi- ja häiriöviestinnän organisoituminen

***Tunnista, kartoita, määrittele, laadi ja kokoa häiriö- sekä kriisitilanteisiin liittyvät viestinnälliset asiat, kuten prosessit ja toiminnot, ryhmät, kanavat, ohjeet ja mallipohjat.***

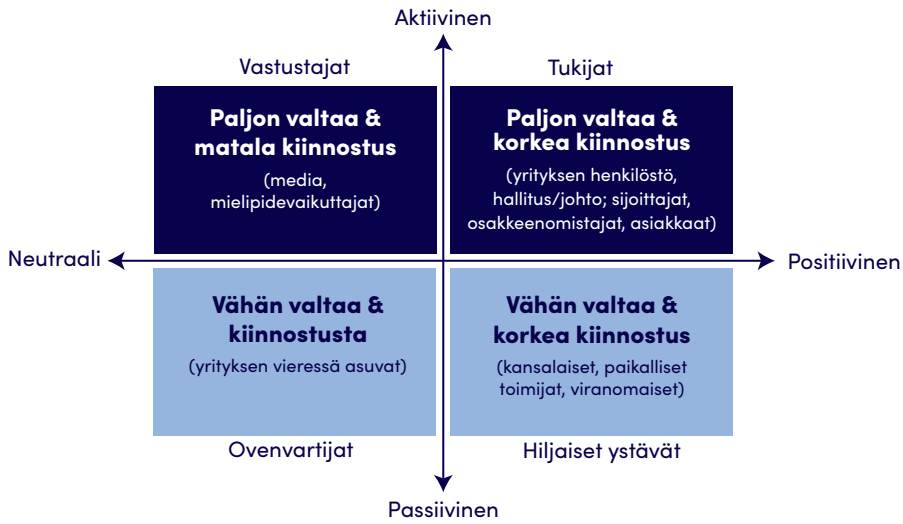
Häiriö- ja kriisiviestinnässä tulee huomioida palveluiden ja tietojärjestelmien kriittisyys. Tunnista ja listaa yrityksesi palvelut ja tietojärjestelmät. Luokittele ne kriittisiksi tai ei-kriittisiksi. Kriittinen palvelu tai tietojärjestelmä on sellainen, johon kohdistuva kyberpoikkeama aiheuttaa merkittävää haittaa tai vahinkoa liiketoiminnalle. Ei-kriittinen palvelu tai tietojärjestelmä on sellainen, johon kohdistuva kyberpoikkeama aiheuttaa haittaa tai vahinkoa liiketoiminnalle. Liiketoimintaa voidaan kuitenkin jatkaa jonkin aikaa ilman kyseistä palvelua tai tietojärjestelmää (tai järjestelmän toimiessa vain osittain).

### Palveluiden ja tietojärjestelmien raja-arvot poikkeamille

Ostamissasi palveluissa tai tietojärjestelmissä on palvelutasosopimuksia (SLA, Service Level Agreement), jotka määrittelevät palvelulle tietyt vaatimustasot/ raja-arvot palvelupoikkeamille. Yleensä myös palveluaika (esim. arkisin 8–16 tai 24/7), prioriteetit ja vastuut määritellään. Lisäksi määritellään mahdolliset seuraamukset, jos palvelusopimusta ei pystytä noudattamaan. Liiketoiminnallesi ja sen prosessille on myös lakisääteisiä tai viranomaisen asettamia raja-arvoja. Selvitä ja listaa palvelusopimusten vaatimustasot jokaisen palvelun ja tietojärjestelmän osalta erikseen, huomioi myös lakisääteiset velvoitteet.

**Sidosryhmät**

Kartoita liiketoimintasi sidosryhmät ja tee sidosryhmäanalyysi (Kuvio 9.).

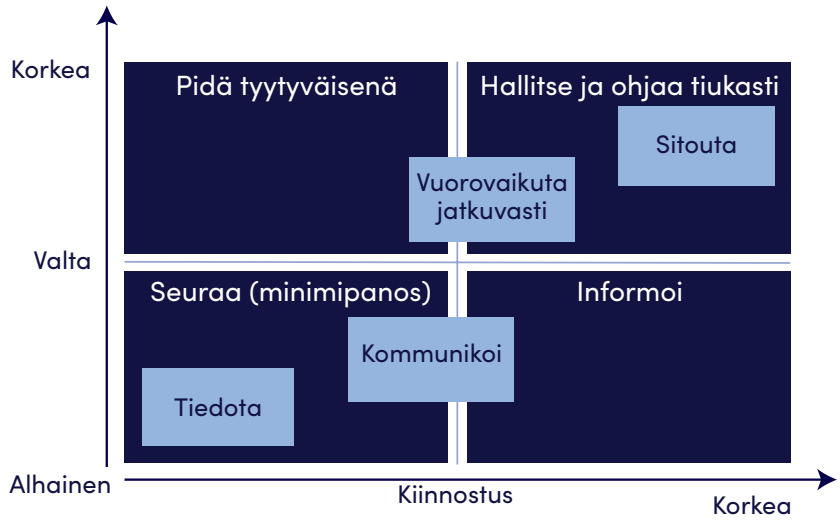



*Kuvio 9. Sidosryhmäanalyysin toteuttaminen (mukaillen Certified PMO Manager -koulutus, Adapro).*

Ymmärrä sidosryhmien tiedontarve:

- Mitä taloudellista tai emotionaalista kiinnostusta heillä on yritystä tai sen tuottamia palveluita tai heidän käyttämiään palveluita tai tietojärjestelmiä kohtaan?
- Mitä odotuksia heillä on tai mikä motivoi heitä?
- Mitä informaatiota he haluavat?
- Miten he haluavat saada informaatiota?
- Kuka/mikä vaikuttaa heidän yleisiin mielipiteisiinsä yrityksestä/organisaatiosta tai sen palveluista/tietojärjestelmistä?
- Mikä on heidän suhtautumisensa ja miten sitä voidaan muuttaa?
    - › Ellei suhtautuminen ole muutettavissa, miten voi hallita heitä niin, että heistä aiheutuu mahdollisimman vähän haittaa yritykselle/organisaatiolle tai sen tuottamille palveluille/tietojärjestelmille.

Priorisoi sidosryhmät (Kuvio 10.).




*Kuvio 10. Sidosryhmien priorisointi (mukaillen Certified PMO Manager -koulutus, Adapro).*

### Media sidosryhmänä

Kartoita yrityksellesi/organisaatiollesi tärkeät tiedotusvälineet (lehdet, radioasemat, valtakunnalliset tiedotusvälineet, oman toimialan tiedotusvälineet/kanavat, some jne.). Koosta tiedotusvälineiden yhteystiedot, jotta tiedot ovat tarvittaessa nopeasti saatavilla. Mikäli mahdollista, verkostoidu median yhteyshenkilöiden kanssa. On tärkeää tuntea toimijat ja tahot, joiden kanssa joutuu tekemisiin mahdollisen kriisitilanteen aikana. (Henriksson & Karhu 2002, 55.)

### Hälytysjärjestelmä ja -ohjeet

Suunnittele, miten yrityksen sisäisesti tai ulkoisesti hälytetään, ohjeistetaan ja viestitään: kun fyysisessä toiminnassa tapahtuu häiriö/kriisi (esim. varaston kuljetusrobotin vikaantuminen) tai virtuaalisessa palvelussa/tietojärjestelmässä tapahtuu häiriö/kriisi (esim. yksikkötilaus muuttuu massatilaukseksi).

**Häiriö- ja kriisiviestintäryhmän kuvaus, roolit ja viestintävastuut / sijaisuusjärjestelyt (ajantasaiset yhteystiedot)**

Kuvaa ja sovi yrityksesi poikkeustilanteen viestinnän roolit ja vastuut.

**Tiedottaja tai viestintävastaava (viestinnällinen 1. kontaktipiste, eli POC, Point Of Contact):**

- On ryhmän kokoonkutsuja.
- Annetaanko kasvot julkisuuteen? (mielellään vain yhdet kasvot).
- On median kontaktihenkilö.
- Seuraa häiriön/kriisin ympärillä tapahtuvaa keskustelua ja viestintää eri medioissa – laatii niistä koosteet.

**Tietoturva- tai turvallisuusvastaava:**

- Antaa tilannestatuksen (vastuullaan tilannekuvan tuottaminen ja tiedon kerääminen).

**Johto/toimitusjohtaja:**

- Tekee päätökset.
- Annetaanko kasvot julkisuuteen? (mielellään vain yhdet kasvot).

**Kyberpoikkeaman käynnistämät häiriö- ja kriisiviestinnän mekanismit**

Tunnista liiketoimintaasi kohdanneet häiriöt/kriisit ja ovatko ne mahdollisia kyber-poikkeamia.

Mihin palveluun/tietojärjestelmään kohdistui?

- Mitkä raja-arvot ylittyivät?
- Onko kyse häiriö/kriisitilanteesta vai kyberpoikkeamasta?
  - › Hoidetaanko häiriötilanneviestinnällä (esim. 'Palvelukeskus' tiedottaa)?
  - › Kutsutaanko kokoon kriisiryhmä?

Otetaan yhteys viestinnälliseen 1. POC:iin:

- POC kutsuu koolle kriisiryhmän (millä välineellä: esim. tekstiviesti tai puhelu?).
- Ryhmä kokoontuu – tilanteen mukaan päätös (fyysinen vai virtuaalinen):
  - Fyysinen tilannehuone (varustus > listaa).
  - Virtuaalinen tilannehuone (varustus > listaa, mukaan lukien yhteyksien turvallisuus).

**Häiriö- ja kriisiviestintäkokous**

Ryhmän vastuut kokouksessa:

- **Tiedottaja:** vastaa muistiosta ja kirjaa ylös sovitut toimenpiteet.
- **Tietoturva- tai turvallisuusvastaava:** vastaa ajantasaisesta tilannetiedosta.
- **Johto/toimitusjohtaja:** vastaa päätöksenteosta.

Millainen kyberpoikkeama on kyseessä:

- Kuka havaitsi, milloin, missä, miten?
- Kuka informoi tiedottajaa, toimitusjohtajaa, johtoryhmää, viestintäyksikköä?
- Miten nopeasti kriisiryhmä saatiin koolle?

Tiedotustarpeen arviointi (onko tarpeen tiedottaa?):

- Vahingon laajuus.
- Vahingon vakavuus.
- Mikä on uutisen arvopotentiaali, moraalinen ja eettinen kulma?
- Aiheuttaako asia huolta tai pelkoa?
- Aikataulu: onko asia jo julkinen vai tulossa julkiseksi?

Ketä koskee – sidosryhmät:

- Sidosryhmäkohtainen viestintä:
  - › Mitä tietoa sidosryhmä tarvitsee?
  - › Kuka tiedottaa, milloin/miten?
  - › Miten usein tietoa tarvitaan (säännöllisesti vai tarvittaessa)?

Tiedotuksen toimintamalli kyberpoikkeamatilanteessa:

- Tiedotuksen laajuus: sisäinen, paikallinen, maakunnallinen, kansallinen, globaali?
- Ensivaiheen tiedotus: mitä on tapahtunut, milloin ja mistä saa lisätietoja?
- Muut tiedotteet ja infot.
- Yrityksen/organisaation verkkosivut ja sosiaalinen media.
- Tiedottamisen prosessi:
  - › Tiedotussykli: milloin tiedotetaan seuraavan kerran?
  - › Keneen voi olla yhteydessä?
  - › Mikä/ mitkä ovat tiedotuskanavat?

Milloin pidetään seuraava kokous ja miten usein kokoustetaan?

**Häiriö- ja kriisiviestintäryhmän työkalut:**

- Mietitään tiedon tallennuslokaatiot (ja annetaan ryhmälle oikeudet).
- Päätetään, miten tilanteen dokumentoinnista huolehditaan.
- Päätetään ryhmän viestintäkanavat tilanteen aikana.

### Kyberpoikkeaman aiheuttaman häiriö- ja kriisiviestinnän aikaikkuna

Häiriöviestinnän aikaikkuna riippuu palvelun tai tietojärjestelmän palvelutasosopimuksesta. Tämä tarkoittaa havaitun häiriön laajuutta, vakavuutta sekä häiriöön reagointi- ja korjausaikaa. Kriisiviestinnässä puolestaan pari ensimmäistä tuntia ovat ratkaisevan tärkeitä. On tärkeää olla itse aloitteellinen eikä pelkästään vastata ulkoa tuleviin reaktioihin. Kyberpoikkeamasta viestiminen tulee päättää tapauskohtaisesti. Liian pikainen viestiminen voi aiheuttaa paniikkia, kun taas pitkällisestä tilanteen kehittymisen seuraamisesta ja myöhäisestä viestimisestä voi aiheutua suuria haittoja.

Tehostaaksesi ajanhallintaa kyberpoikkeamatilanteesta viestimisessä mieti valmiiksi seuraavat asiat:

**1. Häiriö- ja kriisiviestintämallipohjat kyberpoikkeamatilanteeseen**

- Vastataan kysymyksiin: mitä, missä, milloin, miksi, millaisin seurauksin, kuka antaa lausunnon?

**2. Häiriö- ja kriisiviestintäkanavat - viestintä ulos**

- Mediatiedotteet: tiedotepohjaluonnos/-luonnokset ovat valmiina.
- Tiedotustilaisuus.
- Sosiaalinen media.
- Verkkosivut: sivupohjien rakenteet ovat valmiina.

**3. Yleinen varautuminen**

- Toimintakaaviot ja eri ryhmien toimintamallit & tehtävät.
- Organisaation sisäiset yhteystiedot.
- Keskeiset sidosryhmät ja yhteystiedot (media, asiakkaat, alihankkijat, viranomaiset, pelastusviranomaiset jne.).
- Koulutukset.
    - › Kenelle kaikille ja mitä koulutusta?
    - › Avainhenkilöiden valmentaminen viestintätehtäviin.

- Häiriö-/kriisiviestintäharjoitukset.
    - › Osataanko toimia suunnitelmien mukaisesti?
    - › Miten ohjeet toimivat käytännössä?
    - › Pelaako tekniikka?
    - › Onko roolitusten resurssointi ajan tasalla?
    - › Miten toimii koordinointi ja yhteistyö eri toimijoiden kanssa?
    - › Kirjataan/analysoidaan puutteet/kehityskohteet?
- Ohjeiden päivitys.
- Tallennuslokaatioiden ylläpito.
- Oikeuksien ajantasaisuus.
- Viestintäskenaarioita.
    - › Tiedottaja ja viestintäryhmä miettivät etukäteen toimialan näkökulmasta uhkia, häiriöitä, kriisejä ja laativat tiedotteiden mallipohjat.

**4. Kriisiviestintä on ennakoivaa toimintaa ja kriiseistä oppimista.**

Ennakoinnilla kehitetään omaa kriisiviestinnällistä toimintaa ja operatiivisella jatkuvalla ympäristön luotauksella tunnistetaan kriisin idut ajoissa. Jotta luotaus on tuloksellista, pitää määrittää:

- Luotauksen tavoitteet eli miksi luodataan.
- Mitä luodataan (keskusteluteemoja, toimialalle potentiaaliset kriisityypit, sidosryhmien toiminta).
- Miten luodataan (keinot > miten tietoa hyödynnetään kriisiviestinnän suunnittelussa).
- Miten tietoa analysoidaan systemaattisesti.

(Juholin 2001, 229.)

**Kyberpoikkeamatilanteen ollessa meneillään huomioi seuraavat asiat**

Mediajulkisuuden seuranta tilanteen aikana:

- Mistä mediasta tulivat ensimmäiset tiedustelut?
- Milloin?
- Mitä tiedusteltiin?
- Keneltä tiedusteltiin?
- Ohjattiinhan häiriö-/kriisiviestinnän POC:lle?
- Mitä tiedusteluun vastattiin?
- Annettiinko tiedote vai lausunto (ja mikä oli sen sisältö?
- Järjestettiinkö tiedotustilaisuus (missä/ milloin se järjestettiin)?
- Miten media reagoi?
- Vastasiko tiedotustilaisuutta varten laadittu kysymysluettelo toimittajien kysymyksiä (listan päivitys)?
- Kuinka monta tiedotetta/tiedotustilaisuutta järjestettiin?

(Henriksson & Karhu 2002, 95.)

**Kyberpoikkeamatilanteesta palautumisessa on tärkeää tehdä yhteenveto ja tunnistaa opit mahdollisimman pian**

Mediajulkisuus (yhteenveto):

- Missä medioissa / some-kanavissa häiriö/kriisi oli esillä?
- Miten paljon siitä kirjoitettiin?
- Mikä oli julkisuuden sävy?
- Miten pitkään häiriö/kriisi oli julkisuudessa?
- Kuka muu (ulkopuolinen) antoi medialle lausuntoja tai tietoja kriisitilanteessa?

(Henriksson & Karhu 2002, 95.)

**Mieti lopuksi, miten palataan normaaliin toimintaan. Päivitä tarvittaessa varautumisprosessi.**

# Viranomaiset elintarvikearvoketjun toimijoiden kyberturvallisuuden tukena Suomessa

## Ruokavirasto

**”Ruokavirasto toimii ihmisten, eläinten ja kasvien terveyden hyväksi, tukee maaseudun elinvoimaisuutta ja kehittää ja ylläpitää tietojärjestelmiä** (Mikä on Ruokavirasto? 2022)**.”**

Maa- ja metsätalousministeriön hallinnonalaan kuuluva Ruokavirasto toimii Suomessa valtakunnallisesti. Ruokavirasto on erittäin olennainen viranomainen elintarvikeketjun toimijoiden näkökulmasta. Ruokavirastoon tulee olla yhteydessä myös kyberpoikkeamatilanteessa, jos tilanteesta on aiheutunut tai saattaa aiheutua elintarviketurvallisuuspoikkeama.

**Ruokaviraston tehtävinä on edistää, valvoa ja tutkia:**

- Elintarvikkeiden turvallisuutta ja laatua.
- Eläinten terveyttä ja hyvinvointia.
- Kasvinterveyttä.
- Maa- ja metsätalouden tuotantoon käytettäviä lannoitevalmisteita, rehuja ja kasvinsuojeluaineita.
- Siemeniä ja taimiaineistoa.

**Virasto vastaa EU-tasolla:**

- EU:n maataloustuki- ja maaseuturahastojen varojen käytöstä Suomessa.
- Toimii EU:n maksajavirastona.
- Huolehtii EU- ja kansallisten tukien toimeenpanosta.

**Tietohallinnon osalta Ruokaviraston vastuisiin kuuluu:**

- Kehittää ja ylläpitää maaseutuelinkeinohallinnon tietojärjestelmiä.
- Kehittää ja ylläpitää toimialansa rekistereitä.
- Kehittää sähköisiä asiointipalveluja.
- Tuottaa tietohallinnon palveluita maa- ja metsätalousministeriön hallinnonalan tahoille.

(Mikä on Ruokavirasto? 2022.)

## Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus

Kyberturvallisuuskeskus tuottaa tilannekuvaa kyberturvallisuuteen vaikuttavista tapahtumista ja ilmiöistä suomalaisten organisaatioiden ja kansalaisten käyttöön. Esimerkkinä tästä on kybersää, joka kertoo edellisen kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä sekä keskuksen julkaisemat varoitukset merkittävistä tietoturvapoikkeamista. (Tilannekuva ja verkostot 2022.)

Kyberturvallisuuskeskus auttaa havaitsemaan organisaatioihin kohdistuvia tietoturvaloukkauksia sekä selvittämään niitä. Yksityiset henkilöt, organisaatiot ja yritykset voivat ilmoittaa keskukselle tietoturvaloukkauksista, kuten haittaohjelma- tai tietojenkalasteluepäilyistä, palvelunestohyökkäyksistä sekä näiden yrityksistä. Yhteydenottojen perusteella voidaan tarjota apua suomalaisille toimijoille tietoturvaloukkauksen selvittämiseksi sekä koordinoida tarvittavia toimenpiteitä. (Havainnointi ja avunanto 2022.)

Kyberturvallisuuskeskus toimii määrättynä turvallisuusviranomaisena ja kansallisena tietoturvaviranomaisena (NCSA, National Communications Security Authority), joka vastaa turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista. NCSA-toiminnon lakisääteisenä tehtävänä on tarjota arviointi- ja hyväksyntäpalveluita. Lisäksi keskus tarjoaa tietoturvaneuvontaa valtionhallinnolle sekä huoltovarmuuskriittisille toimijoille. (Arviointi, hyväksyntä ja neuvonta 2022.)

**Kyberturvallisuuskeskus tarjoaa myös seuraavia verkostopalveluita:**

- Haavoittuvuuskoordinaatio avustaa haavoittuvuuden tai vakavan ohjelmistovirheen löytäjää tekemään yhteistyötä esimerkiksi ohjelmistovalmistajien kanssa. Haavoittuvuudesta voi ilmoittaa Kyberturvallisuuskeskukselle sähköisellä lomakkeella.
- Huoltovarmuuskriittisten organisaatioiden kybervarautumista tuetaan harjoitustoiminnalla.
- Häiriötilanteiden yhteistoimintaryhmä (HÄTY) auttaa Liikenne- ja viestintävirastoa häiriötilanteiden hallinnassa ja sovittaa yhteen häiriötilanteiden hallintatoimenpiteitä (ryhmän jäseninä on viranomaisia sekä edustajia tele- ja sähköyrityksistä).
- Toimialakohtaisten kyberturvallisuuden yhteistyöelinten eli ISAC-tiedonvaihtoryhmien tehtävä on mahdollistaa tietoturva-asioiden, kuten uhkien, ilmiöiden ja hyvien käytäntöjen luottamuksellinen käsittely osallistujien kesken. Tiedonvaihtoryhmät lisäävät mukana olevien organisaatioiden tietoturvaosaamista. Ryhmien toiminta auttaa myös Kyberturvallisuuskeskusta kokonaistilannekuvan kehittämisessä. Elintarviketuotannon ja -jakelun toimialalla toimii ISAC-tiedonvaihtoryhmä.
- Kybermittari auttaa parantamaan organisaatioiden ja yritysten kykyä torjua kyberuhkia. Kybermittari on konkreettinen työkalu johdolle sekä tietoturva-alan ammattilaisille kyberuhkien parempaan hallintaan.

- Kyberturvallisuuskeskus kokoaa joka vuosi kansallisen raportin Suomessa raportoiduista tieto-turvapoikkeamista ja toimittaa sen Euroopan komission NIS-direktiivitiimille (EU:n verkko- ja tietoturvadirektiivi), joka seuraa direktiivin toimeenpanoa ja tilannekuvaa Euroopan tasolla. Yhteiskunnan kriittisen infrastruktuurin tarjoajien ja toimijoiden tietoturvavelvollisuuksista ja tietoturvahäiriöistä ilmoittamisesta säädetään NIS-direktiivissä.
- Tietoturvan standardiverkoston tavoite on parantaa kotimaisten laitevalmistajien sekä palveluntarjoajien mahdollisuuksia vaikuttaa eurooppalaiseen ja kansainväliseen tietoturvastandardointiin. Verkosto myös edistää viestinnän luottamuksellisuutta parantavien tietoturvallisten laitteiden sekä palveluiden käyttöä, saatavuutta ja vientiä.
- Tietoturvailmiöiden seurannan ja ennakoinnin tarkoituksena on havainnoida ja ennakoida digitaalisen yhteiskunnan nousevia trendejä ja ilmiöitä sekä niiden vaikutuksia kyberturvallisuuteen.

(Tilannekuva ja verkostot 2022.)

## Huoltovarmuuskeskus

**”Huoltovarmuuskeskuksen missiona on huolehtia yhdessä yrityselämän, kolmannen sektorin ja viranomaistahojen kanssa siitä, että myös kriisitilanteissa yhteiskunta toimii ja elämä jatkuu mahdollisimman häiriöttä** (Huoltovarmuuskeskus 2022)**.”**

Huoltovarmuuskeskuksen (HVK) keskeisiin tehtäviin normaaliaikoina kuuluu materiaalinen varautuminen (ml. varastointi). Elintarvikearvoketjun yritykset ovat keskeisessä roolissa materiaalisessa varautumisessa. HVK:lla on sopimuksia varautumisjärjestelyistä alan yritysten kanssa. Häiriötilanteissa HVK vastaa muun muassa varmuus- ja turvavarastojen käyttöönotosta ja niihin liittyvän logistiikan järjestämisestä. (Huoltovarmuuskeskus 2022.)

HVK:n yhteydessä toimii sektoreita ja pooleja. Niiden tehtävänä on ylläpitää ja kehittää huoltovarmuutta ja jatkuvuudenhallintaa oman toimialansa yritysten ja organisaatioiden verkostossa. Huoltovarmuussektoriin kuuluu ministeriöiden, viranomaisten, keskusvirastojen, elinkeinoelämän järjestöjen sekä keskeisten yritysten edustajia. Yhtenä kuudesta sektorista on elintarvikehuoltosektori.

**Sektoreiden tehtävänä on muun muassa:**

- Koordinoida, ohjata ja seurata oman alansa varautumista.
- Selvittää huoltovarmuuden kehittämiskohteita.
- Arvioida ja analysoida huoltovarmuuden kehityssuuntia sekä oman alansa uhkia.
- Edistää yhteistyötä huoltovarmuusasioissa alan toimijoiden kesken.
- Seurata oman alansa poolien toimintaa.
  (Sektorit ja poolit 2022.)

Sektoreihin kuuluvat poolit taas vastaavat toimiala- ja toimipaikkakohtaisesta operatiivisesta varautumisesta. Toimintaa suunnitellaan ja toteutetaan yhteistyössä elinkeinoelämän kanssa. Toiminta perustuu sopimuksiin toimialajärjestöjen ja HVK:n välillä. Elintarvikearvoketjun toimijoiden osalta olennaiset poolit ovat alkutuotantopooli, elintarviketeollisuuspooli sekä kauppa ja jakelupooli.

**Poolien tehtävänä (yhteistyössä alan yritysten kanssa) on muun muassa:**

- Seurata ja suunnitella oman alansa huoltovarmuutta.
- Määritellä ja laatia yleissuunnitelmat poikkeusolojen toimintoja koskien.
- Ohjata ja seurata alansa yritysten varautumista.
- Suunnitella henkilöstön ja muiden voimavarojen käyttöä poikkeusoloissa.
- Tehdä selvityksiä sekä esityksiä varmuus- ja turvavarastoinnin tarpeesta.
- Järjestää tiedotus-, koulutus- ja harjoitustilaisuuksia alan valmiuden ylläpitämiseksi.

(Sektorit ja poolit 2022.)

Elintarvikehuollon varautumista ohjaavat lait koskevat siemenkauppaa ja kasvinjalostustoimintaa, ajantasainen lainsäädäntö osoitteessa www.finlex.fi

Elintarvikehuoltosektorista ja siihen kuuluvista pooleista löytyy lisätietoja Huoltovarmuuskeskuksen sivuilta.

## Poliisi

Kyberrikoksen esitutkinta käynnistyy, kun poliisi saa tiedon epäillystä rikoksesta. Rikosilmoituksen tekeminen tuottaa viranomaisille arvokasta tietoa ajankohtaisista kyberrikosilmiöistä, ja tiedon avulla voidaan ennaltaehkäistä tulevia rikoksia. Varautuminen tietoverkkorikoksiin auttaa merkittävästi tapahtumien selvittämistä, esim. ajantasaiset kuvaukset tietojärjestelmästä helpottavat poliisin tutkintatyötä. Poliisiin tulee olla yhteydessä mahdollisimman aikaisessa vaiheessa, jotta tietoverkkorikoksen todistusaineisto saadaan turvattua ja tarvittaessa aloitettua kansainvälinen yhteistyö. (Kyberrikosten tutkinta 2022.)

**Lue lisää poliisin sivuilta:**

- Rikosilmoituksen tekemisestä https://poliisi.fi/tee-rikosilmoitus
- Kyberrikoksista https://poliisi.fi/kyberrikokset

# Lähteet


10 kohtaa kyberturvallisuuden parantamiseksi matkailualalla. 2021. Matkailun vastuullisuus näkyväksi Keski-Suomessa -hanke. Viitattu 10/2022. https://visitjyvaskyla.fi/professionals/wp-content/uploads/sites/2/2021/09/10-kohtaa-kyberturvallisuuden-parantamiseksi-matkailualalla.pdf

Aalto-Setälä, M., & Viitala, M. 2018. Tietosuoja pähkinänkuoressa—Tietosuojaopas yrityksille. Keskuskauppakamari. Viitattu 10/2022. https://kauppakamari.fi/wp-content/uploads/2020/05/tietosuoja-pahkinankuoressa.-tietosuojaopas-yrityksille.verkkoversio.pdf

Abrams, L. 2021. Coop supermarket closes 500 stores after Kaseya ransomware attack. BleepingComputer. Viitattu 8/2022. https://www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/

Arviointi, hyväksyntä ja neuvonta. 2022. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 6/2022. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/arviointi-hyvaksynta-ja-neuvonta

Davis, A. 2015. Building Cyber-Resilience into Supply Chains. Viitattu 10/2022. https://timreview.ca/article/887

Elliott, J. 2021. What is the 3-2-1 Backup Rule? Viitattu 9/2022. Https://Www.Uschamber.Com/Co. https://www.uschamber.com/co/co/run/technology/3-2-1-backup-rule

Havainnointi ja avunanto. 2022. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 6/2022. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto

Henriksson, A. & Karhu, M. 2002. Kriisit ja viestintä. Inforviestintä Oy.

Huoltovarmuuskeskus. 2022. Viitattu 6/2022. https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio/huoltovarmuuskeskus

Ilkka, J., Sahlman, A., Mäntylä, H., Hartikainen, J., Janhunen, K., Grönroos, K., Raappana, M., Kinnunen, P.,Heikkinen, P., Niinikorpi, S., Lehtinen, T., Törmälä, J. & Pajunen, K. 2017. Tietoturvapoikkeamatilanteiden hallinta. Valtiovarainministeriö, VAHTI. Viitattu 8/2022. https://www.suomidigi.fi/sites/default/files/2020-06/VM_8_2017.pdf

Juholin, E. 2001. Communicare! Viestintä strategiasta käytäntöön. Inforviestintä Oy.

Katakri – tietoturvallisuuden auditointityökalu viranomaisille. 2020. Kansallinen turvallisuusviranomainen NSA. Viitattu 10/2022. https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

Kohti toimintavarmaa myymäläverkkoa—Varmuuden Vuoksi. 2021. Huoltovarmuuskeskus. Viitattu 9/2022. https://www.varmuudenvuoksi.fi/artikkeli/kohti-toimintavarmaa-myymalaverkkoa

Kyberhäiriötilanteet – Varautuminen ja toiminta. 2019. Huoltovarmuuskeskus. Viitattu 10/2022. https://ficom.fi/wp-content/uploads/2021/03/HVK_ohjeet-ja-lainsaadanto-kyberhairiotilanteessa_2019_978-952-5608-73-1_.pdf

Kybermittarin uusi versio saatavilla. 2022. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 10/2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybermittarin-uusi-versio-saatavilla-syksyn-koulutukset-kaynnistyvat-viikolla-41

Kyberrikosten tutkinta. 2022. Poliisi. Viitattu 6/2022. https://poliisi.fi/kyberrikosten-tutkinta

Kyberturva ICT-sopimuksissa. 2021. Huoltovarmuuskeskus. Viitattu 10/2022. https://www.huoltovarmuuskeskus.fi/files/c9bab5825e7d15ba2062e5f47e485e5d02d63c45/kyberturva-ict-sopimuksissa.pdf

Kyberturvallisuuden nykytila eri toimialoilla. 2020. Huoltovarmuuskeskus. Viitattu 8/2022. https://www.huoltovarmuuskeskus.fi/files/b3671ecb5d0b5b431174fec9350e0251b75227ba/kyberturvallisuuden-nykytila-eri-toimialoilla2-verkkosivuille.pdf

Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa - Ohje johdolle ja asiantunti-joille. 2022. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 10/2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Kyberturvallisuuden_vahvistaminen_suomalaisissa_organisaatiossa_-_ohje_johdolle_ja_asiantuntijoille.pdf

Mikä on ruokavirasto? 2022. Ruokavirasto. Viitattu 9/2022. https://www.ruokavirasto.fi/tietoa-meista/mika-on-ruokavirasto/

Muona, P. 2021. Haavoittuvuuksien havaitseminen pienten ja keskisuurien yritysten verkossa. JAMK, opinnäytetyö. Viitattu 10/2022. https://www.theseus.fi/bitstream/handle/10024/509673/Opinnaytetyo_Muona_Severi.pdf

Nyman, A. 2021. Monimutkaiset toimitusketjut lisäävät kyberriskejä. Viitattu 10/2022. https://kehittyvaelintarvike.fi/artikkelit/teemajutut/digitalisaatio-robotiikka/monimutkaiset-toimitusketjut-lisaavat-kyberriskeja/

Onko organisaatiosi suojautunut toimitusketjuhyökkäykseltä? 2021. Suojelupoliisi. Viitattu 10/2022. https://supo.fi/-/kolumni-onko-organisaatiosi-suojautunut-toimitusketjuhyokkaykselta-nailla-vinkeilla-paaset-alkuun

Pidempi parempi – Näin teet hyvän salasanan. 2022. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 10/2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan

Pienyritysten kyberturvallisuusopas. 2020. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 9/2022. https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pienyritysten-kyberturvallisuusopas

Pöyhönen, J. 2020. Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa – Systeemiajattelu. Jyväskylän Yliopisto, väitöskirja. Viitattu 8/2022. https://jyx.jyu.fi/handle/123456789/71395

Sektorit ja poolit. 2022. Huoltovarmuuskeskus. Viitattu 6/2022. https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio/sektorit-ja-poolit

Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta. 2019. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 10/2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Suojautuminen%20Microsoft%20Office%20365%20-tunnusten%20kalastelulta%20ja%20tietomurroilta%20web.pdf

Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta. 2020. Valtiovarainministeriö. Viitattu 10/2022. https://julkaisut.valtioneuvosto.fi/handle/10024/162433

Target Hackers Broke in Via HVAC Company. 2014. Viitattu 10/2022. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company

TIETO22. 2021. Digipooli. Viitattu 10/2022. https://www.digipooli.fi/fi/tieto22

Tietosuojaperiaatteet. N.d. Tietosuojavaltuutetun toimisto. Viitattu 10/2022. https://tietosuoja.fi/tietosuojaperiaatteet

Tilannekuva ja verkostot. 2022. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 6/2022. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot

Verkkohyökkäys lukitsi autotarvikeliikkeen kassat, salasi tiedot ja sulki ovet – Tiedätkö miten varautua, sillä voit olla rikollisen seuraava kohde? 2020. Yle Uutiset. Viitattu 9/2022. https://yle.fi/uutiset/3-11456333

Vertainen V., Suni E., Vatanen M., Hautamäki J., Laava T., & Piispanen J. 2021. Kyberhäiriöiden hallinta—Käsikirja terveydenhuollon toimijoille. Jyväskylän ammattikorkeakoulu, IT-instituutti, JYVSECTEC. Viitattu 10/2022. https://jyvsectec.fi/wp-content/uploads/2020/12/kyberhairioiden-hallinta-kasikirja-terveydenhuollon-toimijoille.pdf

Yrityksiin kohdistuvat kyberuhat 2019. 2019. Helsingin seudun kauppakamari. Viitattu 10/2022. https://rihykauppakamari.fi/files/yrityksiin-kohdistuvat-kyberuhat-2019.pdf

# Sanasto

**Elintarvikearvoketju**
Ketju, jossa elintarvike vaiheittain jalostuu raaka-aineesta valmiiksi tuotteeksi.

**ICS-järjestelmä**

Teollisuuden ohjausjärjestelmä.

**IDS-järjestelmä**

Tunkeutumisenhavaitsemisjärjestelmä eli tekninen järjestelmä, jonka tarkoitus on havaita järjestelmiin tunkeutumiset ja niiden yritykset. IDS tulee englannin kielen sanoista Intrusion Detection System.

**ISMS (Information Security Management System)**

Tietoturvallisuuden hallintajärjestelmä.

**Kriittinen tieto**

Kaikki tieto ei ole yhtä arvokasta. Kriittinen tieto on sellaista, jonka häviäminen, vääristyminen tai käytön estäminen vaikuttaa vakavasti tai merkittävästi organisaation toimintaan. Kriittinen tieto on suojattava tietoturva- ja kyberuhkia vastaan.

**Kyberpoikkeama/kyberhäiriö**

Tietojen ja palvelujen tietoturvan vaarantava ja organisaation toimintaan epäsuotuisasti vaikuttava ei-toivottu tai odottamaton toteutunut kyberuhka (tai useampia toisiinsa liittyviä kyberuhkia).

**Kyberresilienssi**

Yksilöiden ja yhteisöjen kyky ylläpitää toimintakykyä muuttuvissa olosuhteissa sekä valmius kohdata häiriöitä ja kriisejä ja palautua niistä.

**Kybertoimintaympäristö**
Sähkö- ja tietoverkosta riippuvainen ympäristö.

**Kyberturvallisuus**

Tavoitetila, jossa digitaalisista tietojärjestelmistä muodostuvaan toimintaympäristöön (kybertoimintaympäristö) voidaan luottaa. Laajemmin myös pyrkimys sähköisen ja verkotetun yhteiskunnan turvallisuuteen.

**Kyberuhka**

Digitaalisista tietojärjestelmistä muodostuvaan toimintaympäristöön (kybertoimintaympäristö) kohdistuva mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku. Toteutuessaan vaarantaa toimintaympäristön. Kyberuhat voivat aiheutua toteutuneista tietoturvauhkista tai digitaalisessa viestintäympäristössä toteutettavista teoista.

**NCSA**

National Communications Security Authority, kansallinen tietoturvaviranomainen.

**POC (Point Of Contact)**

Yhteyspiste tarkoittaa henkilöä tai yrityksen osastoa, joka toimii kyseistä toimintaa koskevien tietojen koordinaattorina tai yhteyspisteenä.

**SLA (Service Level Agreement)**

Palvelutasosopimus (palveluntarjoajan ja asiakkaan välinen sopimus, jossa määritellään palvelulle tietyt vaatimustasot).

**Tietosuoja**

Henkilötietojen asianmukaista käsittelyä ja niiden yksityisyyden säilymistä varmistavat järjestelyt.

**Tietoturvallisuus**

Tiedon saatavuuteen, eheyteen ja luottamuksellisuuteen tähtäävä järjestely. Esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus, varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö.

**Tietoturvauhka**

Tietoturvallisuuteen kohdistuva mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku. Toteutuessaan vaarantaa tietoturvan.

*Käsikirjan sanasto on koottu hyödyntäen Sanastokeskuksen kyberturvallisuuden sanastoa ja TEPA-termipankkia.*

# Kirjoittajat

**Vesa Vertainen, asiantuntija**

Toimin Kyberpoikkeamanhallinnan prosessit ja toimintaohjeet elintarviketuotannossa ja -jakelussa -projektissa asiantuntijana. Koulutukseltani olen tieto- ja viestintätekniikan insinööri AMK sekä automaatioteknikko. Työskentelen Jamkin IT-instituutissa kyberturvallisuuden, data-analytiikan ja tekoälyn TKI-projekteissa asiantuntijana.

**Reijo Lähteenmäki, asiakkuuspäällikkö**

Toimin Kyberpoikkeamanhallinnan prosessit ja toimintaohjeet elintarviketuotannossa ja -jakelussa -projektissa asiantuntijana. Koulutukseltani olen filosofian maisteri (FM), tietoliikenneteknikko ja RTV-asentaja. Työskentelen Jamkin IT-instituutissa asiakkuuspäällikkönä. Tehtäviini kuuluu JYVSECTEC:in asiakasrajapinnassa toimiminen sekä kansallisten kyberharjoitusten kehittämis- ja suunnittelutehtävät. Aikaisemmin olen työskennellyt puolustusvoimissa useissa kyberturvallisuuteen liittyvissä tehtävissä.

**Sampo Kotikoski, lehtori**

Toimin Kyberpoikkeamanhallinnan prosessit ja toimintaohjeet elintarviketuotannossa ja -jakelussa -projektissa asiantuntijana. Koulutukseltani olen filosofian lisensiaatti (FL) ja diplomi-insinööri (DI). Työskentelen Jamkin IT-instituutissa lehtorina. Erityisosaamistani ovat mm. IT-palveluiden hallinta, tietoturvastandardit, konesalit, algoritmit ja tietorakenteet sekä tietoverkkotekniikka ja -protokollat.

**Paavo Nelimarkka, asiantuntija**

Toimin Kyberpoikkeamanhallinnan prosessit ja toimintaohjeet elintarviketuotannossa ja -jakelussa -projektissa asiantuntijana. Koulutukseltani olen tieto- ja viestintätekniikan insinööri AMK, jonka lisäksi minulla on insinööri YAMK tutkinnon opinnot loppusuoralla. Työskentelen Jamkin IT-instituutissa ohjelmistokehityksen tehtävien parissa sekä opetan tieto- ja viestintätekniikan insinööriopiskelijoita.

**Jaana Brandt, projektipäällikkö**

Toimin Kyberpoikkeamanhallinnan prosessit ja toimintaohjeet elintarviketuotannossa ja -jakelussa -projektissa asiantuntijana. Koulutukseltani olen Filosofian Maisteri (FM). Työskentelen Jamkin IT-instituutissa projektipäällikkönä TKI-projekteissa, tällä hetkellä Huoltovarmuuskriittisten toimijoiden kyberturvallisuusharjoitustoiminnan kehittäminen -projektissa. Aikaisemmin olen työskennellyt mm. viestinnän toimialapäällikkönä sekä viestinnän asiantuntijana.

**Elina Suni, projektipäällikkö**

Toimin Kyberpoikkeamanhallinnan prosessit ja toimintaohjeet elintarviketuotannossa ja -jakelussa -projektissa projektipäällikkönä. Koulutukseltani olen tieto- ja viestintätekniikan insinööri AMK sekä tradenomi AMK ja YAMK. Työskentelen Jamkin IT-instituutissa projektipäällikkönä TKI-projekteissa. Tämän projektin lisäksi toimin tällä hetkellä projektipäällikkönä Elintarvikeketjun kyberturvallisuus -hankkeessa sekä Jamkin edustajana Robocoast EDIH-konsortiossa.

# Kyberturvallisuus kaupan ja jakelun alalla -käsikirja kyberpoikkeamien hallintaan

Jyväskylän ammattikorkeakoulun Elintarviketuotannon
ja -jakelun kyberpoikkeamanhallinnan julkaisut, osa 3/3

**Ulkoasu: Jamk / Heli Sutinen**
**Kuvittaminen: Jamk / Heli Sutinen ja Suvi Sormunen**

ISBN 978-951-830-680-4 (PDF)

**Jakelu**
Jyväskylän ammattikorkeakoulun IT-instituutti,
JYVSECTEC – Jyväskylä Security Technology
Piippukatu 2, 40100 Jyväskylä

www.jyvsectec.fi



jamk | Jyväskylän ammattikorkeakoulu

Maa- ja metsätalous-
ministeriö