Kyberturvallisuus elintarviketeollisuudessa

-käsikirja kyberpoikkeamien hallintaan

ELINA SUNI (TOIM.)

Jyväskylän ammattikorkeakoulun Elintarviketuotannon ja -jakelun kyberpoikkeamanhallinnan julkaisut, osa 2/3

jamk | Jyväskylän ammattikorkeakoulu

Maa- ja metsätalous-ministeriö

Sisältö

Tekijät:

Paavo Nelimarkka
Jyväskylän ammattikorkeakoulu

Sampo Kotikoski
Jyväskylän ammattikorkeakoulu

Jaana Brandt
Jyväskylän ammattikorkeakoulu

Elina Suni
Jyväskylän ammattikorkeakoulu

Kustantaja: Jyväskylän ammattikorkeakoulu

ISBN 978-951-830-679-8 (PDF)

Jyväskylä 2023

1 Johdanto

Elina Suni

Tämän käsikirjan päätavoitteena on tuottaa elintarviketeollisuuden yrityksille kyberpoikkeamatilanteissa tarvittavia toimintaohjeita. Kohderyhmänä ovat kaikki elintarviketeollisuuden alalla työskentelevät, mutta erityisesti erikokoisten elintarviketeollisuusyritysten kyberturvallisuuden johtamisesta sekä teknisestä ja hallinnollisesta toteutuksesta vastaavat henkilöt. Käsikirjan tarkoituksena on varmistaa yhteiskunnan kannalta kriittisten elintarviketeollisuuden 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 elintarviketeollisuus 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 kaupan ja jakelun alalla –käsikirja kyberpoikkeamien hallintaan (Elintarviketuotannon ja -jakelun kyberpoikkeamanhallinnan julkaisut Jamk, osa 3/3)

Projektin on rahoittanut maa- ja metsätalousministeriö ja sen on 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. Julkaisu tuottaa uutta tietoa kyberpoikkeamanhallintaan elintarviketeollisuuden toimijoille.

Luku 2

Kyberturvallisuus elintarviketeollisuudessa

Luvussa kaksi kerrotaan yleisesti kyberturvallisuudesta painottaen elintarviketeollisuuden näkökulmaa. Lisäksi käydään läpi ajankohtaisia alaan kohdistuneita kyberhyökkäyksiä maailmalta, sekä paneudutaan suurimpiin teknisiin haavoittuvuuksiin ja niiltä suojautumiseen elintarviketeollisuuden kyberturvallisuuden näkökulmasta.

2 Kyberturvallisuus elintarviketeollisuudessa

Paavo Nelimarkka

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.

Miksi kyberturvallisuus on tärkeää?

Kyberuhkien toteutuessa seuraukset voivat olla laajat ja kriittiset yhteiskunnalle, yrityksille ja ihan yksilöllekin. Digitalisaation mukanaan tuoma automaatioteknologia ja esimerkiksi tietoverkkoon kytketyt IoT-laitteet (Internet of Things) lisäävät tuottavuutta, mutta tuovat mukanaan uhkia ja mahdollisia haavoittuvuuksia. Internetiin ja toisiinsa yhteydessä olevien laitteiden aiheuttamat riskit tulisi osata ottaa huomioon jo järjestelmien ja laitteiden hankintavaiheessa.

Kyberturvallisuuden voidaan katsoa rakentuvan kolmen perus-pilarin varaan: ihmiset, prosessit ja teknologia. Ihmiset, esimerkiksi yrityksen henkilökunta, koulutetaan ylläpitämään kyberturvaa ja toimeenpanemaan turvallisuutta lisääviä prosesseja ja käytänteitä. Kyberturvallisuus vaatii jatkuvaa perehtymistä, dokumentointia ja prosessien uudistamista. Kolmas perus-pilari on teknologia, jolla voidaan suojautua kyberuhkia vastaan. Huonosti suunniteltu ja toteutettu tekninen ratkaisu voi kuitenkin aiheuttaa tietoturvauhkan tai sisältää haavoittuvuuksia.

Henkilötunnuksen joutuminen vääriin käsiin voi johtaa identiteettivarkauteen eli tilanteeseen, jossa rikollinen esiintyy toisen ihmisen henkilöllisyydellä. Rikollinen voi esimerkiksi tehdä osamaksukaupan, tilata lehden

varastettua identiteettiä käyttämällä tai aiheuttaa haittaa esiintymällä sosiaalisessa mediassa uhrin nimellä. (Identiteettivarkaudessa esiinnytään toisen henkilöllisyydellä 2019.) Yritykseen kohdistuneen kyberhyökkäyksen kautta esimerkiksi asiakkaiden tietoja voisi joutua vääriin käsiin. Tämä aiheuttaisi muun muassa suurta mainehaittaa yritykselle sekä taloudellisia seurauksia asian selvittämisen ja mahdollisten korvausten muodossa.

Kyberturvallisuus on tärkeää yrityksen toiminnan jatkuvuuden näkökulmasta. Mikäli kyberhyökkäyksellä onnistutaan aiheuttamaan häiriötä tuotantoon, tästä koituu välittömiä taloudellisia seurauksia. Kyberrikollinen voi myös myydä kaapattuja tietoja esimerkiksi teollisuusvakoilun käyttöön. Tietomurrosta seuraa usein myös mainehaittaa, joka näkyy epäsuorasti taloudellisena haittana pitkällä aikavälillä.

Elintarviketeollisuusyritysten kyberturvallisuudella on tärkeä rooli myös kansallisen huoltovarmuuden näkökulmasta. Mikäli suureen elintarviketeollisuusyritykseen kohdistuisi laaja kyberhyökkäys, jonka seurauksena tuotanto olisi pitkiä aikoja pysähdyksissä, voisi se pahimmillaan horjuttaa tiettyjen peruselintarvikkeiden saatavuutta.

Ruoka-aineet ovat herkkiä lämpötilan vaihteluille: joillekin ruoka-aineille riittävä kuumennus on tärkeää ja joillekin taas kylmäketjun katkeamattomuus. Mikäli kyberhyökkäyksellä onnistuttaisiin vaikuttamaan kylmäketjuun tai ruoan kuumennusprosessiin niin, että pilaantunut ruoka-aine päätyisi kuluttajalle asti, seuraukset voisivat olla todella ikäviä. Tuotanto-erän hävitys, tuotteiden takaisinveto ja mahdolliset korvaukset aiheuttaisivat merkittävää taloudellista haittaa.

Tuotantotiloissa työskentelevien tulee saada koulutusta kyberturvallisuusasioissa.

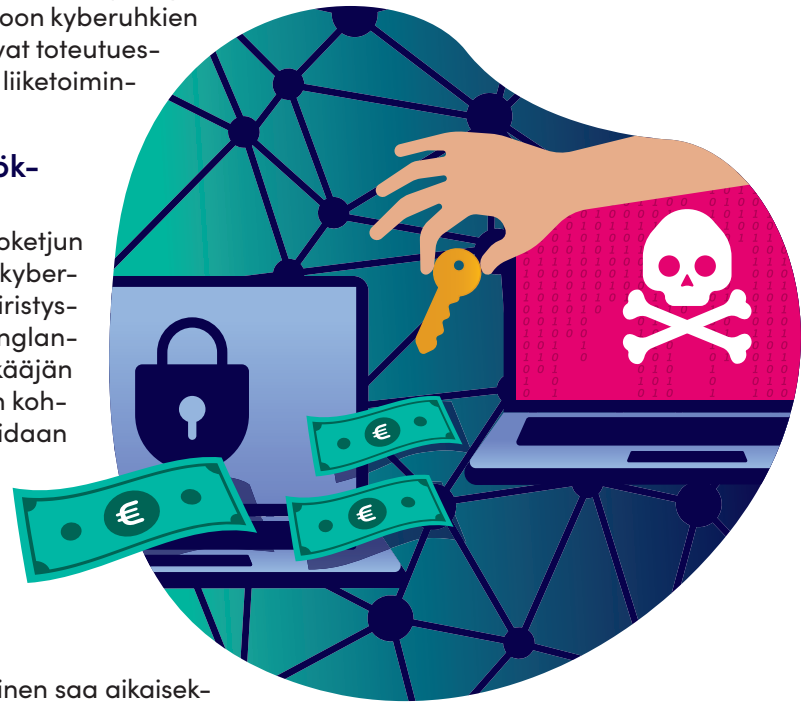
Henkilöstön huolimattomuus tai heikko kulunvalvonnan prosessi voi myös välillisesti johtaa kyberhyökkäykseen. On esimerkiksi tärkeää, että tuotantotiloihin pääsevät vain ne työntekijät, joiden työtehtävien kannalta pääsy on välttämätöntä. Tuotantotiloissa työskentelevien tulee myös saada koulutusta kyberturvallisuusasioissa. Paperilapulle kirjoitettu salasana, lattialta löytynyt tunnistamaton muistitikku tai kulkurajoitettuun tilaan pyrkivä vierailija voivat myös aiheuttaa kyberuhan. Kyberturvallisuus muodostuu teknologisten ratkaisujen ja järjestelmien turvallisuuden lisäksi prosesseista, toimintatavoista ja käytänteistä.

Lue lisää:

Kyberturvallisuuden perusteista ja organisaation hallituksen vastuista (pdf)

Elintarviketeollisuuden kyberuhkia

Pilvipalveluita hyödynnettäessä tuotantoon liittyvä tieto voi levittyä maantieteellisesti laajalle alueelle. Tietoverkosta eristetty järjestelmäkään ei ole vailla haavoittuvuuksia. Vaikka laite olisi tietoverkosta eristetyssä omassa aliverkossaan, se voi silti joutua kyberhyökkäyksen kohteeksi esimerkiksi päivityksiä asennettaessa. Palveluita ulkoistettaessa tulee myös muistaa vastuiden määritys, jotta tiedetään miten toimia ja kuka on vastuussa, jos palveluna ulkopuolelta ostettuun järjestelmään kohdistuisi hyökkäys. Nämä ovat esimerkkejä tilanteista ja tapahtumista, jotka tulee ottaa huomioon kyberuhkien näkökulmasta. Kyberuhat voivat toteutuessaan vaikuttaa pahimmillaan liiketoiminnan jatkuvuuteen.



Kiristyshaittaohjelmahyökkäykset

Viimeaikaiset elintarvikearvoketjun toimijoihin kohdistuneet isot kyberhyökkäykset ovat liittyneet kiristyshaittaohjelmien käyttöön (englanniksi ransomware). Hyökkääjän tavoite on päästä kiristämään kohteelta lunnaita. Lunnaita voidaan vaatia salattujen tietojen palauttamista varten, mutta rikolliset saattavat myös varastaa salattuja tietoja ja kiristää yritystä tietovuodon uhalla.

Mitä suuremman haitan rikollinen saa aikaiseksi kohteelleen, sitä suurempia lunnasrahoja voidaan vaatia. Todennäköisyydet lunnaiden maksuun kasvavat myös haitan ollessa merkittävämpi (lunnaiden maksu ei kuitenkaan ole ratkaisu, sillä kiristäminen voi maksusta huolimatta jatkua). Kiristyshaittaohjelmahyökkäyksessä rikollinen voi pyrkiä esimerkiksi lamauttamaan operatiivista toimintaa tai kaappaamaan kriittistä tietoa.

Maailman suurin lihan prosessointiin keskittynyt yritys JBS joutui valtavan kiristyksen kohteeksi kesäkuussa 2021. Kyberrikolliset onnistuivat ottamaan haltuun yrityksen tietojärjestelmiä ja uhkasivat häiritä sekä poistaa tietoa, mikäli lunnaita ei makseta. (Meat giant JBS pays $11m in ransom to resolve cyber-attack 2021.) JFC Internationalin, suuren aasialaisen elintarvikkeiden tukkumyyjän ja jakelijan Euroopan konserni joutui myös kiristyshaittaohjelman kohteeksi keväällä 2021. Yritys onnistui kuitenkin ylläpitämään tuotantoa. Haittaohjelma häiritsi lyhyen aikaa yhtiön IT-järjestelmiä Euroopassa. (Paganini 2021.)

Yhdysvaltojen liittovaltion poliisi on varoittanut maatalousalan toimijoita kiristyshaittaohjelmahyökkäyksistä erityisesti tuotannon kannalta kriittisinä ajankohtina. Alku-

tuotannon lamaannuttaminen kylvön tai sadonkorjuun aikana aiheuttaisi merkittäviä taloudellisia tappioita sekä häiritsisi koko toimialaa ja arvoketjua. (Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons 2022.)

Kiristyshaittaohjelmilta voi suojautua esimerkiksi tekemällä varmuuskopioita tärkeästä datasta, pitämällä ohjelmistopäivitykset ajan tasalla ja suhtautumalla varauksella sähköpostitse jaettuihin linkkeihin. (Mikä on ransomware? 2022.) Kiristyshaittaohjelmahyökkäyksen kohteen ei tule maksaa lunnaita. Ei ole mitään takeita siitä, että järjestelmät tai tiedot palautettaisiin vastineeksi lunnaiden maksusta. Hyökkäyksestä kannattaa aina ilmoittaa viranomaisille. (Toiminta kiristyshaittaohjelmatilanteessa - johdon ohje 2022, 2.)

Esimerkki kiristyshaittaohjelmahyökkäyksestä:

Huijaussähköposti
Kiristyshaittaohjelmat leviävät usein sähköpostiviestien välityksellä. Ne voivat olla naamioituina sähköpostin liitteiksi tai linkin takana.

Haittaohjelman lataus
Viestissä olleen linkin painaminen johtaa siihen, että käyttäjä tietämättään lataa tietokoneelleen haitallisen ohjelman.

Haittaohjelman leviäminen
Haittaohjelma hyödyntää laitteistoissa ja ohjelmistoissa olevia haavoittuvuuksia leviten laitteelta toiselle.

Tietojen salaus
Haittaohjelma salaa tiedot ja rikollinen vaatii lunnaita tietojen palauttamista vastaan. Organisaatio on nyt joutunut kyberrikoksen kohteeksi.

Ohjeita kiristyshaittaohjelmien varalle:

- FBI on julkaissut yksityiskohtaisen ohjeistuksen kiristyshaittaohjelmien varalle elintarviketuotannossa. FBI:n ohjeen voit lukea täältä (pdf).
- Liikenne- ja viestintäministeriö Traficomin Kyberturvallisuuskeskus on julkaissut (2022) toimintaohjeen yrityksille, jotka epäilevät joutuneensa kiristyshaittaohjelman uhriksi. Kyberturvallisuuskeskuksen ohjeen voit lukea täältä (pdf).

Teollisuuden ohjausjärjestelmien (ICS) haavoittuvuudet

Automaatiolaitteiden ja teollisuusrobottien toimintaa ohjaavat ohjausjärjestelmät ja laitteistot (ICS eli Industrial Control Systems) ovat erityisen alttiita haavoittuvuuksille elintarviketeollisuudessa, joten niiden haavoittuvuudet tulisi ymmärtää hyvin. Käytössä on vielä paljon ICS-järjestelmiä ja laitteita, jotka on suunniteltu ennen kuin kyberrikollisuutta pidettiin uhkana, eikä niille ole saatavissa ohjelmistopäivityksiä. ICS-ympäristöt käyttävät usein myös vanhentuneita protokollia, joissa käyttäjää ei millään lailla tunnisteta; tällöin kuka tahansa samaan verkkoon päässyt pystyy antamaan käskyjä laitteelle. Teolliset ohjausjärjestelmät ovat kalliita, eikä niiden uusiminen turvallisempiin ole aina helppoa. Lisäksi ne ovat olennaisessa osassa toteuttamassa kriittisiä tuotannon prosesseja ja käsittelevät tärkeää tietoa. (Adulterating More Than Food: The Cyber Risk to Food Processing and Manufacturing 2019.)

Yhdysvaltojen Kyberturvallisuuskeskus (NCCIC eli National Cybersecurity and Communications Integration Center) listaa seitsemän tapaa lujittaa ICS-ympäristöjä kyberhyökkäyksiä vastaan:

1. **Allowlisting eli sallittujen ohjelmien, toimintojen ja käyttäjien luettelointi**

   Tällä tekniikalla voidaan rajata esimerkiksi laitteen eri toimintoja pois käytöstä tai rajoittaa niitä vain huoltohenkilökunnan käytettäviksi. Allowlisting-tekniikan lähtökohtana on, että kaikki on kiellettyä ja käytön kannalta tarpeelliset toiminnot sallitaan yksitellen. Kyberrikollisen päästessä käsiksi laitteeseen rikollinen ei välttämättä kuitenkaan pysty käyttämään haitallisia toimintoja laitteella. Toiminnasta jää kuitenkin merkintä lokitiedostoon.

2. **Konfiguraatioiden ja päivitysten järjestelmällinen lataus ja asennus**

   Erityisesti työpisteiden PC-laitteistojen päivitysten systemaattinen lataus ja asennus on tärkeää, sillä esimerkiksi kannettavat tietokoneet ovat merkittävä uhka ICS-ympäristössä. Riittämättömästi suojattujen laitteiden käyttö on syytä estää ICS-ympäristössä. Myös päivitysten latauksessa tulee huomioida, että ne ladataan suoraan valmistajalta ja päivitystiedostot ovat digitaalisesti allekirjoitettuja.

3. **Verkkojen segmentointi ja ICS-ympäristöjen eristäminen**

   On varmistettava, ettei ICS-järjestelmä ole liitoksissa sellaiseen tietoverkkoon mihin sen ei kuuluisi olla liitoksissa ja ettei laitteessa ole päällä käyttämättömiä palveluita. Jos toiseen tietoverkkoon tarvitsee lähettää tietoa vain yksisuuntaisesti, on syytä harkita ”datadiodi”-laitetta varmistamaan tietoväylän yksisuuntaisuus. Erityisesti on vältettävä julkiseen Internetiin pääsyä.

4. **Tietoverkkojen segmentointi**

   Segmentoimalla tietoverkot voidaan rajata mahdollinen kyberhyökkäys vain yhdelle verkkosegmentille. Näin toimimalla voidaan yrittää minimoida hyökkäyksestä aiheutuvat kustannukset ja haitat.

5. **Käyttäjän tunnistaminen**

   Mikäli kyberrikollinen kaappaisi käyttäjätilin, jolle on annettu laajat valtuudet, pystyisi rikollinen toimimaan ympäristössä liki näkymättömästi. Tästä syystä on suositeltavaa antaa käyttäjälle vain työn kannalta oleelliset oikeudet ja toiminnallisuudet, rajata kaikki muu pois. On myös syytä ottaa käyttöön kaksivaiheinen tunnistus, mikäli se on mahdollista. Lisäksi tuotantoverkkoon tulee olla eri tunnukset kuin esimerkiksi yrityksen liiketoiminnan intra-verkkoon. Käyttäjiltä tulee vaatia vahvoja salasanoja sekä niiden uusimista tasaisin väliajoin.

6. **Liiketoiminnan kannalta välttämättömien etäyhteyksien toiminnallisuuksien rajoittaminen**

   Mikäli ICS-järjestelmästä tarvitaan yksisuuntainen liikenne ulospäin toiseen verkkoon (esimerkiksi monitorointia varten), tulee käyttää ”datadiodeja” eikä luottaa ohjelmistojen ”read-only” toimintoihin.

7. **Tietoliikenteen ja lokitiedostojen monitorointi**

   Tulee pitää silmällä IP-osoitteita ICS-laitteiden rajapinnoilla sekä kyseisessä verkossa, kirjautumistietoja ja käyttäjätunnusten asetusmuutoksia. Tulee suunnitella ennakkoon prosessi poikkeamanhallintaan, missä esimerkiksi tietoverkot ajetaan väliaikaisesti alas, jos havaitaan kriittinen poikkeama.

(Seven Steps to Effectively Defend Industrial Control Systems n.d.)

SCADA-järjestelmien haavoittuvuudet

Ihmisen ja koneen välisiä käyttöliittymiä kutsutaan englannin kielellä nimellä Human Machine Interface (HMI) ja niissä suoritettavia valvontaohjelmistoja nimellä Supervisory Control and Data Acquisition (SCADA). (Hacker Machine Interface - The State of SCADA HMI Vulnerabilities 2017). SCADA-järjestelmät ovat teollisuudessa käytettäviä ohjelmistoista ja laitteista syntyviä kokonaisuuksia. Niillä esimerkiksi hallitaan, monitoroidaan ja prosessoidaan tietoa. Järjestelmillä voidaan myös hallita esimerkiksi sensoreita ja automaatiolaitteita logiikkaohjainten ja automaatiosäätimien avulla. Kokonaisuuteen kuuluukin usein myös sensoreita, joista tuleva tieto ohjataan ohjelmistolle logiikkaohjainten välityksellä. (What is SCADA? 2018). SCADA-ohjelmistoissa saattaa olla puutteita kyberturvallisuuden näkökulmasta. Myös standardoinnissa voi olla puutteita, ja siksi SCADA-ohjelmistot olisi hyvä pitää joko täysin eristettynä muista tietoverkoista tai liittää ne ainoastaan turvallisiin verkkoihin (mikäli liittäminen muihin verkkoihin on toiminnan kannalta ehdotonta).

ICS-ympäristöjen selkein hyökkäyskohde on SCADA-järjestelmien käyttöliittymärajapinnat (HMI). Koska SCADA-järjestelmien HMI-rajapinnat ovat alttiita haavoittuvuuksille, ohjelmistojen turvallisuuteen tulisi kiinnittää erityistä huomiota. Tutkijat ovat tunnistaneet useita haavoittuvuuksia näistä ohjelmistoista ja vaikka tutkijat tai käyttäjät raportoivat tietoturvaongelmasta valmistajalle, voi tietoturvapäivityksen julkaisuun mennä pitkäkin aika, jolloin ohjelmisto on alttiina hyökkäyksille. (Hacker Machine Interface - The State of SCADA HMI Vulnerabilities 2017, 3.)

Tyypillisesti HMI-käyttöliittymäohjelmistojen haavoittuvuudet johtuvat virheistä muistinkäsittelyssä, huonosta oikeuksien hallinnasta, puutteellisesta käyttäjän tunnistamisesta/ käyttövaltuuksien antamisesta tai mahdollisuudesta injektoida omaa ohjelmistokoodia sovelluksen ajossa. Huonossa oikeuksienhallinnassa korostuvat esimerkiksi niin sanotut tehdasmääritellyt salasanat tai salasanojen talletus turvattomassa formaatissa. Sekä kuluttajien että ammattilaisten käytössä olevista tietoverkkolaitteissa on löytynyt paljon tämänkaltaisia haavoittuvuuksia. Laitteistoa hankkiessa kannattaa myös varmistaa, että laite on todettu turvalliseksi ja siihen on saatavilla tietoturvapäivityksiä jatkossakin. Jos käyttäjän tunnistaminen tai käyttövaltuuksien antaminen on ohjelmistossa huonosti totutettu, voi peruskäyttäjällä olla pääsy arkaluontoiseen tietoon tai vaikka järjestelmän asetuksiin. Tähän liittyy myös tiedon puutteellinen suojaus. Ohjelmistokoodin injektoinnista tyypillisin esimerkki on SQL-injektio. Tällä tekniikalla on mahdollista päästä sisään järjestelmään ohjelmiston tietoturva-aukon kautta. SQL-injektiohyökkäyksessä kyberrikollinen pystyy antamaan tietokannalle käskyjä, joita ohjelmistosuunnittelija ei ole tarkoittanut sille annettavaksi. (Hacker Machine Interface - The State of SCADA HMI Vulnerabilities 2017, 7–20.)

Lue lisää SCADA-ohjelmistojen kyberturvallisuusongelmista englanniksi (pdf).

Lähteet

Adulterating More Than Food: The Cyber Risk to Food Processing and Manufacturing. 2019. Food Protection and Defense Institute (FPDI). Viitattu 6/2022. https://conservancy.umn.edu/bitstream/handle/11299/217703/FPDI-Food-ICS-Cybersecurity-White-Paper.pdf

Hacker Machine Interface - The State of SCADA HMI Vulnerabilities. 2017. Trend Micro. Viitattu 6/2022. https://documents.trendmicro.com/assets/wp/wp-hacker-machine-interface.pdf

Identiteettivarkaudessa esiinnytään toisen henkilöllisyydellä. 2019. Rikosuhripäivystys. Viitattu 9/2022. https://www.riku.fi/erilaisia-rikoksia/identiteettivarkaus-2/

Meat giant JBS pays $11m in ransom to resolve cyber-attack. 2021. BBC. Viitattu 6/2022. https://www.bbc.com/news/business-57423008

Mikä on ransomware?. 2022. F-secure. Viitattu 6/2022. https://www.f-secure.com/fi/home/articles/what-is-a-ransomware-attack

Paganini, P. 2021. Distributor of Asian food JFC International hit by Ransomware. Security Affairs. Viitattu 6/2022. https://securityaffairs.co/wordpress/115150/malware/jfc-international-ransomware-attack.html

Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons. 2022. Yhdysvaltain liittovaltion poliisin tiedote. Viitattu 6/2022. https://www.ic3.gov/Media/News/2022/220420-2.pdf

Seven Steps to Effectively Defend Industrial Control Systems. N.d. NCCIC. Viitattu 7/2022. https://www.cisa.gov/uscert/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

Toiminta kiristyshaittaohjelmatilanteessa - johdon ohje. 2022. Viitattu 6/2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Toiminta%20kiristyshaittaohjelmatilanteessa%20-%20johdon%20ohje.pdf

What is SCADA?. 2018. Inductive Automation. Viitattu 9/2022. https://inductiveautomation.com/resources/article/what-is-scada

Luku 3

Kyberpoikkeamien hallinta elintarviketeollisuudessa

Luvussa kolme käydään läpi kyberpoikkeamiin varautumista, poikkeamatilanteiden hallintaa, kriisi- ja häiriöviestintää sekä olennaiset viranomaisyhteydet kyberpoikkeamatilanteissa.

3 Kyberpoikkeamien hallinta elintarviketeollisuudessa

Paavo Nelimarkka, Sampo Kotikoski, Jaana Brandt, Elina Suni

Kyberpoikkeamiin varautuminen

Riskienhallinta

Elintarviketeollisuuden yrityksissä on tärkeää toteuttaa järjestelmällistä riskienhallintaa. Mikäli riskienhallintaa ei aktiivisesti toteuteta, organisaation on vaikea tunnistaa tavoitteitaan uhkaavia riskejä ja 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 ympäristöön. Määritys pohjautuu yrityksen tietoturvapolitiikassa määriteltyihin asioihin, kuten esimerkiksi tietoturvan laajuuteen ja sen merkitykseen 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 seuraavasti: julkinen, luottamuksellinen ja salainen tieto.

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 eli 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 ovat järjestetty siten, että riskiarvon mukaan luokiteltuna pahin uhka on ylimmäisenä.

Riskiarvotaulukon (Taulukko 1.) riskit sijoitetaan riskimatriisiin (Kuvio 1.) 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**

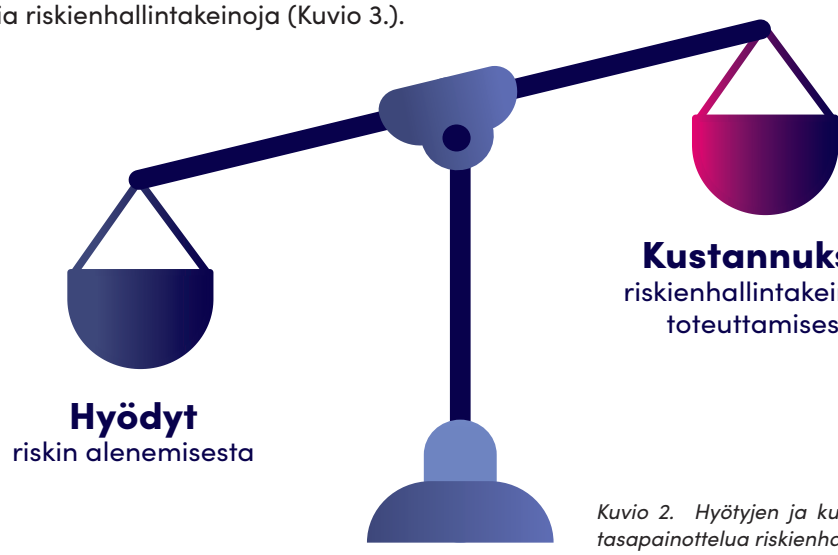
Kuvio 1. Riskimatriisi

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

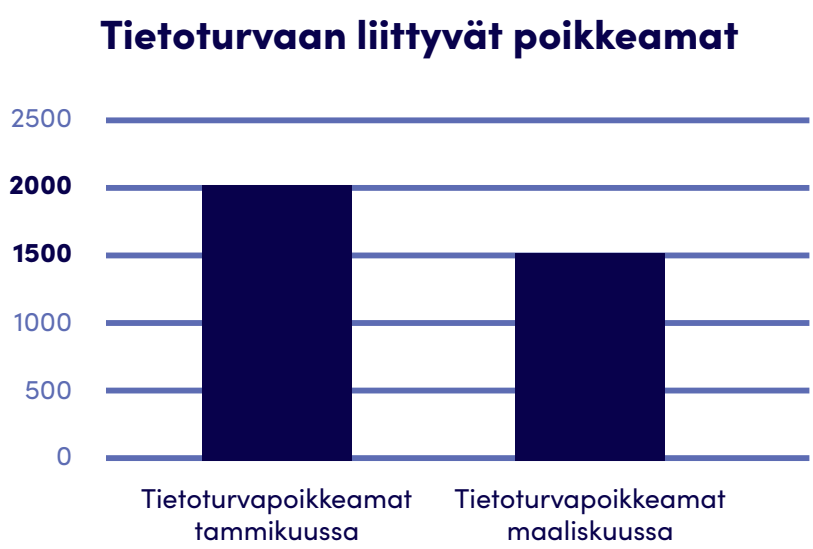
- Suojattavien kohteiden arvo.
- Yksilöidään niihin kohdistuvat uhkat ja olemassa olevat (tai mahdolliset) haavoittuvuudet.
- Yksilöidään käytössä olevat hallintakeinot ja niiden vaikutus tunnistettuihin riskeihin.
- Määritetään mahdolliset seuraukset ja asetetaan näistä tiedoista johdetut riskit tärkeysjärjestykseen 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 2.). Parhaassa tapauksessa tietoturvapoikkeamien määrä laskee, kun käyttöönotetaan erilaisia riskienhallintakeinoja (Kuvio 3.).



Kuvio 2. Hyötyjen ja kustannusten tasapainottelua riskienhallinnassa



Kuvio 3. 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.

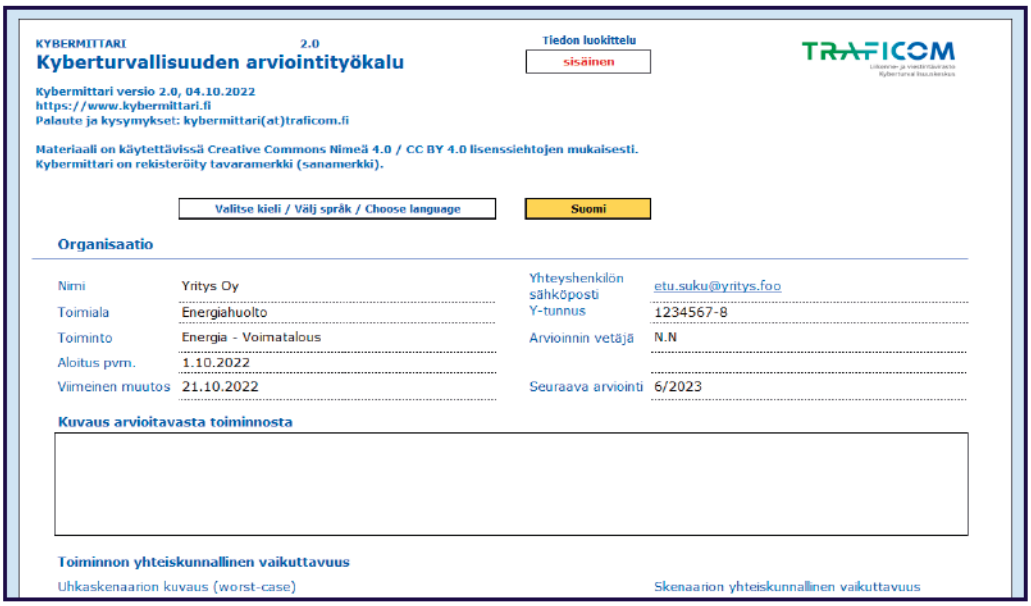
Liiketoiminnan jatkuvuuden hallinta

Riskienhallinta sivuaa myös liiketoiminnan jatkuvuuden hallintaa. Yrityksen johdon tulee keskittyä erityisesti riskeihin, jotka voisivat aiheuttaa liiketoiminnan pysähtymisen väliaikaisesti tai lopullisesti. Esimerkiksi tietomurron seurauksena vuodettu kriittinen (ja arkaluontoinen) tieto voisi aiheuttaa yritykselle niin suuren luottamuspulan asiakkaiden keskuudessa, että sen toiminta jouduttaisiin lakkauttamaan. Esimerkkejä tästä on jo valitettavasti Suomessakin. Toisentyyppinen riski voisi olla ulkoinen luonnonilmiö, esimerkiksi tulipalo tai vesivahinko. (Tietoturvariskien hallinta 2018.) Jatkuvuuden hallinnasta löytyy ohje VAHTI 2/2016 Toiminnan jatkuvuuden hallinta (pdf).

Kyberturvallisuuden kokonaiskuvan kartoitus ja kehittäminen

Organisaatiolla on hyvä olla jonkinlainen tapa arvioida toiminnan ja ympäristön kyberturvallisuutta. Hyvin toteutettu kartoitus auttaa löytämään niinsanottuja kipupisteitä, eli kehityksen kohteita. Tähän on olemassa sekä kansainvälisiä että kansallisia ohjeistuksia.

Suomessa organisaation kokonaiskuvan kartoitukseen on olemassa Kyberturvallisuuskeskuksen kehittämä ja vuonna 2020 julkaisema Kybermittari (Kuva 1.). Kybermittari on suunniteltu kyberturvallisuuden arviointiin ja kehittämiseen organisaatioiden johdolle sekä tietoturva-ammattilaisille. Sen tavoite on edistää, mutta myös yhtenäistää eri organisaatioiden tapaa arvioida kyberturvallisuuttaan ja täten tehdä vertailukelpoisemmaksi niitä keskenään. Mittari on suunniteltu erityisesti huoltovarmuuden kannalta kriittisille yrityksille, mutta se soveltuu myös muillekin yrityksille. (Kybermittari 2022.) Kybermittarin uusin versio julkaistiin lokakuussa 2022, uuden version muutokset löytyvät Kyberturvallisuuskeskuksen sivuilta. Kybermittarin arviointiprosessi on viisivaiheinen ja se perustuu iteroivaan malliin, jossa mittari tuodaan osaksi organisaation jatkuvaa kehittämistoimintaa. Itse työkalu on Microsoft Excel -taulukko-ohjelmalla luotu kokonaisuus. Kyberturvallisuuskeskuksen sivuilta löytyy myös yksityiskohtainen ohjeistus työkalun käyttöön.


KYBERMITTARI 2.0

Kyberturvallisuuden arviointityökalu

Tiedon luokittelu: sisäinen

TRAFICOM

Kybermittari versio 2.0, 04.10.2022
https://www.kybermittari.fi
Palaute ja kysymykset: kybermittari(at)traficom.fi

Materiaali on käytettävissä Creative Commons Nimeä 4.0 / CC BY 4.0 lisenssiehtojen mukaisesti.
Kybermittari on rekisteröity tavaramerkki (sanamerkki).

Valitse kieli / Välj språk / Choose language: Suomi

Organisaatio

Nimi	Yritys Oy	Yhteyshenkilön sähköposti	etu.suku@yritys.foo
Toimiala	Energiahuolto	Y-tunnus	1234567-8
Toiminto	Energia - Voimatalous	Arvioinnin vetäjä	N.N
Aloitus pvm.	1.10.2022		
Viimeinen muutos	21.10.2022	Seuraava arviointi	6/2023

Kuvaus arvioitavasta toiminnosta

Toiminnon yhteiskunnallinen vaikuttavuus

Uhkaskenaarion kuvaus (worst-case) | Skenaarion yhteiskunnallinen vaikuttavuus

Kuva 1. Kuvakaappaus Kybermittari-työkalusta (Kybermittari 2022).

Tutustu Kyberturvallisuuskeskuksen Kybermittari-työkaluun tarkemmin www.kybermittari.fi

Henkilöstön osaamisen kehittäminen

Kyberturvallisuuden opiskeluun on olemassa erilaisia koulutuksia niin yksilö- kuin organisaatiotasolla. Koulutuksia toteutetaan myös toimenkuvan mukaan; yrityksen toimitusjohtajalla on erilaisia vastuita kuin esimerkiksi tietoturvapäälliköllä. Koulutuksia tarjoavat sekä kaupalliset toimijat että korkeakoulut. Voit tutustua erilaisiin kaupallisiin tietoturvakoulutuksiin koulutus.fi -sivustolta. Monien korkeakoulujen avoimessa tarjonnassa (avoin ammattikorkeakoulu ja avoin yliopisto) on myös tarjolla yksittäisiä opintojaksoja kyberturvallisuuden opiskeluun.

Kyberpoikkeamiin ja -hyökkäyksiin pystyy varautumaan myös harjoittelemalla. Kyberharjoituksissa mallinnetaan erilaisia kyberhäiriötilanteita. Näin saadaan luotua kuvitteelliset olosuhteet, joissa häiriön vaikutukset nähdään, ja niistä toipumista voidaan testata käytännössä. (Kyberharjoitusohje 2019, 4.) Elintarviketeollisuuden toimijoille suunnatussa kyberharjoituksessa voisi esimerkiksi harjoitella teollisuuden ohjaus-/hallintajärjestelmiin kohdistettua tarkoituksellista hyökkäystä tai sitä miten toimitaan, jos joudutaan kiristyshaittaohjelmahyökkäyksen uhriksi. Harjoituksesta organisaatio saa hyviä oppeja toimintatapojen ja prosessien kehittämiseen.

Kyberturvallisuuskeskuksen Elintarvike ISAC-tiedonvaihtoryhmä järjesti elintarviketuotantoon ja -jakeluun keskittyneen kyberturvallisuusharjoituksen vuonna 2021 Trasim-harjoitusalustaa hyödyntäen. Iltapäivän pituinen, tiivis harjoitus oli osa Kyberturvallisuuskeskuksen ISAC-harjoituskonseptia. (Suunnittelulla on merkittävä rooli onnistuneessa kyberharjoituksessa 2021.) Lue lisää Kyberturvallisuuskeskuksen harjoitustoiminnasta.

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.)

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).

Kyberturvallisuuskeskus on julkaissut organisaation kyberturvallisuudesta vastuussa oleville kyberharjoitusohjeen: Käsikirja harjoituksen järjestäjälle. Ohjeessa kerrotaan muun muassa miten kyberharjoitus järjestetään ja miten harjoittelusta saadaan parhaat hyödyt organisaation varautumistyöhön.

Kyberturvallisuudesta teollisuuden näkökulmasta löytyy myös kirjallisuutta. Yksi hyvä esimerkki on Automaation Tietoturva -julkaisu.

Henkilöstöturvallisuus

Ennen työsuhteen alkua

Työnhakijoiden tausta tulee tarkistaa (osaaminen, lainsäädännön rajoitukset, eettisyys). Erityisesti osaamisessa kannattaa kiinnittää huomiota hakijan IT-osaamiseen haettavan työtehtävien vaatimusten valossa. Pätevyyteen ja asenteeseen tulee kiinnittää erityistä huomiota, kun haetaan uutta työntekijää turvallisuusrooleihin. Eettisyys pitäisi selvittää sopivilla kysymyksillä hakulomakkeella ja/tai työhönottohaastattelussa. Ulkoistamistapauksissa organisaation ja vuokratyöntekijöiden välisessä sopimuksessa tulee määritellä vastuut taustatarkistusten suorittamisesta sekä ilmoitusmenettely, mikäli sovitusta on jollain tavalla poikettu. Hakutietoja tulee käsitellä ja tallentaa Eurooppalaisen GDPR-säännösten mukaisesti. Työsopimuksessa tulee eritellä erityiset vastuut tietoturvallisuuden osalta, ja nämä on avattava hakijalle selvästi ennen työsopimuksen allekirjoittamista. ENISA (The European Union Agency for Cybersecurity) on julkaissut syyskuussa 2022 dokumentin, joka listaa 12 tyypillistä rooliprofiilia kyberturvallisuuden ammattilaisten osalta European Cybersecurity Skills Framework. Yrityksen kannattaa tutustua roolimääritelmiin, kun se hakee uutta työntekijää työskentelemään erilaisissa kyberturvallisuuden tehtävissä tai miettii ovatko yrityksen nykyiset tehtävänkuvaukset sopivat/ riittävät yrityksen kyberturvallisuuden näkökulmasta.

Työsuhteen aikana

Vastuut tietoturvallisuudesta on konkretisoitava uudelle työntekijälle soveltuvan tietoturvakoulutuksen avulla heti työsuhteen alkaessa. Koulutuksen tulisi olla personoitu työntekijän tehtävien mukaan. Tässä auttaa keskeisten prosessien määrittely, joista ilmenee työntekijän rooli tietoturvankin kannalta. Esimerkiksi asiakasrajapinnassa toimiville tulee painottaa muun muassa asioita, joita tulee käsitellä asiakkaiden kanssa varoen. Ylläpito- ja asennustehtävissä toimiville pitää painottaa enemmän keskittymistä teknisiin uhkiin. Yrityksellä tulee myös olla määriteltynä mitä siitä seuraa, jos työntekijä tekee todennetusti tietoturvarikkomuksen.

Työsuhteen päättyessä tai muuttuessa

Tietoturvavastuut ja -velvollisuudet, jotka jäävät voimaan työsuhteen päättyessä tai muuttuessa, on määriteltävä. Jos yrityksen tietoturvapolitiikka tai työntekijän tehtävät muuttuvat, tulisi tietoturvakoulutustakin muokata ja tarjota lisää tarpeen mukaan.

(Mukaillen standardia SFS-EN ISO/IEC 27002:2017 ja ISO/IEC 27002:2022(E) Information security, cybersecurity and privacy protection — Information security controls.)

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-ryhmät (Information Sharing and Analysis Center) 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.

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.

Tietoturvastandardit ja ohjeistukset

Kansainväliset standardit

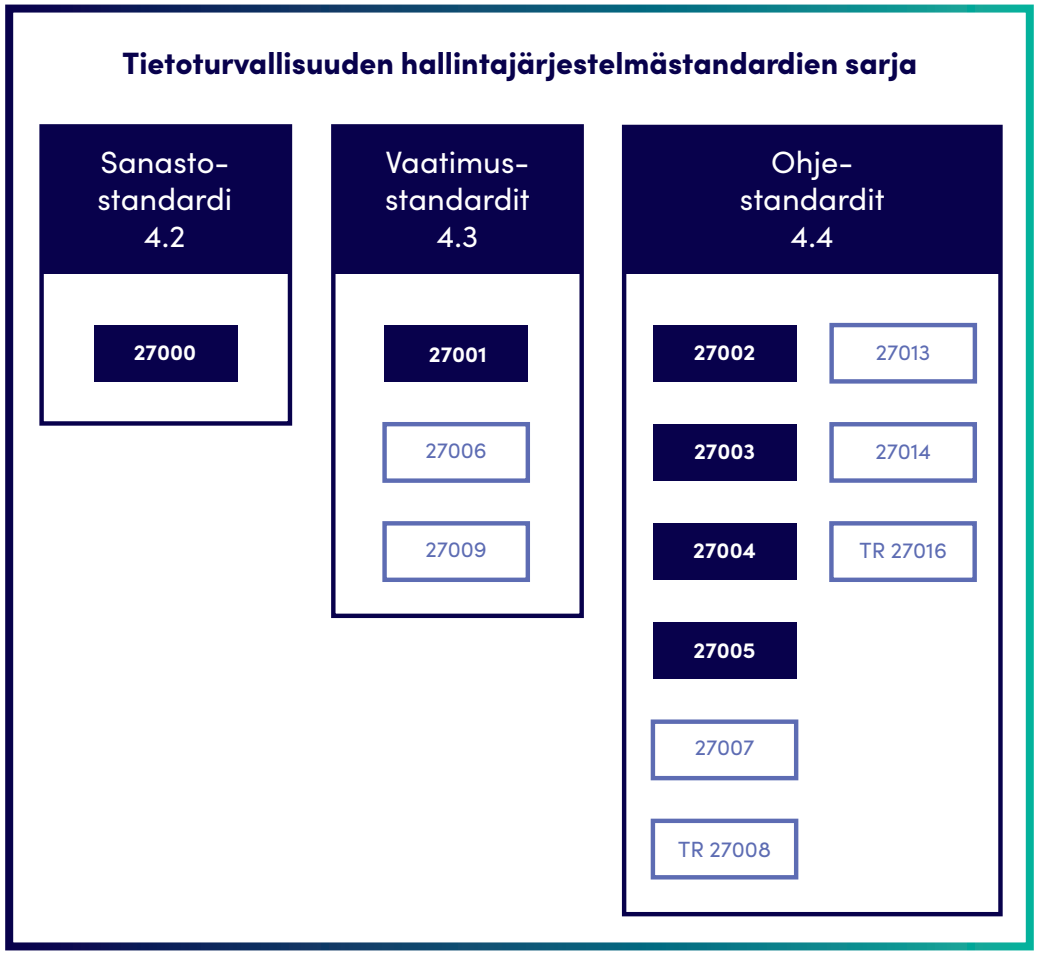
Seuraavaksi esitellään kaksi kansainvälistä standardiperhettä elintarviketeollisuusyritysten tieto- ja kyberturvallisuuden parantamiseksi.

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 (Kuvio 4.) 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 4. 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

Seuraavaksi esitellään kolme suomalaista tietoturvaohjeistusta elintarviketeollisuusyrityksen tietoturvan parantamiseksi.

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 (kansallinen turvallisuusauditointikriteeristö) on viranomaisten auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Myös elintarviketeollisuuden yritys voi hyödyntää Katakria, kun se ulkoistaa palveluitaan konesali- tai pilvipalveluun. Ainakin keskeisimmät Katakrin vaatimukset on hyödyllistä selvittää palvelun tuottajalta.

Lue Katakri – tietoturvallisuuden auditointityökalu viranomaisille (pdf).

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)

Pilvipalveluiden käyttö on yleistynyt nopeasti myös elintarviketuotannon alalla. Tietotekniikan toteutuksesta päättävät joutuvat alati pohtimaan tuotannon uudelleenjärjestelyä esimerkiksi siirtyessään omasta tuotannosta pilvipalveluihin. Pilvipalveluiden turvallisuus on keskeinen asia muutoksista päätettäessä. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) edistää viranomaisten salassa pidettävän tiedon turvallisuutta silloin, kun tietoja käsitellään pilvipalveluissa. Kriteeristö on työkalu pilvipalvelujen turvallisuuden arviointiin kansallisesta näkökulmasta. PiTuKri v1.1 oppaan löydät täältä (pdf).

Poikkeamatilanteiden hallinta

Poikkeamatilanteiden hallinta on keskeinen osa IT-palvelun hallintaa. Se kuvataan yleensä prosessina yrityksen toiminnassa. Tähänkin on olemassa erilaisia kansainvälisiä ja kansallisia ohjeistuksia. Tässä kappaleessa esitellään sekä Vahti-ohjeistuksen että ITIL-prosessikehyksen mukainen poikkeamanhallinta.

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:

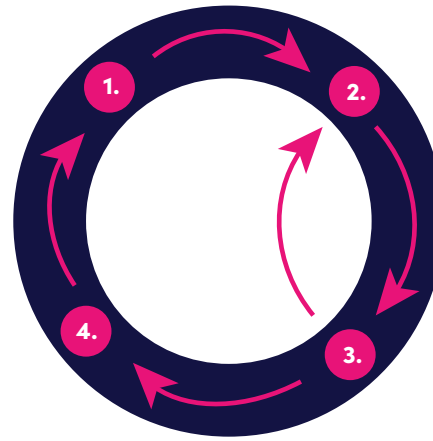
1. Käsittelykyvyn muodostaminen

2. Havaitseminen ja analysointi

3. Reagointi

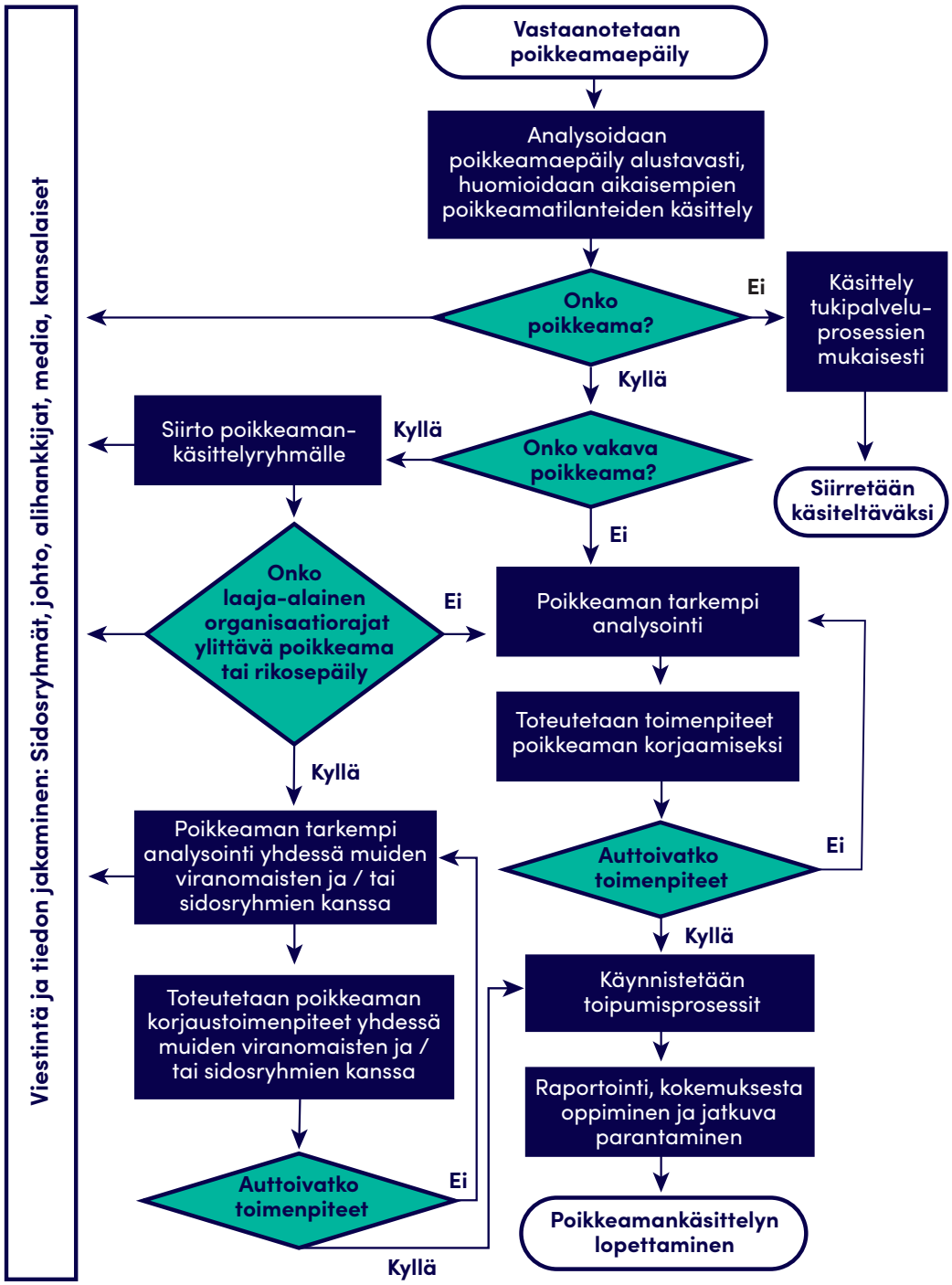
4. Toipuminen

(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 5.



Kuvio 5. 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 toimii 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 6.).

Kuvio 6. 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).

Kaikki VAHTI-ohjeet löydät https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet

ITIL-prosessikehys

ITIL-prosessista saa havainnollisen ja kuvaavan laatimalla siitä uimaratakaavion (swimlane diagram). Ajatuksena uimaratakaaviossa on, että avataan jokaiselle keskeiselle toimijalle oma uimarata, jolloin voidaan nähdä prosessin rajapinnat, velvollisuudet ja vastuut kunkin toimijan kannalta. Jos poikkeaman hallintaprosessi kuvataan uimaratakaaviona, voidaan myös tietoturvakoulutus kohdentaa tehokkaammin. Tietoturvapoikkeaman syöte (input) saadaan joko palvelun käyttäjältä tai teknisiltä hallinnointijärjestelmiltä. Mieluiten syöte saadaan hallintajärjestelmiltä, jolloin käyttäjä ei parhaassa tapauksessa ehdi edes huomata poikkeamaa.

IT-palvelun hallintaa käsitellään perusteellisesti standardistoissa ITIL versio 3 ja 4. ITIL® on Britannian OGC:n (Office of Government Commerce) rekisteröimä tavaramerkki ja se oli aiemmin lyhenne sanoista Information Technology Infrastructure Library - Tietotekniikan infrastruktuurikirjasto. Versio 3 julkaistiin 2007, se päivitettiin 2011, ja siihen viitataan yleisesti ITILv3. Malli on julkaistu viitenä kirjana. Mallissa kuvataan keskeiset IT-palvelutuotannon hyvät käytänteet. Vaikka malli ei ole erityisesti tietoturvaan painottuva, sen pohjalta voidaan laatia yrityksen poikkeaman hallinta. ITILv4 julkaisu alkoi 2019 ja siinä mallia on laajennettu ketterien ohjelmistomenetelmien hyödyntämiseen.

ITILv3 standardin asettaneen viiden kirjan sarjaa kutsutaan nimellä ITILv3 Core Books ja ne ovat nimeltään (kirjasarjan tarkemmat tiedot löytyvät lähdeluettelosta):

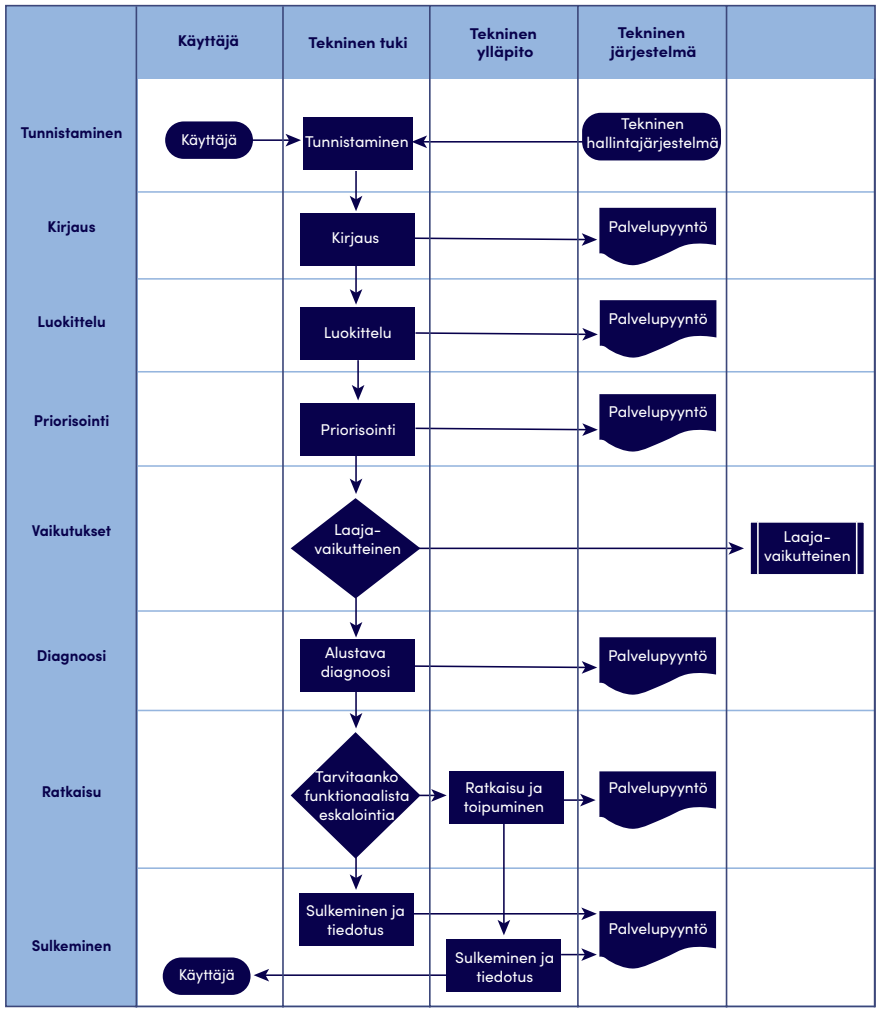
- ITIL Service Strategy
- ITIL Service Design
- ITIL Service Transition
- ITIL Service Operation
- ITIL Continual Service Improvement

ITILv3 määrittelee tietoturvapoikkeaman (englanniksi incident) olevan suunnittelematon keskeytys it-palveluun tai it-palvelun laadun laskeminen. Konfiguraation rakenneosan toimintahäiriö, joka ei ole vielä vaikuttanut palveluun on myös tietoturvapoikkeama. Esimerkkinä voidaan mainita yhden peilatun levyn toimintahäiriö. Näin poikkeaman voidaan ajatella ilmenevän ITILin tietoturvapoikkeamana. ITILiä on ajateltu käytettäväksi ensisijaisesti IT-palvelua tuottavissa yrityksissä, mutta se on sovellettavissa myös pelkästään palveluita käyttäviin organisaatioihin. Lähes kaikissa pienissä yrityksissäkin tuotetaan vähintään toimiston peruspalvelut.

IT-ylläpito ei yleensä tunne palveluiden erityispiirteitä. Sen vuoksi on usein syytä laajentaa prosessikuvausta lisäämällä IT-palvelun paremmin tuntevat asiantuntijat (palveluspesialistit) uimaratakaavioon (Kuvio 7.). Tarvittaessa voidaan käyttää järjestelmän toimittajatahon asiantuntijoita tasolla 2.

Kun tapahtumanhallinta on määritelty etukäteen prosessina, vastuut ja toiminta etenevät ennalta suunnitellusti (varautuminen). Prosessi ei ota kantaa siihen, miten ja missä palvelu tuotetaan. Tuotanto voi olla omassa hallinnassa tai ulkoistettu esimerkiksi pilvipalveluun.

Keskeinen idea ITIL-mallin käytössä on hyödyntää poikkeamatilanteessa tarvittaessa eskalointia, mikä tarkoittaa, että poikkeamat pyritään ratkaisemaan mahdollisimman usein ensimmäisellä asiantuntijatasolla ja mahdollisimman nopeasti, mutta tarvittaessa käsittely siirretään seuraavalla asiantuntijatasolle. Tarvittaessa tasoja voi olla useampiakin ja jopa ulkoistettuja asiantuntijaresursseja. Jokainen eskalointi aiheuttaa lisäkustannusta, joten sitä pyritään minimoimaan. Eskalointi tarjoaa joustavuutta poikkeamanhallinnassa.



Kuvio 7. Tietoturvapoikkeaman käsittelyprosessiesimerkki uimaratakaaviossa, mukaillen ITILv3.

Kuviossa 7 ratkaisun kohdalla voidaan joutua turvautumaan funktionaaliseen eskalointiin eli siirtymään alemmalle uimaradan radalle. Poikkeamaprosessin kuvaus tulee räätälöidä kunkin yrityksen ominaispiirteiden pohjalta. Keskeistä on, miten IT-palvelun käyttäjien palvelu ja teknisten hallintajärjestelmien seuranta yhdistetään yleensä niin sanotussa palvelupisteessä. Palvelupisteen toteutus voi vaihdella yrityksen tarpeiden mukaan hyvin paljon. Se voi olla niinsanottu Service Desk, joka palvelee asiakkaita hyvin laajalta alueelta (ulkoisia ja sisäisiä) tai se voi olla Help Desk, joka keskittyy enemmän teknisten asioiden ratkomiseen. Isommissa organisaatioissa voi olla tarvetta käyttää tietoturvaan erikoistunutta omaa tai ulkoistettua tietoturvan hallintapalvelua SOC (Security Operations Center). Tiedonsiirron väylänä voidaan käyttää fyysistä tapaamista, puhelinyhteyttä, www-lomaketta ja niin edelleen. Palvelupiste voi olla keskitetty, hajautettu tai ulkoistettu. Palvelupisteellä on keskeinen rooli myös viestinnässä niin sisäisesti kuin ulkoisestikin muihin yrityksiin ja viranomaisiin päin yrityksen käyttämien tai tuottamien IT-palveluiden suhteen.

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 elintarviketeollisuuden 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.

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 elintarviketeollisuuden 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.”

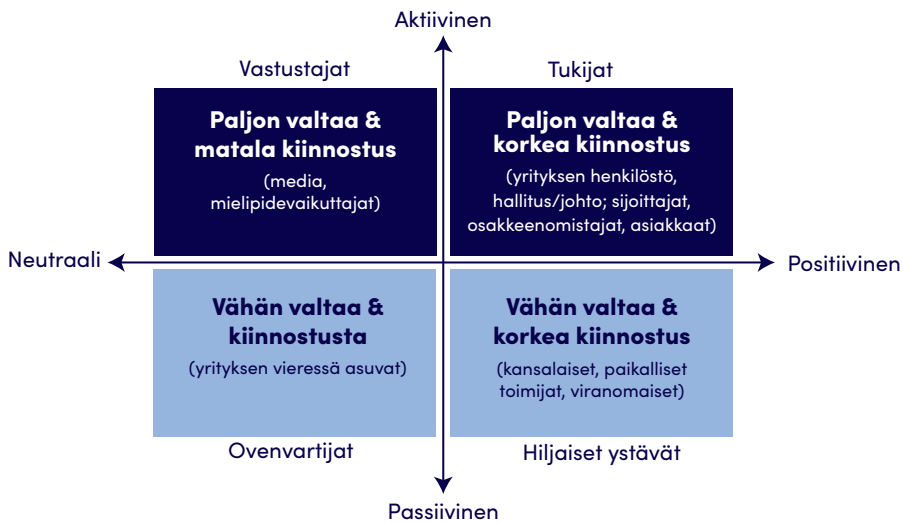
Häiriö- ja kriisiviestinnässä tulee huomioida palveluiden ja tietojärjestelmien kriittisyys. Tunnista ja listaa yrityksesi palvelut ja tietojärjestelmät. Luokittele ne kriittisiksi tai ei-kriittisiksi. Kriittinen palvelu tai tietojärjestelmä on sellainen, johon kohdistuva kyberpoikkeama aiheuttaa merkittävää 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 8.).

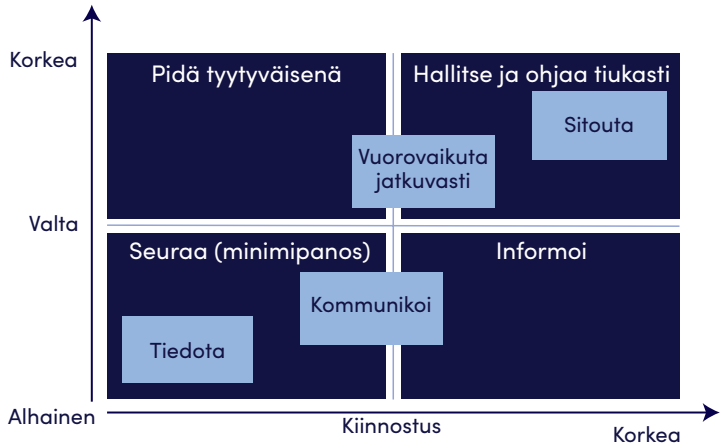


Kuvio 8. Sidosryhmäanalyysin toteuttaminen (mukaillen Certified PMO Manager -koulutus, Adapro).

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 9.).



Kuvio 9. 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 & 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

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

Cannon, D., Wheeldon, D., Lacy, S. & Hanna, A. 2011. ITIL service strategy. Toinen painos. Iso-Britannia. Cabinet Office, TSO (The Stationery Office).

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.

Hunnbeck, L., Rudd, C., Lacy, S. & Hanna, A. 2011. ITIL service design. Toinen painos. Iso-Britannia. Cabinet Office, TSO (The Stationery Office).

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.

Kyberharjoitusohje. 2019. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus ja Huoltovarmuuskeskus. Viitattu 7/2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusopas.pdf

Kybermittari. 2022. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 7/2022. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari

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

Lloyd, V., Wheeldon, D., Lacy, S. & Hanna, A. 2011. ITIL continual service improvement. Toinen painos. Iso-Britannia. Cabinet Office, TSO (The Stationery Office).

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

Rance, S., Rudd, C., Lacy, S. & Hanna, A. 2011. ITIL service transition. Toinen painos. Iso-Britannia. Cabinet Office, TSO (The Stationery Office).

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

SFS-EN ISO/IEC 27002:2017. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Aihealueet: Informaatioteknologia, turvallisuustekniikat. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 03.03.2017. Viitattu 20.8.2022. https://janet.finna.fi, SFS Online.

Steinberg R., Rudd, C., Lacy, S. & Hanna, A. 2011. ITIL service operation. Toinen painos. Iso-Britannia. Cabinet Office, TSO (The Stationery Office).

Suunnittelulla on merkittävä rooli onnistuneessa kyberharjoituksessa. 2021. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 10/2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suunnittelulla-merkittava-rooli-onnistuneessa-kyberharjoituksessa

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

Tietoturvariskien hallinta. 2018. SFS-EN ISO/IEC 27005. Aihealueet: Informaatioteknologia, turvallisuustekniikat. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 28.12.2018. Viitattu 18.8.2022. https://janet.finna.fi, SFS Online.

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

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

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.

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.

POC (Point Of Contact)
Yhteyspiste tarkoittaa henkilöä tai yrityksen osastoa, joka toimii kyseistä toimintaa koskevien tietojen koordinaattorina tai yhteyspisteenä.

Ransomware
Kiristyshaittaohjelma, joka voi tulla tietokoneeseen esimerkiksi sähköpostin liitetiedoston kautta. Käyttäjä avaa liitetiedoston ja sen seurauksena haittaohjelma latautuu koneelle. Seurauksena ohjelma esimerkiksi muuntaa tiedostoja salakirjoitettuun muotoon. Täten tiedostoja ei voida avata ilman oikeaa salauksenpurkuavainta. Kiristyshaittaohjelman levittäjä pyytää lunnaita avaimen toimitusta vastaan.

SLA (Service Level Agreement)
Palvelutasosopimus (palveluntarjoajan ja asiakkaan välinen sopimus, jossa määritellään palvelulle tietyt vaatimustasot).

SOC (Security Operations Center)

Tietoturvavalvomossa (SOC) seurataan sekä analysoidaan tilannekuvaa tietoturvan osalta. Lisäksi tunnistetaan, ehkäistään ja analysoidaan tietoturvahäiriöitä, dokumentoidaan ne ja reagoidaan tietoturvahäiriöihin organisaation ohjeistuksen mukaisesti. Tietoturvavalvomo voi olla organisaation sisäinen tai ulkoistettu palvelu.

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

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.

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.

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.

Jyväskylän ammattikorkeakoulu

IT-instituutti
Piippukatu 2, 40100 Jyväskylä
Puh. +358 20 743 8100

jamk.fi

Kyberturvallisuus elintarviketeollisuudessa -käsikirja kyberpoikkeamien hallintaan

Jyväskylän ammattikorkeakoulun Elintarviketuotannon
ja -jakelun kyberpoikkeamanhallinnan julkaisut, osa 2/3

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

ISBN 978-951-830-679-8 (PDF)

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

www.jyvsectec.fi

jamk | Jyväskylän ammattikorkeakoulu

Maa- ja metsätalous-
ministeriö