Kyberturvallisuus alkutuotannossa

-käsikirja kyberpoikkeamien hallintaan

ELINA SUNI (TOIM.)

Jyväskylän ammattikorkeakoulun Elintarviketuotannon ja -jakelun kyberpoikkeamanhallinnan julkaisut, osa 1/3

jamk | Jyväskylän ammattikorkeakoulu

Maa- ja metsätalous-ministeriö

Sisältö

Tekijät:

Vesa Vertainen
Jyväskylän ammattikorkeakoulu

Jaana Brandt
Jyväskylän ammattikorkeakoulu

Elina Suni
Jyväskylän ammattikorkeakoulu

Kustantaja: Jyväskylän ammattikorkeakoulu

ISBN 978-951-830-677-4 (PDF)

Jyväskylä 2023

1 Johdanto

Elina Suni

Käsikirjan päätavoitteena on tuottaa alkutuotannon toimijoille ymmärrystä kyberuhkista sekä ohjeita kyberpoikkeamatilanteisiin varautumiseen. Kohderyhmänä ovat alkutuotannon toimijat Suomessa. Käsikirja auttaa alkutuotannon toimijoita ymmärtämään omaan digitaaliseen ympäristöönsä kohdistuvia uhkia sekä tarjoaa konkreettisia ohjeita ja toimintatapoja kyberpoikkeamanhallintaan. Käsikirjan tarkoituksena on varmistaa yhteiskunnan kannalta kriittisten alkutuotannon 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, sillä voi olla merkittävät vaikutukset kansalliseen ruokaturvaan ja kyberresilienssiin. On tärkeää, että alkutuotanto 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 elintarviketeollisuudessa –käsikirja kyberpoikkeamien hallintaan (Elintarviketuotannon ja -jakelun kyberpoikkeamanhallinnan julkaisut Jamk, osa 2/3)
- Kyberturvallisuus kaupan ja jakelun alalla –käsikirja kyberpoikkeamien hallintaan (Elintarviketuotannon ja -jakelun kyberpoikkeamanhallinnan julkaisut Jamk, osa 3/3)

Projektin on rahoittanut maa- ja metsätalousministeriö ja 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.

Maatilan kyberturvallisuus -infopaketti

Käsikirjan lisäksi aiheesta on tehty lyhyempi julkaisu, joka sisältää kyberturvallisuuden tarkistuslistan sekä vuosikello- ja mallitilaesimerkin. Lyhyt julkaisu on nopeasti sisäistettävä infopaketti.

Maatilan kyberturvallisuus -infopaketti on ladattavissa verkkosivuiltamme suomen- ja ruotsinkielisenä.

Luku 2

Alkutuotannon kyberturvallisuus

Luvussa kaksi kerrotaan mitä on kyberturvallisuus ja käydään läpi yleisimpiä alkutuotannon kyberuhkia.

2 Alkutuotannon kyberturvallisuus

Vesa Vertainen

Mitä on kyberturvallisuus ja miksi siihen pitäisi kiinnittää huomiota?

Kun digitaalisia laitteita sisältävä toimintaympäristö on luotettava ja uhkilta suojattu, voidaan puhua kyberturvallisuudesta. Kyberuhkilla tarkoitetaan sellaisia tapahtumia, jotka voivat häiritä järjestelmiä, ohjelmistoja, laitteita ja tietoliikenneyhteyksiä ja vaikuttaa haitallisesti yrityksen toimintaan, talouteen, tietoon ja liiketoiminnan jatkuvuuteen (Kyberturvallisuus ja yrityksen hallituksen vastuu 2020).

Miksi kyberturvallisuus on tärkeää?

Yritykset, myös maatilat, ovat enenevässä määrin riippuvaisia digitaalisista palveluista ja järjestelmistä. Samalla kun uusien järjestelmien käyttöönotto helpottaa monia työvaiheita, se voi myös lisätä muun muassa internetin kautta tulevia uhkia.

Maatilan tietoverkkoon pääsy voi antaa hyökkääjälle mahdollisuuden muun muassa

- Lukita tietokone tai laite tai tehdä se käyttökelvottomaksi.
- Tuhota tietoa tai salata tietoa niin, ettei sitä voida lukea tai varastaa ja mahdollisesti julkaista verkossa luottamuksellisia tietoja.
- Häiritä ja jopa pysäyttää maatilan koneita.
- Häiritä mitä tahansa automaatiojärjestelmiä.
- Kytkeä yrityksen laitteilta käyttöön palveluita, joista koituu lisäkustannuksia. (Cyber security for farmers 2020.)

Miksi juuri minun yritykseni olisi hyökkääjän kohde?

Sen lisäksi, että hyökkäyksiä tarkoituksella kohdennetaan potentiaalisiin kohteisiin, kohdistamattoman hyökkäyksen uhriksi voi joutua aivan kuka tahansa. Muun muassa saastuneen nettisivuston kautta voi saada laitteelleen haittaohjelman, joka voi esimerkiksi salata tietokoneen tiedot lukukelvottomiksi ja mahdollisesti vaatia lunnaita vastineeksi tietojen uudelleen avaamisesta. Valitettavan yleisiä ovat myös ns. tietojenkalasteluviestit, joissa yritetään huijata käyttäjä paljastamaan pankki- tai käyttäjätunnuksiaan tai henkilötietojaan. Hyökkääjät etsivät myös automatisoiduilla skannauksilla internetiin liitetyistä laitteista haavoittuvuuksia, joiden kautta laitteen voisi ottaa haltuun ja esimerkiksi valjastaa se tekemään työtä hyökkääjien hyväksi osana useiden laitteiden verkostoa, niin kutsuttua bottiverkkoa. Näin ollen mikä tahansa yritys tai henkilö on mahdollinen uhri. Motiivina hyökkäyksissä on usein raha, jota voidaan saada esimerkiksi myymällä tietoja tai tunnuksia eteenpäin.

”Motiivina hyökkäyksissä on usein raha”

Alkutuotannon kyberuhkia

Suuri osa digitaaliseen toimintaympäristöön kohdistuvista hyökkäyksistä tapahtuu joko laitteissa olevien virheiden tai ihmisten tekemien virheiden välityksellä. Tieto siitä, miten rikolliset käyttävät näitä virheitä hyväkseen, auttaa itse kutakin suojaamaan ympäristöä.

Huijausviestit ja tietojenkalastelu

Tietojenkalastelu on huijauksen muoto, jossa udellaan henkilötietoja, maksukorttien tietoja, pankkitunnuksia tai muita tunnuksia ja salasanoja sähköpostilla, tekstiviestein, sosiaalisessa mediassa tai puhelinsoitolla, tai viesteissä olevien linkkien tai liitetiedostojen avulla tartutetaan haittaohjelmia käyttäjän laitteelle. Sähköpostit saattavat näyttää tulevan luotettavalta taholta, kuten joltakin tunnetulta yritykseltä, ja puhelimelle viestit voivat tulla jopa samaan viestiketjuun kuin aidotkin viestit (Tekstiviestihuijauksia liikkeellä runsaasti 2019). Viestejä voi tulla myös vaikkapa tuttavan sähköpostiosoitteesta (Pienyritysten kyberturvallisuusopas 2020). Huijauspuheluissa huijari esiintyy usein viranomaisena tai esimerkiksi pankin työntekijänä (Mitä on tietojenkalastelu? Nd). Käyttäjä saattaa eksyä kalastelusivuille myös vahingossa hakukoneen kautta.

Millä tavalla meitä huijataan?

Lahjakortti- ja arvontahuijaus: Kehotetaan osallistumaan arvontaan tai lunastamaan lahjakortti, usein jonkin tunnetun yrityksen nimissä. Kutsu voi tulla myös esimerkiksi ystävän kautta Facebook Messengerissä.

Tilauksen seuranta- tai paketin saapumisilmoitukset: Pyydetään avaamaan linkkejä ja antamaan pankki- tai luottokorttitietoja esimerkiksi tekaistujen kuljetus- tai tullimaksujen vuoksi.

Asiakastutkimus- ja kyselypalkkiot: Houkutellaan avaamaan linkkejä, jotka johtavat huijaussivustoille, usein tunnettujen yritysten nimissä.

”Pankki” pyytää vahvistamaan tietoja: Pankin nimissä lähetetty viesti, joka pyytää syystä tai toisesta kirjautumaan asialliselta näyttävälle, mutta väärennetylle sivustolle.

Olemattomien tai väärennettyjen tuotteiden kaupittelu: Erityisesti tilanteissa, joissa tietyn tuotteen saatavuudessa on ongelmia. Esimerkiksi adBlue-lisäaineen saatavuusongelmat voisivat synnyttää epäilyttävän hyviä ”tarjouksia”, tai ”halpa kasvinsuojeluaine” olisikin jotain aivan muuta kuin oikeaa tavaraa.

Viranomaisena, pankin työntekijänä, IT-tukihenkilönä tms. esiintyminen: Huijari soittaa ja yrittää erilaisten verukkeiden varjolla kysellä pankkitietoja, käyttäjätunnuksia tai henkilötietoja tai pyytää asentamaan koneelle etähallintaohjelman, jonka kautta voisi ”korjata” uhrin tietokoneen.

Tori.fi -huijaukset: Huijari esittää olevansa tuotteesta kiinnostunut ja haluaa tuotteen tietyn kuriiripalvelun kautta. “Ostaja” lähettää linkin kuriiripalvelun valesivustolle, jossa pyydetään luottokorttitietoja.

Romanssihuijaukset: Kuviteltuna henkilönä esiintyvä huijari pyrkii luomaan luottamussuhteen uhriin tarkoituksenaan saada rahaa.

Sijoitushuijaukset: Huijari tekaisee valeuutisia ja -mainoksia tunnettujen henkilöiden nimiä hyväksi käyttäen ja yllyttää sijoittamaan rahaa tekaistuihin kohteisiin.

Valekeräykset: Pyydetään rahaa tunnettujen humanitääristä apua tarjoavien järjestöjen nimissä. Valekeräykset voivat muistuttaa oikeiden järjestöjen kampanjoita.

Tekstiviesteinä tulevat huijaukset: "Uusi ääniviesti", "Vastaamaton puhelu", "Ilmoitus saapuneesta lähetyksestä", hyvityksiä "Verohallinnolta" tai muuta vastaavaa.

Kiristyshuijausviestit: Huijari väittää kaapanneensa uhrin tietokoneen tai sähköpostitilin tai kuvanneensa uhria salaa ja uhkaa julkaista arkaluontoisia kuvia, ellei hänelle makseta. Yleensä kuvia ei todellisuudessa ole otettu tai konetta kaapattu, eikä huijarin vaatimuksiin pidä suostua.

(Tietojenkalastelu 2022; Lähetitkö tietosi mukatutulle Messengerissä? 2022; Tekstiviestihuijauksia liikkeellä runsaasti 2019; Tilitietosi yritetään kaapata – älä usko "Nordealta" tulevaa viestiä 2022; Mitä on tietojenkalastelu? Nd; Tori.fi varoittaa käyttäjiään: Huijarit yrittävät viedä pankkitunnuksesi 2022; Näin suojaudut nettihuijaukselta 2021; Huijaukset ja nettihuijaukset Nd; Valekeräykset Ukrainan pakolaisten auttamiseksi leviävät verkossa 2022; FluBot-haittaohjelmaa levitetään jälleen tekstiviestitse 2022.)

Lisätietoja huijauksista Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen sivuilta:

- Saitko tekstiviestin Postin nimissä? Varothan, viesti voi olla huijaus
- Väärennettyjä puheluita teknisen tuen nimissä

Mitä nettihuijauksista voi seurata?

Linkin tai liitetiedoston välityksellä uhrin laitteelle saattaa asentua haittaohjelma, jonka kautta hyökkääjä voi muun muassa varastaa, tuhota tai salata tietoja. Haltuunsa saamien tietojen avulla rikollinen voi hankkia rahaa kiristämällä, verkkopankkitunnuksia käyttämällä, tekemällä tilauksia uhrin nimissä tai johdattelemalla tilausansaan, jossa uhri tulee sopineeksi pitkäkestoisesta tilauksesta, jonka kulut veloitetaan tililtä säännöllisesti. Hyökkääjä voi myös ottaa laitteen hallintaansa ja liittää sen osaksi omaa verkostoaan ja saastuneen laitteen kautta päästä käsiksi myös muihin verkkoympäristön laitteisiin. Tästä voi aiheutua pitkäkestoisia katkoja yrityksen toiminnassa, kun kriittiset järjestelmät toimivat huonosti tai kun niitä ei pystytä käyttämään tai kriittistä tietoa menetetään.

Miten voin tunnistaa, milloin kyseessä on tietojenkalastelu tai muu huijaus?

Sähköposti- ja tekstiviestit voivat näyttää hyvinkin uskottavilta. Viestissä olevan linkin sijaan on turvallisempaa kirjautua suoraan palveluntarjoajan sivulta, esim. ”www.posti.fi”. Huijaukseen liittyviä merkkejä voivat olla muun muassa:

- Viestissä kysytään luottokortin tietoja, salasanoja tai muita henkilökohtaisia tietoja.
- Viesti sisältää kirjoitusvirheitä tai epätavallisia termejä.
- Viestin saajaa vaaditaan reagoimaan nopeasti tai muuten jokin uhkakuva voi toteutua tai tarjous mennä ohi.
- Tarjolla on epäilyttävän halpa tuote tai lahjakortti; tarjous on liian hyvä ollakseen totta.
- Sähköpostin lähettäjän osoite on epämääräinen, mahdollisesti aivan eri kuin viestin lähettäjän nimi tai taho, jota lähettäjä väittää edustavansa.
- Sähköpostin ulkoasu ei täsmää lähettäjän ”edustaman” yrityksen normaaliin visuaaliseen tyyliin.
- Nettiosoite ei vastaa mainitun yrityksen oikeaa osoitetta.
- Viesti on lähetetty epätavalliseen aikaan kuten yöllä.
- Viestissä on kirjaimista ja numeroista koostuva epämääräinen linkki.
- Viestissä mainitun nettiosoitteen alku on muotoa ”http”, suojatusta yhteydestä kertovan ”https” sijaan.
- Pyydetään lataamaan jokin ohjelmisto.
- Ilmoitetaan paketista, jota ei ole tilattu.

(Kalasteluviestit ovat edelleen kasvava ongelma 2022; Digihuijausten tunnistaminen ja niiltä suojautuminen 2021; Tietojenkalastelu 2022.)

Jos et ole varma yhteydenottajan aitoudesta, älä klikkaa linkkiä, avaa liitetiedostoa tai muuten luovuta tietojasi. Pankit tai luottokorttiyhtiöt eivät koskaan pyydä vahvistamaan tietoja sähköpostin välityksellä.

Entä jos tulin huijatuksi?

- Vaihda salasana. Jos olet antanut kirjautumistunnuksen ja salasanan väärään paikkaan, vaihda salasanasi välittömästi kaikkiin palveluihin, joissa kyseinen salasana on käytössä. Käytä jokaisessa palvelussa eri salasanaa, se tuo turvaa erityisesti tällaisten tilanteiden varalta.
- Ota tarvittaessa yhteyttä pankkiin. Jos annoit pankkitunnuksesi, ota heti yhteyttä pankkiin, jotta pankki voi yrittää estää väärinkäytöksen.
- Tee rikosilmoitus poliisille osoitteessa https://poliisi.fi/tee-rikosilmoitus
- Ilmoita tapahtuneesta Kyberturvallisuuskeskukselle. https://www.kyberturvallisuuskeskus.fi/fi/ilmoita
- Jos epäilet tulleesi huijatuksi, voit ottaa yhteyttä rikosuhripäivystykseen. https://www.riku.fi/palvelut/rikosuhripaivystys-116-006/

(Kalasteluviestit ovat edelleen kasvava ongelma 2022.)

Jos epäilet, että asensit haittaohjelman:

- Palauta laite tehdasasetuksiin.
- Jos palautat tietoja varmuuskopiosta, varmista että kopio on otettu ennen kuin haittaohjelma asennettiin.
- Jos kyse on SIM-kortillisesta laitteesta, ota yhteyttä operaattoriin, koska liittymästä on saattanut lähteä maksullisia viestejä.

(FluBot-haittaohjelmaa levitetään jälleen tekstiviestitse 2022.)

Lisää apua huijausten tunnistamiseen ja niiltä suojautumiseen:

- www.jamk.fi/fi/projekti/cyberdi/tietopankki
- www.kyberturvallisuuskeskus.fi/nain-suojaudut-nettihuijaukselta

Kiristyshaittaohjelmat

Yleinen haittaohjelman muoto on kiristyshaittaohjelma, joka voi päätyä käyttäjän tietokoneelle esimerkiksi sähköpostin liitetiedoston tai linkin kautta. Ohjelma salaa tietokoneella olevat tiedostot, toisin sanoen, vaikka tiedot vielä sijaitsevat käyttäjän koneella, ne ovat salatussa muodossa, eikä niitä voi lukea ilman salausavainta. Kiristäjät lupaavat palauttaa tiedot luettavaan muotoon lunnasmaksua vastaan. Tosiasiassa ei ole mitään takeita sille, että rahat saatuaan kiristäjät palauttaisivat tiedot. Kyberturvallisuuskeskus ohjeistaa, että vaadittuja rahoja ei missään tapauksessa pidä maksaa. Nykyään tietojen salaamisen lisäksi hyökkääjä usein myös kopioi tiedot itselleen ja saattaa julkaista ne internetissä kaikkien nähtäville tai myydä henkilö- ym. arkaluontoista tietoa eteenpäin pimeillä markkinoilla. Haittaohjelman kautta saatetaan lisäksi tuhota myös tiedostojen varmuuskopiot, jos niihin päästään käsiksi.

Kiristyshaittaohjelmat ovat yksi tämän hetken merkittävimmistä kyberuhkista, ja ne kehittyvät ja lisääntyvät entisestään.

Maailman talousfoorumin raportin mukaan kiristyshaittaohjelmat ovat yksi tämän hetken merkittävimmistä kyberuhkista, ja ne kehittyvät ja lisääntyvät entisestään (Global Cybersecurity Outlook 2022, 6). Yhdysvalloissa FBI havaitsi kiristyshaittaohjelmahyökkäyksiä kuutta viljaosuuskuntaa vastaan syksyn 2021 sadonkorjuun aikana ja kaksi hyökkäystä alkuvuodesta 2022. Hyökkäyksen tarkoitus oli vaikuttaa kylvökauteen häiritsemällä siementen ja lannoitteiden toimituksia. FBI:n mukaan maatalouteen kohdistetaan kyberhyökkäyksiä erityisesti kriittisimpinä kylvö- ja sadonkorjuukausina, vaikkakin hyökkäyksiä havaitaan muinakin aikoina koko elintarviketuotannon ja -jakelun sektorilla. (Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons 2022.) Kiristyshaittaohjelmien uhreiksi on joutunut globaaleja maataloustuotteiden toimialan yrityksiä, näiden vaikutukset ovat näkyneet myös Suomessa.

Palvelunestohyökkäykset

Palvelunestohyökkäyksessä suuret määrät verkkoliikennettä kohdistetaan tiettyyn palveluun, esimerkiksi pankin sivuille, tarkoituksena kuormittaa palvelua niin paljon, että sen käyttö estyy. Tavalliselle käyttäjälle tämä ilmenee niin, että kyseiseen palveluun ei pääse ollenkaan tai se toimii hitaasti. Myös käyttäjien omia laitteita voidaan kaapata haittaohjelmien välityksellä osaksi hajautettua hyökkäystä, jolloin kohdetta kuormitetaan yhtä aikaa useiden laitteiden voimin. Jos oma laite on kaapattu, se voi ilmetä käyttäjälle laitteen hidastumisena. Esimerkiksi Suomen puolustusministeriön ja ulkoministeriön verkkosivut kaatuivat 8.4.2022 tällaisen hyökkäyksen seurauksena ja olivat pois käytöstä joitakin tunteja (Viime viikon palvelunestohyökkäykset olivat mahdollista esimakua 2022). Alkutuotannossa harmia voisi aiheuttaa esimerkiksi pitkäkestoinen palvelunestohyökkäys nautarekisterisovellusta tai viljelysuunnittelupalveluita kohtaan.

Lue lisää palvelunestohyökkäyksistä Kyberturvallisuuskeskuksen sivuilta: Palvelunestohyökkäykset ovat arkipäivää Suomessa

Tietojen vääristäminen ja laitteiden väärinkäyttö

Pahantahtoinen toimija voi maatilan tietoverkkoon päästessään aiheuttaa monenlaista haittaa muun muassa tietoja vääristämällä. Salmonellatartuntaan liittyvät saneeraustoimenpiteet ovat kotieläintilojen kannalta toteutuessaan raskaita, pitkäkestoisia ja kalliita operaatioita. Vaikka saneeraukseen ei jouduttaisikaan, niin jo pelkkä salmonellatartuntaepäilys saisi aikaan paljon ylimääräistä työtä ja luottamuksen rapautumista tuotantoketjun toimijoiden kesken. Tämä voisi toteutua esimerkiksi kotieläintiloilla rajoitetusti käytettävän rehun tai välityseläinten salmonella-todistusten vääristämisellä.

Viljaerien tuotetietojen vääristäminen voisi johtaa tilanteeseen, jossa merkittävä osa jonkin toimijan varastoimasta viljasta jouduttaisiin ohjaamaan toisarvoiseen käyttöön, koska viljaerien alkuperää ja laatua ei pystyttäisi varmentamaan. Esimerkiksi siilon lämpötila-anturia voitaisiin manipuloida näyttämään valheellisesti liian korkeaa lämpötilaa. Harmia voitaisiin aiheuttaa myös vaikkapa lisäämällä tuotteiden pakkausten painatuksiin kantaa ottavia tekstejä tai tilaamalla teurasauto ja ilmoittamalla poistot nautarekisteriin.

Laitteiden luvattomalla hallinnalla voidaan tehdä monenlaista vahinkoa. Esimerkiksi broilerituotannon kamera- tai ruokintajärjestelmiä käyttäen voitaisiin saada aikaan turhia hälytyksiä. Kameravalvonnasta kaapattuja kuvia voitaisiin myös irrottaa asiayhteydestä ja julkaista negatiivisessa valossa. Myös tilallisen itsensä sosiaalisessa mediassa julkaisemaa materiaalia voidaan ymmärtää väärin tai käyttää tahallaan tilaa vastaan. (Kyberin taskutieto maatiloille 2018.)

Laitteiden luvattomalla hallinnalla voidaan tehdä monenlaista vahinkoa.

Maatalousrobotin kaappaamisella voitaisiin aiheuttaa vaikkapa ruokinnan häiriintymistä, mutta seurauksena voisi pahimmillaan olla jopa puristuskuolema (Elintarvike- ja maataloussektorin tietoturva kehittyy 2022). Lypsyrobotin kaappaus puolestaan voisi johtaa siihen, että lääkittyjen lehmien antibioottimaitoja ei lypsettäisikään asianmukaisesti erilliseen säiliöön tai että sinne ohjattaisiin turhaan ylimääräistä maitoa. Myös kiinteistöautomaatiolaitteita ja jopa kodinkoneita voidaan kaapata osaksi hyökkääjän hallitsemaa verkostoa. Esimerkiksi erääseen roskapostihyökkäykseen tiedetään olleen osallisena yli 100 000 televisiota, reitititintä ja jääkaappia (Jääkaapit mukana bottiverkossa: älykkäät kodinkoneet syytivät 750 000 roskapostia 2014).

Informaatiovaikuttaminen

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.)

Alkutuotannon osalta informaatiovaikuttamista voisi olla vaikkapa tarkoituksellinen paniikin lietsominen väittämällä, että jokin tarpeellinen tuote uhkaa loppua. Tuotantotilat voisivat alkaa hamstraamaan esimerkiksi siemeniä tai karjatilat eläinlääkkeitä, jos näiden uskottaisiin olevan loppumassa. Hamstraaminen voisi nostaa hintoja ja aiheuttaa todellisia vaikeuksia saatavuuteen ja siten ongelmia yksittäisille tiloille. Ostokäyttäytymisen muutoksia voitaisiin saada aikaan myös vaikkapa levittämällä väärää tietoa, että jokin vihanneserä on myrkytetty.

Yksi tehokkaimpia keinoja vastata informaatiovaikuttamiseen on kansalaisten hyvä yleissivistys ja medialukutaito.

Valtioneuvoston viestintäsuosituksen (2016, 13) mukaan yksi tehokkaimpia keinoja vastata informaatiovaikuttamiseen on kansalaisten hyvä yleissivistys ja medialukutaito. Jokainen voi osaltaan tukea yhteiskunnan kyberturvallisuutta suhtautumalla sopivan kriittisesti kaikkeen tietoon ja huolehtimalla siitä, ettei itse jaa väärää tietoa eteenpäin (Informaatiosota on jo käynnissä 2022).

Lue Kyberturvallisuuskeskuksen ohje: Vinkkejä informaatiovaikuttamisen tunnistamiseksi - Ole tarkkana ja toimi vastuullisesti

Lähteet

Cyber security for farmers. 2020. National Cyber Security Centre. Viitattu 5/2022. https://www.ncsc.gov.uk/guidance/cyber-security-for-farmers

Digihuijausten tunnistaminen ja niiltä suojautuminen. 2021. CYBERDI-hanke. Viitattu 4/2022. https://www.jamk.fi/fi/file/cyberdi-digiturvallisuus-yritykset

Elintarvike- ja maataloussektorin tietoturva kehittyy. 2022. Centria-ammattikorkeakoulun verkkolehti. Viitattu 5/2022. https://centriabulletin.fi/elintarvike-ja-maataloussektorin-tietoturva-kehittyy/

FluBot-haittaohjelmaa levitetään jälleen tekstiviestitse. 2022. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 4/2022. https://www.kyberturvallisuuskeskus.fi/fi/varoitus_1/2022

Global Cybersecurity Outlook 2022. 2022. Maailman talousfoorumi. Viitattu 5/2022. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

Huijaukset ja nettihuijaukset. N.d. Kuluttajaliitto. Viitattu 4/2022. https://www.kuluttajaliitto.fi/materiaalit/huijaukset/

Informaatiosota on jo käynnissä. 2022. Yle. Viitattu 6/2022. https://yle.fi/uutiset/3-12324705

Jääkaapit mukana bottiverkossa: älykkäät kodinkoneet syytivät 750 000 roskapostia. 2014. Tivi. Viitattu 5/2022. https://www.tivi.fi/uutiset/jaakaapit-mukana-bottiverkossa-alykkaat-kodinkoneet-syytivat-750-000-roskapostia/c78a8dd1-1355-345f-bb8c-fddcc7c6acf3

Kalasteluviestit ovat edelleen kasvava ongelma. 2022. Artikkeli Elisan sivustolla. Viitattu 4/2022. https://elisa.fi/ideat/kalasteluviestit-ovat-edelleen-kasvava-ongelma

Kyberin taskutieto maatiloille. 2018. Jyväskylän yliopisto ja Maanpuolustuskoulutusyhdistys. Viitattu 3/2022. https://jyx.jyu.fi/handle/123456789/62640

Kyberturvallisuus ja yrityksen hallituksen vastuu. 2020. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 5/2022. https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/kyberturvallisuus-ja-yrityksen-hallituksen-vastuu-opas

Lähetitkö tietosi mukatutulle Messengerissä? 2022. Yle. Viitattu 5/2022. https://yle.fi/uutiset/3-12450551

Mitä on tietojenkalastelu? N.d. Artikkeli F-Securen sivustolla. Viitattu 4/2022. https://www.f-secure.com/fi/home/articles/what-is-phishing

Näin suojaudut nettihuijaukselta. 2021. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 4/2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-nettihuijaukselta

Pienyritysten kyberturvallisuusopas. 2020. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 4/2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

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

Tekstiviestihuijauksia liikkeellä runsaasti. 2019. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 4/2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tekstiviestihuijauksia-liikkeella-runsaasti-lue-tarkasti-mihin-olet-sitoutumassa

Tietojenkalastelu. 2022. Ohje Kilpailu- ja kuluttajaviraston sivuilla. Viitattu 4/2022. https://www.kkv.fi/kuluttaja-asiat/huijaukset/tietojenkalastelu

Tilitietosi yritetään kaapata – älä usko ”Nordealta” tulevaa viestiä. 2022. Iltalehti. Viitattu 5/2022. https://www.iltalehti.fi/tietoturva/a/f8b5bbac-eb23-4566-8df4-24e4366c66f8

Tori.fi varoittaa käyttäjiään: Huijarit yrittävät viedä pankkitunnuksesi. 2022. Iltalehti. Viitattu 5/2022. https://www.iltalehti.fi/tietoturva/a/71f87d42-5f43-4338-a3a7-8c47704df152

Valekeräykset Ukrainan pakolaisten auttamiseksi leviävät verkossa. 2022. Tivi. Viitattu 6/2022. https://www.tivi.fi/uutiset/valekeraykset-ukrainan-pakolaisten-auttamiseksi-leviavat-verkossa-rahat-menevat-rikollisille/9b1cd8ff-f454-41dd-a9eb-deba78dd2b9e

Valtionhallinnon viestintäsuositus. 2016. Valtioneuvoston kanslia. Viitattu 5/2022. https://vnk.fi/documents/10616/3541383/Valtionhallinnon-viestintasuositus-2016.pdf

Viime viikon palvelunestohyökkäykset olivat mahdollista esimakua. 2022. Yle. Viitattu 4/2022. https://yle.fi/a/3-12400481

Luku 3

Kyberpoikkeamien hallinta alkutuotannossa

Luvussa kolme kerrotaan kyberuhkiin varautumisesta alkutuotannossa, esitellään kyberturvallinen mallitila, kriisi- ja häiriöviestinnän skenaario sekä olennaiset viranomaisyhteydet kyberpoikkeamatilanteessa.

3 Kyberpoikkeamien hallinta alkutuotannossa

Vesa Vertainen, Jaana Brandt, Elina Suni

Kyberuhkiin varautuminen

Virustorjunta ja palomuuriohjelma ovat luontainen osa nykyaikaisen tietokoneen käyttöjärjestelmää. Hyvien laitteiden ja ajantasaisten ohjelmistojen lisäksi verkon käyttäjän pienilläkin teoilla voi olla suuri vaikutus sekä kodin että yrityksen digitaalisen toimintaympäristön turvallisuuteen. Näitä keinoja käymme läpi tässä luvussa.

Salasanojen hyvät käytänteet

On tärkeää, että jokaiselle verkkopalvelulle luodaan oma yksilöllinen salasana. Jos samaa salasanaa käytetään useissa eri palveluissa, pääsee yhdestä palvelusta salasanan haltuunsa saanut rikollinen kirjautumaan muihinkin palveluihin. Henkilökohtaisia tunnuksia ei kannata myöskään antaa toisten käyttöön vaan mahdollisuuksien mukaan luoda omat tunnukset myös esimerkiksi kausityöntekijöille, ja nekin vain työssä välttämättömiin palveluihin ja laitteisiin. Hyvä käytänne on myös poistaa tunnukset työsuhteen päättyessä. Huijarit voivat myös udella tunnuksia ja salasanoja esiintyen esimerkiksi viranomaisina. On hyvä muistaa, että viranomaiset, pankit tai muut tahot eivät oikeasti kysele kenenkään salasanoja.

Myös kaikkien verkkoon liitettyjen laitteiden tehdasasetuksena tulleet salasanat on syytä vaihtaa vahvempiin ja säilyttää laitteiden hallintaan liittyvät tiedot turvallisessa paikassa. Kyberturvallisuuskeskus antaa seuraavanlaisia vinkkejä hyvään salasanaan:

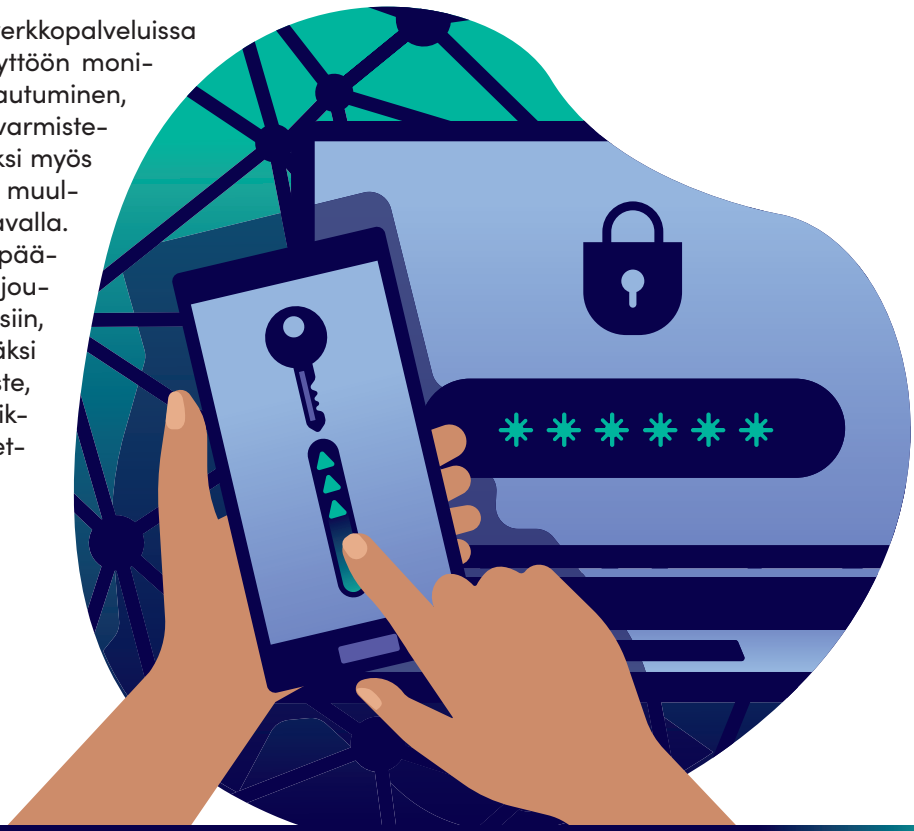
- Mitä pidempi, sen turvallisempi.
- Helppo muistaa, mutta vaikea arvata.
- Kokonainen lause on hyvä salasana.
- Käytä sekä isoja että pieniä kirjaimia sekä erikoismerkkejä.
- Kirjoitusvirheet, murre, puhekielen ilmaisut ja muut perusmuodoista poikkeavat sanat vahventavat salasanaa.

(Pidempi parempi – Näin teet hyvän salasanan 2022.)

Heikkoja salasanoja ovat esimerkiksi ”123456” tai ”kissa”. Myöskään kirjaimien korvaaminen numeroilla, kuten ”k1ssa”, ei nykypäivänä tuo lisäturvaa. Kyberturvallisuuskeskus ohjeistaa, että hyvä salasana on pitkä lause. Voidaan vaikkapa keksiä lause ”kissa seikkaili maalla” ja tehdä siitä hyvä salasana lisäämällä isoja kirjaimia ja merkkejä, sekä taivuttamalla sanoja, esimerkiksi ”Kissamm3eSeikkail!iMaallamme”. Näin rakennettu salasana on hyvä, mutta silti muistettavissa. (Pidempi parempi – Näin teet hyvän salasanan 2022.)

Salasanojen hallintaan on suositeltavaa käyttää salasanamanageria. Tällaista salasanojen hallintasovellusta käyttäessä ei tarvitse muistaa kuin yksi hyvä salasana, jonka takana muut salasanat ovat tallessa. Tällöin salasanat voivat olla hyvinkin pitkiä ja mutkikkaita, toisin sanoen vahvoja, koska niitä ei tarvitse itse muistaa tai edes tietää. Kyberturvallisuuskeskus esittelee sivustollaan erilaisia salasananhallintasovelluksia, kuten 1Password, Bitwarden, Dashlane, Enpass, F-Secure ID PROTECTION, KeePass, Keeper, LastPass ja RoboForm, ja antaa neuvoja salasanan hallintasovelluksen käyttöönottoon.

Jos mahdollista, verkkopalveluissa kannattaa ottaa käyttöön monivaiheinen tunnistautuminen, jolloin henkilöllisyys varmistetaan salasanan lisäksi myös vähintään yhdellä muulla tunnistautumistavalla. Tällöin palveluun ei pääse, vaikka salasana joutuisikin vääriin käsiin, koska salasanan lisäksi tarvitaan lisätunniste, joka voi olla esimerkiksi puhelimeesi lähetettävä koodi.



Lue ohjeita monivaiheisesta tunnistautumisesta Kyberturvallisuuskeskuksen sivuilta: Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi

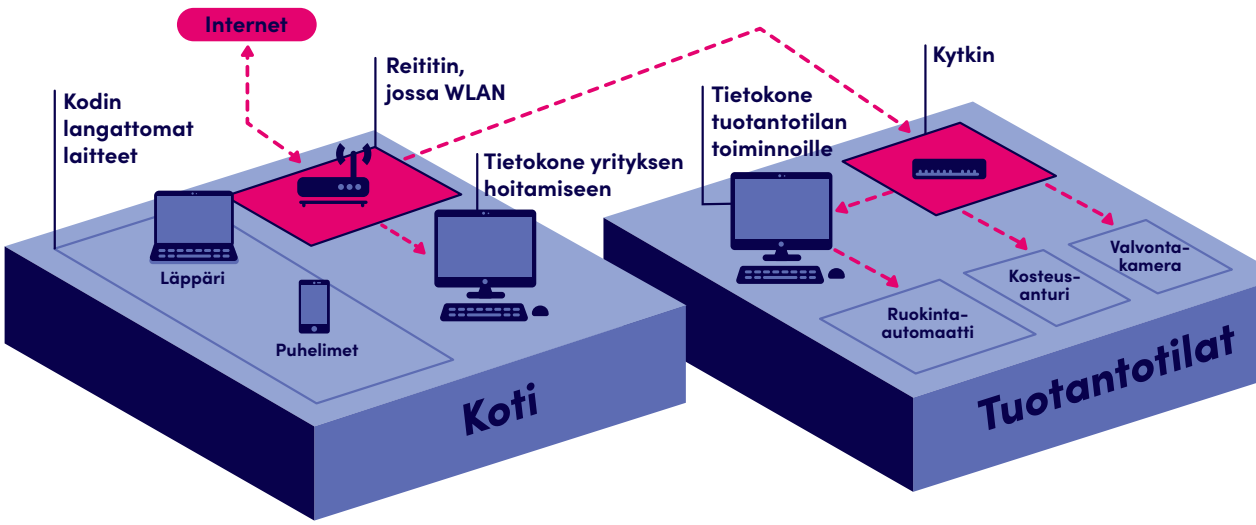
Tietoverkon hyvät käytänteet

Olemassa olevan verkon kartoittaminen

Maatiloille laitteita hankitaan usein tarpeen mukaan ilman etukäteen tehtyä suunnitelmaa. Suurella tilalla voi näin olla verkossaan lopulta jopa satoja vähitellen hankittuja laitteita. Kokonaiskuva siitä mitä kaikkea verkossa on ja miksi, sekä minkälaiseksi verkon rakenne on muodostunut voi jäädä häilyväksi.

Olisikin tärkeää kartoittaa, mitä kaikkia laitteita tilan verkkoon on liitetty, ja miten ne ovat toisiinsa kytköksissä.

Hyvä alku on piirtää yksinkertainen kartta verkosta (Kuvio 1.), dokumentoimalla sen laitteet ja mahdolliset käyttäjät tai käyttäjäryhmät ja kirjata ylös suunnitelma laitteiden ylläpitämiseen. Verkkokartta auttaa vian etsimisessä mahdollisessa ongelmatilanteessa, mutta myös verkon laajentamisen suunnittelussa siitä on apua. Vaikka ammattilainen tekee verkon asennukset, on asiakkaankin syytä saada itselleen tunnukset laitteiden hallinnointiin sekä dokumentointi kaapelointiin, laiteasennuksiin, IP-osoitteisiin, konfiguraatioihin ym. liittyen (Manninen 2018, 58). Dokumentit, erityisesti tunnuksia ja salasanoja sisältävät, on syytä pitää hyvässä tallessa ja sivullisten ulottumattomissa. Verkkokartan lisäksi laadittavasta ylläpitosuunnitelmasta tulisi löytyä tieto siitä, miten eri laitteiden ja ohjelmistojen päivitykset pidetään ajan tasalla ja miten laitteiden fyysinen kunto ja suojaukset tarkistetaan. Esimerkiksi jyrsijät voivat nakertaa johtoja rikki, ja kosteus, lämpötilanvaihtelut ja pöly voivat aiheuttaa vikaantumisia. On hyvä varmistaa myös, että kaikki laitteet osataan tarpeen tullen käynnistää uudelleen.



Kuvio 1. Yksinkertainen esimerkki maatilan verkkokartasta

Fyysinen turvallisuus

Tärkeä osa tietoverkon hyviä käytänteitä, on fyysisten ja teknisten turvatoimien avulla estää asiaton pääsy tietojärjestelmiin. Tilat on syytä pitää mahdollisuuksien mukaan lukittuina, erityisesti kauempana talouskeskuksesta sijaitsevat tilat, joihin sivullisen on helpompi päästä huomaamattomasti (Laajalahti & Nikander 2017, 18). Jos hyökkääjä pääsee fyysisesti käsiksi johonkin tietoverkkoon kuuluvaan laitteeseen, hänen voi olla mahdollista sitä kautta vaikuttaa laitteen lisäksi koko verkon tietojärjestelmiin. Siltä varalta, että tiloihin päästään luvattomasti, on laitteiden käyttäminen suojattava salasanalla ja lukitus laitettava päälle aina kun laitteen käyttö lopetetaan.

Palomuurit

On tärkeää, että lähiverkon suojaamisessa käytetään palomuureja. Palomuuri voi olla tietokoneen ohjelmisto, erillinen laite tai sisältyä esimerkiksi reitittimeen. Paras ratkaisu on erillinen yrityskäyttöön tarkoitettu palomuuri. Palomuurien tarkoitus on tarkkailla ja estää haitallista verkkoliikennettä. Niiden avulla voidaan myös määritellä, mistä laitteesta ja minne liikenne on sallittua. Esimerkiksi valvontakamerajärjestelmiin pääsy kannattaa evätä kaikkialta muualta paitsi valvontaan tarkoitetuilta tietokoneilta varmistaen, ettei kenelläkään ole oman lähiverkon ulkopuolelta pääsyä kameroihin tai tallenteisiin.

Verkon segmentointi

Palomuurin avulla maatilan verkko voidaan myös jakaa useampaan aliverkkoon eli segmentoida. Esimerkiksi kodin viihdelaitteita, työtietokoneita, tuotantotiloja ja valvontakameroita varten voidaan tehdä omat segmentit, jolloin hyökkääjän päästessä murtautumaan johonkin laitteeseen hyökkäys rajoittuu vain kyseiseen segmenttiin. Tällöin esimerkiksi hyökkäyksen kohdistuessa viihdelaitteisiin, työasioihin käytettävät laitteet säilyvät koskemattomina (Laajalahti & Nikander 2017, 22). Verkko voidaan segmentoida joko fyysisesti tai loogisesti. Fyysisessä segmentoinnissa tarvitaan omat verkkolaitteet jokaiselle segmentille, joten helpompi ja yleisempi keino on looginen segmentointi, jossa verkko jaetaan virtuaalisesti aliverkkoihin (Lahti 2021, 17–18). Yrityksen hoitamiseen ja kotikäyttöön tulisi muutenkin olla erilliset laitteet. Muun muassa pelien pelaaminen ja netissä surffailu lisäävät riskiä haittaohjelmatartuntaan, joten yrityksen koneet kannattaa pitää tiukasti vain työkäytössä. Haittaohjelmat saattavat esimerkiksi kaapata tietokoneella olevia yrityksen tunnuksia tai tärkeitä tiedostoja, ja koneelle asennetut pelit ja muut ylimääräiset ohjelmat lisäävät niin sanotusti hyökkäyspinta-alaa.

Langattomat verkot

Langattomia verkkoja käytettäessä on tärkeää, että yhteys on reitittimen asetuksista määritelty käyttämään WPA2-salausta, että se on suojattu salasanalla ja ettei salasana ole helposti arvattava. Jos laitteet ovat uusia, saattaa niistä löytyä mahdollisuus vielä turvallisemman WPA3-salaustekniikan käyttöön, jota kannattaa hyödyntää. Esimerkiksi vuonna 2015 Kiuruvedellä ihmeteltiin lypsyrobotin puhelinliittymästä tullutta suurta puhelinlaskua.

Maatilan langattoman verkon salasanan selvittänyt sivullinen oli ohjannut tilan lypsyrobotin soittelemaan palvelunumeroihin yli tuhannen euron edestä

(Lypsyrobotti soitteli yli tonnin laskun – Hakkeri jätti jälkeensä viestin 2015).

Tällaisten laitteiden väärinkäytöksiä voi hillitä asettamalla niiden käyttämiin puhelinliittymiin muun muassa palvelunumeroiden estot. Tiloilla voi olla useita SIM-kortillisia laitteita, jotka lähiverkon sijaan kommunikoivat pelkän mobiilidatan välityksellä (Laajalahti & Nikander 2017, 12).

Päivitykset

Laitteissa ja ohjelmistoissa ilmenee jatkuvasti ”aukkoja”, joita pahantahtoinen toimija voi hyödyntää. Tietoturvapäivitykset sisältävät korjauksia tällaisiin havaittuihin tietoturva-aukkoihin, joten päivitysten käyttöönoton tulisi olla säännöllistä. Kannattaa selvittää, mitä kautta minkäkin laitteen päivittäminen tapahtuu ja jos mahdollista, asettaa käyttöön automaattiset päivitykset.

Lisätietoja erityisesti modeemien ja reitittimien päivittämisestä, sekä ohjeita eri operaattoreiden tuotteiden päivittämiseen löytyy Kyberturvallisuuskeskuksen ohjeesta: Muista laitteiden, ohjelmistojen ja sovellusten päivittäminen!

Tietoa ajankohtaisista haavoittuvuuksista:
https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

Vanhentuneet laitteet

Vanhat tietoverkkoon kytketyt laitteet ja ohjelmistot, joihin ei tuoteta enää uusia päivityksiä, lisäävät riskiä joutua kyberhyökkäyksen uhriksi. Maatilan laitteiden elinkaari on tyypillisesti varsin pitkä, jopa kymmeniä vuosia, kun taas tietokoneen tai mobiililaitteen sen sijaan vain muutamia vuosia. Tästä johtuen esimerkiksi maatilan automaatioon kytketty käyttöjärjestelmä voi vanhentua huomattavasti itse laitteita nopeammin. (Laajalahti & Nikander 2017, 14.) Jopa Windows XP-käyttöjärjestelmää, jonka päivitykset loppuivat jo vuonna 2014, saattaa vielä löytyä maatilan tietoverkkoon liitetyistä koneista. Muita vanhentuneita käyttöjärjestelmiä ovat muun muassa Windowsin versiot Vista, 7 ja 8.

Huomioi vanhentuneiden laitteiden kanssa:

- Laitteet ja käyttöjärjestelmät, joihin ei ole enää saatavilla tietoturvapäivityksiä, olisi syytä vaihtaa uudempiin.
- Ellei vanhentuneita järjestelmiä voida uusia, kannattaa ne vähintäänkin irrottaa tietoverkosta, jos se vain on mahdollista.

Uudet hankinnat

Maatiloilla käytetään usein kotikäyttöön suunniteltuja tietokoneita ja verkkolaitteita, jotka eivät välttämättä kestä hyvin ulkorakennusten vaihtelevia ja pölyisiä olosuhteita. Sopivien laitteiden valitsemisessa kannattaakin turvautua asiantuntija-apuun, jotta ne kestävät haastavia olosuhteita, ovat oikein mitoitettuja käyttötarkoitukseensa ja kyberturvallisuus on huomioitu niissä mahdollisimman hyvin. Esimerkiksi eläinsuojat ovat vaativia toimintaympäristöjä pölyn ja likakerrostumien vuoksi. Herkkien laitteiden sijoittaminen niihin kannattaa miettiä niin, etteivät ne ole alttiita sään vaihtelulle. Pölyisiin tiloihin sopivat paremmin passiivijäähdytteiset laitteet. Jos käytetään aktiivijäähdytteisiä laitteita, niiden tulisi olla suunniteltu kestämään pölyisiä olosuhteita, tai muuten niiden puhtaudesta on huolehdittava säännöllisesti. (Laajalahti & Nikander 2017.)

Myös laitteiden laajennettavuus kannattaa huomioida, esimerkiksi siten, että kytkin on mitoitettu nykyistä tarvetta suuremmaksi ja vapaita portteja on myös tulevaisuutta ajatellen (Manninen 2018, 58). Laitteiden hankinnassa kannattaa suosia sellaisia, joista löytyy Kyberturvallisuuskeskuksen myöntämä tietoturvamerkki: https://tietoturvamerkki.fi/fi/vaatimukset

Kaapelointireititkin on suunniteltava olosuhteet ja eläinten käyttäytyminen huomioiden. Asuinkäyttöön tarkoitetun asuinkiinteistön, toimitilakiinteistön ja julkisen kiinteistön sisäverkkojen suunnittelussa, rakentamisessa ja ylläpidossa sovelletaan Liikenne- ja viestintäviraston määräystä 65 D/2019. Määräys 65 kiinteistön sisäverkoista ja teleurakoinnista ei koske maatilan tuotantorakennuksia, mutta se toimii silti hyvänä ohjeena laadukkaan verkon rakentamiseen. (Manninen 2018, 15.) Määräys 65 D/2019 on luettavissa Liikenne- ja viestintäviraston sivuilta: https://www.traficom.fi/fi/sisaverkot

VPN-yhteydet

Yksityisyyden suojan parantamiseksi tietokoneilla ja älylaitteilla voi ottaa käyttöön myös VPN-yhteyden eli virtuaalisen erillisverkon. Internetiin suuntautuva liikenne kulkee salattuna VPN-palvelimen kautta, ja käyttäjän oikea sijainti ei paljastu muille, eivätkä ulkopuoliset voi seurata verkkoliikennettä. Esimerkiksi nettisivuilla olevat seurantaohjelmat eivät saa kerättyä tietoa netin käytöstä. Kannattaa kuitenkin varmistaa palveluntarjoajan luotettavuus, esimerkiksi kaikki ilmaiset VPN-palvelut eivät välttämättä ole turvallisia. (Mikä on VPN? nd.)

Suomalaisia VPN-palveluita saa käyttöönsä muun muassa seuraavilta tahoilta:

- ✓ F-Secure https://www.f-secure.com/fi/home/articles/what-is-a-vpn
- ✓ Elisa https://yrityksille.elisa.fi/vpn-suojattu-etayhteys
- ✓ Telia https://www.telia.fi/asiakastuki/palvelut/freedome-vpn
- ✓ DNA https://www.dna.fi/tietoturva/vpn

Varajärjestelmät

Varavirta

Tuotannon jatkuminen ja kriittisten järjestelmien toiminta on syytä varmistaa sähkökatkon varalta. Tätä varten on ensin tunnistettava mitkä järjestelmät ovat tuotannon kannalta kriittisiä. Maatilan tuotantolaitteiden sähkönsaanti on usein varmistettu varajärjestelmin, mutta niitä ohjaavat tietokoneet eivät kuitenkaan välttämättä ole varavirran perässä. Niidenkin virransaanti olisi tärkeää varmistaa UPS-varavirtalähteillä, jotta tuotantolaitteita voidaan niiden kautta valvoa ja ohjata. Varavirtalähteiden lisäksi on syytä miettiä tarvittavat maadoitukset ja ylijännitesuojaukset. (Laajalahti & Nikander 2017, 24.)

Nettiliittymät

Hyvä käytänne internetyhteyden varmistamiseen on, että kaapeliliittymän lisäksi varalla on myös mobiiliyhteys. Palomuurilaitteilla voidaan mahdollistaa katkotilanteessa myös automaattinen vaihto varayhteydelle. Varmuutta tuo myös useamman eri operaattorin liittymien käyttö. Suomessa mobiiliverkon tukiasemat on varustettu akustoilla, jotka pitävät verkon toiminnassa sähkökatkon aikana 2–6 tuntia, ja pitkässä katkossa niitä voidaan tarvittaessa käydä lataamassa myös polttoainekäyttöisellä varavoimalla. (Näin varaudut pitkiin sähkökatkoihin 2019.)

Pankkitunnistautuminen

Pankkitunnistautumista vaativien palveluiden ongelmiin voi varautua ottamalla käyttöön useamman kuin yhden pankin sähköisen tunnistautumisen. Lisäksi puhelinliittymän mobiilivarmenteen avulla voi tunnistautua palveluihin ja viranomaisten järjestelmiin, jos varmenne on aktivoitu. Myös henkilökortin kansalaisvarmennetta voi käyttää tunnistautumiseen. Tätä varten tarvitaan erillinen kortinlukija ja ohjelmisto. Hyvä käytäntö on tehdä tunnistautumista vaativat toimet hyvissä ajoin, ennakoiden mahdolliset ongelmatilanteet. (Näin sinä voit varautua mahdollisen Nato-jäsenyyden aiheuttamiin kyberuhkiin 2022.)

Lisätietoja mobiilivarmenteen käyttöönotosta:

- Elisa https://elisa.fi/varmenne/
- Telia https://www.telia.fi/asiakastuki/palvelut/mobiilivarmenne
- DNA https://www.dna.fi/mobiilivarmenne

Ohjeet kansalaisvarmenteen käyttöön löytyvät Digi- ja väestötietoviraston sivuilta: https://dvv.fi/kansalaisvarmenne

Varmuuskopiointi

Tärkeistä tiedoista, jotka tallentuvat tilan omille laitteille, on syytä ottaa varmuuskopiot säännöllisesti. Tällöin esimerkiksi jonkin laitteen rikkoutuessa tai kiristyshaittaohjelman lukittua tietokoneen menetetyt tiedot pystytään palauttamaan kopioista. Paras tapa olisi, että varmuuskopiointi tapahtuisi automaattisesti tietyin väliajoin. Esimerkiksi eräässä keminmaalaisessa autovaraosaliikkeessä menetettiin kiristyshaittaohjelman takia asiakas- ja varastotiedot, eikä kassaa saatu auki.

Toimintaa päästiin jatkamaan kahden päivän tauon jälkeen, kun vanhalta koneelta löytyi kopio tietokannasta, vaikkakin tiedot olivat osittain vanhentuneet.

(Verkkohyökkäys lukitsi autotarvikeliikkeen kassat, salasi tiedot ja sulki ovet 2020.)

Varmuuskopio voi sijaita pilvipalvelussa tai fyysisellä laitteella, mieluiten molemmissa. Fyysistä tallennusvälinettä, kuten ulkoista kovalevyä tai DVD:tä, on varminta säilyttää eri rakennuksessa kuin missä tietoja käytetään, jolloin esimerkiksi tulipalossa molemmat tietovälineet eivät tuhoudu. Erityisen tärkeää on tunnistaa, mitkä tiedot ovat toiminnan jatkumisen kannalta merkittäviä ja mitoittaa varmuuskopiointi sen mukaan. Tietojen palauttamista varmuuskopioista kannattaa myös harjoitella aika ajoin.

Sähköisessä muodossa olevien sopimusten ja muiden asiakirjojen säilyvyys on myös turvattava. Maataloudessa sopimusten kesto voi olla jopa vuosikymmeniä. Tietojärjestelmien kehittyessä on varmistettava, että vanhentuneissa tiedostomuodoissa tal-

lennetut tiedot saadaan tarvittaessa luettua. Vanhentuneessa muodossa olevat tiedostot kannattaa muuntaa nykyaikaisempaan tallennusmuotoon. Mikäli tämä ei ole mahdollista, on pidettävä huoli, että vanhat sovellukset, jotka osaavat tiedostoja lukea, pysyvät käytössä tai ovat palautettavissa käyttöön. (Laajalahti & Nikander 2017, 31.)

Nykypäivänä monet maatilankin järjestelmät toimivat pilvipalveluna, eivätkä välttämättä tallenna tietoa tilan omille laitteille. Tällöin tietojen säilymisen varmistaminen on palveluntarjoajan vastuulla. Jos on epävarmaa, kenen vastuulla varmuuskopiointi jonkin järjestelmän kohdalla on, kannattaa se selvittää palveluntarjoajan tai järjestelmän toimittajan kanssa. Pilvipalvelun toimittajan luotettavuus kannattaa myös varmistaa, ettei esimerkiksi palvelun loppuminen pääse yllättämään.

Ohjeita pilvipalvelun valintaan, ja muun muassa siihen, millaista tietoa pilvipalveluissa kannattaa käsitellä sekä tietoa eri käyttötapausten riskeistä, löytyy Kyberturvallisuuskeskuksen oppaasta:

Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille

Tiedon turvallinen käsittely

Kuten missä tahansa yrityksessä, myös maatilalla tallennetaan luottamuksellista tietoa. Tällaisia voivat olla esimerkiksi työntekijöiden palkanmaksu- ja henkilötiedot, sopimukset, tukihakemukset ja -päätökset, tositteet, raportit ja kuitit. On syytä huomioida, että työsopimukset, terveystiedot, palkkalaskelmat ja muut henkilöihin liittyvät tiedot muodostavat mahdollisesti ns. henkilörekisterin. (Laajalahti & Nikander 2017, 28.) Tällaisen rekisterin ylläpito velvoittaa, että tietoa on käsiteltävä luottamuksellisesti ja turvallisesti niin, että tietoihin pääsevät käsiksi vain ne henkilöt, joilla on siihen todellinen tarve. Tietoa on käsiteltävä muutenkin asianmukaisesti, kerättävä vain tarpeellisessa määrin ja vain tiettyä laillista tarkoitusta varten.

Myös monenlaista vähemmän luottamuksellista tietoa saattaa tilalla tallentua erilaisista sensorijärjestelmistä, esimerkiksi lehmien käytökseen liittyvää dataa, tietoa eläinsuojien lämpötilasta ja kosteudesta tai pellon ravinnepitoisuudesta.

Laitteita uusittaessa on pidettävä huoli, ettei luottamuksellista tietoa sisältävää vanhaa laitetta kierrätetä huolimattomasti, vaan kovalevy tyhjennetään tai hävitetään niin, ettei tietoa voi päätyä väärin käsiin.

(Laajalahti & Nikander 2017, 28.)

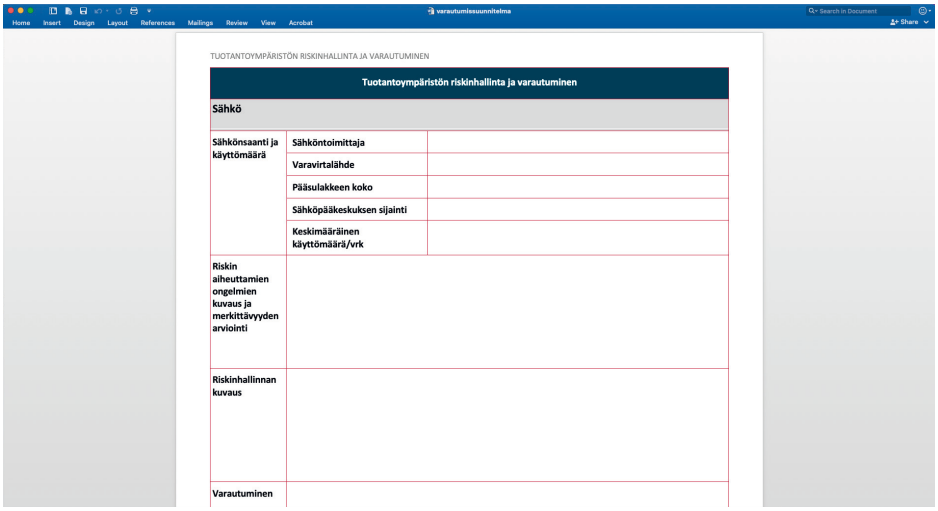
Vaikka nykypäivänä suuri osa tiedosta tallennetaan pilveen, on hyvä huomioida, että tiedoista saattaa jäädä kopioita tietokoneillekin.

Henkilötietojen käsittelyä koskevista tietosuojaperiaatteista löytyy lisätietoja tietosuojavaltuutetun toimiston sivuilta: https://tietosuoja.fi/tietosuojaperiaatteet

Varautumissuunnittelu ja riskienhallinta

Toiminnan jatkuvuuden varmistamisen kannalta on tärkeää, että jo ennakolta tunnistetaan mahdolliset riskit ja varaudutaan niihin. Riskit saattavat liittyä muun muassa toimintaympäristöön, laitteisiin tai henkilöihin. Poikkeuksellisten tilanteiden varalle on syytä laatia kirjallinen varautumissuunnitelma, joka auttaa tilanteista toipumisessa ja haittojen minimoimisessa. Varautumissuunnitelma on myös vaatimuksena muun muassa tarkastettaessa tiettyjä maatalouden tukia (Eläinvalvonnassa tarkastettavat asiakirjat 2019).

- MTK ja Huoltovarmuuskeskus ovat julkaisseet oppaan maatilan varautumiseen liittyen: Turvallinen tila – Opas maatilan varautumiseen (pdf)
- Hyvät ohjeet varautumissuunnitelman laatimiseen löytyvät Maavara-hankkeen sivuilta. Sivuilla voi mallitilojen kautta tutustua eri tuotantosuuntien riskienhallinta- ja varautumissuunnitelmiin. Varautumissuunnitelman mallipohjaa (Kuva 1.) kannattaa käyttää oman varautumissuunnitelman pohjana: https://maavara.savonia.fi/



TUOTANTOYMPÄRISTÖN RISKINHALLINTA JA VARAUTUMINEN

Tuotantoympäristön riskinhallinta ja varautuminen		
Sähkö		
Sähkönsaanti ja käyttömäärä	**Sähköntoimittaja**	
	Varavirtalähde	
	Pääsulakkeen koko	
	Sähköpääkeskuksen sijainti	
	Keskimääräinen käyttömäärä/vrk	
Riskin aiheuttamien ongelmien kuvaus ja merkittävyyden arviointi		
Riskinhallinnan kuvaus		
Varautuminen		

Kuva 1. Ote varautumissuunnitelman mallipohjasta (Varautumissuunnitelma nd)

Varautumissuunnitelmassa kartoitetaan muun muassa tilan tuotantoympäristö, tärkeät asiakirjat, vastuut sekä riskienhallinta ja varautuminen sähkönsaannin, vedensaannin ja eri prosessien osalta. Olennaisena osana varautumisessa on myös sidosryhmien tunnistaminen ja tärkeiden yhteystietojen kokoaminen. Maavaran riskienhallinta- ja varautumisohjeissa ei ole erityisesti otettu kantaa kyberturvallisuuteen. Varmista, että kyberturvallisuus on huomioitu osana riskienhallintaa. Apuna voit käyttää seuraavien kappaleiden tarkistuslistaa, vuosikelloa ja mallitilaa.

Kyberturvallisuuden tarkistuslista

Tarkistuslistaan on kerätty keinoja varautua alkutuotantoon kohdistuviin kyberpoikkeamatilanteisiin. Tulosta lista toimitilasi seinälle ja ruksi kohdat, kun ne ovat kunnossa!

Kyberturvallisuuden tarkistuslista

Kunnossa

- ☐ Panosta kyberturvallisuuteen, kouluta itseäsi ja muita työntekijöitä ajankohtaisiin uhkiin liittyen. Opettele tunnistamaan nettihuijaukset sekä muista tarkkaavaisuus sähköpostien, linkkien avaamisen ja omien tunnusten käsittelyssä. (Huijausviestit ja tietojenkalastelu s. 8)
- ☐ Käytä vahvoja salasanoja, vältä saman salasanan käyttöä eri tileillä ja vaihda salasanat säännöllisesti. (Salasanojen hyvät käytänteet s. 17)
- ☐ Älä anna omia tunnuksiasi ja salasanojasi kenenkään toisen käyttöön. Jokaiselle työntekijälle luodaan omat tunnukset tarpeen mukaan. (Salasanojen hyvät käytänteet s. 17)
- ☐ Vaihda laitteiden tehdasasetuksena tulleet salasanat vahvempiin. (Salasanojen hyvät käytänteet s. 17)
- ☐ Käytä mahdollisuuksien mukaan monivaiheista tunnistautumista. (Salasanojen hyvät käytänteet s. 17)
- ☐ Päivitä säännöllisesti käyttöoikeudet ja poista tunnukset käytöstä työntekijän työsuhteen päättyessä. (Salasanojen hyvät käytänteet s. 17)
- ☐ Käytä yrityksen hoitamiseen eri tietokoneita ja älylaitteita kuin kotikäyttöön. (Tietoverkon hyvät käytänteet s. 19)
- ☐ Varmista, että käytössä olevat langattomat verkot on suojattu vahvalla salasanalla. (Tietoverkon hyvät käytänteet s. 19)
- ☐ Kartoita verkkoon liitetyt laitteet ja laadi suunnitelma, jota noudattaen päivitykset saadaan käyttöjärjestelmiin, ohjelmistoihin ja laitteisiin mahdollisimman pian, kun niitä julkaistaan. Seuraa valmistajien tiedotteita. (Tietoverkon hyvät käytänteet s. 19)
- ☐ Pyri uusimaan vanhentuneet järjestelmät. (Tietoverkon hyvät käytänteet s. 19)
- ☐ Poista laitteilta ohjelmat ja palvelut, jotka eivät ole välttämättömiä. (Tietoverkon hyvät käytänteet s. 19)
- ☐ Harkitse VPN-yhteyden ottamista käyttöön. (Tietoverkon hyvät käytänteet s. 19)
- ☐ Uusia laitteita hankittaessa varmista, että tietoturva on huomioitu. Suosi laitteita, joista löytyy tietoturvamerkki. (Tietoverkon hyvät käytänteet s. 19)
- ☐ Suojaa laitteet fyysisesti luvattomalta käytöltä, mutta myös mahdollisuuksien mukaan haastavilta olosuhteilta. (Tietoverkon hyvät käytänteet s. 19)

- [ ] Tunnista kriittiset toiminnot ja suunnittele, miten toimitaan, jos järjestelmät eivät toimi, esimerkiksi mitä töitä voidaan tehdä manuaalisesti. (Varajärjestelmät s. 23)
- [ ] Sähkökatkon varalta varmista tuotantolaitteiden varavoima ja tarvittaessa painevesi. (Varajärjestelmät s. 23)
- [ ] Varmista, että myös tuotantoa ohjaavat tietokoneet ovat varavirtalähteen perässä. (Varajärjestelmät s. 23)
- [ ] Pidä varalla kiinteän nettiliittymän lisäksi mobiililiittymää. (Varajärjestelmät s. 23)
- [ ] Järjestä tietojen säännöllinen varmuuskopiointi ja useiden kopioiden säilyttäminen fyysisesti eri paikoissa, kuten ulkoinen kiintolevy, DVD, pilvipalvelu. Varmista myös, että osaat palauttaa tiedot varmuuskopioista tilanteen niin vaatiessa. (Varmuuskopiointi s. 24)
- [ ] Varmista henkilötietojen ja muiden arkaluontoisten tietojen asiallinen käsittely niiden koko elinkaaren ajalta. (Tiedon turvallinen käsittely s. 26)
- [ ] Asenna ja päivitä säännöllisesti virus- ja haittaohjelmien torjunta, mieluiten automaattisesti.
- [ ] Jos mahdollista, laita sähköpostisovelluksissa viestien sisältämät linkit ja kuvat pois käytöstä. (Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons 2022)
- [ ] Mieti etukäteen poikkeustilanteen viestintä. (Kriisi- ja häiriöviestintä kyberpoikkeamatilanteessa s. 34)

Seuraavat suositeltavat toimenpiteet saattavat vaatia asiantuntijan apua:

- [ ] Käytä palomuureja, estä kaikki paitsi välttämätön liikenne oman verkon ja internetin välillä. (Tietoverkon hyvät käytänteet s. 19)
- [ ] Salli liikenne valvontakamerajärjestelmiin vain niistä IP-osoitteista, joille se on välttämätöntä. (Tietoverkon hyvät käytänteet s. 19)
- [ ] Toteuta verkon segmentointi, edellytä segmentoinnin järjestämistä esimerkiksi laitetoimittajalta uusia järjestelmiä asennettaessa. (Tietoverkon hyvät käytänteet s. 19)
- [ ] Tee vain yhdet järjestelmänvalvojan tunnukset ohjelmistojen asentamista varten. Luo peruskäyttöön jokaiselle omat tunnukset, joissa ei ole järjestelmänvalvojan oikeuksia. (Tietoverkon hyvät käytänteet s. 19)
- [ ] Poista tarpeettomat etäyhteysohjelmat ja etäyhteyteen käytettävät RDP-portit käytöstä (Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons 2022). (Huijausviestit ja tietojenkalastelu s. 8)
- [ ] Ota käyttöön lokien kerääminen ja niiden seuranta. Lue Kyberturvallisuuskeskuksen vinkit: Näin keräät ja käytät lokitietoja

Laajempaan oman toiminnan arviointiin ja riskienhallintaan on olemassa myös muun muassa seuraavia ilmaisia työkaluja, jotka alkutuotannon osalta voivat soveltua lähinnä suurempien yritysten käyttöön:

- Kyberturvallisuuskeskuksen kybermittari yrityksen kyberturvallisuuden tilan arviointiin ja kehityskohteiden tunnistamiseen.
- VAHTI-ohje 22/2017. Riskienhallintatyökalu ja -ohje uhkien tunnistamiseen.

Kyberturvallisuuden vuosikello

Maatilan vuosirytmiin kuuluu useita kiireisiä ajanjaksoja. Kyberturvallisuuden varmistamisen toimenpiteet voidaan suurelta osin ajoittaa näiden sesonkien ulkopuolelle. Tätä varten voidaan laatia vuosikello, jossa toimenpiteet jaetaan sopiviin kohtiin kalenterivuotta. Osa toimenpiteistä saattaa olla useaan kertaan vuodessa toistuvia, osa kerran vuodessa toistuvia ja osa myös sesonkikauden läpi jatkuvia (10 kohtaa kyberturvallisuuden parantamiseksi matkailualalla 2021).

Vuosikellon tekeminen kannattaa aloittaa listaamalla kaikki toimenpiteet ja jatkaa sijoittamalla ne sopiviin ajankohtiin. Esimerkiksi kausikäyttöisten laitteiden tarkistus ja päivittäminen kannattaa ajoittaa tehtäväksi aina ennen niiden käyttöönottoa (Laajalahti & Nikander 2017, 18).

Lista voi näyttää esimerkiksi tältä:

- Varautumissuunnitelman päivittäminen.
- Salasanojen vaihto.
- Digitaalisen toimintaympäristön kartoitus/ kokonaiskuvan päivitys.
- Varmuuskopioinnin toiminnan tarkistaminen, palauttamisen harjoittelu.
- Ajankohtaisten uhkien kartoittaminen ja kyberturvallisuusosaamisen päivitys/kertaus.
- Käyttäjien käyttöoikeudet ajan tasalle.
- Valvontakamerajärjestelmien tarkastus fyysisesti ja ohjelmistojen päivitys.
- Antureiden ja työkoneiden fyysinen tarkastus ja päivittäminen.
- Tuotantotilojen verkkoon liitettyjen laitteiden fyysinen tarkastus ja päivitykset.

Kyberturvallisuuden vuosikello esimerkki

1. Varautumissuunnitelman päivittäminen.
2. Salasanojen vaihto.
3. Digitaalisen toimintaympäristön kartoitus/kokonaiskuvan päivitys.
4. Varmuuskopioinnin toiminnan tarkastaminen.
5. Päivitykset + fyysinen tarkastus antureihin/työkoneisiin.
6. Salasanojen vaihto.
7. Salasanojen vaihto & käyttäjien käyttöoikeudet ajan tasalle.
8. Päivitykset + fyysinen tarkastus valvontakamerajärjestelmiin.
9. Ajankohtaisten uhkien kartoittaminen & työntekijöiden kyberturvallisuusosaamisen kertaus/päivitys.
10. Päivitykset + fyysinen tarkastus tuotantotilan verkkoon liitettyihin laitteisiin.

Mallitila kyberturvallisuuden näkökulmasta

Päärakennus

- Osataan tunnistaa huijaukset.
- Ajankohtaisia kyberuhkia seurataan Kyberturvallisuuskeskuksen sivuilta.
- Yrityksen tietokoneet erillään kotikäytöstä.
- Virus- ja haittaohjelmantorjunta käytössä.
- Yrityksen laitteista poistettu pelit ja muut ylimääräiset ohjelmat.
- Vahvat salasanat sähköpostissa ja muissa tietojärjestelmissä.
- Kaikilla käyttäjillä omat tunnukset tarvittaviin palveluihin.
- Automaattisesti asentuvat päivitykset käytössä.
- VPN-yhteys käytössä.
- Varakeinot mietitty poikkeustilanteita varten.
- Säännöllinen varmuuskopiointi käytössä ja kopiot eri sijainnissa kuin alkuperäinen.
- UPS-varavirtalähde tuotantoa ohjaavissa/valvovissa tietokoneissa.
- Mobiili varayhteys kiinteän nettiliittymän lisäksi.
- Pankkitunnistautumiseen useita keinoja.
- Tietoa käsitellään asianmukaisesti (EU:n yleinen tietosuoja-asetus GDPR huomioiden).

Tuotantotilat

- Laitekanta kartoitettu ja kriittiset järjestelmät tunnistettu.
- Kriittiset järjestelmät varmistettu varavirralla.
- Harjoiteltu laitteiden uudelleenkäynnistämistä.
- Mietitty, miten toimitaan, jos järjestelmät ovat poissa käytöstä.
- Laitteet fyysisesti suojattu sekä luvattomalta käytöltä että haastavilta olosuhteilta.
- Luotu suunnitelma laitteiden ylläpitoon, päivittämiseen, fyysisen kunnon tarkastukseen, vanhentuneiden laitteiden/järjestelmien uusimiseen.
- Hankintoja tehdessä otettu huomioon tietoturvallisuus sekä laitteiden kestävyys haastavissa olosuhteissa.

Tilan tietoverkko

- Langaton verkko käyttää suojattua yhteyttä ja vahvaa salasanaa.
- Internetin suuntaan lähiverkosta näkyvät vain välttämättömät laitteet.
- Verkko jaettu osiin laiteryhmien mukaan.
- Hankitaan vain tietoturvallisia verkkolaitteita.

Pilvipalvelut

Vipu, Wisu, Wakka, Google Drive ym.

- Vahvat salasanat käytössä (jokaiseen palveluun eri salasana).
- Tärkeimmät tiedot varmuuskopioidaan pilveen.
- Käytetään palveluita, jotka tunnistetaan luotettaviksi.
- Käytetään monivaiheista tunnistautumista aina kun mahdollista.

Anturit ja työkoneet

Ravinnepitoisuus-, kosteus-, lämpötila-anturit, valvontakamerat, traktorit ym.

- Verkon kautta laitteisiin pääsee käsiksi vain siihen tarkoitetuilta tietokoneilta/älylaitteilta.
- Alkuperäiset salasanat vaihdettu.
- Puhelinliittymistä estetty palvelunumerot.

Kriisi- ja häiriöviestintä kyberpoikkeamatilanteessa

Skenaario:

Hakkeri tunkeutuu yrityksen tietojenkäsittely-ympäristöön ja horjuttaa kuluttajien luottamusta elintarviketuotantoketjuun

Tausta

Aviopari Hannu ja Kaisa Peltosella on alkutuotannon mikroyritys, automatisoitu lypsytila. Yritys on kartoittanut toimintansa sidosryhmät yhteystietoineen jo aiemmin osana yrityksen toimintaa. Sidosryhmätiedot on tallennettu tietokoneelle, ja ne on myös tulostettu. Sidosryhmälistauksessa on huomioitu, että mikäli sidosryhmälistaus sisältää tietoja, jotka eivät ole avoimesti verkosta saatavilla, huomioidaan henkilötietojen käsittelyyn (GDPR) liittyvät velvoitteet. Yritys on myös jo aiemmin listannut käyttämänsä tietojärjestelmät ja palvelut. Yritys on priorisoinut ne sen mukaan, miten tärkeitä ja olennaisia ne ovat yrityksen liiketoiminnan kannalta. Mikäli tietojärjestelmissä tai palveluissa tapahtuu katkoksia, häiriöitä tai vikaantumista, ne palautetaan toimintakykyisiksi tai korjataan priorisointilistauksen mukaisesti. Yrityksen viestintä- ja markkinointivastuu on sovittu Kaisa Peltoselle.

Lähtötilanne

Ulkopuolinen toimija hakkeroituu yrityksen valvontakamerajärjestelmään. Hakkerin pyrkimyksenä on kaapata valvontakameratallenteita, irrottaa tallenteet asiayhteyksistään ja liittää ne uusiin asiayhteyksiin luoden uusia tulkintoja. Hakkerin tarkoituksena on horjuttaa kuluttajien luottamusta elintarviketuotantoon ja aiheuttaa imago- ja liiketoimintahaittaa niin mikrotason yritykselle, lypsyrobottivalmistajalle kuin maitopohjaisia tuotteita myyville päivittäiskaupan toimijoille. Hakkeroinnin syy on ideologisen hyödyn tavoittelu.

Hakkeri tunkeutuu navetan valvontakamerajärjestelmään. Hän etsii kamerat, jotka kuvaavat lääkittäviä lehmiä sekä lypsyrobottia. Hän tunkeutuu myös yrityksen tietojenkäsittely-ympäristöön ja kopioi valvontakameratallenteet. Hakkeri editoi tallenteista uuden videon ja julkaisee sen. Avioparin yritys ja lypsyrobottivalmistaja ovat tun-

nistettavissa videolta. Video kommentteineen antaa mielikuvan, että lääkehoidossa olevien lehmien erottelumaito ohjataan erottelumaitolinjalta normaaliin maitolinjaan. Videossa näytetään myös päivittäiskaupan maitotuotteita. Video luo mielikuvan, että elintarviketuotantoketju käyttää tietoisesti ja tarkoituksella lääkehoidossa olevien lehmien maitoa maitopohjaisten elintarviketuotteiden raaka-aineena. Hakkeri kommentoi, jakaa ja linkittää materiaalia valeprofiileilla eri somealustoille.

Aviopari alkaa saada palautetta ja yhteydenottoja kuluttajilta, elintarviketuotantoketjun toimijoilta ja medialta eri viestintäkanavien kautta. Yhteydenottojen myötä selviää, että avioparin liiketoiminnan tietojenkäsittely-ympäristöön on tunkeuduttu, valvontakameratietoa varastettu ja sen sisältöä on muokattu sekä muokatun sisällön kautta heidän yrityksensä on saatettu maalittamisen kohteeksi.

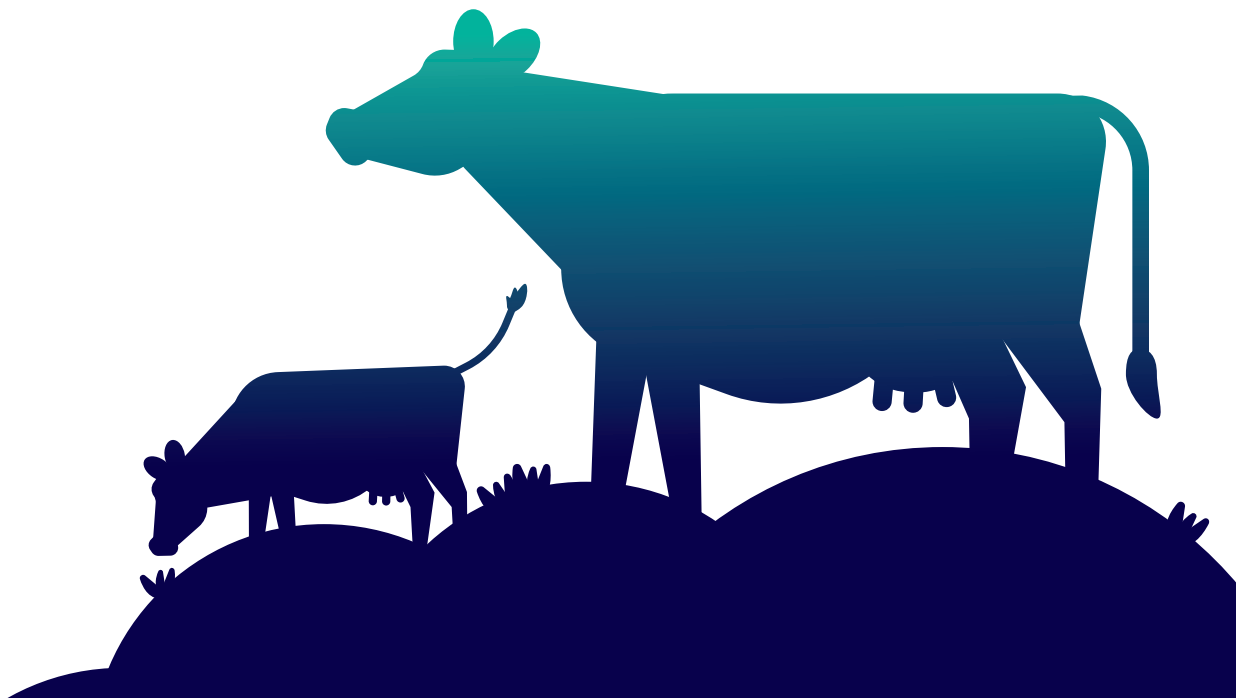
Toimenpiteet

Aviopari

- Turvaa ihmisten ja eläinten turvallisuuden tarkistamalla korkeimmalle tasolle priorisoidut järjestelmät ja palvelut kuten lypsyjärjestelmän, -robotin sekä valvontakameran järjestelmineen.
- Rajaa tapahtuneen haitat olemassa olevan tiedon mukaan estäen lisähaittojen synnyn.
- Kartoittaa tapahtuneen ja sen vaikutukset.

Viestintä sidosryhmille

Kaisa Peltonen määrittelee, onko tapahtuneessa kyse normaali- vai poikkeustilanteen viestinnästä, ja toimii sen mukaisesti. Kaisa tunnistaa sidosryhmälistasta sidosryhmät, joiden tulee saada tietoa juuri tästä tapahtumasta lainsäädäntöön perustuen, viranomaisvelvoitteena, osana alkutuotannon tuotantoketjua tai yleisen kiinnostavuuden nimissä.



Kaisa tunnistaa sidosryhmien tiedonsaannin tärkeys- ja kiireellisyysjärjestyksen ja mitä tietoa kukin sidosryhmä tarvitsee. Kaisa viestii sidosryhmille joko sidosryhmien kanssa etukäteen sovituilla tai sidosryhmien tilanteeseen tarkoittamilla viestintäkanavilla. Mikäli viestinnän muotoa ei ole etukäteen sovittu kunkin sidosryhmän kanssa, Kaisa rakentaa tilanne- ja sidosryhmäkohtaisen viestinsä vastaamalla seuraaviin kysymyksiin: **kuka, mitä, kenelle, miksi, milloin, miten**. Kaisa käyttää viestin rakentamiseen tilanneharkintaa ja viestii tapahtuneesta riittävästi, mutta ei liikaa. Tarkoituksena ei ole kertoa tapahtuneesta mahdollisimman laveasti, vaan ainoastaan riittävästi vastaamaan kunkin sidosryhmän tiedontarpeeseen.

Sidosryhmien tunnistus

Kaisa tunnistaa sidosryhmät, joille viestii tapahtuneesta. Lainsäädännön velvoittamaa viestintää ei tarvita tässä tapauksessa, koska tunkeutuminen ei ole aiheuttanut toiminnallista haittaa yritykselle tai sen liiketoiminnalle.

Viranomaiset:

- Poliisi.
  - › Rikosilmoituksen teko https://poliisi.fi/tee-rikosilmoitus.
- Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus.
  - › Ilmoituksen teko ilmoituslomakkeella.

Asiakkaat, kumppanit, alihankkijat:

- Meijerille ilmoitus.
  - › Yrityksen tietojenkäsittely-ympäristöön on tunkeuduttu.
  - › Navetan valvontakameroiden tallenteita varastettu.
  - › Tallenteita on editoitu ja niistä julkaistu video, joka levittää mielikuvaa, että lääkehoidossa olevien lehmien erottelumaito ohjataan erottelumaitolinjalta normaaliin maitolinjaan. Lisäksi elintarviketuotantoketju (mukaan lukien meijeri) käyttää tietoisesti ja tarkoituksella lääkehoidossa olevien lehmien maitoa maitopohjaisten elintarviketuotteiden raaka-aineena.

Palveluntarjoajat tai palvelun toimittajat:

- Lypsyjärjestelmän toimittajalle tai toimittajan tukeen ilmoitus.
  - › Yrityksen tietojenkäsittely-ympäristöön on tunkeuduttu.
  - › Navetan valvontakameroiden tallenteita on varastettu.
  - › Tallenteita on editoitu ja niistä julkaistu video, joka levittää mielikuvaa, että lääkehoidossa olevien lehmien erottelumaito ohjataan erottelumaitolinjalta normaaliin maitolinjaan. Lisäksi elintarviketuotantoketju (mukaan lukien lypsyjärjestelmän toimittaja ja lypsyrobotti) käyttää tietoisesti ja tarkoituksella lääkehoidossa olevien lehmien maitoa maitopohjaisten elintarviketuotteiden raaka-aineena.

- Yrityksen tietojenkäsittely-ympäristöstä vastaavaan IT-tukeen ilmoitus.
    - › Yrityksen tietojenkäsittely-ympäristöön on tunkeuduttu.
        - » Tutkinta, miten/mistä ympäristöön on tunkeuduttu.
        - » Tutkinta, mitä ympäristössä on tehty.
    - › Navetan valvontakameroiden tallenteita varastettu.
        - » Tutkinta, mitä tallenteita on varastettu.
        - » Tutkinta, mitä ympäristössä on tehty.
- Valvontakamerajärjestelmän toimittajalle ilmoitus.
    - › Navetan valvontakameroiden tallenteita on varastettu.
        - » Ilmoitus varastamisesta.
        - » Ilmoitus tallenteiden muokkaamisesta uudeksi materiaaliksi.
- Operaattoreille ilmoitus.
    - › Yrityksen tietojenkäsittely-ympäristöön on tunkeuduttu ja navetan valvontakameroiden tallenteita on varastettu.
        - » Tutkinta, miten/mistä ympäristöön on tunkeuduttu (tietoliikenneyhteydet).
- Vakuutuslaitokselle ilmoitus.
    - › Yrityksen tietojenkäsittely-ympäristöön on tunkeuduttu.
    - › Navetan valvontakameroiden tallenteita on varastettu.
    - › Tallenteista on editoitu video, josta aiheutuu imagohaittaa ja taloudellisia tappioita.
    - › Mitä vakuutuslaitoksen edellyttämiä ilmoituksia yritys on tehnyt (poliisille on tehty rikosilmoitus jne.).

Media:

Mikäli mediayhteydenottoja tulee, Kaisa:

- › Viestii samalla asiasisällöllä kuin meijerille.
- › Informoi lain edellyttämistä toimenpiteistä maidon testaamiseksi.
- › Kertoo esimerkkien kautta maidon testaamisen yrityksessä, maitokuormasta ja meijerillä.

Sidosryhmien priorisointi

Sidosryhmien priorisointi ja viestintäjärjestys viestinnän osalta juuri tässä skenaariossa on esitelty alla olevassa taulukossa (Taulukko 1.).

TAULUKKO 1. Sidosryhmien viestintäkanavien priorisointi ja viestintäjärjestys

Sidosryhmä	**Puh. nro**	**Sähköposti**	**Verkkosivun osoite (ilmoituslomake)**	**Viestintä-järjestys**
Meijeri	1	2	3	**2**
Kontaktin tiedot	*puh.*	*spostiosoite*	*ilmoituslomakkeen URL*	
Poliisi	1	-	2	**1**
Kyberturvalli-suuskeskus	2	-	1	**7**
Lypsyjärjestel-män tuki	1	-	2	**4**
Maatilan IT-tuki	1	-	2	**3**
Operaattori 1	1	-	2	**5**
Operaattori 2	1	-	2	
Vakuutuslaitos	1	-	2	**6**

Sidosryhmäkohtainen viestintä, esim. meijeri

Poikkeustilanteen viestintäkanavat tärkeysjärjestyksessä, esimerkki:

1. Soitto

2. Sähköposti

3. Sähköinen ilmoituslomake

Huomioi myös sidosryhmien viestintäjärjestys.

Soitto (meijerin poikkeustilanteen puhelinnumeroon)

Kaisa soittaa meijerille, antaa tilannetiedon puhelimessa. Soitto käynnistää meijerin oman viestintäketjun.

Tietosisältö

Kuka: Tilan tiedot.

Mitä: Viestin aihe:

- Yrityksen tietojenkäsittely-ympäristöön on tunkeuduttu.
- Navetan valvontakameroiden tallenteita on varastettu.
- Tallenteista on editoitu video. Video levittää mielikuvaa, että meijeri on osallisena:
  - › lääkehoidossa olevien lehmien erottelumaidon ohjaamisessa erottelumaitolinjalta normaaliin maitolinjaan ja
  - › siihen, että elintarviketuotantoketju (ml. meijeri) käyttää tietoisesti ja tarkoituksella lääkehoidossa olevien lehmien maitoa maitopohjaisten elintarviketuotteiden raaka-aineena.

Missä: Yrityksen osoite.

Milloin: Päivämäärä (pp.kk.vvvv), kellonaika.

Miten: Editoitu video on julkaistu useilla somekanavilla.

Miksi: Annetaan meijerille tilannetieto päätöksentekoa varten, jotta meijeri voi aloittaa tarvittaessa omat viestintätoimensa.

Sähköinen yhteydenotto (meijerin poikkeustilanteen sähköpostiosoitteeseen tai ilmoituslomakkeella)

Välittömästi puhelun jälkeen sama tietosisältö välitetään sähköpostitse. Sähköposti varmistaa tiedon pysymisen eheänä.

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 tietojenkalastelupäilyistä, 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 6/2022. https://visitjyvaskyla.fi/professionals/wp-content/uploads/sites/2/2021/09/10-kohtaa-kyberturvallisuuden-parantamiseksi-matkailualalla.pdf

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

Eläinvalvonnassa tarkastettavat asiakirjat. 2019. Ohje Ruokaviraston sivustolla. Viitattu 6/2022. https://www.ruokavirasto.fi/viljelijat/tuet-ja-rahoitus/valvonta/elaintukien-valvonta/elainvalvonnassa-tarkastettavat-asiakirjat/

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

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

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

Laajalahti, M. & Nikander, J. 2017. Luonnonvara- ja biotalouden tutkimus 32/2017 - Alkutuotannon kyberuhat. Viitattu 5/2022.https://jukuri.luke.fi/bitstream/handle/10024/539088/luke-luobio_32_2017.pdf

Lahti, J. 2021. Yrityksen tietoturvallisen verkon suunnittelu, opinnäytetyö. Viitattu 8/2022. https://urn.fi/URN:NBN:fi:amk-2021052510960

Lypsyrobotti soitteli yli tonnin laskun – Hakkeri jätti jälkeensä viestin. 2015. Savon Sanomat. Viitattu 5/2022. https://www.savonsanomat.fi/paikalliset/3182499

Manninen, O. 2018. Cybersecurity in Agricultural Communication Networks - Case Dairy Farms, opinnäytetyö. Viitattu 8/2022. https://urn.fi/URN:NBN:fi:amk-2018121822276

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

Mikä on VPN? N.d. Artikkeli F-Securen sivustolla. Viitattu 8/2022. https://www.f-secure.com/fi/home/articles/what-is-a-vpn

Näin sinä voit varautua mahdollisen Nato-jäsenyyden aiheuttamiin kyberuhkiin. 2022. Yle. Viitattu 9/2022. https://yle.fi/uutiset/3-12440524

Näin varaudut pitkiin sähkökatkoihin. 2019. Puolustusministeriö. Viitattu 9/2022. https://www.defmin.fi/julkaisut_ja_asiakirjat/oppaat/nain_varaudut_pitkiin_sahkokatkoihin

Pidempi parempi – Näin teet hyvän salasanan. 2022. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 5/2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan

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

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

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

Varautumissuunnitelma. N.d. Maatilojen varautumisen työkalut –hanke. Viitattu 6/2022. https://www.savonia.fi/app/uploads/2021/08/varautumissuunnitelma.docx

Verkkohyökkäys lukitsi autotarvikeliikkeen kassat, salasi tiedot ja sulki ovet. 2020. Yle. Viitattu 8/2022. https://yle.fi/uutiset/3-11456333

Sanasto

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

GDPR
EU:n tietosuoja-asetus, joka säätelee henkilötietojen luottamuksellista käsittelyä ja kansalaisten oikeuksia tietosuojaan.

IP-osoite
Jokaisella verkkoon liitetyllä laitteella on yksilöllinen osoite, jonka se tarvitsee toimiakseen verkossa ja josta sen voi tunnistaa.

Konfigurointi
Laitteen tai ohjelmiston asetusten määrittäminen tiettyä tarkoitusta varten.

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

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

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

Kytkin
Tietoliikenteestä puhuttaessa tarkoittaa laitetta, joka välittää toisesta verkon osasta tulevan liikenteen edelleen siihen kytketyille päätelaitteille.

Reititin
Internetiin kytketty laite, joka jakaa internet-yhteyden muille verkon päätelaitteille.

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.

WLAN, WiFi
Langaton verkko, joka luodaan kiinteään verkkoon liitetyn reitittimen avulla.

WPA2
Salaustekniikka, jota käytetään langattomien verkkojen suojaukseen. Uudempi versio tästä on WPA3.

Käsikirjan sanasto on koottu hyödyntäen Sanastokeskuksen kyberturvallisuuden sanastoa ja Ylen Digitreenit sanastoa.

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.

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 alkutuotannossa -käsikirja kyberpoikkeamien hallintaan

Jyväskylän ammattikorkeakoulun Elintarviketuotannon ja -jakelun kyberpoikkeamanhallinnan julkaisut, osa 1/3

Ulkoasu ja kuvitus: Jamk / Heli Sutinen

ISBN 978-951-830-677-4 (PDF)

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

www.jyvsectec.fi

jamk | Jyväskylän ammattikorkeakoulu

Maa- ja metsätalous-ministeriö