Kyberturvallisuus automaattilypsytiloilla

Kyberturvallisuus osana tilan toimintakulttuuria

Päivi Hänninen

Maija Kinnunen

Opinnäytetyö, AMK
Lokakuu 2023
Maaseutuelinkeinojen tutkinto-ohjelma

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Hänninen, Päivi & Kinnunen, Maija

Kyberturvallisuus automaattilypsytiloilla. Kyberturvallisuus osana tilan toimintakulttuuria.

Jyväskylä: Jyväskylän ammattikorkeakoulu. Lokakuu 2023, 59 sivua.

Maaseutuelinkeinojen tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: Kyllä

Tiivistelmä

Tutkimuksessa tutkittiin automaattilypsyä harjoittavien tilojen sekä lypsyrobotteja toimittavien laitevalmistajien varautumista kyberturvallisuuden ja tietoturvan vaarantumiseen automaattilypsytilalla. Toimeksiantajana tutkimuksessa toimi Maa- ja Metsätaloustuottajain Keskusliitto MTK, jonka tavoitteena on edistää maanviljelijöiden, metsänomistajien ja maaseutuyrittäjien elinkeinon kannattavuutta sekä maaseutuvarallisuuden kestävää käyttöä. MTK on osa huoltovarmuusorganisaatiota, jossa poolien tehtävänä on seurata, selvittää, suunnitella ja valmistella oman alan huoltovarmuutta esimerkiksi kyberturvallisuuden osalta.

Tutkimuksen tavoitteena oli näkemyksen muodostaminen tekijöistä, joilla lisätään kyberturvallisuus osaksi tilan toimintakulttuuria. Tutkimus toteutettiin kvalitatiivisena eli laadullisena tutkimuksena. Aineistonkeruutapana käytettiin kyselylomaketta Maitoyrittäjät ry:n jäsentiloille sekä MTK:n Maitovaliokunnalle ja Maitovaltuuskunnalle. Lisäksi haastateltiin kolmea lypsyrobotteja toimittavaa laitevalmistajaa. Dokumentaatio toimi pohjana tietoperustan kirjoittamisessa.

Tutkimustuloksista analysoitiin automaattilypsytilallisten varautumista kyberuhkiin ja tietoturvan vaarantumiseen. Laitetoimittajien näkökulma toi lisäarvoa tutkimukseen, koska yhteistyö tilallisen ja lypsyrobottitoimittajan välillä on tiivistä. Tutkimuksen tuloksissa havaittiin, että tiloilla on kehitettävää varautumisen suhteen. Tilallisista vain neljännes piti kyberuhkaa todennäköisenä. Yrityksen tietoturvaa ajatellen kulunvalvonta on yksi tärkeimmistä asioista. Se oli käytössä neljäsosalla kyselyyn vastanneista. Maatiloilla tunnistetaan hyvin riippuvuus sähköstä. Jotta kyberturvallisuus saadaan osaksi automaattilypsytilan toimintakulttuuria, on tunnistettava riippuvuus tietotekniikasta ja siihen liittyvät riskit.

Avainsanat (asiasanat)

digitalisaatio, kyberturvallisuus, tietoturva, automaattilypsy, maatilan johtaminen,

Muut tiedot (salassa pidettävät liitteet)

-

jamk

Description

Hänninen, Päivi & Kinnunen, Maija

Cybersecurity in automated milking parlours. Cybersecurity as part of the farm culture.

Jyväskylä: JAMK University of Applied Sciences, October 2023, 59 pages.

Field of Natural Resources. Degree Program in Agricultural and Rural Industries. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

The research investigated the preparedness of automatic milking farms and equipment manufacturers supplying milking robots for cybersecurity and information security breaches on automatic milking farms. The study was assigned by the Federation of Agricultural and Forestry Producers (MTK), whose aim is to promote the profitability of farmers, forest owners and rural entrepreneurs and the sustainable use of agricultural and rural assets. MTK is part of a security of supply organization, where the pools are responsible for monitoring, analysing, planning and preparing security of supply in their own sector, for example in terms of cybersecurity.

The aim of the study was to develop a vision of the factors that make cybersecurity part of the operational culture of the farm. The study was implemented as a qualitative study. The data was collected by means of questionnaire for the member farms of the Dairy Farmers Association and the MTK Milk Committee and Milk Delegation. In addition, three equipment manufacturers supplying milking robots were interviewed. The documentation served as a basis for writing the knowledge base.

The research results were used to analyse dairy farmers' preparedness for cyber threats and information security risks. The perspective of the equipment suppliers added value to the study because of the close cooperation between the farmer and the milking robot supplier. The results of the study showed that farms have room for improvement in terms of preparedness. Only a quarter of the respondents thought the cyber threats are probable. Access control is one of the most important aspects of a company's security. A quarter of the respondents had it in place. The dependence on electricity is well recognized on farms. To make cybersecurity part of the culture of automated dairy farms, the dependence on information technology and the risks of it needs to be recognized.

Keywords/tags (subjects)

digitalisation, cybersecurity, information security, automatic milking, farm management,

Miscellaneous (Confidential information)

-

Sisältö

Kuviot

1 Kyberturvallisuus osana tilan toimintakulttuuria

Maitotilallinen menee aamulla navetan toimistoon ja avaa lypsyrobotin tuotannonhallintaohjelman. Tietokoneen käyttö on estetty. Puhelinsoitolla lypsyrobottilaitteita toimittavan yrityksen tukipalveluun selviää, että muillakin tiloilla on sama ongelma. Ongelman laajuus on selvityksessä. Mitä tilallinen ajattelee tässä tilanteessa? Ensimmäisenä on varmasti mielessä eläinten hyvinvoinnista huolehtiminen ja se, miten lypsy saadaan järjestettyä. Onko tuotannonhallintajärjestelmän sisältämä tieto tallessa? Milloin varmuuskopiointi on viimeksi tarkistettu?

Lypsykarjatilojen määrän vähentyessä ja tilakoon kasvaessa maatilat ovat yhä enemmän riippuvaisia digitaalisista palveluista ja järjestelmistä. Jäljelle jäävät tilat tehostavat tuotantoaan ja kasvattavat tuottavuutta. Tutkimuksen mukaan vuonna 2030 Suomessa tuotetusta maidosta 86 % tulee lypsyrobottitiloilta (Saarivaara & Pirttijärvi 2022). Teknologian lisäämisen avulla on mahdollisuus kasvattaa tuottavuutta, mutta se tuo samalla haasteita tietoverkoissa. Yksittäisen tilan näkyvyys tietoverkoissa ulospäin kasvaa. Eri järjestelmien ja palvelujen tuottama tieto on erittäin tärkeää yrityksen liiketoiminnan ja maatilan johtamisen kannalta. EU-direktiivit tiukentuvat ruokaketjussa kyberturvallisuuden osalta. NIS2 –direktiivi tuli voimaan joulukuussa 2022 ja siirtymäaika kansalliseen lainsäädäntöön on käynnissä. Tämä direktiivi asettaa toimijoille uuden minimitason kyberturvallisuusriskien hallintaan ja yrityksien vastuulla on huolehtia toimitusketjujen turvallisuudesta. Elintarvikkeiden valmistus, tuotanto ja jakelu kuuluvat direktiivin sovellettaviin aloihin. Opinnäytetyön tekemisen aikana ei ole vielä tietoa siitä, miten tämän direktiivin vaikutukset kohdistuvat maitotiloille. (NIS2:2022, 127–128.)

Tuotantorakennukseen mentäessä vaihdetaan tilan suojavaatteet, jotta uhka erilaisten eläintautien leviämisestä vältetään. Tämä on varautumista. Miten yrittäjä suojautuu tietoverkoissa, jotta lypsykarjatilan kriittiset tiedot, kuten lypsyrobotin tuottama tieto suojataan? Yrittäjän tietämyksen kasvattaminen ja erilaiset toimintaohjeet suojaavat sekä itseä että yritystoimintaa. Aikaisemmat aiheesta tehdyt tutkimukset ovat vahvistaneet oletusta, että maatiloilla on tarvetta tietoturvakoulutukselle sekä yleisille ohjeistuksille suojautumisesta kyberuhkia vastaan. Laajalahti ja Nikander (2017) ovat todenneet alkutuotannon kyberuhkia tutkiessaan kyberturvallisuuden osaamisen kehittämisen olleen ajankohtaista alkutuotannossa jo tuolloin (Laajalahti & Nikander 2017, 3). Kun tilalle hankitaan lypsyrobotti tai useampia, mukaan tulevat tietotekniikkaan liittyvät riskit sekä se,

miten oman alansa hallitseva yrittäjä osaa varautua kyberturvallisuuteen liittyviin ongelmiin ja tunnistaa riippuvuuden tietotekniikasta.

Opinnäytetyön tavoitteena on lisätä kyberturvallisuus osaksi tilan toimintakulttuuria. Tässä työssä automaattilypsy tarkoittaa sitä, että lypsytyön suorittaa lypsyrobotti. Automaattilypsyä harjoittava tilallinen on tiiviissä yhteistyössä lypsyrobotteja toimittavan yrityksen kanssa. Jotta kyberturvallisuuden toimintakulttuuria saataisiin luotua, tulee olla selvillä ajatuksista ja näkemyksistä sekä tilallisen että laitetoimittajan näkökulmista. Näihin päästiin käsiksi tilallisille osoitetun kyselyn ja laitetoimittajille suunnattujen teemahaastattelujen keinoin. Kyselyillä ja haastatteluilla saadun tiedon avulla osoitettiin esimerkkitilan avulla, mitä asioita huomioon ottamalla kyberturvallisuus saadaan osaksi tilan toimintakulttuuria.

Toimeksiantajana tässä opinnäytetyössä on Maa- ja Metsätaloustuottajain Keskusliitto MTK. Järjestö edistää maanviljelijöiden, metsänomistajien ja maaseutuyrittäjien elinkeinon kannattavuutta sekä maaseutuvarallisuuden kestävää käyttöä. MTK on osa huoltovarmuusorganisaatiota, jossa poolien tehtävänä on seurata, selvittää, suunnitella ja valmistella oman alan huoltovarmuutta esimerkiksi kyberturvallisuuden osalta. Opinnäytetyössä tehtiin kyselytutkimus Maitoyrittäjät ry:n automaattilypsyä harjoittaville jäsentiloille toukokuussa 2023. Kyselytutkimus laajennettiin toukokuussa toimeksiantajan toimesta jaettavaksi MTK:n maitovaliokunnan ja maitovaltuuskunnan kautta. Kolmen suurimman lypsyrobottitoimittajan varautumista kyberuhkiin ja yhteistyötä tilallisen kanssa kartoitettiin haastattelemalla laitteiden tietoturvasta vastaavia avainhenkilöitä toukokuussa 2023. Case -tutkimuksessa parannettiin esimerkkitilan avulla tilan varautumista kyberuhkiin. Opinnäytetyö on rajattu maidontuotantoon ja lypsyrobotteihin liittyviin järjestelmiin. Valittu lypsyjärjestelmä on maitotilan ydintoimintaa. Siirtyminen automaattilypsyyn lisää tilan verkkoliikennettä sekä näkyvyyttä tietoverkoissa ulospäin. Lisäksi ennuste on, että tulevaisuudessa maitoa tuotetaan yhä enemmän automaattilypsytiloilla. Pellot ja metsät sekä niihin liittyvät koneet ja laitteet on jätetty pois tutkimuksesta. Keskeiset käsitteet on määritelty asiatekstin yhteydessä.

Opinnäytetyö toteutettiin kahden henkilön yhteistyönä. Opinnäytetyön tekijöiden kiinnostus kyberturvallisuutteen heräsi agrologiopintojen Maatalouden uusi teknologia -opintojaksolla. Toisen opinnäytetyöntekijän automaattilypsyä harjoittava maatila oli mukana Jyväskylän Ammattikorkea-

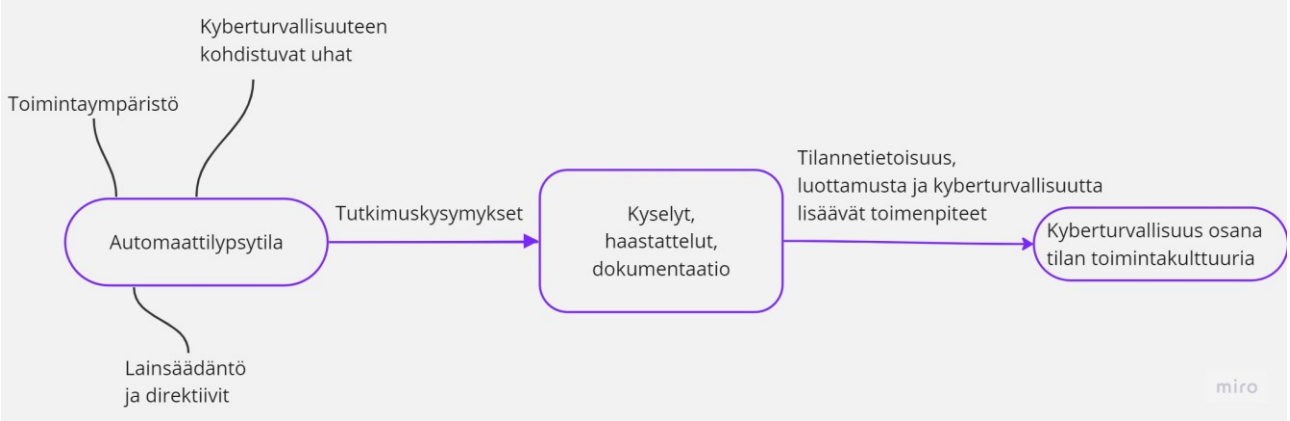
koulun Elintarvikeketjun kyberturvallisuus -hankkeessa. Molemmat opinnäytetyön tekijät osallistuivat opinnäytetyön alkuvaiheessa alkutuotannon pilottiharjoitukseen Jyväskylän ammattikorkeakoulun tiloissa ja kasvattivat tietämystään aiheeseen. Kahden henkilön osallistuessa aineiston keruuseen laadunarviointi on luotettavampaa. Tietoperustaa kirjoitettiin yhteistyönä. Aineistoja arvioitiin ensin itsenäisesti ja myöhemmin yhdessä. Maijan vastuualueena oli kyselytutkimuksen toteuttaminen ja Päivin vastuulla laitetoimittajien teemahaastattelut. Tiivistä tiedonvaihtoa käytiin lähes viikoittain. Toisen tekemän työn arvostus ja avoimuus säilyi koko opinnäytetyöprosessin ajan.

2 Viitekehyksenä kyberrakenne

Pirinen ja Rajamäki (2015) ovat määritelleet yhteiskunnan kriittisen infrastruktuurin digitaaliset palvelut kolmeen kerrokseen (kuvio 1), jota kutsutaan myös kyberrakenteeksi. Alustakerrokset muodostavat fyysisen verkon, johon sisältyvät laitteet. Kestävä fyysinen verkko on perusta, jonka avulla informaation jakaminen pystytään toteuttamaan eri sidosryhmien välillä ohjelmistokerrosta hyödyntämällä. Ohjelmistokerrokset käsittävät ohjelmistoverkon ja ihmiskerrokset sosiaalisen verkon. Verkon ja informaation käyttöä määrittelee sosiaalinen verkosto. Jaettavan tiedon määrää sosiaalisissa verkoissa määrittää luottamus, joten se olisi ymmärrettävä hyvin. Luottamuksen ja kyberturvallisuuteen liittyvien näkökohtien huomioiminen tulisi ulottaa järjestelmän kaikilla tasoille ja toimintaan liittyville verkostoille. (Pirinen & Rajamäki 2015.)

Kuvio 1. Digitaalisten palveluiden kolme kerrosta (Pirinen & Rajamäki 2015, muokattu).

Maatilalla alustakerrokseen kuuluvia fyysisiä laitteita ovat tietokoneet ja esimerkiksi erilaiset UPS-varavirtalaitteet sähköhäiriöiden varalle. Ohjelmistokerros muodostuu maatilan käyttämistä ohjelmistoista kuten tuotannonhallintaohjelmasta tai eläinrekisteriä ylläpitävästä Minun Maatilani -ohjelmistosta. Lypsyrobotteja voidaan käyttää ja huoltaa etänä käytettävillä ohjelmilla. Ihmiskerroksessa ovat tilalla työskentelevät ja ohjelmistoja käyttävät ihmiset sekä myös ohjelmistoja etänä käyttävät ihmiset. Nämä digitaalisten palvelujen kolme kerrosta ovat opinnäytetyömme viitekehys. Automaattilypsytilan toimintaa ohjaa toimintaympäristö, lainsäädäntö ja direktiivit sekä kyberturvallisuuteen kohdistuvat uhat (kuvio 2). Digitaalisten palveluiden kolme kerrosta huomioidaan tutkimuksen eri vaiheissa.



Kuvio 2. Tutkimustilanne

3 Tutkimusasetelma

Opinnäytetyön tavoitteena on parantaa automaattilypsytilojen varautumista kyberturvallisuusuhkiin ja lisätä kyberturvallisuus osaksi tilojen toimintakulttuuria. Alkutuotannon häiriötön toiminta osana elintarvikeketjua on tärkeää. Tutkimuskysymykset tässä opinnäytetyössä ovat:

1. Ovatko automaattilypsyä harjoittavat tilat varautuneet riittävästi kriittisen tiedon suojaamiseen ja säilyttämiseen?
2. Millaisia tarpeita tiloilla on kyberturvallisuuden suhteen ja miten ne saadaan kohdennettua nykytilanteeseen?
3. Miten lypsyrobottitoimittajat huomioivat kyberturvallisuuden tilallisen näkökulmasta?
4. Miten luodaan kyberturvallisuuskulttuuria automaattilypsytiloille?

3.1 Tutkimusmenetelmät

Tutkimuskysymyksiä ratkaistaan tutkimusmenetelmillä. Tällainen menetelmä on sääntö, keino tai menettelytapa, jolla voidaan saada ratkaistua kysymykset tai ongelma. Tutkimusmenetelmä täytyy valita tutkittavan ongelman mukaan. Tutkimusmenetelmän tavoite on tuottaa sellaista tietoa, jota voidaan pitää luotettavana ja jonka pohjalta voidaan ratkaista tutkimuskysymyksiä. (Kananen 2015, 64–65.) Opinnäytetyössä käytettiin tutkimusmenetelmänä kvalitatiivista eli laadullista tutkimusta. Lähtökohtana on todellisen elämän kuvaaminen, jolloin tapahtumat muovaavat samanaikaisesti toinen toistaan. Kohdetta pyritään tutkimaan mahdollisimman kokonaisvaltaisesti sekä löytämään ja paljastamaan tosiasioita. (Hirsijärvi, Remes & Sajavaara 2016, 161, 185–186.)

3.2 Aineistonkeruu- ja analyysimenetelmät

Kvalitatiivisen tutkimuksen aineistonkeruun menetelmiä ovat kyselyt, haastattelut, havainnointi ja dokumenttien käyttö (Hirsijärvi ym. 2016, 186). Tässä opinnäytetyössä aineiston keruu tehtiin Webropol -kyselyllä, teemahaastatteluilla, asiantuntijahaastatteluilla ja dokumenteilla.

Webropol -kysely lähetettiin ensiksi Maitoyrittäjät ry:n jäsentiloille. Kyselyn vastaanottajakuntaa laajennettiin lähettämällä kysely myös MTK:n Maitovaliokunnalle ja Maitovaltuuskunnalle. Kyselyn pohjana käytettiin Kyberturvallisuus alkutuotannossa -käsikirjaa, jonka päätavoitteena on tuottaa alkutuotannon toimijoille ymmärrystä kyberpoikkeamien hallintaan (Vertainen, Brandt & Suni 2023, 4). Teemahaastatteluilla haluttiin laitetoimittajien näkökulmaa maitotilojen kyberturvallisuuteen. Suomessa suosituimmat lypsyrobottien laitetoimittajat ovat NHK LeLy, DeLaval VMS sekä GEA (Mälkiä 2023, 7). Haastattelu tehtiin näille kolmelle suurimmalle laitetoimittajalle. Haastatteluihin osallistui yrityksen tietoturvasta vastaavat avainhenkilöt sekä yhden toimijan haastattelussa oli mukana myös tilaneuvoja. Haastattelut toteutettiin Teams -ohjelmalla. Haastatteluissa käytiin läpi, miten yritykset huomioivat tietoturvan uuden laitteen käyttöönottotilanteessa ja miten riittävästä tietoturvan tasosta huolehditaan jatkossa. Kyberturvallisuus automaattilypsytiloilla on varsin uusi aihe, joten asiantuntijahaastatteluilla saatiin parempaa ymmärrystä aiheeseen.

3.3 Luotettavuuden varmistaminen

Kvalitatiivinen tutkimus pyrkii ymmärtämään ilmiötä, joten on erityisen tärkeää, että tutkimustulokset ovat totuudenmukaisia eli ne vastaavat tutkittavaa ilmiötä. Tutkimuksessa tiedonhakeminen on suoritettu käyttämällä useita luotettavia lähteitä ja vältelty virhelähteiden käyttöä. Dokumentointi on tehty tarkasti tutkimusaineistosta, menetelmistä sekä analyysivaiheista. Laadullisessa tutkimuksessa tutkijoilla on mahdollisuus vaikuttaa tutkittavaan. Reaktiivisuutta on kuitenkin pyritty välttämään tutkimustulosten oikeellisuuden vuoksi. (Kananen 2015, 339, 353–355.)

4 Tietoperusta

Opinnäytetyön tässä osiossa käsitellään huoltovarmuutta, maatalouden rakennemuutosta sekä digitalisoitumisen mukanaan tuomia haasteita kyberturvallisuuden suhteen. Aiheen kannalta keskeisimmät käsitteet tietoturva ja kyberturvallisuus määritellään luvuissa 4.2 ja 4.3. Tiedon suojaaminen vaatii tilalliselta toimia sekä laitteistoilta ja järjestelmiltä ajantasaisuutta. Automaattilypsytilalliselta vaaditaan myös tilannetietoisuutta, jotta mahdollisilta uhkatilanteilta vältyttäisiin. Nämä edellä mainitut liittyvät maatilan johtamiseen.

4.1 Tuotantoympäristö

Alkutuotanto on osa elintarvikeketjua. Kotieläintuotanto on riippuvainen sähkö-, energia- ja vesihuollosta, kuljetuslogistiikasta sekä varsinaisista kotieläintuotantoa ohjaavista tietojärjestelmistä. Se on alkutuotannossa kasvinviljelyä haavoittuvampi tuotantomuoto. Kotieläintuotannon haavoittuvuutta ovat lisänneet alueellinen keskittyminen, kasvanut yksikkökoko sekä automaatio- ja konejärjestelmien yleistyminen. Uhat kohdistuvat samalla yritysten liiketoimintaan ja koko yhteiskunnan elintärkeisiin toimintoihin.

4.1.1 Huoltovarmuus

Huoltovarmuus tarkoittaa väestön ja yhteiskunnan elintärkeiden toimintojen turvaamisesta poikkeusoloissa ja kriisitilanteessa. Huoltovarmuus on yhteiskunnan kokonaisturvallisuuden taloudellinen omaisuus. Yhteiskunnan kokonaisedun kannalta huoltovarmuus toteutuu parhaiten, kun se huomioidaan yleisessä talous- ja elinkeinopolitiikassa. Huoltovarmuuden perusta on toimivissa markkinoissa ja kilpailukykyisessä taloudessa. (Kananen 2015, 7,301.)

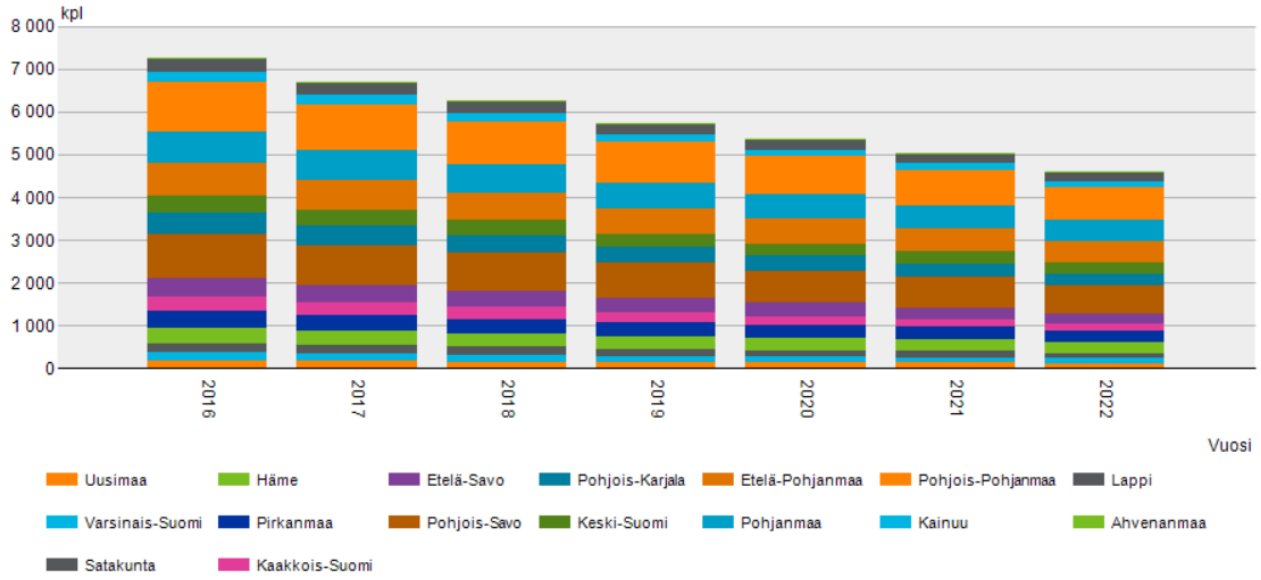
Suomen kyberturvallisuusstrategian mukaan vuonna 2013 visiona oli, että Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkia vastaan. Elinkeinoelämän varautumista koskevissa linjauksissa mainittiin tavoite, jossa ylläpidetään ja kehitetään yhteiskunnan elintärkeiden toimintojen turvaamista. Yritysten ja organisaatioiden kyvyllä havaita ja torjua kyberuhkia ja -häiriötilanteita sekä torjua niitä, on merkittävä rooli elinkeinoelämän jatkuvuuden kannalta. Huoltovarmuusorganisaatio sai tehtäväkseen tukea selvityksin, ohjeistuksin ja koulutuksin suojautumista kyberuhkia ja niiden aiheuttamia häiriöitä vastaan. (Kananen 2015, 274–275.)

EU päivitti kyberturvallisuussääntöjä NIS2-direktiivillä, joka tunnetaan myös verkko- ja tietoturvadirektiivinä. Direktiivi velvoittaa aloja, jotka ovat taloudelle ja yhteiskunnalle elintärkeitä. Direktiivin sovellettaviin aloihin kuuluvat elintarvikkeiden valmistus, tuotanto ja jakelu. Toimijoiden tulee direktiivin mukaan huolehtia kyberturvallisuudesta tarvittavilla turvatoimilla sekä ilmoittaa vakavista vaaratilanteista kansallisille viranomaisille. (Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) 2023.)

Väestön ja tuotantoeläinten ravinto turvataan elintarvikehuollolla häiriötilanteissa ja poikkeusoloissa. Mikäli kansallista maataloustuotantoa ei ole, yhteiskunnan kokonaisvarautuminen heikkenee. Yritykset huolehtivat osaltaan toiminnan jatkumisesta poikkeusoloissa varautumalla ja verkottumalla. Elintarvikehuolto turvaa riittävän alkutuotannon, elintarviketeollisuuden jalostuskapasiteetin sekä toimivan teollisuuden ja kaupan jakelujärjestelmän kuluttajille. (Huoltovarmuuskeskus.) Turvallisuusympäristön ennakoiva ja ajanmukainen seuranta sekä kyky havainnoida lähialueen lisäksi kauempaa tulevia uhkia on tärkeä osa huoltovarmuutta. (Fjäder n.d.,9.)

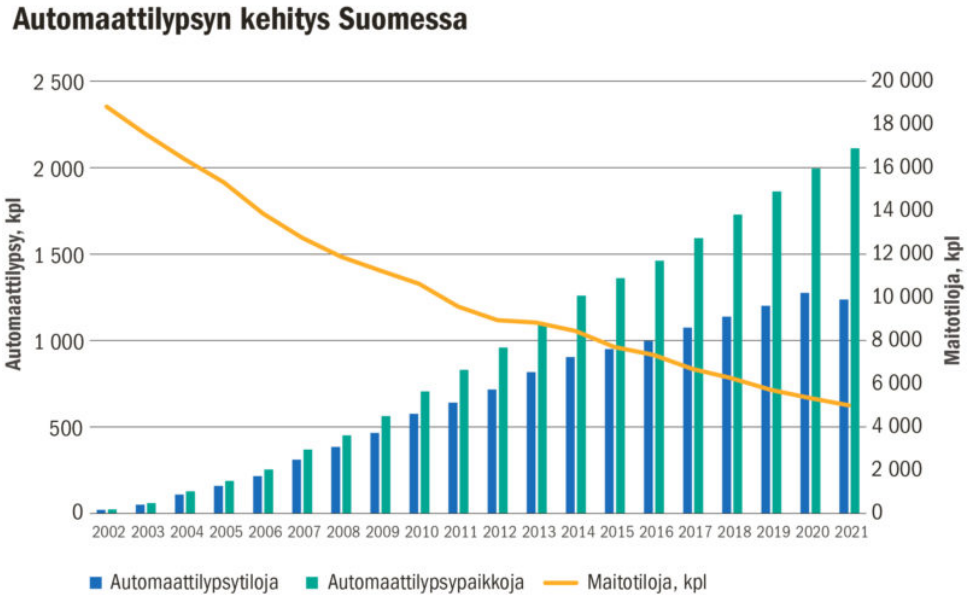
4.1.2 Maatalouden rakennemuutos

Maidontuotanto keskittyy tulevaisuudessa yhä suurempiin tuotantolaitoksiin. Luonnonvarakeskuksen tilastotietokannan mukaan (kuvio 3) vuonna 2016 lypsykarjatiloja oli 7276 ja vastaavasti vuonna 2022 tilojen lukumäärä oli 4584. Eniten tiloja vuonna 2022 oli Pohjois-Pohjanmaalla (784 kpl), toiseksi Pohjois-Savossa (648 kpl) ja kolmanneksi eniten Etelä-Pohjanmaalla (514 kpl). Kolmen Ely-keskuksen alueella oli 42 % kaikista Suomen lypsykarjatiloista. (Tilastotietokanta, Luke).



Kuvio 3. Lypsykarjatalouksien lukumäärät vuosina 2016 -2022 (Maatalous- ja puutarhayritysten lukumäärä tuotantosuunnittain ELY-keskuksittain 2023).

Kuviosta 4 nähdään, miten maatilojen lukumäärän vähetessä robottilypsy on kasvattanut suosiotaan 2000 –luvun alusta lähtien. Automaattilypsytilojen määrä oli 26 % kaikista maidontuotantotiloista vuoden 2021 lopussa (Maitohygienialiitto).



Kuvio 4. Automaattilypsyn kehitys Suomessa (Mälkiä 2023).

Valion keräämien tietojen, lypsyrobotteja maahan tuovien yritysten mukaan vuoden 2021/2022 vaihteessa Suomessa oli 1328 maitotilaa, joilla oli lypsyrobotti tai useampia. Automaattilypsy on lisääntynyt tasaisesti Suomessa ja vuoden 2021 aikana automaattilypsyyn siirtyi 52 tilaa. Keskimäärin automaattilypsytiloilla oli 1,59 lypsyrobottia. (Mälkiä 2023). Lypsykarjataloutta harjoittavien viljelijöiden keski-ikä oli 49 vuotta vuonna 2021 (Viljelijöiden keski-ikä tuotantosuunnittain 2021). Maatalouden kustannusten nousu, koronapandemia sekä valiolaisten meijereiden käyttöönottamat tuotantosopimukset ovat rajoittaneet maatilojen investointeja vuosien 2020–2022 aikana.

Digitalisaation kehittymisen myötä automatisaatio on keskiössä jatkavilla maatiloilla tulevaisuudessa. Ollakseen tarkoituksenmukainen ja taloudellisesti kannattava, moni nykyaikainen tuotantomenetelmä tai -teknologia vaatii riittävän suuren tuotannon (Koivumäki 2022.) Robotilla lypsettävän maidon ennustetaan kasvavan vuoteen 2030 mennessä niin, että 86 % tuotetusta maidosta tulee automaattilypsytiloilta. Vuonna 2021 osuus oli 50 %. (Saarivaara & Pirttijärvi 2022.) Jos jäljelle jää tulevaisuudessa 2500 tilaa, joilla on paljon digitalisaatiota, kotieläintuotannon haavoittuvuus lisääntyy merkittävästi.

4.1.3 Maatilan kriittiset tiedot

Digitalisaation kehittyminen maatiloilla lisää kerättävän ja säilytettävän tiedon määrää. Kerätyt tiedot ovat joko välttämättömiä tai lisäarvoa tuottavia maatilan toiminnan kannalta. Maatilan toiminnan kannalta tärkeät ja suojattavat tiedot ovat kriittisiä tietoja. Erityisesti lypsyrobotin tuottama tieto tulee kopioida säännöllisesti automaattisella varmuuskopioinnilla. Kriittisten tietojen säilyvyys tulee olla varmistettu. Suojaamalla kriittisiä tietoja suojataan omaisuutta ja toiminnan jatkuvuutta.

Tuotantoeläinten merkitsemisen ja rekisteröinnin tavoitteena on seurata elintarvikkeen kulkua tuotantoketjun alusta loppuun. Eläinten pitopaikoista ja siirroista sekä syntymistä ja kuolemista on pidettävä rekisteriä. Eläinrekisterin avulla varmistetaan myös eläinten hyvinvointi valvomalla eläinten syntymätiloja ja jatkokasvatuspaikkoja. Tuotantoeläinten merkitsemisellä ja rekisteröinnillä torjutaan myös eläintauteja. Tauteja voidaan torjua, kun tiedetään, missä taudille alttiita eläimiä on ja miten eläimiä on liikkunut tautialueelta pois. (Eläinten merkintä ja rekisteröinti 2023.)

Tuotosseuranta muodostuu maidontuotantotiedoista, joita kerätään tilalta. Tuotosseurantaan kuuluminen antaa maitotilan johtamiseen arvokasta tietoa yksittäisestä eläimestä sekä koko karjasta terveys- ja tuotostietoineen. Kerätystä tiedosta lasketaan tuloksia ja tietoa analysoidaan. Suomessa maitotiloista 73,4 prosenttia kuuluu tuotosseurantaan. Keskimääräistä isommista tiloista, missä on yli 60 lehmää, tuotosseurantaan kuuluu yli 90 prosenttia. (Lypsykarjan tuotosseuranta 2023.) Tuotosseurantaan kuuluvan tilan tiedot eivät ole pelkästään tilallisen hallussa, vaan ne ovat tallentuneena myös Minun Maatilani –ohjelmaan. Tuotostietoja tarvitaan myös tuotantokustannuksen laskentaan, joten ne liittyvät olennaisesti maatilan johtamiseen.

Päivittäisen työn kannalta tärkeitä tietoja ovat siemennykset, tiineystarkastukset, poikimiset, umpeenpanot, tunnutukset, kiimantarkkailun aloitukset, lääkittävien lehmien tiedot sekä varoajalliset hoidossa olleet eläimet. Eläinlääkintätiedot kertovat eläimen toimenpiteet sekä lääkityksen ja sen varoajan. Lääkehoidossa olevat varoajalliset eläimet ohjataan tuotannonhallintaohjelmassa erottelumaidoksi, jotta lääkejäämiä sisältävä maito ei ohjaudu tilasäiliöön. Elintarviketurvallisuuden kannalta erityisesti erottelumaidolla olevien lehmien tieto on tärkeä, jotta varoajallista lääkittyä lehmää ei lypsettäisi tilasäiliöön. Lääkekirjanpitoa pidetään nautojen terveydenhuoltojärjestelmä Nasevassa, ja sieltä voidaan tarkistaa lääkityn eläimen maidon ja lihan varoajat.

Tilitystietoja automaattilypsytilalla saadaan sekä maidosta että nautaeläimestä. Maidon tilitystiedoista käy ilmi tuotetun maidon määrä, rasva- ja valkuaispitoisuus, bakteerit, somaattiset solut sekä laatuluokka. Korkealaatuinen maito varmistaa tuottajalle parhaan tilityshinnan. Eläinrekisterin, kirjanpito- ja maataloustukiohjelmien osalta tilallisen on luotettava siihen, että palveluntarjoaja hoitaa varmuuskopioinnin.

4.1.4 Investoiva maatila

Investoitaessa isompiin tuotantorakennuksiin yrittäjän on huomioitava monia asioita. Tilan normaalien töiden ohessa yrittäjän on valmistauduttava rakennusprojektin suunnitteluun ja toteuttamiseen. Toiseksi on otettava huomioon karjamäärän ja peltopinta-alan kasvattaminen. Kolmantena on tuotannon kasvattaminen rakennusprojektin toteuttamisen jälkeen ja uuden tekniikan haltuunotto. Investoinnit ovat kalliita, joten yrittäjän on kiinnitettävä erityistä huomiota siihen, kuinka uudet lypsypaikat saadaan mahdollisimman nopeasti tuottamaan. Tämä kaikki saattaa kes-

tää hyvinkin noin viisi vuotta ja koko ajan on huolehdittava myös jo olemassa olevasta tuotannosta. Teknologian kehittyessä yrittäjän on löydettävä omalle tilalleen sopivat ratkaisut, joiden avulla kasvanut tuotanto pystytään hallitsemaan. Rakennustyömaalla liikkuu paljon erilaisia toimijoita urakkavastaavista työmiehiin. Samaan aikaan liikkuu myös paljon tietoa eri toimijoiden välillä.

Maatilan kasvaessa koti- ja kuluttajalaitteet eivät sovellu enää yrityskäyttöön. Tietoteknisissä laitteissa on siirryttävä yrityslaitteisiin, sovelluksiin ja palveluihin. Kun laitteita hankitaan, maatilakokonaisuutta ymmärtävien asiantuntijoiden merkitys korostuu. Kyberturvallisuus ja tietoturva ovat maatilan liiketoiminnalle erittäin tärkeitä, joten ne kannattaa suunnitella jo silloin, kun ollaan perustamassa tietojen käsittelyjärjestelmää ja ottamassa käyttöön uusia laitteita. Ohjelmistojen ja oheislaitteiden asennus, käyttäjäoikeuksien määrittely, maatilan tietoverkkoon liittyminen, tietojen siirtäminen aikaisemmista järjestelmistä sekä tietoturva ja varmuuskopioinnin määrittely vaativat asiantuntijuutta. (Kyberin taskutieto maatiloille 2018, 20–21.)

4.2 Tietoturva

Maatiloilla tietojärjestelmien määrät ovat lisääntyneet digitalisaation myötä. Ilman niitä maatilat eivät tule toimeen. Voidaan ajatella, että eläinten hyvinvoinnin kannalta tietotekniikka on elintärkeässä osassa. Ilman tietotekniikkaa ilmastointi, ruokinta, vedensaanti ja lypsäminen ei onnistu tai ainakin vaikeutuu erittäin paljon. Ennen muinoin ilman tietotekniikkaa on pärjätty, mutta silloin myös eläinmäärät olivat huomattavasti pienempiä. (Hietala, Ilomäki, Kotilainen, Laajalahti, Lassheikki, Luukkainen, Mantila, Moilanen, Niemi, Nikander, Nuutila & Tikkanen 2018.)

Maatiloilla tutkitaan eläimiä ja tuotoksia paljon, joten tietoa syntyy. Tiedon turvallinen tallentaminen ja sen säilyttäminen siten, että vain asianomaiset sen näkevät, on ensisijaisen tärkeää. Itse tieto syntyy laitteissa ja laitteistoissa, jotka pitävät sisällään tietotekniikkaa. Internet-yhteyden kautta saadaan tietoa liikuteltua tietojärjestelmiin. Tällaiset hankinnat on oltava harkittuja ja yhteensopivia, jotta eri järjestelmät toimivat yhteistyössä. (Hietala ym. 2018.)

Tämän opinnäytetyön keskeisimmät käsitteet ovat tietoturvallisuus ja kyberturvallisuus. Nämä ovat olennaisia käsitteitä, kun kehitetään kyberturvallisuuden toimintakulttuuria automaattilypsytiloille. Tiedon suojaaminen ja tietoon liittyvien järjestelmien toiminnan varmistaminen on molem-

pien käsitteiden idea, selkeä ero liittyy toiminnan tavoitteisiin (Järvinen 2018, 14). Tietoturva tiivistyy tiedon saatavuuteen, eheyteen ja luottamuksellisuuteen, kun taas kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin (Sanastokeskus 2018, 21–22).

Tietoturvan keskeinen ajatus on suojata tietoa, tiedostoja ja yksittäisiä koneita. Tietoturvan kanssa ollaan tekemisissä esimerkiksi silloin, kun tehdään varmuuskopioita tiedostoista tai asennetaan päivityksiä. Voidaan sanoa, että toimimalla tietoturvallisesti, saadaan suojattua toimintoja. Tietoturvaan liittyvät uhat ovat vahinkoja, kuten esimerkiksi laitteen putoaminen, levyn rikkoutuminen tai virheellisesti tärkeän tiedoston poistaminen. Tietoturvan uhkia on myös internetverkkoihin murtautuminen tai salasanojen urkkiminen. (Järvinen 2018, 14–15.)

Tietoturva pitää sisällään sekä hallinnollisia että teknisiä toimia. Näillä toimilla pyritään varmistamaan tiedon luottamuksellisuutta, eheyttä ja käytettävyyttä. Luottamuksellisuudella tarkoitetaan sitä, että tietty tieto on vain oikeutettujen saatavilla. Eheydestä puhuttaessa tarkoitetaan sitä, että vain oikeutetulla on oikeus muuttaa tietoja. Käytettävyys tarkoittaa nimensä mukaisestikin sitä, että tarvittava tieto ja tietojärjestelmät ovat oikeutettujen käytettävissä. (Tietoturva 2020.)

4.2.1 Tunnistautuminen

Tietojen suojaamisen edellytyksenä on, että tarvittava tieto on oikeiden ihmisten saatavilla. Tästä voidaan varmistua pyytämällä tunnistautuminen järjestelmään. Tunnistautumisella saadaan myös lokimerkintä, mikäli järjestelmässä tällainen on käytössä.

Ensinnäkin käyttäjä tulee todentaa, jotta käyttöoikeudet palveluihin ja järjestelmiin saadaan tarkastettua. Käyttäjätunnuksen salasana on yksi keino todentaa käyttäjä. Salasanan tarkoituksena on estää käyttäjätunnuksen mahdollinen luvaton käyttö. Käyttäjätunnus-salasanaparia pidetään heikkona käyttäjätunnistamisena. Tällöin salasanan laadulla on merkitystä. Riittävän pitkä salasana Kyberturvallisuuskeskuksen julkaiseman Salasanat -haltuun julkaisun mukaan on 15 merkkiä. Lisäksi merkkien sekä isojen ja pienien kirjaimien käyttäminen tekee salasanasta vahvemman. Myös salalausetta voi käyttää. (Salasanat haltuun n.d.)

Vahvasta tunnistamisesta puhutaan silloin, kun henkilö yksilöidään ja tunnisteen aitous ja oikeellisuus saadaan todennettua (Salasanat haltuun n.d). Tällainen menetelmä on henkilöllisyyden todentaminen sähköisesti vahvalla sähköisellä tunnistamismenetelmällä. Tällöin sähköisten palvelujen käyttäjä voi vahvistaa henkilöllisyytensä turvallisesti. Samalla palveluntarjoaja voi tunnistaa käyttäjän. Vahva sähköinen tunnistautuminen on käytössä kuluttajilla. Yleisimmät sähköiset tunnistuspalvelut ovat verkkopankkitunnukset, mobiilivarmenteet ja henkilökortin kansalaisvarmenteet. (Sähköinen tunnistaminen 2023.)

4.2.2 Käyttöoikeudet

Laajat käyttöoikeudet tuovat tietoturvariskin sekä käyttäjälle että organisaatiolle. Lähtökohtana käyttöoikeuksien antamisessa voidaan pitää sitä, että käyttäjällä tulee olla riittävät oikeudet, jotta työtehtävien suorittaminen onnistuu. Kun nämä täyttyvät, tulisi tämän jälkeen käytön olla estettynä. (Lindberg 2019.)

Lindberg (2019) kirjoittaa, että organisaation tulisi huolehtia, ettei tavallisella käyttäjällä ole järjestelmänvalvojan oikeuksia. Järjestelmänvalvojan oikeuksilla voidaan suorittaa sellaisia toimintoja, joita haittaohjelmien toiminta edellyttäisi. Pääsääntönä Lindbergin (2019) mukaan voidaan pitää sitä, että mikäli järjestelmänvalvojan oikeuksia ei tarvita, niitä ei anneta. (Lindberg 2019.)

4.2.3 Palomuurit ja virustorjuntaohjelmat

Digitaaliset ja näkymättömät palomuurit toimivat ikään kuin paloseinänä. Niiden tavoitteena on tulipalon sijasta estää epäilyttävä verkkoliikenne internetyhteydessä olevaan laitteeseen kuten tietokoneeseen. Palomuuri on tietokoneeseen asennuttu ohjelmisto, jolla estetään haitallinen verkkoliikenne. Se suojaa tietokonetta viruksilta ja lisäksi palomuuri tarkkailee laitteesta lähtevää liikennettä. Useimmissa laitteissa palomuuri on valmiiksi asennettuna, joten käyttäjän tarvitsee vain kytkeä se päälle. Palomuuri ei kuitenkaan yksin riitä suojaamaan vaan tarvitaan myös virustorjuntaohjelma. Palomuuri hallitsee saapuvaa ja lähtevää liikennettä, mutta se ei kykene tarkistamaan verkkoliikenteen sisältöä. Kunnollinen virustorjuntaohjelma tutkii ladattuja tiedostoja ja sivustoja, joilla käyttäjä vierailee. Se pysäyttää turvallisuutta uhkaavat uhat ennen kuin ne ehtivät aiheuttaa haittaa. (Mikä on palomuuri? n.d.)

4.2.4 Varmuuskopiointi

Varmuuskopioinnissa tieto kopioituu alkuperäisen tallennuspaikan lisäksi myös jonnekin muualle. Näin ollen, mikäli alkuperäiseltä tallennuspaikalta tiedot häviävät, ovat ne saatavissa käyttöön varmuuskopioinnin kautta. Varmuuskopioinnissa pääsääntönä on, että mitä enemmän muutoksia tietoihin tulee, sitä useammin tiedostot tulee varmuuskopioida. Esimerkiksi automaattilypsytilalla uutta tietoa tulee jokaisen lypsykäynnin yhteydessä, joten varmuuskopiointi olisi hyvä suorittaa päivittäin. Varmuuskopioinnit voidaan säilyttää esimerkiksi verkkolevyillä tai pilvipalveluissa. Muistitikku tai ulkoinen kovalevy on myös yleinen tallennusväline. Erityisesti muistitikulla riski on katoamisessa tai rikkoutumisessa. Tämä riski tulee tiedostaa. (Tiedostojen varmuuskopiointi n.d.)

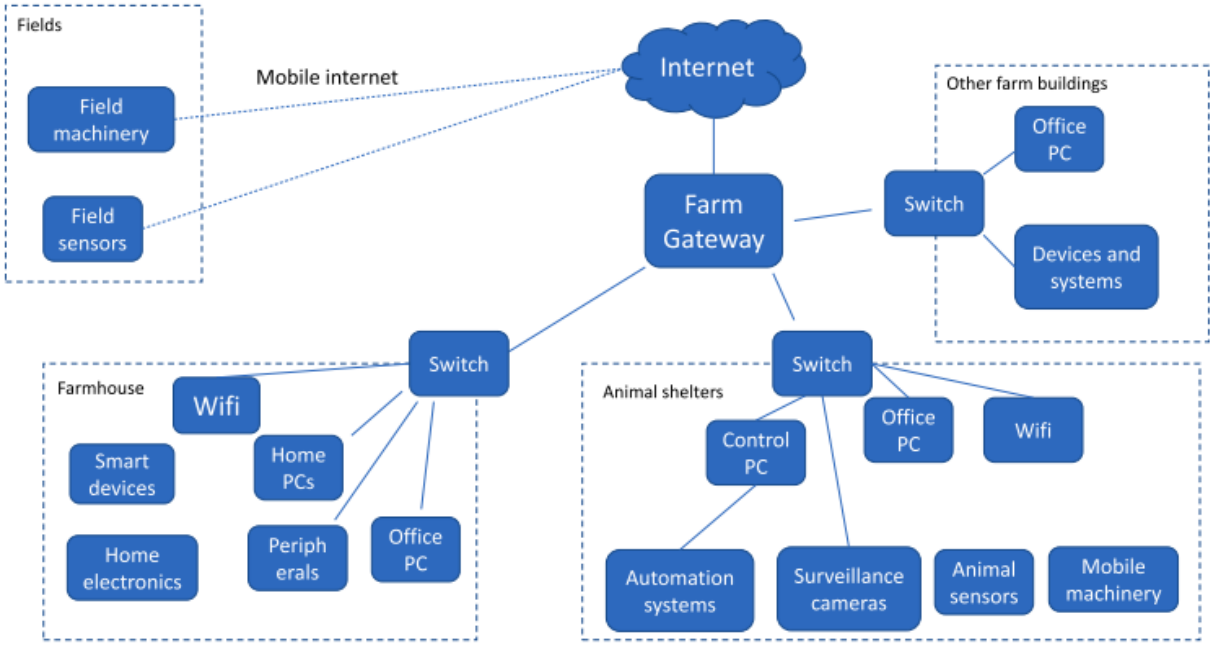
4.2.5 Tietoverkot

Maatalouden digitalisoituminen on jatkuva prosessi, joka tuo mukanaan sen, että yhä useammat maatalousjärjestelmät ovat yhteydessä toisiinsa internetin välityksellä. Järjestelmien lisääntynyt liitettävyys ja yhteydenpito toisiinsa sekä mahdollistaa parannuksia tuottavuuteen että tehostaa eri maatalousprosesseja. Monet näistä järjestelmistä ovat kriittisiä ja käyttökatkokset voivat nopeastikin heikentää karjan hyvinvointia ja aiheuttaa vahinkoa tilalle. Myös maatalousalalla on tullut ymmärrys siihen, että koneiden ja järjestelmien liittäminen internetiin tuo mukanaan mahdollisuuden joutua kyberuhkien kohteeksi. (Nikander, Manninen & Laajalahti 2020.)

Nykyaikaisen maatilan tarve tietoverkoilta on monisyinen, sillä monet maatalouden automaatiojärjestelmät ovat liitetty internetiin etävalvontaa tai -ohjausta varten. Tietoverkot mahdollistavat myös järjestelmätoimittajien etäkäytön huoltoja ja päivityksiä varten. Näiden lisäksi tiloilla saatetaan tarvita ulkopuolisia palveluita, kuten neuvonta- tai hallintapalveluita. Myös tilallisen internetin vapaa-ajan käyttö saattaa tapahtua saman sisäverkon ja internet-palveluntarjoajan kautta kuin muukin maatilan liiketoiminta. (Nikander ym. 2020.)

Kuviossa 5 on esitetty esimerkki maatilan tietoverkoista. Verkossa on neljä aliverkkoa, jotka sisältävät erilaisia internetiin liitettyjä tietokoneita ja laitteita: Pellot, maatilan asuinrakennus, eläinsuojat ja muut maatilan rakennukset. Tietoverkko voi olla langaton (WLAN) tai langallinen (LAN), ja sen internetyhteys voi olla mobiiliyhteydellä tai kiinteällä yhteydellä. Kuviossa 2 peltojen interne-

tyhteys tulee mobiiliyhteydellä ja muut tulevat kiinteällä yhteydellä. Nikander ja muut (2020) pohtivat esimerkissä olevan todennäköisesti aliverkkoihin kytkettynä suuri määrä laitteita, kuten toimiston päätietokone, muita työtietokoneita ja maatilan laitteita sekä myös yksityisiä tietokoneita ja laitteita. Nikander ja muut (2020) sanovat esimerkkitilalla olevan huomattava tarve jakaa maatilan verkko kahdeksi erilliseksi verkoksi: Toinen työlaitteilla ja toinen yksityisille ja vapaa-ajan laitteille. (Nikander ym. 2020; Kyberin tietoisku maatiloille 2018, 8.)



Kuvio 5. Esimerkki maatilan tietoverkosta (Nikander ym. 2020).

4.2.6 Kulunvalvonta

Kulunvalvonta on yhtenä osana yrityksen tietoturvaa. Suomalaisten organisaatioiden tietoturva 2023–2025-tutkimuksen mukaan se on yrityksen tietoturvaa ajatellen tärkeimpien asioiden joukossa (Suomalaisten organisaatioiden tietoturva 2023–2025 2022, 4–5). Kulunvalvonnan ideana on, että tiettyihin tiloihin pääsee vain tietyt henkilöt. Ilman tarvittavia oikeuksia henkilön kulku estyy. Sähköisen kulunvalvonnan hyötyinä on myös lokitieto.

4.3 Kyberturvallisuus

Kyberturvallisuudessa on kyse tietoturvasta, jota ulotetaan erilaisiin yhteiskunnan palveluihin suuremmassa kuvassa. Käsitteellä kyberturvallisuus tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta on turvattu. Kybertoimintaympäristö muodostuu yhdestä tai useammasta digitaalisesta tietojärjestelmästä. Tämä digitaalinen toimintaympäristö kehittyy yhteiskunnan osana ja palveluina nopeasti. Tällaisia ovat esimerkiksi elintarvikkeiden kuljetus- ja logistiikkajärjestelmä tai sähkön jakeluverkko. Tietoturva on keskeinen tekijä kyberturvallisuudessa, koska toteutunut tietoturvauhka aiheuttaa usein häiriötä kybertoimintaympäristön toimintaan. Kyberturvallisuuden uhkien voidaan sanoa olevaan vaikutuksiltaan laajempia kuin tietoturvaan liittyvät uhkakuvat. (Järvinen 2018, 14–15; Sanastokeskus 2018, 21–22.)

Kyberturvallisuus pyrkii suojaamaan laitteita ja niiden tietoa häiriöiltä ja hyökkäyksiltä. Kyberturvallisuudesta puhuttaessa tarkoitetaan kaikkia toimia ja ohjelmistoja, joilla pyritään turvaamaan tällaiset vaaratilanteet. Kyberturvallisuus nousee nykypäivänä aina vain suurempaan rooliin, sillä digitalisaatio lisääntyy ja internet ottaa yhtä enemmän roolia ihmisten arjessa tänä päivänä. Suomi on myös valtion tasolla panostanut kyberturvallisuuteen. Suomessa toimii Kyberturvallisuuskeskus Liikenne- ja viestintävirasto Traficomin alaisuudessa, joka tekee töitä kyberturvallisuuden eteen. (Mitä on kyberturvallisuus? 2022.)

Kyberturvallisuuden näkökulmasta tulee ensinnäkin tiedostaa riskit. Kyberriskit liittyvät maatiloilla usein sääoloihin. Niihin emme pysty vaikuttamaan, ainoastaan varautumaan. Sään ääri-ilmiöt lisääntyvät ja esimerkiksi myrskytuhot voivat aiheuttaa sähkökatkoksia ja vesivahinkoja. Myös ihmisten tekemät virheet ovat tiedostettava kyberriski. Tämän vuoksi ammattitaito ja osaaminen tietoteknillisten laitteiden käyttöön on oltava kaikilla tilan työntekijöillä. Toki virheitähän kaikille sattuu ja ihmisten kanssa toimiessa on muistettava inhimillisyys. Näitä tilanteita voidaan vähentää kouluttamalla henkilökuntaa. Lisäksi järjestelmien ja laitteiden käytön suunnittelu ennaltaehkäisee riskitilanteita. (Hietala ym. 2018.)

Kyberhyökkäyksiä voi olla suunniteltu tilaa vastaan, mutta useimmiten itse tilaan ei ole suoraan kohdistettu hyökkäystä. Kyse voi olla esimerkiksi haittaohjelmasta, joka on sattumanvaraisesti valikoitunut juuri kyseisen tilan ohjelmiston kohdalle. Haittaohjelman on mahdollista tunkeutua tilan

tietojärjestelmiin silloin, kun niitä ei ole riittävästi suojattu. Yksi esimerkki suunnitellusta tunkeutumisesta tilan tietojärjestelmiin on esimerkiksi silloin, kun navetan tai sikalan valvontakamerakuvaa kopioidaan ei-tarkoituksenmukaiseen käyttöön. (Hietala ym. 2018.)

Tietojen varmuuskopiointi on tärkeä osa kyberturvallisuutta. Ohjelmistoihin voidaan asentaa haittaohjelmia, jotka estävät tiedon saamisen tai jopa poistavat tiedon. Varmuuskopioita saatetaan tarvita myös tilanteissa, joissa varsinaista kyberhyökkäystä ei ole tapahtunut. Tällainen tilanne voi tulla esimerkiksi tulipalon sattuessa. Tällöin on hyvä olla varmuuskopiot, jotta kerätty tieto olisi edelleen käytettävissä.

Kyberturvallisuudesta huolehtimiseen maatiloilla on paljon keinoja. Maatilan tietoturvan ylläpitämiseen yksi yksinkertainen keino on järjestelmien päivitys. Voidaan jopa sanoa, että paras turva järjestelmille on päivittäminen. Tärkeänä osana ovat myös palomuurit. Ne rajoittavat esimerkiksi haittaohjelmien leviämistä. (Hietala ym. 2018.)

4.3.1 Informaatiovaikuttaminen

Tiedon luotettavuuden ja oikeellisuuden arviointi on vaikeaa, sillä saatavilla oleva tiedon määrä on suuri. Se, miten tietoa käytetään, hallitaan ja hyödynnetään strategisesti, on yhä suuremmassa merkityksessä. (Avoimesti, rohkeasti ja yhdessä - Valtionhallinnon viestintäsuositus 2016, 13.)

Informaatiovaikuttamisen keinojen katsotaan olevan osa kyberturvallisuutta. Informaatiovaikuttamisessa pyritään vaikuttamaan painostamalla tai ohjaamalla yleiseen mielipiteeseen, käyttäytymiseen tai päätöksentekoon. Näin saadaan vaikutettua myös yhteiskunnan kykyyn toimia. Esimerkkinä informaatiovaikuttamisen keinosta voidaan pitää väärän tai harhaanjohtavan tiedon levittämistä. Pyrkimys on saada strategisesti toimimalla vaikuttamisen kohde toimimaan itseään vastaan ja tekemään päätöksiä, jotka eivät ole kohteelle itselleen hyväksi. (Järvinen 2018, 15; Avoimesti, rohkeasti ja yhdessä - Valtionhallinnon viestintäsuositus 2016, 13.)

Informaatiovaikuttamisen vastakeinoja on myös olemassa. Tällaisia ovat esimerkiksi yhteistyö eri viranomaisten kanssa, medialukutaito ja yleissivistys. Oikea tapa reagoida virheelliseen tietoon ja sen levittämiseen, on nopea reagointi oikealla tiedolla. (Avoimesti, rohkeasti ja yhdessä – Valtionhallinnon viestintäsuositus 2016, 13.)

4.3.2 Kyberriskien merkittävyys

Digitalisaation kehittyminen uusien teknologioiden käyttöönoton myötä tuo mukanaan uhkia ja riskejä tietoverkoissa. Kyberturvallisuuden professori Limnéllin mukaan elämme maailmassa, jossa monet asiat ovat kietoutuneet yhteen. Kokonaisuuksien ymmärtäminen korostuu uhkien ja riskien torjunnassa. Sisäisen ja ulkoisen sekä yksilön ja yhteisön turvallisuuden raja-aidat ovat hämärtyneet. Tarkasteltaessa kyberiin liittyviä asioita turvallisuuden, talouden ja yhteiskuntapolitiikan näkökulmasta, saadaan paremmin selvyyttä vuorovaikutussuhteista ja tarvittavista toimenpiteistä. (Turvallisuutta tuotetaan yhdessä 2018.)

Kyberriskit ovat nousseet kärkisijoille riskiluokituksissa. Maailman talousfoorumi julkaisee vuosittain raportin globaaleista riskeistä. Raportin mukaan hyökkäyksiä odotetaan kohdistuvan huoltovarmuuden kannalta merkittäviin kohteisiin kuten maatalouteen, vesihuoltoon ja energiaan. Sekä seuraavien kahden että kymmenen vuoden tarkastelujaksoilla laajalle levinnyt tietoverkkorikollisuus ja turvallisuuden puuttuminen tietoverkoissa on globaalien riskien listalla kahdeksantena. (Global Risks Report 2023, 8,11.) Allianzin riskibarometrin julkaisemaan vuosittaiseen riskiluokitukseen on koottu 2712 riskienhallinnan asiantuntijan näkemys 94 eri maasta. Häiriöt tietoverkoissa ja liiketoiminnan keskeytyminen ovat yritysten suurimmat huolenaiheet jo toisena vuonna peräkkäin. (Allianz Risk Barometer 2023.)

Turvallisuusympäristömme muuttuu koko ajan ja siksi kyky ennakoida tulevaa on tärkeää. Niin Limnéll kuin Neittaanmäki, Lehto ja Savolainen (2021, 131) korostavat, että vaikuttaja pyrkii löytämään yhteiskunnan herkät ja haavoittuvat kohdat. Neittaanmäki ja muut (2021, 131) käsittelevät digitalisaation myötä syntyviä uusia uhkia yritysten luodessa yhä syvempiä ja reaaliaikaisia suhteita. Suhteita luodaan palvelun- ja tavarantoimittajiin, kumppaneihin, asiakkaisiin sekä julkishallintoon. Erilaiset informaatiovaikuttamisen muodot, palvelunestohyökkäykset, haittaohjelmat ja kyberhyökkäykset lisääntyvät yhteiskunnassa koko ajan. Kyberhyökkäysten valmistelua voidaan toteuttaa pitkään salassa, kun itse hyökkäys voidaan toteuttaa hyvin lyhyessä ajassa. Siksi aika on keskeisin kybermaailman muutosajuri. Kybermaailman rikolliset etsivät koko ajan uusia mahdollisuuksia varastaa, hyödyntää ja myydä tietoa. Tämän kehityksen takia on lisättävä varautumista kyberuhkiin ja -häiriötilanteisiin. (Turvallisuutta tuotetaan yhdessä 2018; Neittaanmäki ym. 2021, 131.)

4.3.3 Toimintaympäristö tilallisen näkökulmasta

Häiriötilanteet yritystoiminnassa voivat aiheutua toimintaympäristöstä, laitteista tai ihmisistä. Riskienhallinnan ja varautumisen avulla yritys voi hallita ja estää erilaisia häiriötilanteita. Varautumisen avulla säästetään aikaa kriisitilanteessa ja varmistetaan maatilan toiminnan jatkuminen mahdollisimman nopeasti kriisin jälkeen. Riskienhallinnan ja varautumisen toimenpiteet ovat usein tekoja ja rutiineja, joita jo tiloilla toteutetaan. Varautumissuunnitelmassa käsitellään tilanteita ja toimenpiteitä, joihin ryhdytään häiriötilanteen sattuessa. (Viisas varautuu hyvän sään aikaan n.d.)

Toimiakseen luotettavasti lypsyrobotit ja monet muut maatilan laitteet tarvitsevat laadukasta sähköä. Maaseutumaisilla alueilla sähkökatkot ja jännitteen vaihtelut on syytä huomioida varavirta- eli UPS –laitteilla. Sähköturvallisuusmääräykset antavat hyvän pohjan myös kyberturvallisuuden huomioimiseen. Varavoima tulee mitoittaa toimintaan nähden niin, että kaikki tuotannon ylläpitämiseen olennaisesti liittyvät asiat veden lämmittämisestä maidon jäähdytykseen saadaan hoidettua. Laitteet on osattava käynnistää uudelleen, sillä myrskyjen aiheuttamat sähkökatkot sammuttavat tietojärjestelmät. (Kyberin taskutieto maatiloille 2018, 6–7.)

Maatilalta kerättävää tietoa hyödynnetään sekä tuotannon ohjaukseen että tuotteiden kaupalliseen sertifiointiin. Maatilalla syntyy paljon tietoa, josta ulkopuoliset tahot, kuten esimerkiksi lypsyrobotteja toimittavat tahot ovat kiinnostuneita. Järjestelmiä hankittaessa on sovittava kaikkia osapuolia kunnioittavasta omistus- ja käyttöoikeuksista. Maatilan on päästävä käsiksi omistamaansa tietoon ja yrittäjän on oltava tietoinen siitä, mihin maatilalla tuotettua tietoa käytetään. Syntynyt tieto voi olla EU:n tietosuoja-asetuksen eli GDPR:n tarkoittamaa tietoa, joten sitä pitää osata käsitellä noudattamalla tietosuojaperiaatteita. (Kyberin taskutieto maatiloille 2018, 10.)

Karhinen (2019) toteaa raportissaan, että suomalainen maatalous on nostettava edelläkävijäksi digitalisaation, tekoälyn, alustatalouden ja avoimen datan hyödyntäjänä. Tätä kehitystä ohjaava tekijä on kuluttaja ja kuluttajan tarpeiden parempi ymmärtäminen. On siis tärkeää, että alkutuotannon tuottama tieto on luotettavaa ja siitä saadaan avointa dataa koko ruokaketjun saataville. (Karhinen 2019, 68–71.)

4.3.4 Käyttäjä riskitekijänä

Jäykän (2021) suorittamien haastattelujen mukaan kyberriskit ovat muutakin kuin kyberhyökkäyksiä, sillä käyttäjän osaamattomuus saattaa myös aiheuttaa uhkia. Tietojen palauttaminen voi olla hankalaa johtuen puutteellisesta osaamisesta tai epäpätevästä tietotekniikka-asiantuntijasta, joka saattaa olla vaikkapa oman perheen lapsi. Esimerkiksi tuotannonhallintajärjestelmiä sisältäviä tietokoneita olisi hyvä käyttää ainoastaan työkoneina eikä vapaa-ajalla varsinkaan, jos ei olla varmoja suojauksen tasosta kuten esimerkiksi palomuurista. Huomiota tulisi kiinnittää myös siihen, kuinka usein tietotekniikkaa pitää uudistaa rakennuksen käyttöiän aikana. Jäykkä (2021) sekä Lönnqvist ja Moilanen (2018) korostavat käyttäjän osaamisen ja tiedon merkitystä arvioitaessa informaation lähdettä. Käyttäjä voi kehittää modernin yhteiskunnan uutta kansalaistaitoa, medialukutaitoa, tutkimalla samaa aihetta useasta eri lähteestä ja arvioimalla lähdettä sitä koskevan tiedon perusteella. (Jäykkä 2021, 58–59; Lönnqvist & Moilanen 2018, 13.)

Maatilan ohjelmistoja sisältävät koneet ja laitteet vaativat ohjelmistopäivityksiä. Oksanen (2022) ja Järvinen (2022) toteavat kyberturvallisuuden olevan muutakin kuin päivitysten asentamista ja salasanojen vaihtamista, mutta näitä perusasioita ei tule unohtaa. Päivitykset vaihtelevat täysin automaattisista itsestään päivittyvistä ohjelmista monivaiheisiin käsin ohjelmoitaviin päivityksiin. Vaatimus ylläpitäjän osaamisesta korostuu kyberturvallisuusuhkien hallitsemiseksi. Kun valmistaja lopettaa tuotteen tukemisen, loppuvat myös päivitykset ja laitteen käyttäminen kyberturvallisuuden näkökulmasta ei ole enää suositeltavaa. Oksanen (2022) esittää ratkaisuksi vuosikelloa, jotta tarvittavat koneisiin ja laitteisiin liittyvät huollot tulisi tehtyä ajallaan. Kalenteriin merkittäisiin kullekin kuukaudelle kuuluvat huoltotoimenpiteet kuten esimerkiksi tapahtumalokien katsomiset virheiden varalta, ohjelmistopäivitykset ja niiden saatavuudet sekä varmuuskopioinnit. Käyttösesongin alkaessa huolletaan kyllä peltoviljelykoneet, mutta vuosikellon avulla tulisi huollettua myös ne koneet, joilla ei ole varsinaista käyttösesonkia. (Oksanen 2022, 13; Järvinen 2022, 36)

4.3.5 Elintarvikeketjun tukena olevat viranomaiset kyberturvallisuudessa

Kyberturvallisuuteen liittyvissä asioissa elintarvikeketjussa toimivien tahojen tukena ovat ruokavirasto, kyberturvallisuuskeskus, huoltovarmuuskeskus ja poliisi (Vertainen ym. 2023, 40–43). Ruokavirastolla on erityisen suuri rooli elintarvikeketjussa. ”Ruokavirasto toimii ihmisten, eläinten ja

kasvien terveyden hyväksi, tukee maaseudun elinvoimaisuutta ja kehittää ja ylläpitää tietojärjestelmiä" (Mikä on Ruokavirasto? 2023). Kun organisaation tietoturva on vaarantunut, kannattaa siitä tehdä ilmoitus kyberturvallisuuskeskukseen. Keskus neuvoo tilanteen hahmottamisessa, lisävahinkojen estämisessä sekä tilanteesta toipumisesta. Saatujen ilmoitusten perusteella kyberturvallisuuskeskus voi antaa varoituksia, ja organisaatiot sekä yritykset saavat tilannekuvaa kyberturvallisuuteen vaikuttavista tapahtumista. (Pysy ajan tasalla kyberturvallisuuden kiinnostavimmista ilmiöistä n.d.)

Huoltovarmuuskeskus varmistaa yhdessä yrityselämän, kolmannen sektorin ja viranomaistahojen kanssa yhteiskunnan toimivuuden myös kriisitilanteessa. Jotta tuotantoa pystytään pitämään yllä, välttämättömistä raaka-aineista ja tuotteista ylläpidetään turvavarastoja. Elintarvikehuolto turvaa riittävän alkutuotannon, elintarviketeollisuuden jalostuskapasiteetin sekä toimivan teollisuuden ja kaupan jakelujärjestelmän kuluttajille. (Elintarvikehuolto n.d.) Kyberrikoksen tutkinnan kannalta poliisiin kannattaa olla yhteydessä mahdollisimman varhain. Tutkinnan kannalta tärkeä tietotekninen aineisto on saatava turvattua oikeusvarmalla tavalla. (Kyberrikoksen tutkinta n.d.)

4.3.6 Esimerkkejä kyberuhista

Suomessa uutisoitiin keväällä 2022 yhdysvaltalaisen, kansainvälisesti toimivan Agco -konsernin joutumisesta kiristyshaittaohjelman hyökkäyksen kohteeksi. Hyökkäys häiritsi konsernin tuotantolaitosten toimintaa ja esimerkiksi Valtran traktoritehdas suljettiin hetkellisesti Suolahdessa. Vedoten kommentoinnin itsessään olevan kyberturvallisuusriski, tehtaan johdolta ei saatu tarkkaa tietoa hyökkäyksen vaikutuksista esimerkiksi varaosien saantiin ja laskutukseen. (Ala-Kleemola 2022, 68.) Maatilat eivät ole säästyneet kyberhyökkäyksiltä. Navetan valvontakameran kuvaa on ollut netissä kaikkien nähtävissä, lehmien kiimanhallintaohjelma on levittänyt haittaohjelmia ja lypsyrobotti on soittanut maksullisiin numeroihin tehden ison puhelinlaskun. (Manninen 2019.)

Lounais-Englannissa sijaitsevasta Dorsetista on esimerkki, jossa automaattilypsytilalla tilallinen oli avannut sähköpostin liitetiedoston ja seurauksena tilan tietoverkko kaatui. Ilman verkkoa ei ollut tietoa, mitkä lehmistä oli lypsetty ja mitkä piti seuraavaksi lypsää. Tilanne aiheutti paniikkia ja stressiä tilalliselle. Kun tilan toimistoa ja tietoverkkoja tutkittiin tarkemmin, havaittiin puutteita tietoturvaohjelmissa, salasanoissa ja varmuuskopioinnissa. Älykkäitä maatalouslaitteita kehitetään,

mutta viljelijöille ei ole juurikaan koulutusta tarjolla aiheeseen. Viljelijät tekevät työtä ruuantuotannossa eivätkä kyberhyökkäysten torjumisessa. (Moore 2022.)

4.3.7 Kyberbioturvallisuus

Kyberbioturvallisuus on osa kyberturvallisuuden kokonaisuutta. Siinä keskitytään muun muassa maatalous- ja elintarvikkeisiin liittyvän biologisen datan suojaamiseen. Kyberbioturvallisuuden esimerkkinä on Covid -19 rokote, jonka lääketieteellisiin testauksiin ja kehittelyyn kyberhyökkäykset kohdistuivat. Pyrkimyksenä on esimerkiksi estää tulevaisuuden mahdolliset zoonoosi –pandemiat ja suojella biologista dataa, jota on kerätty eri tietolähteistä. (Drape, Magerkorth, Sen, Simpson, Seibel, Murch & Duncan 2021.)

Tekniikoiden yhteen liitettävyys tietojen vaihdossa maatilojen ja laitetoimittajien sekä myyjien kanssa luo valvomattomia tietoverkkoja. Uusien teknologioiden myötä kyberriski maatiloilla kasvaa ja hyökkäyksillä voi olla vaikutusta elintarvikeketjuihin. Koko maatilan tuotanto voi vaarantua älykkäisiin teknologioihin kohdistuvista riskeistä kuten vääristä anturitiedoista. (Drape ym. 2021.)

Maatalouden näkökulmasta tämän aihealueen tutkimisesta olisi maanviljelyksessä hyötyä, jotta pystyttäisiin suojaamaan tuotantoketjut ja niihin liittyvä yritystoiminta. Kyberturvallisuuskäytäntöjen parantamiseksi olisi kuitenkin kehitettävä koulutusta maatalousalan ammattilaisille. Kyberturvallisuuden ja bioturvallisuuden välisten kuilujen kuromiseksi umpeen tarvitaan jatkuvaa monialaista yhteistyötä elintarvikeketjun toimijoiden kesken. (Drape ym. 2021.)

4.4 Maatilan johtaminen

Yrittäjä muodostaa tiimin johtajana tavoitteellisen näkemyksen siitä, mihin yritys on menossa tulevaisuudessa ja se on vietävä liiketoimintamallin avulla käytännön tehtäviksi ja toimenpiteiksi. Liiketoimintasuunnitelmassa pyritään kuvaamaan mahdollisimman tarkasti mitä ja miten tuotetaan sekä miten tuotanto ja toiminnot tullaan toteuttamaan käytännössä. Kirjoitetusta suunnitelmasta on hyötyä maatalousyrittäjälle ajatuksen tasolla, sillä se mahdollistaa pitkälti uusien ajatusten synnyn ja lisää valmiutta kehittää yritystoimintaa. (Ryhänen & Sipiläinen 2018, 25–26.)

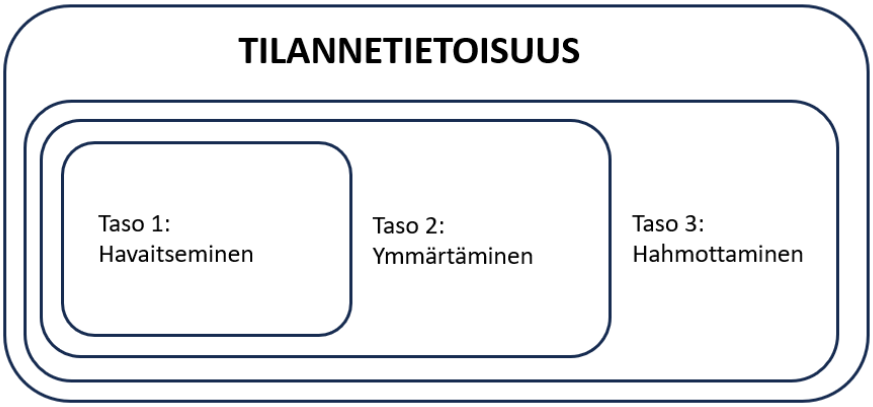
Päivittäisten asioiden ja rutiinien johtaminen on operatiivista, lyhyellä aika välillä tapahtuvaa johtamista. Päivittäin tehdyt päätökset ovat nykyhetkeen vaikuttavia, mutta ne tähtäävät strategian toteuttamiseen. Lyhyen aikavälin ratkaisut vievät harvoin yrityksen vakaviin vaikeuksiin. Strategisissa ratkaisuissa näin voi käydä, jos tehdään esimerkiksi liian suuria investointeja tuotantorakennuksiin tai maatalouskoneisiin. (Ryhänen & Sipiläinen 2018, 17.)

4.4.1 Tilannetietoisuus

Tilannetietoisuudella tarkoitetaan yksinkertaisesti sitä, mitä ympärillä tapahtuu juuri nyt ja sitä, mitä tulee tapahtumaan seuraavaksi. Tilannetietoisuus on päätöksentekoa tukeva asia. Ei voi johtaa, jos ei ole tilanteen tasalla.

Pöyhösen (2023) mukaan tilannetietoisuus on erittäin tärkeä ja keskeinen osa kyberturvallisuuden johtamista. Erityisesti maatiloilla verkostot tulevat suureen rooliin tilannetietoisuuden ylläpitämisessä. Pöyhönen (2023) pitää tärkeänä, että kyberturvallisuuden uhkamahdollisuuksista ja toteutuneista tilanteista sekä niistä toipumisista keskusteltaisiin avoimesti. Maatiloille saataisiin näin luotua kyberturvallisuuden tilannetietoisuutta. (Pöyhönen 2023.)

Yhdysvaltalainen tutkija Mica R. Endsley on luonut mallin, jossa käydään läpi tilannetietoisuuden kolme eri tasoa (kuvio 6). Tasolla 1 tehdään havaintoja datasta, joka on tilannehetkellä saatavilla. Taso 2 perustuu puolestaan datan tulkitsemiseen ja sen merkityksen ymmärtämiseen. Tasolla 3 hahmotetaan, mitä tulee todennäköisimmin tapahtumaan seuraavaksi. Tilannetietoisuudessa tulee päätöksentekijän ottaa huomioon kokonaistilanne ja tilanteeseen liittyvä informaatio. (Endsley 1995, 34–37.)



Kuvio 6. Tilannetietoisuuden määritelmä (Endsley 1995, 35, muokattu).

Kyberturvallisuuskeskuksen ylläpitämä Kybersää -tiedotepalvelu kertoo kybermaailman tapahtumista ymmärrettävässä muodossa tietoturva-asioista kiinnostuneille. Kybersäätiedotteita julkaistaan kuukausittain ja näissä käydään lävitse tapahtumat kuluneen kuukauden ajalta. Tiedotteessa kerrotaan esimerkiksi tietomurrot ja -vuodot, huijaukset ja tietojenkalastelut, haittaohjelmat ja verkkojen toimivuus. Lisäksi tiedote käy lävitse kyberturvallisuuden ilmiöt lähitulevaisuudessa ja pitkällä aikavälillä. (Kybersää 2023.)

4.4.2 Riittävä suojautuminen

Riittävän suojautumisen tasoa tarkasteltaessa voidaan lähtökohtana pitää sitä, missä ajassa pystytään palautumaan ilman merkittävää haittaa. Riittävä suojautuminen pitää sisällään sekä varautumista että poikkeustilanteissa toimimista. Lähtökohtana on kuitenkin se, että eläinten hyvinvointi ei pääse vaarantumaan.

Kun puhutaan lypsylehmistä, pitäisi lypsyväli olla korkeatuottoisella lehmällä noin 7 tuntia, eli lypsykertoja vuorokaudessa on 3,5. Lehmän utareen vastustuskyky heikkenee, mikäli lypsyväli on yli 14 tuntia. (Hulsen 2009, 32). Jotta merkittävää haittaa ei pääsisi tapahtumaan utareterveyden suhteen, ongelmatilanteesta pitäisi pystyä palautumaan 10–12 tunnin sisällä. Automaattilypsyssä lehmät kulkevat vapaasti oman rytminsä mukaan lypsyllä. Pitkät tauot lypsyssä sekoittavat eläinliikennettä useiksi päiviksi.

4.4.3 Kyberriskit osaksi riskienhallintaa

Yrityksen kyberturvallisuuden perustana toimii pitkän aikavälin strateginen suunnittelu huomioiden liiketoiminnan riskit ja tavoitteet sekä kyberturvallisuuteen liittyvät päätökset ja investoinnit. Tunnistetut toiminnan jatkuvuutta uhkaavat riskit ja haasteet auttavat strategisten tavoitteiden saavuttamisessa. Jotta kyberturvallisuusriskejä pystytään ymmärtämään ja arvioimaan paremmin, niitä tulisi käsitellä osana yrityksen koko riskienhallintaa. Kyberturvallisuuden kehittäminen riskilähtöisesti vaatii yhteistyötä organisaatioiden kyberturvallisuusvastaavien kanssa, jotta tekninen ymmärrys riskeistä kasvaa. Kyberturvallisuuden hallinnassa on huomioitava tuotannollisen teknologian lisääntyvä liitettävyys, analytiikan hyödyntäminen seurannassa ja ohjauksessa sekä modernisointi. Tilannekuvan selventämiseksi on oleellista löytää mittarit, joiden avulla kyberturvallisuuden tilannekuva on helposti ymmärrettävissä tarvittavien toimienpiteiden suunnitteluun. (Toimialojen kyberkypsyyden selvitys 2022 2023, 9.)

Pöyhösen (2020) mukaan kyberturvallisuuteen liittyvät standardit ja ohjeet ovat käyttäjälleen apuna organisaatioiden toimintojen luotettavuuden, laadun, riskienhallinnan ja varautumisen parantamisessa. Organisaation kyberturvallisuuden kehittämiselle ja organisoinnille on viisi toimintoa, jotka auttavat näissä. Ensinnäkin tulee tunnistaa riskit. Tämän jälkeen tulee suojautuminen. Organisaation tulee kehittää ja toteuttaa suojatoimen riskejä vastaan. Havainnointi on päivittäisissä toiminnoissa oltava mukana koko ajan. Tässä apuna on tilannetietoisuus. Nopea reagointikyky havaittuihin riskitilanteisiin on apuna riskitilanteiden vaikutusten hillitsemisessä. Viimeisenä toimintona tulee palautuminen. Palautuminen ja toimintakyvyn ennalleen saattaminen on tärkeänä osana riskienhallintaa. (Pöyhönen 2022; Calder 2018.)

4.4.4 Viestinnän merkitys

Viestintää tulee suunnitella, arvioida ja kehittää. Viestinnän suunnittelu perustuu ennakointiin, jotta tieto, jota tarvitaan, on täsmällistä ja tasapuolista. Viestinnässä tulee huomioida saatavuus eli tulee käyttää eri kanavia ja keinoja, jotta tieto on saatavilla. (Viestintää johdetaan, suunnitellaan ja arvioidaan n.d.)

Strategisessa, sisäisessä ja kriisitilanneviestinnässä on kaikissa hyvin paljon samoja piirteitä. Viestinnän suunnittelu on aina viestinnän onnistumisen lähtökohta. Tämä pitää sisällään viestimisen

nopeuden ja oikea-aikaisuuden. Olennaista on myös, että tieto välittyy johdonmukaisesti, kaikkien tietoa välittäjien viestin sisällön tulee olla samanlaista. Myös tilannetaju on hyvä huomioida. (Hetemäki 2020; Kankainen 2019.)

EU:n maatalouspolitiikan viestinnän päämääränä on lisätä suomalaisten ymmärrystä siitä, minkälainen merkitys Suomelle on elinvoimaisella maaseudulla ja kestävällä ruoantuotannolla. Lisäksi ymmärryksen lisäys EU:n maatalouspolitiikan rahoituksen mahdollisuuksista ja siihen, että tuensaajilla olisi osaaminen rahoitusten hakemiseen ja hyödyntämiseen. Viestinnällä tuetaan näitä tavoitteita. (EU:n maatalouspolitiikan viestintästrategia 2023–2027 2023.)

Lähtökohtana strategiselle viestinnälle ovat yrityksen tavoitteet, arvot, missio ja visio. Strategisen viestinnän avulla on tarkoitus siis saavuttaa organisaation tavoitteita. Strategisessa viestinnässä tulee myös pohtia, miten viestintä saadaan osaksi yrityksen strategiaa. Strateginen viestintä nähdään myös tärkeänä yrityksen tuloksentekokykyä. (Tikanmäki 2021.)

Hetemäen (2020) mukaan kriisitilanteessa viestintää joudutaan suorittamaan tilanteessa, jossa on epäselvä tilannekuva. Epäselvä tilannekuva on selkeä haaste viestinnälle. Hyvä kriisiviestintä on nopeaa, mutta johdonmukaista. Viestinnässä tulee ottaa huomioon selkeys, yksiselitteisyys ja täsmällisyys. Paasosen (2020) mukaan tutkimuksissa on huomattu negatiivisella uutisoinnilla olleen kolminkertainen vaikutus yrityksen maineeseen positiiviseen uutisointiin verrattuna. Vaikka viestinnässä pyritään pitämään positiivinen sävy, voi julkisuus olla yritykselle ja sen maineelle negatiivista. (Hetemäki 2020; Paasonen 2020.)

Welchin (2016) mukaan tulisi käyttää viittä perusolettamusta kriisihallinnan suhteen. Ensinnäkin tulee olettaa ongelman olevan pahempi kuin miltä se näyttää. Toisekseen ei ole salaisuutta, mikä ei tule julki. Kolmantena kohtana on olettamus, että organisaation kriisinkäsittelytapa tullaan esittämään pahimmassa mahdollisessa valossa. Neljäs olettamus on, että prosesseihin ja ihmisiin joutunee tehdä muutoksia. Viimeisenä kohtana tulee olettaa, että tästäkin kriisistä selvitään ja sen jälkeen ollaan entistä vahvempia. (Welch 2016.)

Johtamisen yhtenä tärkeänä osana viestintä. Sisäisessä viestinnässä tärkeää on avoimuus. Tällainen avoin viestintäkulttuuri on henkilöstön sitouttamisen ja luottamuksen saavuttamisen ja ylläpi-

tämisen peruste. Sisäisessä viestinnässä myös selkeys ja yksiselitteisyys on avainasemassa väärinymmärryksien välttämiseksi. On hyvä myös varmistaa, että viesti on ymmärretty. (Kankainen 2019.)

5 Tutkimusten toteuttaminen ja tulosten raportointi

Tutkimukseen otettiin mukaan kysely tilallisille, teemahaastattelut laitetoimittajille sekä case-esimerkki. Näin saatiin tarpeeksi kattavasti tietoa eri näkökulmista, jotta kyberturvallisuus saataisiin osaksi tilan toimintakulttuuria.

5.1 Kysely tilallisille

Kysely tilallisille toteutettiin Webropol -sovelluksella, jonka tarkoituksena oli selvittää tämän hetken tilannetta tietoturvallisuuden ylläpitämisestä ja kyberuhkiin varautumisesta automaattilypsytilallisilla. Kysely jaettiin Maitoyrittäjät ry:n jäsenille sekä MTK:n Maitovaliokunnalle ja Maitovaltuuskunnalle.

Maitoyrittäjät ry on vuonna 2013 perustettu riippumaton yhdistys, jonka tehtävänä on jäsenyritystensä johtamisosaamisen ja maitoyrittämisen edellytysten parantaminen sekä yhteistyö muiden maitoalan toimijoiden kanssa. Yhdistyksen jäsenet ovat erikokoisia yrityksiä ympäri Suomea. Maitoyritysten lisäksi yhdistyksellä on kannattajajäseninä maitoalan kehittämisestä kiinnostuneita toimijoita. Vuonna 2023 yhdistyksellä on 472 jäsentä. Yhdistys innostaa jäseniään järjestämällä johtamisaiheisia seminaareja, työpajoja ja opintomatkoja kotimaassa ja ulkomailla. Maitoyrittäjät ry on jäsenenä Euroopan Maidontuottajissa (EDF). Yhdistyksen toimintaan kuuluu myös kannanotot maitoyrittämistä koskeviin poliittisiin päätöksiin osallistumalla työryhmiin. Aloitteilla ja esityksillä sekä lausuntoja antamalla yhdistys haluaa edistää suomalaista maidontuotantoa. Maitoyrittäjät ry:n tavoitteena on, että vuonna 2028 jäsenyritykset tuottavat puolet Suomessa tuotetusta meijerimaidosta. (Kaikki lähtee johtamisesta n.d.)

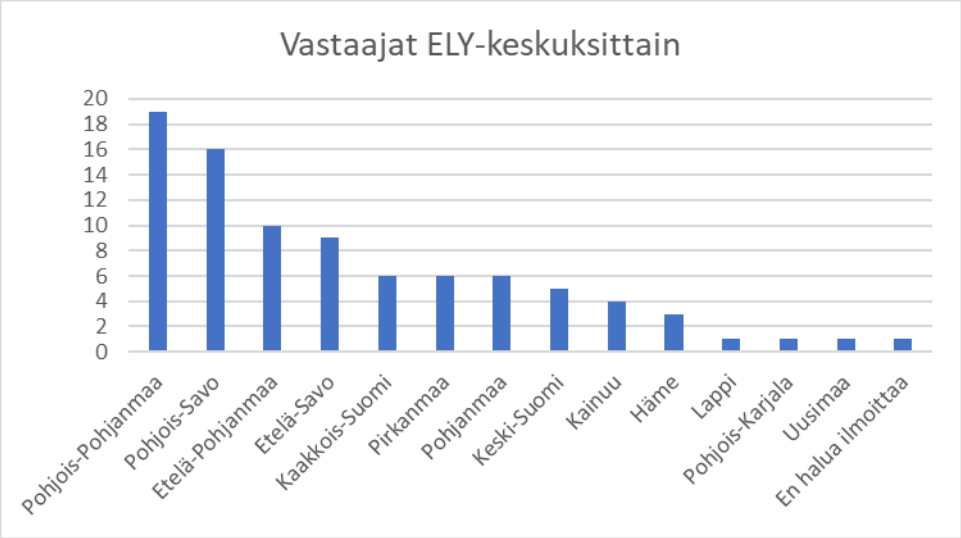
Kysely jaettiin ensiksi Maitoyrittäjät ry:lle. Yhdistyksen kautta kyselyä jaettiin jäsenille sähköpostitse ja uutiskirjeessä sekä sosiaalisen median kautta. Kyselyn lähetteessä mainittiin kyselyn koskevan automaattilypsytiloja. Maitoyrittäjät ry:n jäseniä on 472 kappaletta. Yhdistyksellä ei ole tietoa,

kuinka paljon jäsenistä on automaattilypsytiloja. Lisäksi yhdistyksellä on kannattajajäseninä maitoalan kehittämisestä kiinnostuneita toimijoita. Vastauksia Maitoyrittäjät ry:lle suunnatussa kyselyssä saatiin 83 kappaletta.

MTK:n kautta kyselyä jaettiin sähköpostitse. Maitovaliokunnalla jäsentiloja on 12 ja Maitovaltuuskunnalla 48 kappaletta. Vastauksia tästä jaosta saatiin 5 kappaletta. Yhteensä vastauksia kysely tuotti siis 88 kappaletta. Vastaukset yhdistettiin analysoitaessa. Erityisiä poikkeavuuksia aineistoissa ei ollut ennen yhdistämistä. Kyselyn vastausprosenttia ei pystytty määrittämään, koska kyselyä ei voitu lähettää pelkästään automaattilypsyä harjoittaville tiloille.

5.1.1 Taustatiedot

Kyselyyn vastanneista 41–50-vuotiaita oli 33 %. 31–40-vuotiaita oli 31 % eli kaksi tilaa vähemmän. Yli 51 -vuotiaita kyselyyn vastasi 19 % ja 18–30-vuotiaita 17 %. Kyselyyn vastanneiden koulutus oli 42 prosentilla alempi korkeakoulututkinto. Ammattikoulun tai lukion oli käynyt 39 %, ylemmän korkeakoulututkinnon suorittaneita oli 14 % ja keski- tai perusasteen tutkinnon tai vastaavan oli suorittanut 6 % vastaajista. Kyselyssä kysyttiin tilan sijaintia. Tilan sijainnin mukaan ne jaoteltiin ELY-keskuksittain. Vastaajia eniten oli Pohjois-Pohjanmaan, Pohjois-Savon ja Etelä-Pohjanmaan ELY-keskuksien alueilta (kuvio 7).



Kuvio 7. Vastaajat Ely-keskuksittain.

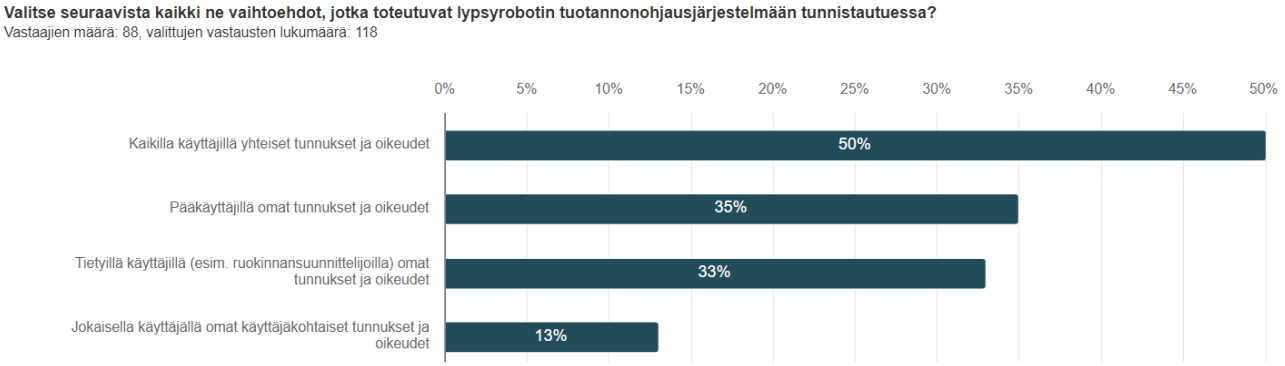
Vastaajista suurimmalla osalla eli 57 %:lla oli käytössään Lely -merkkinen lypsyrobotti. DeLavalin lypsyrobotti oli 36 %:lla vastaajista ja GEAn lypsyrobotti 7 %:lla. Yksi lypsyrobotti löytyi vastaajista noin puolelta eli 51 %:lta. 2 lypsyrobottia oli 33 %:lla vastaajista, 3 lypsyrobottia 9 %:lla vastaajista ja 4 tai enemmän 7 %:lla vastaajista.

5.1.2 Kriittinen varautuminen – sähkö

Kyselyyn vastanneista suurin osa eli 98 % ilmoitti varavoimalähteen olevan käytössä. Ainoastaan kahdella prosentilla tällaista tilannetta ei ole. Kysyimme myös riittääkö varavoima kattamaan tuotantorakennuksen toiminnan. Vastanneista 95 %:lla varavoima riittää kattamaan tuotantorakennuksen toiminnan ja 4 %:lla ei riitä. Vastaajista 1 % ilmoitti, ettei osaa sanoa.

5.1.3 Kriittinen varautuminen – ohjelmistot

Kysyimme tilallisista tuotannonohjausjärjestelmään tunnistautumista (kuvio 8). Vastaajista 50 % vastasi kaikilla käyttäjillä olevan yhteiset tunnukset ja oikeudet. Pääkäyttäjiltä löytyvät omat tunnukset ja oikeudet 35 %:lta. Vastanneista 33 %:lla on tietyillä käyttäjillä, kuten ruokinnansuunnittelijoilla olevan omat tunnukset ja oikeudet. Vastaajista 13 % kertoi jokaiselta käyttäjältä löytyvän omat käyttäjäkohtaiset tunnukset ja oikeudet vastaajista.

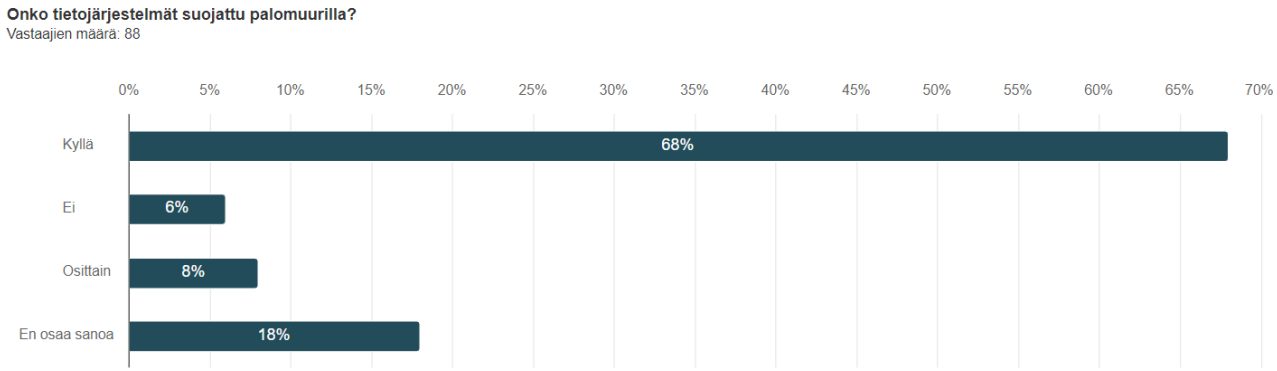


Kuvio 8. Tuotannonohjausjärjestelmään tunnistauminen.

Kysyimme myös mihin käytetään tietokonetta, jossa on tuotannonohjausjärjestelmä. Tuotannonohjauksen lisäksi tietokonetta käyttää 94 % tilan tarvitsemiin oheisohjelmiin kuten Minun Maati-

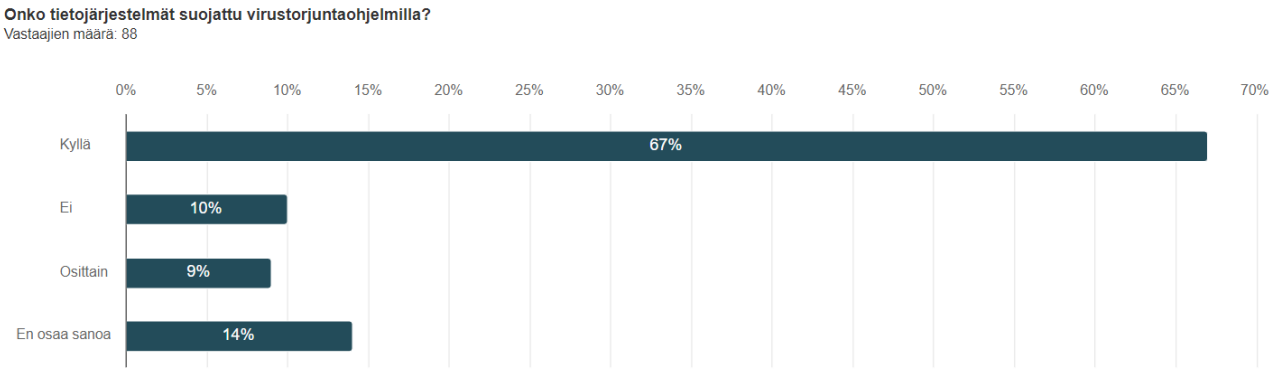
lani -ohjelmaan. Tuotannonohjaukseen tarkoitetulla tietokoneella 34 % käytti sitä myös sähköpostiviestintään. Vastaajista 7 % käytti tuotannonohjaustietokonetta myös muuhun toimintaan kuten esimerkiksi huutokaupan selaamiseen, maatalousalan julkaisuihin ja tiedon hankintaan.

Automaattilypsytiloilla tietojärjestelmät on suojattu palomuureilla 68 %:lla (kuvio 9). Vastaajista 6 % kertoi, ettei palomuurisuojausta ole ja 8 % vastasi, että tietojärjestelmät on suojattu osittain palomuurilla. Vastaajista 18 % ei osannut sanoa palomuurien käytöstä.



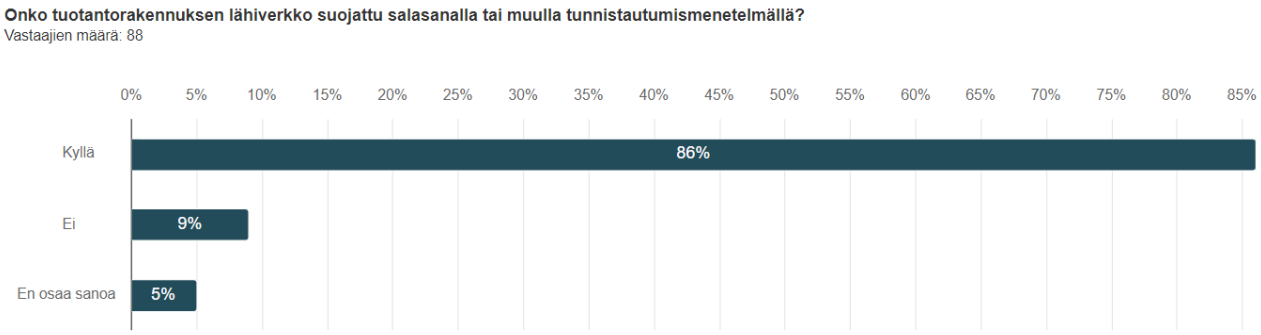
Kuvio 9. Palomuurien käyttö.

Virustorjuntaohjelmat olivat käytössä 67 %:lla vastaajista (kuvio 10). Vastaajista 10 % kertoi, että virustorjuntaohjelmia ei ole käytössä ja 9 % vastasi tietojärjestelmien olevan osittain suojattuna virustorjuntaohjelmilla. Vastaajista 14 % ei osannut sanoa virustorjuntaohjelmien käytöstä.



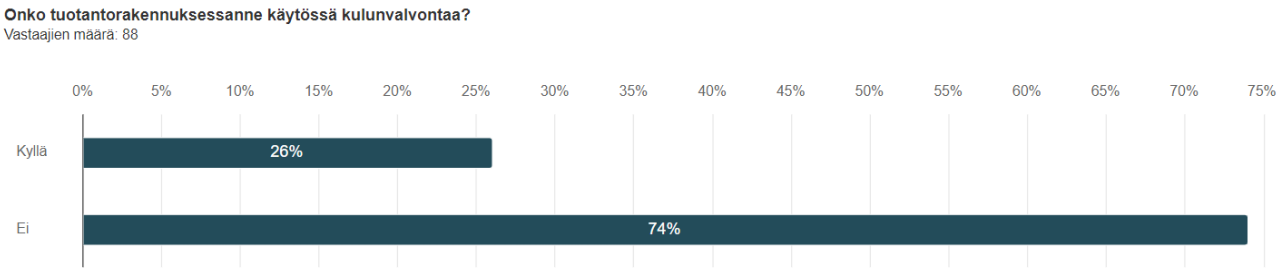
Kuvio 10. Virustorjuntaohjelmien käyttö.

Tuotantorakennuksen lähiverkko on suojattu salasanalla tai muulla tunnistautumismenetelmällä 86 %:lla vastaajista (kuvio 11). Lähiverkkoa ei ole suojattu 9 %:lla vastaajista ja 5 % osannut sanoa suojauksen tilannetta.



Kuvio 11. Tuotantorakennuksen lähiverkon suojaus.

Tuotantorakennuksessa kulunvalvonta on käytössä 26 :%lla vastaajista eli sitä ei ole käytössä 74 %:lla (kuvio 12).

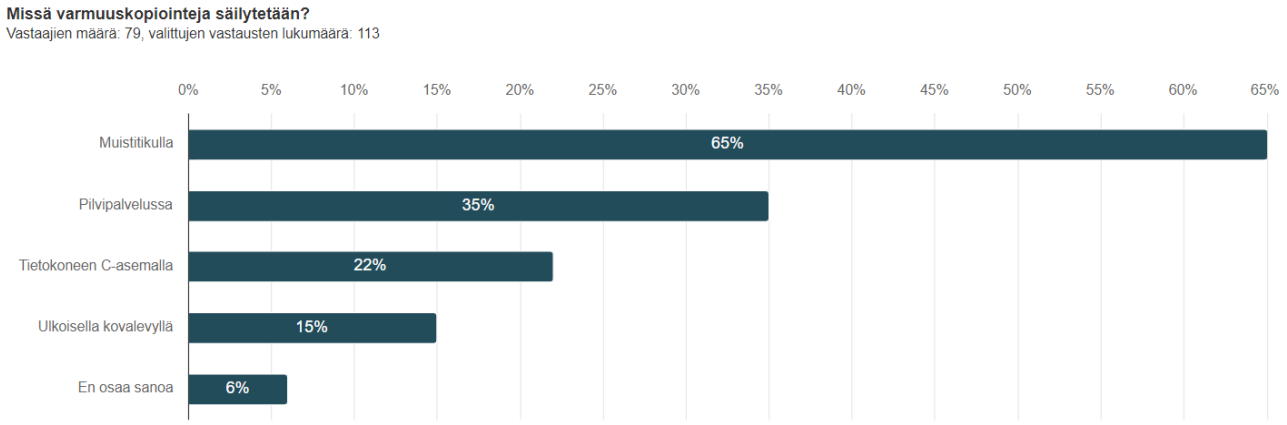


Kuvio 12. Tuotantorakennuksen kulunvalvonta.

5.1.4 Kriittinen varautuminen – varmuuskopiointi

Tuotannonohjausjärjestelmässä varmuuskopiointi on käytössä 90 %:lla vastaajista. Vastaajista 7 % ei osannut sanoa ja 3 % vastasi, ettei varmuuskopiointia ole käytössä. Tiedostot varmuuskopioidaan 63 %:lla päivittäin, 18 %:lla viikoittain ja 4 %:lla kuukausittain. Vastaajista 15 % ei osannut sanoa varmuuskopioinnin tiheyttä.

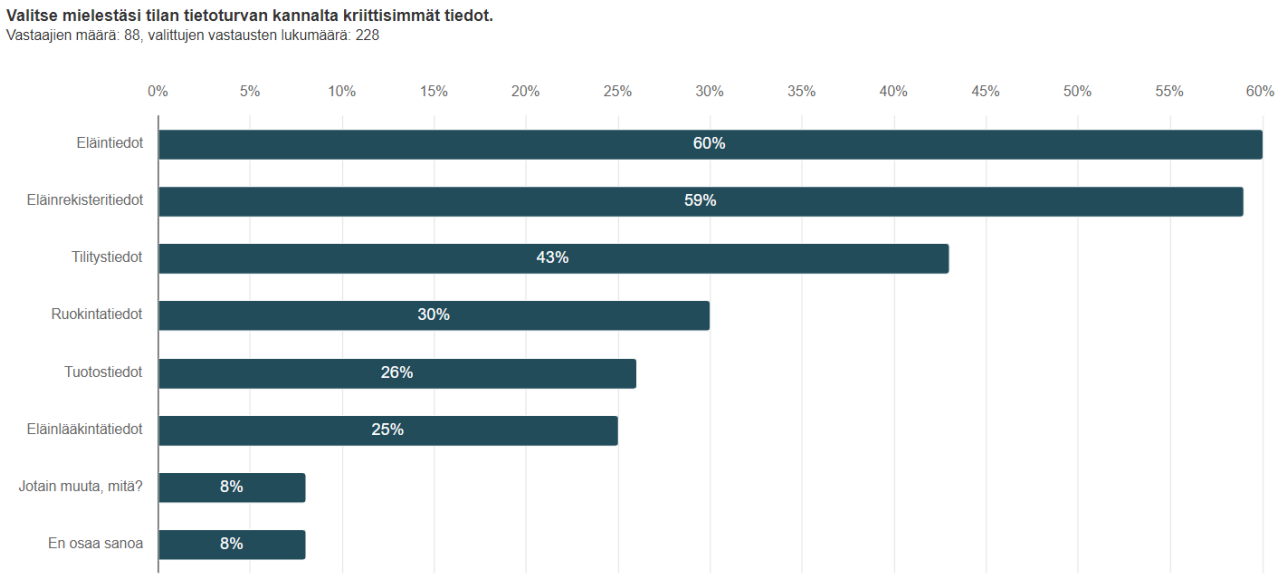
Kuviosta 13 käy ilmi varmuuskopiointien säilytyspaikka. Vaihtoehdoista pystyi valitsemaan useamman. Varmuuskopiointien säilytyspaikkana muistitikku oli käytössä 65 %:lla vastaajista, pilvipalvelu 35 %:lla vastaajista, tietokoneen C-asemalla 22 %:lla ja ulkoisella kovalevyllä 15 %:lla. Vastaajista 6 % ei osannut sanoa varmuuskopiointien säilytyspaikkaa. Varmuuskopioitujen tiedostojen palautuksen oli tehnyt tai harjoitellut 27 % vastaajista, vastaajista 63 % ei ole tehnyt ja 10 % ei osannut sanoa.



Kuvio 13. Varmuuskopiointien säilytys.

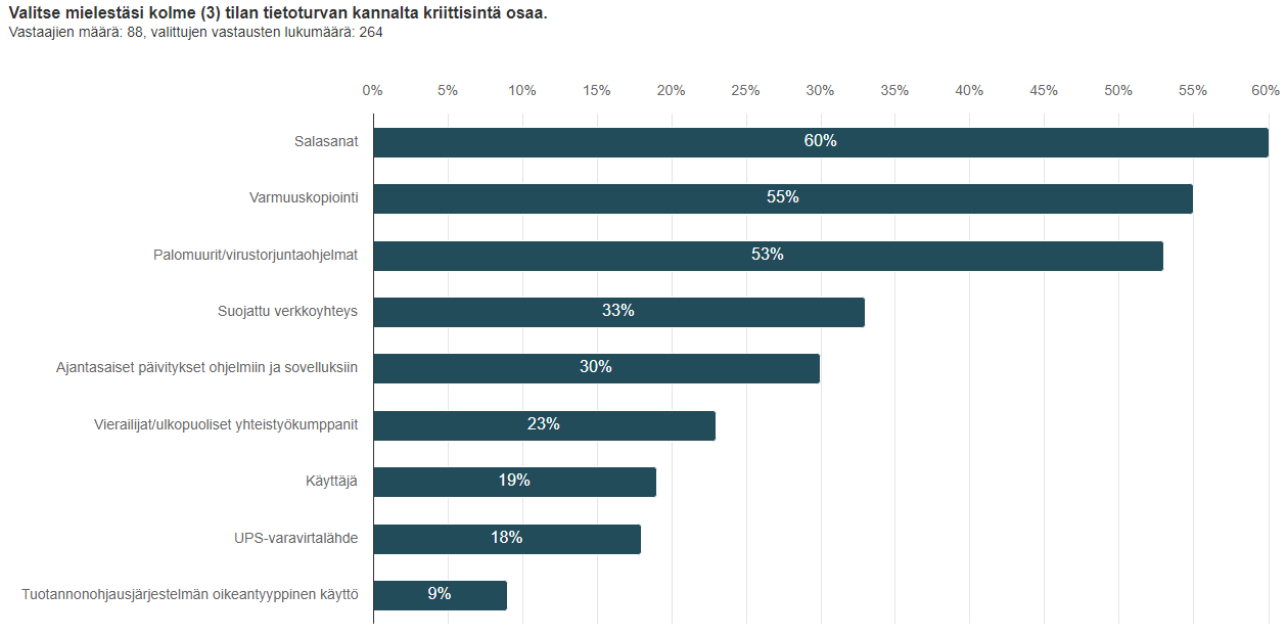
5.1.5 Kriittinen varautuminen – oma toiminta

Alla olevasta kuviosta 14 käy ilmi vastaajan mielestä tilan kriittisimmät tiedot. Kriittisimpinä tietoina pidetään eläin- ja eläinrekisteritietoja. Vastaajista 43 % pitää myös tilitystietoja kriittisinä tietoina. Ruokinta-, tuotos- ja eläinlääkintätiedot ovat alle kolmasosan mielestä kriittisiä. Vastaajista 8 % ei osannut nimetä tilan kriittisiä tietoa. Kriittisinä tietoina pidettiin myös robottiin liittyviä asetustietoja ja tuotannonhallintajärjestelmän asetuksia ja säätöjä.



Kuvio 14. Tilan tietoturvan kannalta kriittisimmät tiedot.

Tietoturvan kannalta kriittisimpien osien kolme suosituinta vastausta olivat salasanat, varmuuskopiointi sekä palomuurit ja virustorjuntaohjelmat (kuvio 15). Kolmasosa vastaajista nimesi myös suojatun verkkoyhteyden sekä ajantasaiset päivitykset tietoturvan kriittisimmiksi osiksi.

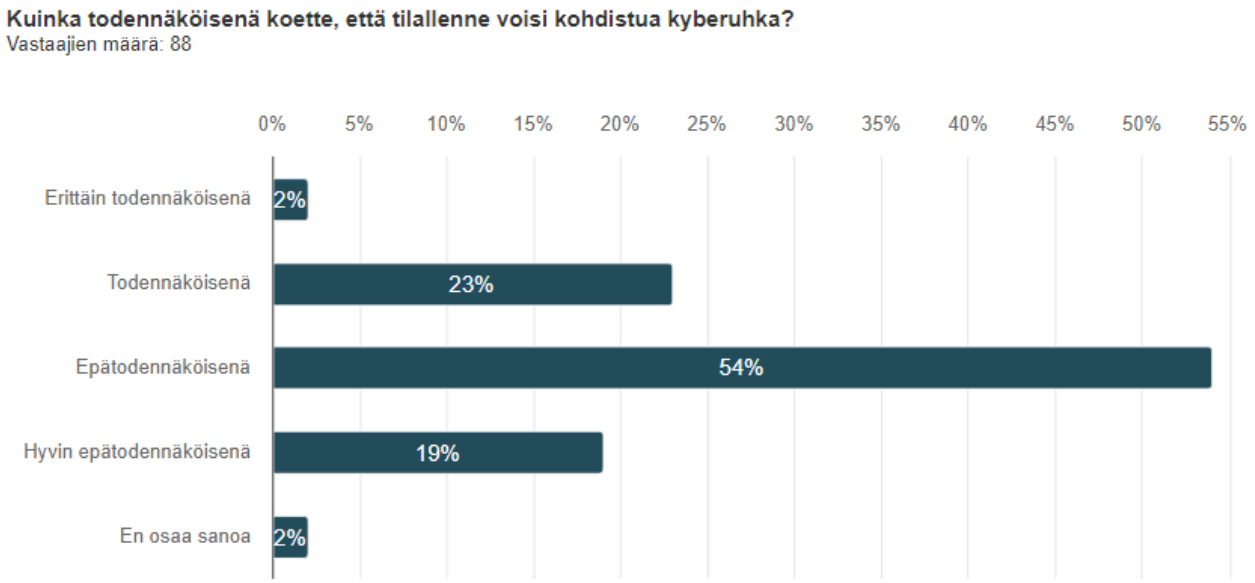


Kuvio 15. Tilan tietoturvan kriittisimmat osat.

5.1.6 Varautuminen kyberuhkiin

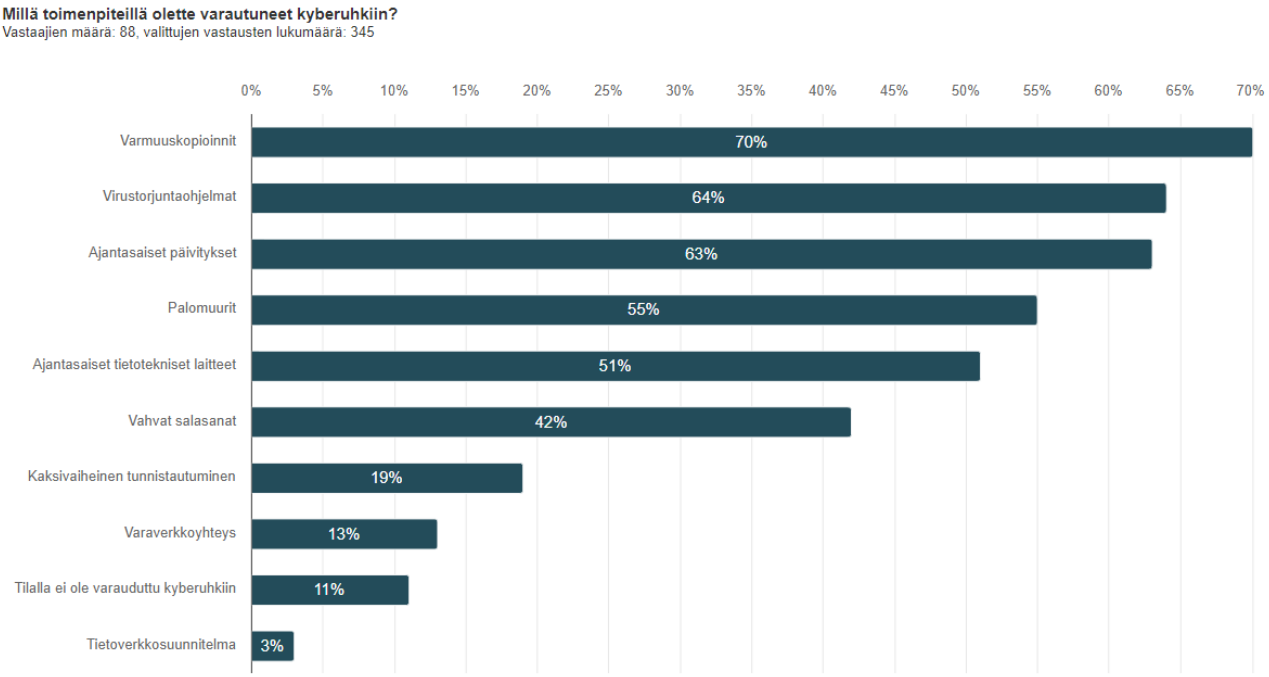
Kysyimme automaattilypsytilallisilta, huomioivatko he kyberturvallisuuden tilan riskienhallinnassa. Vastaajista 49 % huomioi kyberturvallisuuden riskienhallinnassa, 36 % ei huomioi ja 15 % ei osannut sanoa.

Kuviosta 16 käy ilmi, että yli puolet (54 %) pitää kyberuhkaa tilalla epätodennäköisenä. Todennäköisenä sitä pitää 23 % ja erittäin todennäköisenä 2 %. Hyvin epätodennäköisenä kyberuhkan kohdistumista tilanne pitää 19 %. Vastaajista 2 % ei osannut sanoa kantaansa.



Kuvio 16. Kyberuhkan todennäköisyys.

Kuviosta 17 käy ilmi toimenpiteet, joilla vastaajat ovat varautuneet kyberuhkiin. Toimenpiteistä eniten käytössä olivat varmuuskopioinnit (70 %), virustorjuntaohjelmat (64 %) ja ajantasaiset päivitykset (63 %). Myös palomuurit ja ajantasaiset tietotekniset laitteet olivat noin puolella vastaajista varautumistoimenpiteinä. Vastaajista 11 % ilmoitti, ettei tilalla ole varauduttu kyberuhkiin.



Kuvio 17. Kyberuhkiin varautumisen toimenpiteet.

Kysyimme tilallisilta keneltä he saavat apua tilan tieto- ja kyberturvallisuuteen liittyvissä asioista. Kysymys oli avoin kysymys ja vastata sai vapaasti. Vastaajista 56 % sai apua laitetoimittajalta tai palveluntuottajalta. Oma tai lähipiirin osaaminen oli riittävää 33 %:lla. Vastauksissa oli kuitenkin havaittavissa myös epätietoisuutta, mistä apua voisi löytyä.

5.2 Laitetoimittajien haastattelut

Haastattelut suoritettiin kolmelle suurimmalle Suomen markkinoilla toimivalle lypsyrobotteja toimittaville yrityksille. Suomessa suosituimmat lypsyrobottien laitetoimittajat ovat NHK LeLy, DeLaval VMS sekä GEA. Haastateltavat olivat yritysten tietoturvasta ja laitteiden käyttöönotosta vastaavia avainhenkilöitä. Touko-kesäkuussa suoritetut haastattelut jaettiin teemoihin, jotka käsittelivät tietoturvaa ja käyttöönottoa, tilan tietoverkkoja, kyberturvallisuutta yrityksessä tilallisen näkökulmasta, käyttäjäkoulutusta sekä etäkäyttöä. Teemahaastatteluiden vastaukset on koostettu yhteen, sillä tarkoituksena ei ole vertailla laitetoimittajia, vaan tuoda esille mahdollisimman kattavasti laitetoimittajien näkökulmaa maitotilojen kyberturvallisuuteen.

5.2.1 Tietoturva ja käyttöönotto

Lypsyrobottihankinnan mukana laitetoimittaja toimittaa tietokoneen, joka on tarkoitettu tuotannonhallintaan. Laite sisältää tuotannonhallintaan tarkoitetun ohjelmiston ja virustorjunnan. Kaikki haastatellut henkilöt korostivat, että tämä tietokone on tarkoitettu vain tuotannonhallintakäyttöön ja ohjeistus on, että muiden sivustojen käyttöön hankittaisiin toinen kone. Poikkeuksena mainittiin esimerkiksi Minun Maatilani -ohjelma, joka sisältää tilallisen kannalta tärkeät eläintiedot ja tuotostiedot. Toiminnan sujuvuuden kannalta tämän tyyppiset ohjelmat voivat olla samalla koneella tuotannonhallintajärjestelmän kanssa. Yksikään laitetoimittaja ei suoraan sanonut, että kyseinen ohjeistus on dokumentoitu. Asia käydään kyllä suullisesti läpi käyttöönoton yhteydessä. Varmuuskopiointi tapahtuu automaattisesti kaikkien toimijoiden laitteissa useampaan muistipaikkaan päivittäin ja viikoittain. Manuaalisesti tallennuksen voi tehdä pilveen, muistitikulle tai ulkoiselle kovalevylle. Laitetoimittajat ohjeistavat, että varmuuskopioinnin kansio tulisi määräajoin tarkistaa. Yksikään haastatelluista laitetoimittajista ei suositellut varmuuskopioinnin palauttamista tilallisen itsensä tekemänä. Asiantuntija hoitaa lähes aina palautuksen ja yhden haastateltavan mukaan tilallisella ei pitäisi olla tarvetta tehdä varmuuskopioinnin palautuksia.

5.2.2 Tietoverkot ja käyttöoikeudet

Yhdelläkään laitetoimittajalla ei ollut dokumentaatiota tietoverkoista. Yksi haastateltavista kertoi sen olevan suunnitteilla. Kaikkiin laitetoimittajien tuotannonhallintaohjelmiin voidaan antaa käyttöoikeuksia kolmansille osapuolille kuten esimerkiksi ruokinnansuunnittelijoille. Näihin käyttöoikeuksiin tarvittavan luvan antaa aina laitetoimittaja. Kaikki haastateltavat korostivat, ettei tuotannonohjausjärjestelmän tietokonetta saisi käyttää muuhun käyttöön, kuten esimerkiksi netin selailuun. Niin sanottu ”hupikone” pitäisi olla erikseen. Tällä ohjeistuksella vahvistetaan viljelijän turvaa tietoverkoissa.

5.2.3 Tuki ja ohjeet tilallisille

Kaikilla lypsyroboteilla toimittavilla yrityksillä on tukipalvelu, josta tilallinen saa apua ongelmatilanteessa vuorokauden ympäri. Haastateltavilla ei ollut yhtään esimerkkiä kyberuhkauksen aiheuttamasta häiriötilanteesta ja siitä palautumisesta takaisin operatiiviseen tilaan. Yksi ukkosen aiheuttama laiterikko esiteltiin. Esimerkissä tuorein varmuuskopio oli kaksi kuukautta vanha ja Minun

Maatilani – ohjelmiston sekä muiden sovellusten avulla palautuminen kesti noin yhden päivän. Tämän esimerkin myötä korostettiin sähköverkon ukkossuojauksen ja varmuuskopioinnin merkitystä. Lypsyrobotit pystyvät lypsämään ilman tietokonettakin, mutta yhden haastateltavan mukaan lypsyrobottiin mahtuu noin 2–3 päivän tieto ja sen jälkeen tallennus tapahtuu vanhempien tietojen päälle. Kaikki lypsyrobotit huolletaan tietyn huolto-ohjelman mukaisesti useamman kerran vuodessa. Yleensä tämä huoltoväli on noin neljä kuukautta. Järjestelmät olisi hyvä myös sammuttaa ja käynnistää uudelleen kerran viikossa, jotta päivitykset pysyvät ajan tasalla. Huolloissa tarkastetaan, että päivitykset ovat ajan tasalla ja varmuuskopiointi toimii. Yksi laitetoimittajista ohjeistaa, että datakaapelilla toimiva internetyhteys olisi hyvä, mutta tilallinen tekee omat ratkaisunsa.

5.2.4 Koulutusta kyberturvallisuuteen ja etäkäyttö

Kyberturvallisuuteen liittyvää erillistä koulutusta ei ole tarjolla yhdelläkään laitevalmistajalla. Käyttöönottoon ja sovelluksiin liittyy koulutusta sekä it-tukea on tarjolla. Yksi laitevalmistajien edustajista sanoi, että on herännyt ajatus kyberturvallisuuteen liittyvän koulutuksen tarpeesta. Yhden laitetoimittajan mukaan ulkopuoliselle käyttäjälle on turvallisempaa antaa käyttöoikeuksilla lupa käyttää tilan tietokonetta kuin etäkäytöllä. On huomioitava, että selaimeen tallennetut salasanat ovat myös etäkäytössä käytettävissä. Etäkäyttö antaa luvan koko tietokoneelle. Toisen laitetoimittajan mukaan muutoksia tuotannonohjausjärjestelmään pääsee tekemään vain omalta tietokoneelta. Heidän järjestelmässään pääsee etäkäytöllä vain näkemään tietoja, ei muuttamaan. Kolmas haastateltava suositteli etäkäyttöön sovellusta, jossa käytetään vahvaa salasanaa ja siinä voidaan myös määrittää käyttöoikeuksia. Kyseinen haastateltava myös korosti tilallisen vastuuta käyttöoikeuksien rajaamisen suhteen.

Kaikissa kolmessa haastattelussa tuli esille, että tilallisten välillä on erittäin suuria eroja tietoteknisissä taidoissa. Tiloilla on taidoiltaan hyvin eritasoisia käyttäjiä, jotka aiheuttavat omat haasteensa. Myös tiloilla työskentelevien henkilöiden luotettavuuteen tulisi kiinnittää huomiota. Samat tunnukset ja salasanat eri käyttäjillä sekä selaimiin tallennetut salasanat lisäävät tietoturvaan liittyviä riskejä. Koulutusten ja ohjeistusten suhteen on asioita suunnitteilla. Kaikki lypsyrobotteja valmistavat toimijat toimivat maailmanlaajuisesti ja toimintatavat eri maissa ovat erilaisia. Ulkomailla voi olla mukana eri toimijoita, jotka tuovat omat riskinsä. Eri järjestelmien tulee olla yhteneväisiä.

5.3 Kehittämissuunnitelma – Case-esimerkki

Tämän opinnäytetyön yhtenä osana tehtiin kehittämissuunnitelma automaattilypsytilalle. Esimerkki pohjautuu olemassa olevaan tilaan ja sen tietoihin. Tämän esimerkin avulla havainnollistetaan, miten tilan toimintakulttuuriin lisätään kyberturvallisuuden huomioiminen.

Liitteessä 4 on esimerkkitilan alkutilanne. Varavoimalähteen osalta tilanne on kunnossa. UPS-varavirtalähteet ovat tuotantorakennuksessa käytössä, mutta akkujen tilannetta ei ole tarkastettu milloinkaan. Suurin kehittämistarve tilalla on tuotannonohjausjärjestelmän tietokoneen käytössä. Tuotannonohjausjärjestelmään kirjautuminen tapahtuu kaikilla käyttäjillä samoilla tunnuksilla. Tietokonetta myös käytetään muuhunkin kuin tuotannonohjaukseen esimerkiksi sähköpostiviestintään ja internetin selaamiseen. Lisäksi tuotantorakennuksen lähiverkkoa ei ole suojattu. Myös tietoverkkosuunnitelma tilalta puuttuu.

Kehittämissuunnitelmassa korjataan tilannetta tilan kyberuhkiin varautumisessa. Ensinnäkin tilalla tulee tarkastaa UPS-varavirtalähteiden akut ja varmistua siitä, että akkujen kapasiteetti on riittävä. Lisäksi tilalle tulee hankkia tuotannonohjaukseen käytettävän tietokoneen lisäksi toinen tietokone, jotta tuotannonohjausjärjestelmän tietokoneen käyttö on vain tuotannonohjaukseen. Tuotannonohjausjärjestelmään tulee luoda omat tunnukset käyttäjille ja suojata lähiverkko. Tilalle tulee myös laatia tietoverkkosuunnitelma. Tietoverkkosuunnitelma on apuna ratkaistaessa tietoverkkojen ongelmatilanteita, sillä siitä nähdään miten laitteet ovat verkossa sijoittuneet.

5.4 Eettisyys ja luotettavuus

Laadullisessa tutkimuksessa tutkija on paljon vartijana. Hän päättää tutkimuksen kohteet ja sen mitä kysytään, mitä ei kysytä sekä miten kerätty aineisto analysoidaan ja tulkitaan. Luotettavuustarkasteluun ja riskienhallintaan tulee varautua jo työn suunnitteluvaiheessa. Opinnäytetyön riittävä dokumentaatio on luotettavuustarkastelun edellytys. (Kananen 2014, 150–151.)

Tutkimukseen osallistuneille henkilöille informoitiin tutkimuksen alussa tutkimuksen aiheesta, tarkoituksesta sekä luottamuksellisuudesta tietojen suhteen. Kaikki tunnistettavuus, esimerkiksi päivämäärät ja niin edelleen on jätetty pois tuloksien analyysivaiheessa. Tutkimuksessa on esitetty tuloksia rehellisesti, mikä on osa eettisyyttä. Kirjoittajat ovat esittäneet omat ajatuksensa omana

tekstinään, eikä niitä ole kopioitu lähteistä. Tutkijat ovat arvioineet tutkittavaa ilmiötä neutraalisti ja kriittisesti.

Aineistonkeruussa laadukkuutta parannettiin laatimalla kyselykaavake yhdessä toimeksiantajan kanssa. Kyselykaavaketta ja teemahaastattelun runkoa esitettiin tutkimuksen toimeksiantajalle sekä tutkimusta ohjaavalle henkilölle. Tällä varmistettiin, että tutkittiin oikeita asioita. Maitoyrittäjien jäsentiloille lähetettiin kyselyt huhtikuussa ennen peltotöiden alkamista, jotta kyselyyn saataisiin mahdollisimman paljon vastauksia. MTK:n Maitovaliokunnalle ja Maitovaltuuskunnalle kysely lähetettiin toukokuussa, ja heille annettiin pidempi vastausaika. Opinnäytetyön tekijöillä on käsitys automaattilypsytilan toiminnasta, joten yhteinen kieli laitetoimittajien teemahaastatteluissa toteutui. Teemahaastatteluihin pyydetyt laitetoimittajat edustavat valtaosaa Suomen lypsyrobottimarkkinoista. Laitetoimittajien edustajille lähetettiin ennakkoon haastattelun teemat, jolloin heillä oli mahdollisuus valmistautua haastatteluun. Sekä kyselyjen että haastatteluiden vastauksista saatiin muodostettua kokonaiskuva kyberturvallisuuden tilanteesta automaattilypsytiloilla.

Suurin osa kyselyyn vastanneista automaattilypsytilallisista oli 41–50-vuotiaita. Vastaajilla oli keskimäärin 1,7 lypsyrobottia tilallaan. Kyselyyn vastaajia oli eniten Pohjois-Pohjanmaan, Pohjois-Savon ja Etelä-Pohjanmaan ELY-keskuksien alueilta. Kyselyyn vastanneiden otoksessa on siis nähtävissä yhteneväisyyttä, kun tarkastellaan koko Suomen lypsykarjatilallisia. On kuitenkin huomioitava, että kysely on toimitettu vain tietylle joukolle automaattilypsytilallisia. Tällä voi olla vaikutusta vastausten painotukseen ja siten kyselyn luotettavuuteen.

6 Johtopäätökset

Kyselyyn vastanneiden kyvyssä hahmottaa kyberturvallisuuden ja tietoturvan merkitystä yritystoiminnassaan on puutteita. Vastaajista 73 prosenttia piti tilalle kohdistuvaa kyberuhkaa epätodennäköisenä tai hyvin epätodennäköisenä. Kaikki haastatellut laitetoimittajat korostivat, että tietotekninen osaaminen on erittäin vaihtelevaa tiloilla, mikä lisää käyttäjän aiheuttamaa riskiä. Maidontuottajien vastauksista näkyi tukihenkilöiden kirjo. Tietoverkkojen dokumentoinnissa havaittiin puutteita. Vastanneista yli kolmasosa käytti tuotannonohjaustietokonetta esimerkiksi sähköpostien lukemiseen. Laitetoimittajien suositus erillisen ns. hupikoneen käytöstä tulisi tilallisen ottaa vakavasti. Laitetoimittajat korostivat, että tieto tallentuu useampaan paikkaan. Heillä ei ollut tarjota tilallisille esimerkiksi koulutusta kyberturvallisuusasioissa.

Puolella kyselyyn vastanneista tiloista oli käytössä kaikilla yhteiset tunnukset ja käyttöoikeudet. Tästä voidaan päätellä, että tilalliset luottavat työntekijöihin ja toimijoihin, eikä heitä koeta uhkana. On kuitenkin huomioitava se, että mikäli jokaisella käyttäjällä olisi omat käyttäjätunnukset, ongelmatilanteessa päästäisiin paremmin selvyyteen esimerkiksi tiedoissa tapahtuneista muutoksista. Riippuvuus sähköstä tunnistettiin hyvin, sillä lähes kaikilla vastanneista oli varavoima käytössä. Tämä voi johtua siitä, että sään ääri-ilmiöt ovat lisääntyneet ja se on jo tiedossa oleva riski.

Automaattilypsytiloille luodaan kyberturvallisuuskulttuuria lisäämällä kyberriskit liiketoimintasuunnitelmaan ja viemällä ne operatiiviselle tasolle tilan johtamisessa. Toimintakulttuuri syntyy, kun tilallinen:

1. Tunnistaa riippuvuuden tietotekniikasta ja siihen liittyvät riskit
2. Valitsee suojatoimet ja toteuttaa niitä
3. Havainnoi toimintaympäristöä – on tilannetietoinen riskitilanteista
4. Huolehtii toiminnoista, joiden avulla palautuminen on nopeaa

7 Pohdinta

Opinnäytetyössä tuotiin yhteen maidontuottajien ja laitetoimittajien näkemyksiä tietoturvasta ja kyberturvallisuudesta automaattilypsytiloilla. Näistä näkemyksistä sekä haastatteluista ja dokumenteista syntyi neljä tavoitetta toimintakulttuurin luomiseksi automaattilypsytiloille. Yrittäjä hyödyntää toiminnassaan syntyvää dataa tilansa johtamisessa ja kehittämisessä. Siksi on tärkeää, että yritys tunnistaa riippuvuuden tietotekniikasta ja tiedostaa riskitekijät.

Nykyaikainen navettateknologia sisältää erilaisia verkkoympäristöön kytkettyjä seurantalaitteita niin lypsyroboteissa kuin muualla tuotantoympäristössä. Nämä laitteet kerryttävät koko ajan yhä enemmän dataa. Kun kehitetään riittävät suojatoimet, suojataan samalla tätä maatilan kerryttämää dataomaisuutta. Viljelijä varastoi kasvukaudella tuotetun sadon huolellisesti, niin että riskit sadon pilaantumiseen ovat mahdollisimman vähäiset. Myös tuotettu data tulee varastoida turvalliseen paikkaan, jotta se on tarpeen tullen käytettävissä. Investointi uuteen kahden lypsyrobotin pihattoon maksaa noin kaksi miljoonaa euroa. Investoinnin yhteydessä liiketoimintasuunnitelmassa tulisi huomioida riskitekijöissä myös kyberuhat ja niihin varautuminen. Tilakoon kasvattaminen

tarkoittaa usein myös uusien työntekijöiden palkkaamista. Osaavan työvoiman saanti on haastavaa maatiloilla. Jos ajatellaan kyberrakennetta, tämä tuo haasteita kyberrakenteen ihmiskerrokseen. Käyttäjätunnuksilla ja käyttöoikeuksia rajoittamalla voidaan ehkäistä käyttäjän aiheuttamia riskejä.

Maatalouden rakennemuutoksen jatkuessa maitoa tuottavia tiloja on tulevaisuudessa entistä vähemmän. Toimintaympäristö on viime vuosina muuttunut niin, että sitä on yhä vaikeampi ennakoida ja muutostahti on nopeaa. Rikolliset lisäävät tahoja, joihin yrittävät vaikuttaa. On täysin mahdollista, että myös elintarvikeketjuun voi kohdistua uhka. Maatilojen kasvava yksikkökoko, alueellinen keskittyminen ja automaattilypsyyn siirtyminen lisäävät kotieläintilojen haavoittuvuutta. Yksittäisen tilan yhteiskunnallinen arvo tulee kasvamaan. Huoltovarmuuden kannalta ilmiö lisää kansallisen turvallisuuden riskiä. Vaatimukset tietoturvan ylläpitämisessä ja kyberturvallisuudessa kasvavat koko ajan. Maatilan kyvyllä havaita ja torjua kyberuhkia ja -häiriötilanteita on merkittävä rooli elintarvikeketjun jatkuvuuden ja elintarviketurvallisuuden kannalta. Maitotilalla tulojen menetys aiheuttaa taloudellista tappiota, jos maitoa ei saada tuotettua maidon jalostajalle. Mikäli lypsyrobotin erottelumaitotietoja päästäisiin muuttamaan, tilasäiliöön voisi joutua elintarvikekelvotonta maitoa. Eläinten hyvinvointi vaarantuu lypsyn viivästyessä ja tällä voi olla vaikutusta koko maatalousalan imagoon. Laitetoimittajat kehittävät koko ajan erilaisia nautojen hyvinvoinnin mittaamislaitteita, joiden avulla saadaan tietoa eläinten terveydestä ja hyvinvoinnista. Näihin liittyvien sovellusten päivittäinen käyttö siirtyy yhä enemmän älypuhelimiin, mikä lisää uhkia.

Ongelmatilanteessa nopea palautuminen eläinten hyvinvoinnin kannalta on erityisen tärkeää. Ajantasaisesta varmuuskopiosta on tällöin suuri apu. Kuka varmistaa varmuuskopioinnin toimivuuden? Laitetoimittajat sanoivat varmuuskopioinnin tapahtuvan useampaankin paikkaan. He eivät suositelleet tilallisen tekevän palauttamista. Pohdimme sitä, miten tulee varmistettua, että varmuuskopioitu tiedosto on varmasti kunnollinen. Kyselyssä olisimme voineet kysyä erikseen, onko tiloilla kyberturvallisuuden vastuuhenkilöä ja miten osaamista on hankittu. Mikäli nimettyä henkilöä ei ole, asia on silloin ikään kuin kaikkien vastuulla eli ei kenenkään.

Yhteistyötä eri alojen ammattilaisten välillä tarvitaan, jotta maatalouden kyberturvallisuutta voidaan parantaa. Jokaisella suomalaisella maatilalla on mahdollisuus saada ELY-keskuksen myöntä-

mää tuettua neuvontaa maatilan kehittämiseen ja muutoskestävyyteen. Kun maatilojen koko kasvaa, korostuu sekä asiantuntijoiden että viljelijöiden ammattitaito. Tärkeää on myös huolehtia maatalousalan opiskelijoiden perehdyttämisestä kyberturvallisuuteen ja tietoturvaan. Viljelijä seuraa kasvukaudella tarkasti sääennusteita ja ennakoi toimintaansa. Pitäisikö seurantaan ottaa myös kybersää?

Tässä opinnäytetyössä rajasimme tarkastelun pelkkään automaattilypsyyn. Maatiloilla yleistyvät erilaiset tietoverkkoja käyttävät järjestelmät teknologian kehittyessä. Maatilat ovat lisäksi riippuvaisia monenlaisista tuotantopanoksista. Häiriöt edellä mainituissa aiheuttaisivat tuotannon menetyksiä tilalliselle. Jatkoaiheeksi tutkimuksellemme ehdotamme Kyberturvallisuus maatilayrityksessä - koulutuspaketin suunnittelua. Tätä opinnäytetyötä tehdessä olemme tulleet siihen tulokseen, että tietoturva on inhimillistä ja virheitä sattuu. Tietoturvaan liittyvät asiat ovat kuitenkin opittavissa ja ne voivat olla myös kiinnostavia.

Lähteet

Ala-Kleemola, K. 2022. Kyberhyökkäykset kohdistuvat myös maatalouteen. Käytännön Maamies 28.10.2022.

Allianz Risk Barometer 2023. Cyber and business interruption top threats as economic and energy risks rise. Viitattu 1.9.2023. https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2023-press.html.

Avoimesti, rohkeasti ja yhdessä - Valtionhallinnon viestintäsuositus. 2016. Valtioneuvoston kanslian julkaisusarja. Viitattu 3.4.2023. https://vnk.fi/documents/10616/3541383/Valtionhallinnon-viestintasuositus-2016.pdf.

Calder, A. 2018. NIST Cybersecurity Framework: A Pocket Guide. IT Governance Publishing Ltd. Viitattu 15.6.2023. https://viewer.books24x7.com/assetviewer.aspx?bookid=143662&chunkid=1&rowid=2#2&resumebookmarkid=1111e868-6d0b-ee11-80cb-0050569562bd.

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). 2023. Euroopan komissio. Viitattu 15.6.2023. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

Drape, T., Magerkorth, N., Sen, A., Simpson, J., Seibel, M., Murch, R. & Duncan, S. 2021. Assessing the Role of Cyberbiosecurity in Agriculture: A Case Study. Frontiers in Bioengineering and Biotechnology. Volume 9-2021. Viitattu 25.8.2023. https://www.frontiersin.org/articles/10.3389/fbioe.2021.737927/full.

Elintarvikehuolto. N.d. Huoltovarmuuskeskuksen verkkosivu. Viitattu 16.4.2023. https://www.huoltovarmuuskeskus.fi/toimialat/elintarvikehuolto.

Eläinten merkintä ja rekisteröinti. 2023. Ruokavirasto. Viitattu 1.9.2023. https://www.ruokavirasto.fi/elaimet/elaintenpito-tunnistaminen-ja-rekisterointi/elainten-merkinta-ja-rekisterointi/.

Endsley, M.R. 1995. Toward a theory of situation awareness in dynamic systems. Human Factors. The Journal of the Human Factors and Ergonomics Society, 37, 1.

EU:n maatalouspolitiikan viestintästrategia 2023–2027. 2023. Maaseutuverkosto.fi. Viitattu 16.4.2023. https://maaseutuverkosto.fi/wp-content/uploads/2023/03/EUn-maatalouspolitiikan-viestintastrategia-2023-2027_FINAL1-1.pdf.

Fjäder, C. N.d. Huoltovarmuuden toimintaympäristön muutos ja uhkakuvat. Huoltovarmuuskeskus. Viitattu 9.8.2023. https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-174875.pdf.

Global Risks Report 2023. 2023. World Economic Forum. Viitattu 24.4.2023. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

Hetemäki, T. 2020. Millaista on onnistunut kriisiviestintä? Viimeinen sana -ajankohtaisohjelma 21.3.2020. Yle areena -verkkopalvelu. Viitattu 16.4.2023. https://areena.yle.fi/1-50482678.

Hietala, O., Ilomäki, J., Kotilainen, J-P., Laajalahti, M., Lassheikki, M., Luukkainen, K., Mantila, J., Moilanen, P., Niemi, J., Nikander, J., Nuutila, J., Tikkanen, T. 2018. Kyberin taskutieto maatiloille. Jyväskylän yliopisto ja Maanpuolustuskoulutusyhdistys. Viitattu 1.4.2023. https://www.mtk.fi/documents/20143/310288/Maatilan+kyber-opas.pdf/99f34233-633c-6afe-9173-263520aab386?t=1549010214826.

Hirsijärvi, S., Remes, P. & Sajavaara, P. 2016. Tutki ja Kirjoita. 21. p. Porvoo: Tekijät ja Kirjayhtymä

Hulsen, J. 2009. Automaattilypsy. Automaattilypsy-kirja kuuluu Future Farming -sarjaan.

Huoltovarmuuskeskus. Viitattu 29.3.2023. https://www.huoltovarmuuskeskus.fi/toimialat/elintarvikehuolto.

Järvinen, P. 2018. Kyberuhkia ja somesotaa. Digiaikana sinäkin olet etulinjassa. Jyväskylä: Docendo Oy.

Järvinen, P. 2022. Yrityksen tietoturvaopas. 50 aihetta käytännön tietoturvasta. Helsinki: Helsingin kamari.

Jäykkä, I. 2021. Maatalousyritysten riskit ja riskienhallinta toimintaympäristön muuttuessa. Pro Gradu-tutkielma. Tampereen yliopisto. Viitattu 14.4.2023. https://trepo.tuni.fi/bitstream/handle/10024/131898/J%E4ykk%E4lida.pdf;jsessionid=38658305081BC2B40BB6C03E13E64422?sequence=2.

Kaikki lähtee johtamisesta. N.d. Maitoyrittäjät ry. Viitattu 29.6.2023. https://www.maitoyrittajat.fi/yhdistys/.

Kananen, J. 2014. Laadullinen tutkimus opinnäytetyönä. Miten kirjoitan kvalitatiivisen opinnäytetyön vaihe vaiheelta. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas. Näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kananen, I. 2015. Suomen huoltovarmuus. Jyväskylä: Docendo.

Kankainen, S. 2019. Sisäinen viestintä: 10 perusohjetta johtajille ja esimiehille. Helsingin yliopisto: HY+. Viitattu 16.4.2023. https://hyplus.helsinki.fi/sisainen-viestinta-10-perusohjetta-johtajille-ja-esimiehille/.

Karhinen, R. 2019. Uusi alku: Maatalous on myös tulevaisuuden elinkeino. Maa- ja Metsätalousministeriön julkaisuja 2019:3. Viitattu 10.9.2023. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161359/MMM_3_2019_Turvallista%20ruokaa%20Suomesta.pdf?sequence=4&isAllowed=y.

Koivumäki, S. 2022. Maatalouden kilpailukyky. Viitattu 26.3.2023. https://mmm.fi/maaseutu/maatalouden-kilpailukyky.

Kyberin taskutieto maatiloille 2018. Jyväskylän yliopisto ja maanpuolustuskoulutusyhdistys. Viitattu 20.5.2023. https://www.huoltovarmuuskeskus.fi/files/03fc266685b82f9683fb0ccc550a5365f56b4545/maatilojen-kyber-opas.pdf.

Kyberrikoksen tutkinta. N.d. Poliisin verkkosivusto. Viitattu 16.4.2023. https://poliisi.fi/kyberrikosten-tutkinta.

Kybersää. 2023. Kyberturvallisuuskeskus. Viitattu 15.6.2023. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa?toggle=Kybers%C3%A4%C3%A4tiedotteet%202023.

Kyberturvallisuuden sanasto. 2018. Sanastokeskus. Viitattu 30.4.2023. https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf.

Laukkanen, M. 2018. Kyberturvallisuus Suomessa. Tietotekniikan pro gradu -tutkielma. Vaasan yliopisto, Tekniikan ja innovaatiojohtamisen yksikkö. Viitattu 1.4.2023. https://osuva.uwasa.fi/bitstream/handle/10024/9363/osuva_8154.pdf?sequence=1&isAllowed=y.

Lindberg, M. 2019. Työntekijöille ei saa antaa liian laajoja oikeuksia tietojärjestelmiin. Blogikirjoitus Opsec Oy:n sivulla. Viitattu 7.5.2023. https://www.opsec.fi/fi/2019/02/06/tyontekijoille-ei-saa-antaa-liian-laajoja-oikeuksia-tietojarjestelmiin/.

Lypsykarjan tuotosseuranta. 2023. ProAgria verkkosivusto. Viitattu 1.9.2023. https://www.proagria.fi/palvelut/kotielaintuotanto/tuotosseuranta.

Lönnqvist, I. & Moilanen, P. 2018. Kyberin taskutieto. Keskeisin kybermaailmasta jokaiselle. 2. korjattu painos. Jyväskylän Yliopisto. Maanpuolustuskoulutusyhdistys. Viitattu 17.4.2023. https://mpk.fi/wp-content/uploads/2022/05/MPK-JY-Kyberopas_2018-issuu.pdf.

Maatalous- ja puutarhayritysten lukumäärä tuotantosuunnittain ELY-keskuksittain. Luonnonvarakeskuksen tilastotietokannan verkkosivulla. Viitattu 18.9.2023. https://statdb.luke.fi/PxWeb/pxweb/fi/LUKE/LUKE__02%20Maatalous__02%20Rakenne__02%20Maatalous-%20ja%20puutarhayritysten%20rakenne/03_Maatalous_ja_puutarhayrit_lkm_tuotantos_ELY.px/chart/chartViewColumnStacked/?rxid=786f0450-355f-4a91-af51-6898606f4e0f.

Maitohygienialiitto. Viitattu 27.3.2023. http://www.maitohygienialiitto.fi/tilastot.

Manninen, O. 2019. Lypsyrobotti soitteli ison laskun ja valvontakamera vuoti nettiin - kyberriskit uhkaavat myös maatiloja. OP Media. Viitattu 1.9.2023. https://www.op-media.fi/digitalisaatio/lypsyrobotti-soitteli-ison-laskun-ja-valvontakamera-vuoti-nettiin--kyberriskit-uhkaavat-myos-maatiloja/.

Mikä on palomuuri? N.d. F-secure verkkosivu. Viitattu 5.6.2023. https://www.f-secure.com/fi/articles/firewall.

Mikä on Ruokavirasto? 2023. Ruokavirasto. Viitattu 14.42023. https://www.ruokavirasto.fi/tietoameista/mika-on-ruokavirasto/.

Mitä on kyberturvallisuus? 2022. F-Secure. Viitattu 2.4.2023. https://www.f-secure.com/fi/home/articles/what-is-cyber-security.

Moore, J. 2022. Tracktors vs. threat actors: How to hack a farm. Viitattu 25.3.2023. https://www.welivesecurity.com/2022/12/05/tractors-threat-actors-how-hack-farm/.

Mälkiä, P. 2023. Automaattiset lypsyjärjestelmät ovat jo mittavia lehmien terveyden seurantajärjestelmiä. KMVET Kotieläinten terveydenhoitolehti 10.2.2023. Viitattu 20.8.2023. https://kmvet.fi/automaattiset-lypsyjarjestelmat-ovat-jo-mittavia-lehmien-terveyden-seurantajarjestelmia/.

Neittaanmäki, P., Lehto, M. & Savonen, M. 2021. Yhteiskunnan digimurros. Jyväskylä: Jyväskylän yliopiston IT-tiedekunta.

Nikander, J., Manninen, O. & Laajalahti, M. 2020. Requirements for cybersecurity in agricultural communication networks. Computers and Electronics in Agriculture, 179. Viitattu 12.8.2023. https://www.sciencedirect.com/science/article/pii/S0168169920314812?ref=pdf_download&fr=RR-2&rr=7f574b872fb63767.

NIS2. 2022. Direktiivi toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa. Annettu 14.12.2022. Viitattu 15.6.2023. https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32022L2555.

Oksanen, T. 2022. Vuosihuolto ja IT-päivä. Koneviesti. Puolueeton tekninen ammattilehti, 15/2022, 13. Viitattu 14.4.2023. https://www.koneviesti.fi/huolto-ja-tekniikka/9175a930-44bd-4062- 8037-98fdd895ee33.

Paasonen, J. 2020. Kriisijohtaminen ja -viestintä – Miten johtaa kriisitilanteessa? Blogikirjoitus. Julkaistu 30.6.2020. Viitattu 16.4.2020. https://jyripaasonen.fi/kriisijohtaminen-ja-viestinta-miten-johtaa-kriisitilanteessa/.

Pirinen, R. & Rajamäki, J. 2015. Mechanism of critical and resilient digital services for design theory. Viitattu 8.6.2023. https://ieeexplore-ieee-org.ezproxy.jamk.fi:2443/document/7331874?figureId=fig1#fig1.

Pysy ajan tasalla kyberturvallisuuden kiinnostavimmista ilmiöistä. N.d. Liikenne- ja viestintävirasto Traficomin kyberturvallisuuskeskuksen verkkosivu. Viitattu 16.4.2023. https://www.kyberturvallisuuskeskus.fi/fi/.

Pöyhönen, J. 2023. Tutkijatohtori. Jyväskylän yliopisto: IT tiedekunta, kyberturvallisuus. Haastattelu 7.6.2023.

Pöyhönen, J. 2020. Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa. Systeemiajattelu. Väitöstutkimus. Jyväskylän yliopisto, Informaatioteknologian tiedekunta.

Ryhänen, M. & Sipiläinen, T. 2018. Maatalousyrityksen johtaminen ja toiminnan kehittäminen-tuotannon suunnittelu strategisen johtamisen tukena. Helsinki: Tempest. Viitattu 26.3.2023. https://helda.helsinki.fi/bitstream/handle/10138/228594/Ryh%c3%a4nen%26Sipil%c3%a4inen_2018_OPPIKIRJA.pdf?sequence=3&isAllowed=y.

Saarivaara, P. & Pirttijärvi, R. 2022. Maidontuotannon kehitysnäkymät 2030. Kantar TNS Agri.

Salasanat haltuun. N.d. Kyberturvallisuuskeskus. Viitattu 7.5.2023. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Salasanat_haltuun.pdf.

Suomalaisten organisaatioiden tietoturva 2023–2025. 2022. Tutkimus. Loihde Trust & Check Point Software Technologies Ltd.

Sähköinen tunnistaminen. 2023. Liikenne- ja viestintävirasto Traficom. Kyberturvallisuuskeskus. Viitattu 5.5.2023. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen.

Tiedostojen varmuuskopiointi. N.d. Helsingin yliopisto. Opiskelijan digitaidot. Viitattu 5.5.2023. https://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/4-2-suojautuminen-uhkatekijoilta/tiedostojen-varmuuskopiointi/.

Tietoturva. 2020. Liikenne- ja viestintävirasto: Kyberturvallisuuskeskus. Viitattu 2.4.2023. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva.

Tikanmäki, S. 2021. Strateginen viestintä lähtee organisaation tavoitteista. Viesti ry. Julkaistu 6.10.2021. Viitattu 16.4.2023. https://viesti.fi/strateginen-viestinta-lahtee-organisaation-tavoitteista/.

Toimialojen kyberkypsyyden selvitys 2022. 2023. Kansallinen koosteraportti. Huoltovarmuuskeskus. Viitattu 29.3.2023. https://www.huoltovarmuuskeskus.fi/files/29b11d0af56a115126ad490af444f1c4fd7885af/hvk-toimialojen-kyberkypsyyden-selvitys-2022.pdf.

Turvallisuutta tuotetaan yhdessä. 2018. Kausi 2, osa 7. Keva ja Vaasan yliopisto. Podcast- Keskustelusarja kompleksisuusajattelusta. SoundCloud. Viitattu 24.4.2023. https://soundcloud.com/kompleksisuus/podcast-turvallisuutta-tuotetaan-yhdessa-kausi-2-osa-7.

Vertainen, V., Brandt, J. & Suni, E. 2023. Kyberturvallisuus alkutuotannossa. Jyväskylän ammattikorkeakoulun elintarviketuotannon ja -jakelun kyberpoikkeaman hallinnan julkaisut, osa1/3. Viitattu 16.4.2023. https://www.theseus.fi/bitstream/handle/10024/788853/Kyberturvallisuus%20alkutuotannossa%20kasikirja.pdf?sequence=2&isAllowed=y.

Viestintää johdetaan, suunnitellaan ja arvioidaan. N.d. Valtioneuvoston kanslia. Viitattu 16.4.2023. https://vnk.fi/viestintasuositus/luku-3.

Viisas varautuu hyvän sään aikana. N.d. Viitattu 24.8.2023. https://maavara.savonia.fi/.

Viljelijöiden keski-ikä tuotantosuunnittain. Luonnonvarakeskuksen tilastotietokannan verkkosivulla. Viitattu 30.3.2023. https://statdb.luke.fi/PxWeb/pxweb/fi/LUKE/LUKE__02%20Maatalous__02%20Rakenne__02%20Maatalous-%20ja%20puutarhayritysten%20rakenne/08b_Viljelijoiden_ika_tuotantos_ELY.px/table/tableViewLayout2/?rxid=786f0450-355f-4a91-af51-6898606f4e0f

Welch, J. 2016. Five assumptions you have to make when managing a crisis. Blogikirjoitus. Julkaistu 17.10.2016. Viitattu 16.4.2023. https://jackwelch.strayer.edu/winning/crisis-management-five-assumptions/.

Liitteet

Liite 1. Kysely tilallisille – Tietoturvallisuuden ylläpitäminen ja kyberuhkiin varautuminen

TAUSTATIEDOT

1. Vastaajan ikä

    18 – 30

    31 – 40

    41 – 50

    51 –

2. Korkein saavutettu koulutustaso

    Keski- tai perusasteen tutkinto tai vastaava

    Ammattikoulu tai lukio

    Alempi korkeakoulututkinto

    Ylempi korkeakoulututkinto

    Joku muu, mikä?

3. Tilan sijaintikunta

4. Lypsyrobotin merkki

    Lely

    DeLaval

    GEA

    RDS

    Fullwood

    Joku muu, mikä?

5. Lypsyrobottien määrä

    1

    2

    3

    4 tai enemmän

KRIITTINEN VARAUTUMINEN - SÄHKÖ

6. Onko käytössänne varavoimalähdettä?

Kyllä

Ei

7. Riittääkö varavoima kattamaan tuotantorakennuksen toiminnan?

Kyllä

Ei

En osaa sanoa

KRIITTINEN VARAUTUMINEN – OHJELMISTOT

8. Valitse seuraavista kaikki ne vaihtoehdot, jotka toteutuvat lypsyrobotin tuotannonohjausjärjestelmään tunnistautuessa?

Jokaisella okaisella käyttäjällä omat käyttäjäkohtaiset tunnukset ja oikeudet

Pääkäyttäjillä omat tunnukset ja oikeudet

Tietyillä käyttäjillä (esim. ruokinnansuunnittelijoilla) omat tunnukset ja oikeudet

Kaikilla käyttäjillä yhteiset tunnukset ja oikeudet

Jotenkin muuten, miten?

9. Mihin käytetään tietokonetta, jossa on tuotannonohjausjärjestelmä?

Tuotannonohjaukseen

Sähköpostiviestintään

Tilan tarvitsemiin oheisohjelmiin (esim. Minun maatilani)

Johonkin muuhun, mihin?

10. Onko tietojärjestelmät suojattu palomuurilla?

Kyllä

Ei

Osittain

En osaa sanoa

11. Onko tietojärjestelmät suojattu virustorjuntaohjelmilla?

Kyllä

Ei

Osittain

En osaa sanoa

12. Onko tuotantorakennuksen lähiverkko suojattu salasanalla tai muulla tunnistautumismenetelmällä?

Kyllä

Ei

En osaa sanoa

13. Onko tuotantorakennuksessanne käytössä kulunvalvontaa

Kyllä

Ei

KRIITTINEN VARAUTUMINEN – VARMUUSKOPIOINTI

14. Onko tuotannonohjausjärjestelmässänne käytössä varmuuskopiointi?

Kyllä

Ei

En osaa sanoa

15. Kuinka usein tiedostot varmuuskopioidaan?

Päivittäin

Viikoittain

Kuukausittain

Kahden kuukauden välein tai harvemmin

En osaa sanoa

16. Missä varmuuskopiointeja säilytetään?

Tietokoneen C-asemalla

Pilvipalvelussa

Muistitikulla

Ulkoisella kovalevyllä

Jossakin muualla, missä?

En osaa sanoa

17. Oletteko tehneet tai harjoitelleet varmuuskopioitujen tiedostojen palautusta tuotannonohjausjärjestelmään?

Kyllä

Ei

En osaa sanoa

KRIITTINEN VARAUTUMINEN – OMA TOIMINTA

18. Valitse mielestäsi tilan tietoturvan kannalta kriittisimmät tiedot.

Eläintiedot

Tuotostiedot

Tilitystiedot

Ruokintatiedot

Eläinlääkintätiedot

Eläinrekisteritiedot

Jotain muuta, mitä?

En osaa sanoa

19. Valitse mielestäsi kolme (3) tilan tietoturvan kannalta kriittisintä osaa.

Salasanat

Palomuurit/virustorjuntaohjelmat

UPS-varavirtalähde

Suojattu verkkoyhteys

Ajantasaiset päivitykset ohjelmiin ja sovelluksiin

Varmuuskopiointi

Tuotannonohjausjärjestelmän oikeantyyppinen käyttö

Käyttäjä

Vierailijat/ulkopuoliset yhteistyökumppanit

VARAUTUMINEN KYBERUHKIIN

20. Huomioitteko kyberturvallisuuden tilan riskienhallinnassa?

Kyllä

Ei

En osaa sanoa

21. Kuinka todennäköisenä koette, että tilallenne voisi kohdistua kyberuhka?

Erittäin todennäköisenä

Todennäköisenä

Epätodennäköisenä

Hyvin epätodennäköisenä

En osaa sanoa

22. Millä toimenpiteillä olette varautuneet kyberuhkiin?

Ajantasaiset tietotekniset laitteet

Virustorjuntaohjelmat

Palomuurit

Ajantasaiset päivitykset

Vahvat salasanat

Kaksivaiheinen tunnistautuminen

Tietoverkkosuunnitelma

Varaverkkoyhteys

Varmuuskopioinnit

Jotenkin muuten, miten?

Tilalla ei ole varauduttu kyberuhkiin

23. Keneltä saat apua tilan tieto- ja kyberturvallisuuteen liittyvissä asioissa? (Esim. perheenjäsen, palveluntuottaja, laitetoimittaja jne. Voit myös vastata itsesi, mikäli oma osaaminen on riittävää.)

Mikäli kiinnostuit maatilan kyberturvallisuudesta, pääset lukemaan aiheesta lisää Kyberin tasku-tieto maatiloille -julkaisusta.

Linkki julkaisuun:
https://www.mtk.fi/documents/20143/310288/Maatilan+kyber-opas.pdf/99f34233-633c-6afe-9173-263520aab386?t=1549010214826

Liite 2. Saatekirje laitetoimittajille

Hei!

Olemme Jyväskylän ammattikorkeakoulun agrologiopiskelijoita. Teemme opinnäytetyötämme automaattilypsytilojen kyberturvallisuudesta. Tavoitteena on saada kyberturvallisuus osaksi tilan toimintakulttuuria. Olemme lähettäneet kyselytutkimuksen Maitoyrittäjät ry:n jäsentilojen yrittäjille. Kyselyn avulla kartoitamme tilojen varautumisen tasoa tietoturvallisuuden ylläpitämisessä ja kyberuhkiin varautumisessa.

Opinnäytetyömme toisessa vaiheessa teemme haastattelututkimusta lypsyrobottien laitetoimittajille. Tutkimuksen avulla haluamme selvittää esimerkiksi sitä, miten lypsyrobottien käyttöönotossa tietoturvaan ja varautumiseen liittyvät asiat ovat esillä.

Haastattelu toteutetaan Teams-yhteydellä. Arvioimme haastattelun kestävän noin tunnin verran. Käsittelemme haastattelussa seuraavia teemoja: Tietoturva ja käyttöönotto, tietoturva ja tilan tietoverkot, kyberturvallisuus yrityksessä viljelijän näkökulmasta, kyberturvallisuusasiat käyttäjäkoulutuksessa ja etäkäyttö. Olisiko Teidän yrityksessänne henkilö tai vaikka useampiakin, joiden olisi mahdollista osallistua haastatteluun?

Ystävällisin terveisin,

Maija Kinnunen
Päivi Hänninen

Opinnäytetyön ohjaaja:

Jyrki Kataja
Asiantuntija; maatalouden tuotantoprosessit – energiatehokkuus, energian käyttö ja tuotanto, kyberturvallisuus
Biotalousinstituutti
Jyväskylän ammattikorkeakoulu

Liite 3. Teemahaastattelurunko laitetoimittajille

Teema 1. Tietoturva ja käyttöönotto

- Millaisia ohjeita annatte lypsyrobotin käyttöönotossa tilalliselle, jotta tietoturva säilyisi tilan henkilötietojen ja tilan muun tiedon osalta?
- Onko ohjeista dokumenttia?
- Miten varmuuskopiointi tapahtuu laitteessanne? Pilvipalvelu?
- Miten varmistetaan, että tilallinen osaa tehdä varmuuskopioinnin ja varmuuskopioinnin palautuksen?
- Miten häiriötilanteessa palaudutaan takaisin operatiiviseen tilaan?
    - Dokumentaatio
    - Tekninen tuki

Teema 2. Tietoturva ja tilan tietoverkot

- Miten käyttöönoton jälkeen varmistetaan, että suojautuminen tilalla (myyty laite + käyttäjän osaaminen) on riittävällä tasolla?
- Kuinka usein laitteet huolletaan ja kiinnitetäänkö huolloissa huomiota tietoturvaan?
- Miten tila on tietoverkkojen osalta yhteydessä robottivalmistajaan? Onko tietoverkoista saatavilla kuvaa?
- Ymmärtääkö 3. osapuolet (muut yrityksen tarvitsemat yhteistyökumppanit) lypsytilan kriittisyyden?

Teema 3. Kyberturvallisuus yrityksessä

- Digitalisaatio lisääntyy ja uhat kasvavat. Miten yrityksen tuotteisiin ja palveluihin liittyvä kyberturvallisuus toimii viljelijän näkökulmasta?
- Kuinka näette roolinne suhteessa automaattilypsyä harjoittavaan tilalliseen?

Teema 4. Käyttäjäkoulutus kyberturvallisuusasioissa

- Onko yrityksessänne koulutusta maitotilayrittäjälle?

Teema 5. Etäkäyttö ja tietokone, jossa tuotannonohjausjärjestelmä

- Etäkäytön riskit
- Tietokoneen käyttö muihin tilan tarvitsemiin ohjelmiin?
- Miten tilallista ohjeistetaan?

Teema 6. Mitä huomioita tulevaisuudesta?

Maailman talousfoorumi julkaisee vuosittain raportin globaaleista riskeistä. Raportin mukaan hyökkäyksiä odotetaan kohdistuvan huoltovarmuuden kannalta merkittäviin kohteisiin kuten maatalouteen, vesihuoltoon ja energiaan.

- Mihin pitäisi erityisesti kiinnittää huomiota?

Liite 4. Esimerkkitilan kyberturvallisuuskartoitus

Kyberturvallisuuden huomioiminen automaattilypsytilan toiminnassa
Esimerkkitila -case

SÄHKÖN SAATAVUUS	Kunnossa	Ei kunnossa	Huomioitavaa
Varavoimalähde	X		Riittää kattamaan tuotantorakennuksen toiminnan
UPS-varavirtalähde	X		Tuotantorakennuksessa, riittää muutaman päivän
Varavirtalähteiden akkujen tarkastaminen		X	Ei tarkastettu

LAITTEET JA OHJELMISTOT	Kunnossa	Ei kunnossa	Huomioitavaa
Tietoverkkosuuunnitelma		X	
Ajantasaiset tietotekniset laitteet	X		
Automaattiset päivitykset	X		
Palomuurit	X		
Virustorjuntaohjelmat	X		
Varmuuskopiointi (tarpeeksi usein, säilytys)	X		ulkoinen kovalevy, päivittäin
Käyttäjätunnukset (vähintään pääkäyttäjillä omat tunnukset)		X	
Vahvat salasanat		X	
Tuotannonohjausjärjestelmän tietokoneen käyttö vain tuotannonohjaukseen		X	
Lähiverkon suojaus salasanalla tai muulla tunnistautumismenetelmällä		X	
Varaverkkoyhteys	X		
Tuotantorakennuksen kulunvalvonta	X		