Luonnonvara- ja
biotalouden
tutkimus 32/2017

Alkutuotannon kyberuhat

Mikko Laajalahti ja Jussi Nikander

Luke
LUONNONVARAKESKUS

Luonnonvara- ja biotalouden tutkimus 32/2017

Alkutuotannon kyberuhat

Mikko Laajalahti ja Jussi Nikander

Luonnonvarakeskus, Helsinki 2017

Laajalahti, M. & Nikander, J. 2017. Alkutuotannon kyberuhat. Luonnonvara- ja biotalouden tutkimus 32/2017. Helsinki. Luke. 38 s.

ISBN: 978-952-326-410-6 (Painettu)
ISBN: 978-952-326-411-3 (Verkkojulkaisu)
ISSN 2342-7647 (Painettu)
ISSN 2342-7639 (Verkkojulkaisu)
URN: http://urn.fi/URN:ISBN:978-952-326-411-3

Kirjoittajat: Mikko Laajalahti ja Jussi Nikander
Julkaisija ja kustantaja: Luonnonvarakeskus (Luke), Helsinki 2016
Julkaisuvuosi: 2017
Kannen kuva: Mikko Laajalahti
Painopaikka ja julkaisumyynti: Juvenes Print, http://luke.juvenesprint.fi

Tiivistelmä

Tietotekniikan käyttö alkutuotannon prosesseissa lisääntyy nopeasti. Käytössä olevat sekä kiinteät, että liikkuvat laitteet kytketään tietoverkkoon, jotta voidaan mahdollistaa uusia toiminnallisuuksia ja tehostaa toimintaa verkottuneiden ratkaisujen avulla. Samalla laitteiden kyberturvallisuuden merkitys kasvaa, kun niihin on mahdollista vaikuttaa tietoverkon kautta. Alkutuotannon laitteet noudattavat pääosin kyberturvallisuuden toimialasta riippumattomia perusperiaatteita. Toimintaympäristön erityispiirteitä ovat muun muassa laitekokonaisuuksien syntyminen ilman kokonaissuunnitelmaa, järjestelmällisen ylläpidon puute ja tyypilliseen tietotekniikkaan verrattuna pitkät käyttöiät.

Alkutuotannon kyberturvallisuudelle on useita uhkia, joista tärkeimmät liittyvät tietotekniikan nopeaan kehitykseen ja lisääntymiseen, ja sitä kautta tapahtuvaan jatkuvaan muutokseen. Maatalouden ongelmana on tietoteknisen osaamisen hidas leviäminen, varsinkin alkutuotannossa, ja sitä kautta vajavainen tietotekninen ymmärrys joka johtaa kyberturvallisuuskulttuurin puuttumiseen. Alkutuotannossa on myös erityispiirteitä, jotka asettavat lisähaasteita kyberturvallisuudelle.

Alkutuotannon laitteiden elinkaareen tulee jatkossa kiinnittää huomiota. Käytössä olevan ohjaustekniikan nopea vanheneminen voi tarpeettomasti lyhentää investointien muuta taloudellista elinkaarta. Rakennusten elinkaari on tyypillisesti 30–50 vuotta ja ajoneuvojen ja työkoneiden 10-30 vuotta, kun taas tyypillisen tietotekniikan elinkaari on parhaimmillaankin alle 10 vuotta. Täten laitteen eliniän aikana sen tietotekniikka tulisi uusia 2–10 kertaa ja tekniset ratkaisut, jotka olivat laitteeseen asennettuna sitä ostettaessa, ovat todennäköisesti poistuneet tuotannosta kauan ennen taloudellisen käyttöiän päättymistä. Rakennusten ja laitteiden elinkaaripäivittämiseen ja ylläpitoon tulee varata resursseja.

Alkutuotannon käyttämät ratkaisut ovat vielä hyvin heterogeenisiä. Tämä osaltaan vaikeuttaa koko toimialaa vastaan tehtäviä hyökkäyksiä. Yksittäisen toimijan laitteisiin tapahtuvat iskut ovat yleensä johonkin laitealustaan kohdistuvia. Esimerkiksi sulautettujen laitteiden käyttäminen palveluestohyökkäyksen alustana voi tehdä alkutuotannon toimijasta hyökkäysvälineen. Näistä esimerkkinä on valvontakameroiden avulla tehdyt palvelunestohyökkäykset kolmatta osapuolta vastaan.

Toimialan osaamista kyberturvallisuudessa tulisi kehittää kokonaisvaltaisesti. Uhkien tunnistaminen on ensimmäinen askel niiden hallitsemiseen. Useimmat tietoturvaan liittyvät menetelmät vaativat tiettyä toimintakulttuuria. Ymmärtämätön käyttäjä voi omalla toiminnallaan aiheuttaa tarpeettomia riskejä, esimerkiksi jättämällä säännöllisen päivittämisen, varmistamisen ja varmuuskopioinnin tekemättä. Toimialan kyberturvallisuuden kehittämiseksi tulisi havaittuja haavoittuvuuksia nostaa esille toimintaohjeiden kera, ja toimialan kyberturvallisuutta tulisi kehittää jatkossa määrätietoisesti.

Asiasanat:
Alkutuotanto, automaatio, elintarviketuotanto, ISOBUS, kyberturvallisuus, lypsyrobotti, maatalous

Sisällys

1. Hankkeen perustelut ja tavoite

Tämä työ on tehty osana Maa- ja metsätalousministeriön kyberturvallisuuden toimeenpano-ohjelmaa. Ohjelmassa on noussut esiin tarve selvittää elintarvikkeiden alkutuotantoon ja tuotantoketjun turvallisuuteen kohdistuvia kyberuhkia. Alun perin työ rajattiin koskemaan elintarviketeollisuutta ja elintarvikkeiden alkutuotantoa, mutta hankkeen aikana havaittiin, että resurssit riittävät vain alkutuotannon kyberuhkien kartoittamiseen. Elintarvikeketjut ja muu elintarviketeollisuus rajattiin täten selvityksen ulkopuolelle. Työn tavoitteena on koota kokonaiskuva elintarvikkeiden alkutuotannon haavoittuvuuden nykytilasta, sekä tehdä toimenpide-ehdotuksia jotka tähtäävät parempaan kyberturvallisuuteen alkutuotannossa ja koko elintarvikesektorilla. Sähkönjakeluun ja sen häiriöihin liittyvät uhat käsitellään hankkeessa vain siten, kuin ne suoraan vaikuttavat alkutuotannon kybertoimintaympäristöön. Laajempi sähkönjakelun häiriökartoitus suoritetaan Jatkosähkö -hankkeessa.

Hankkeessa tuotetaan raportti, jota voidaan käyttää sekä sinällään kyberuhkatietämyksen levittämisessä, mutta joka voi toimia myös lähtökohtana myöhemmille kehittämis- ja tutkimustoimille.

2. Sanastoa

”Kyber” on etuliite joka tarkoittaa tietokoneisiin, tietoverkkoihin ja tietoliikenteeseen liittyvää toimintaa. Tässä raportissa termiä kyber käytetään kaikesta toiminnasta, mihin liittyy sähköisessä muodossa olevaa tietoa. Täten esimerkiksi termi kyberuhka käsittää uhat, jotka kohdistuvat sähköisessä muodossa olevaan tietoon tai tätä tietoa käyttävään toimintaan. Kyberuhka voi olla esimerkiksi tiedon katoaminen, luvaton kopiointi, vääristyminen, tai siihen käsiksi pääsyn estäminen. Kyberuhka voi kohdistua itse tiedon lisäksi myös kybertoimintaympäristöön, eli sähköisessä muodossa olevan tiedon käsittelyyn tarkoitettuun tietojärjestelmään. Järjestelmään voidaan esimerkiksi tunkeutua, se voi vaurioitua, tai sen käyttäminen voi estyä syystä tai toisesta. Uhka voi myös olla tiedon käytön estymisen aiheuttama maatilan toiminnan vaikeutuminen. Esimerkiksi maataloudessa käytössä olevat automaatiojärjestelmät eivät toimi ilman ohjausta.

Alla olevassa taulukossa on lueteltu ja kuvattu tärkeimmät raportissa käytetyt termit.

Kyberturvallisuus	Tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan (Valtioneuvosto 2013).
Kybertoimintaympäristö	Sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö (Valtioneuvosto 2013).
Kyberuhka	Kybertoimintaympäristöön ja tietoon kohdistuva uhka.
Langaton sisäverkko eli WLAN	Langattomasti toteutettu organisaation sisäinen verkko. ”Wireless Local Area Network”
Langaton ulkoverkko eli WWAN	Langattomasti toteutettu laaja-alainen tietoliikenne. Yleensä 3G, 4G, jne. matkapuhelinverkko. ”Wireless Wide Area Network”
Palvelunestohyökkäys	Tietoverkon välityksellä tehtävä hyökkäys, jonka pyrkimyksenä on häiritä tai estää tietyn verkko-osoitteen, -resurssin tai -sivuston toiminta.
Sisäverkko	Organisaation omassa hallinnassa oleva tietoverkko, johon pääsyä internetistä on rajoitettu palomuurin avulla.
Sulautettu järjestelmä	Tiettyyn tarkoitukseen, yleensä laitteen osaksi, tehty laite- ja ohjelmistokokonaisuus.
Ulkoverkko	Organisaation käyttämä verkko joka ei ole omassa hallinnassa
Väyläohjaus	Menetelmä missä järjestelmän eri osat kytkeytyvät ohjaustiedon välitystä varten toisiinsa. Väylä toimii tiedonsiirtoreittinä. Maatalouskoneissa tyypillisesti CAN väylä on SAE J1939 standardin mukainen ratkaisu. ISO 11783 eli ISOBUS perustuu SAE J1939 standardin mukaiseen ratkaisuun.

3. Maatalouden kyberturvallisuus

Kyberturvallisuus tarkoittaa kybertoimintaympäristön toiminnan turvaamista, missä kybertoimintaympäristö on sähköisessä muodossa olevan tiedon käsittelyyn tarkoitettu tietojärjestelmistä ja niihin liittyvistä fyysisen maailman laitteista muodostuva toimintaympäristö. Yleisesti Suomen valtion kyberturvallisuuden kehittämistä ohjaa kansallinen Kyberturvallisuusstrategia (Valtioneuvosto, 2013). Kyberturvallisuudessa tärkein julkinen toimija on Viestintäviraston kyberturvallisuuskeskus, joka ylläpitää valtion kyberturvallisuuden tilannekuvaa. Keskuksen työhön kuuluu myös ylläpitää julkista kyberturvallisuussivustoa[1]. Sivusto on Suomen valtion viestintäkanava kyberturvallisuudesta, mukaan lukien ohjeet ja tämänhetkinen turvallisuustilanne. Keskus on myös laatinut useita ohjeita, joista muutamat liittyvät kyberuhkiin, joita tässä raportissa käsitellään. Kaikki ohjeet löytyvät keskuksen verkkosivuilta[2].

Ohjeita on muun muassa seuraavista asioista (suluissa ohjeen numero): langattomien verkkojen tietoturva (Ohje 2/2011), palvelunestohyökkäysten ehkäisy ja torjunta (Ohje 3/2016), ja ohje kiristyshaittaohjelmia vastaan (005/2016 J). Ohjeita lukiessa kannattaa tosin muistaa, että tietotekniikka kehittyy erittäin nopeasti. Täten vuonna 2011 julkaistu ohje langattomien verkkojen tietoturvasta on jo monelta osin auttamatta vanhentunut. Kyberturvallisuuskeskukselta löytyy myös yksi toimialakohtainen ohje, joka koskee Terveydenhuoltoalan kyberuhkia (Ohje 1/2016).

Maatalouden kyberturvallisuus tarkoittaa ruuantuotannon kybertoimintaympäristön toiminnan turvaamista siten, että ruoka saadaan pellolta aina pöytään asti (farm-to-fork). Tässä työssä kyberturvallisuutta tarkastellaan maatilan näkökulmasta, joten työ käsittelee ensisijaisesti maatilan kybertoimintaympäristön turvaamista.

Maatalouden alkutuotannon ydintoimintaa on biomassan kasvatus. Tästä biomassasta valtaosa menee ruuan ja rehun tuotantoon. Viimeisten vuosien aikana alkutuotannon automaatio, ja tätä kautta myös käytetyn tietotekniikan määrä, on lisääntynyt. Täten alkutuotannon toimintaympäristössä tiedon käsittely ja käyttö on nykyään erittäin tärkeä osa monen maatilan toimintaa. Alkutuotannossa tietotekniikka kytkeytyy hyvin vahvasti erilaisiin koneisiin ja laitteisiin, kuten traktoreihin ja eläinsuojien sekä kasvihuoneiden automaatiojärjestelmiin. Täten maatalouden kyberturvallisuudessa on myös erittäin voimakas fyysiseen maailmaan liittyvä elementti. Kyberuhat voivat heijastua fyysiseen toimintaympäristöön, ja toimintaympäristö itsessään voi altistaa kyberuhille.

Valtaosa kyberturvallisuuteen tarvittavasta teknologiasta, laitteista ja osaamisesta on toimialariippumatonta; pääosin samoja menetelmiä ja periaatteita voidaan käyttää kaikkien alojen kyberturvallisuuden kehittämiseen ja ylläpitämiseen tähtäävässä toiminnassa. Puhutaan esimerkiksi niin sanotusta 80/20 –periaatteesta, jonka mukaan 80 prosenttia kyberturvallisuudesta on yleisluontoista, ja 20 prosenttia on toimialakohtaista (Manning 2016). Periaate on yksi selitys sille, miksi tieteellisessä kirjallisuudessa on kohtuullisen vähän nimenomaan maatalouden kyberturvallisuuteen liittyvää tutkimusta. Kyberturvallisuuden tutkimus on ensisijaisesti yleistä kyberturvallisuuden tutkimusta, jota voidaan soveltaa useisiin tieteenaloihin. Nimenomaan maatalouteen liittyvä kyberturvallisuustutkimus puolestaan voi olla osa laajempaa maatalouden tietotekniikan tai ruokaturvallisuuden tutkimusta. Täten varsinaista maatalouden kyberturvallisuuden tutkimusta ei välttämättä ole kovinkaan paljoa.

Suomessa julkaistiin helmikuussa 2017 raportti kyberturvallisuuden nykytilasta, tavoitetilasta, ja tarvittavista toimenpiteistä (Lehto *ym.* 2017). Raportti käsittelee kyberturvallisuutta pääosin hyvin yleisellä tasolla, joten suurinta osaa raportista ei voi suoraan soveltaa maatalouden kyberturvallisuuden arviointiin, varsinkaan jos asiaa katsoo maatilan näkökulmasta. Hyödyllisin osa raportista tämän työn kannalta on osio 2, joka sisältää analyysin kyberturvallisuuden nykytilasta Suomessa. Osio sisältää analyysin merkittävimmistä tämänhetkisistä kyberuhista sekä kyberuhkien aiheuttajista. Lehdon *ym.* raportin mainitsemat uhat kohdistuvat seuraaviin kohteisiin:

[1] https://www.viestintavirasto.fi/kyberturvallisuus.html
[2] https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvaohjeet.html

1. Älypuhelimet ja esineiden internet
2. Web
3. Sosiaalinen media
4. Henkilötietokannat
5. Pilvipalvelut

Lisäksi Lehdon *ym.* raportissa puhutaan kohdistetuista hyökkäyksistä tiettyihin kohteisiin, sekä luetellaan toimialat, joihin kohdistuu eniten kyberuhkia; maatalous ei ole suosituimpien kohteiden joukossa. Raportissa mainittujen toimialojen joukossa on kuitenkin liikenne ja kuljetus, johon myös maatalouden logistiikka perustuu, joten ainakin välillisesti voidaan sanoa maatalouden olevan huomattavan kyberuhan kohteena.

Raportissa luetelluista kohteista maatalouden kannalta merkityksellisimmät ovat esineiden internet ja pilvipalvelut. Esineiden internet (Internet of Things) tarkoittaa laitteiden ja koneiden, kuten esimerkiksi traktoreiden tai maatalouden automaatiojärjestelmien, liittämistä internetiin, jolloin niitä voidaan verkon kautta valvoa, mitata, tai ohjata. Monet uudet maatalouden koneet ja laitteet voidaan nykyään liittää verkkoon, ja tulevaisuudessa näiden laitteiden osuus yhä vain kasvaa. Samoin maatalouden tietojärjestelmien lisääntyessä ja monimutkaistuessa maatiloilla on yhä enemmän käytössä erilaisia pilvipalveluita. Tässä työssä käsitellään sekä verkkoon kytkettyjä laitteita, että pilvipalveluissa olevia tietojärjestelmiä.

Web ja sosiaalinen media koskettavat maatalousyrityksiä siinä missä muitakin yrityksiä. Niihin liittyvät uhat tuskin ovat erityisesti maataloutta vastaan suunnattuja. Henkilötietokantoihin liittyvät uhat taas kohdistuvat ensisijaisesti suuriin, tuhansia henkilöitä sisältäviin henkilötietokantoihin, joiden tietoja on mahdollista suoraan hyödyntää rikolliseen tarkoitukseen. Tällaisia ovat esimerkiksi tarkkoja henkilötietoja, kirjautumistietoja eri järjestelmiin, tai luottokorttitietoja sisältävät tietokannat. Maatalouden alkutuotannossa syntyvät henkilötietokannat ovat tyypillisesti pieniä, eivätkä välttämättä sisällä tietoa, joka on asiayhteydestä erotettuna erityisen arvokasta. Täten niihin kohdistuva uhka ei ole yhtä suuri kuin esimerkiksi verkkokauppojen asiakastietokantoihin kohdistuva uhka.

Lehdon *ym.* mukaan tahallisten kyberuhkien tärkeimmät aiheuttajat ovat:

1. Sisäpiiriläiset
2. Kybervandaalit
3. Kybervakoilijat
4. Kyberterroristit ja –sotilaat

Lehdon *ym.* raportissa käsitellään nimenomaan tahallisia kyberhyökkäyksiä järjestelmiä vastaan. Täten kategoria sisäpiiriläiset ei kyseisessä raportissa kata käyttäjien virheistä aiheutuvia kyberuhkia, vaan siinä puhutaan järjestelmän väärinkäytöstä, johon syyllistyy järjestelmän käyttäjä. Vandaaleja ovat muun muassa hakkerit, aktivistit, ja muut tahot, jotka tunkeutuvat tietojärjestelmiin; vakoilijoiden päämääränä on tiedon varastaminen järjestelmästä; ja terroristit sekä kybersotilaat käyttävät tietojärjestelmiä joko osana muuta toimintaa, tai sitten hyökkäävät erityisesti niitä vastaan. Listaa ei voi kuitenkaan pitää kattavana; siitä puuttuvat ainakin rikolliset, jotka pyrkivät levittämään esimerkiksi kiristyshaittaohjelmia.

Lehdon *ym.* raportissa käsitellään myös yritysten kyberturvallisuustilannetta. Fokus on kuitenkin kriittisten toimintojen yrityksissä sekä kyberturvallisuuspalveluita tarjoavissa yrityksissä, joten tämä osa selvityksestä ei lopultakaan ole erityisen relevantti alkutuotannon kyberturvallisuuden kannalta. Valtaosa alkutuotannon yrityksistä on pien- tai mikroyrityksiä, joiden toimintaympäristö ja –edellytykset eroavat suuresti Lehdon *ym.* selvityksen oletuksista.

Maatalouden kyberturvallisuus vaikuttaa kaiken kaikkiaan olevan ala, jotka tutkivat ensisijaisesti valtiovalta sekä yksityinen sektori. Julkisrahoitteisen tutkimuksen osuus vaikuttaa olevan vähäinen. Yksityisellä puolella on maatalouteen kohdistuviin kyberuhkiin vähitellen herätty ja yritykset investoivat

tietotekniikan turvallisuuden parantamiseen. Maatalouden suuryrityksissäkin kyberturvallisuus on kuitenkin vielä uusi asia. Kuten Monsanton teknologiapäällikkö Robert Fraley kommentoi vuonna 2015: ”As an industry, we’re still new to it” (Bunge 2015).

Viimeisen parin vuoden aikana maatalouden kyberturvallisuus on kuitenkin noussut esille yhä enemmän. Vuonna 2016 FBI:n kyberosasto lähetti yksityiselle sektorille asiasta tiedotteen (FBI 2016). Siinä nostettiin esiin erityisesti kolme maatilojen kyberuhkaa (Zorz, 2016).

1. maatalousdatan varastaminen tai tuhoaminen
2. tiedon pahantahtoinen salaaminen kiristystarkoituksessa
3. ruuantuotannon järjestelmien häirintä

Euroopassa aihetta on käsitellyt esimerkiksi Capgemini yhdessä Wageningenin yliopiston kanssa. He näkevät maatalouden suurimpina kyberuhkina tietojärjestelmien heikkoudet, inhimilliset erehdykset, ja eri toimijoiden yhä järjestelmällisemmät hyökkäykset näitä heikkouksia vastaan. Raportissa myös nostetaan esille hyvinkin samoja uhkakuvia kuin FBI:n paperissa: datan varastaminen, datan tuhoaminen, ja datalla kiristäminen kaikki mainitaan, kuin myös järjestelmien ja tuotantoketjujen häirintä. (Viool ym. 2016)

Selkeitä ohjeitakin kyberturvallisuuden parantamiseksi löytyy. Esimerkiksi Cooper (2015) antaa kuusi suositusta maataloussektorin kyberturvallisuuden parantamiseksi:

1. Maataloussektorille tulisi luoda kyberturvallisuuskulttuuri
2. Sektorille tulisi saada enemmän kyberturvallisuuden asiantuntijoita
3. Kyberturvallisuuden arvioimiseksi tulisi kehittää menetelmiä
4. Maatalouden kyberturvallisuusstrategioita, suunnitelmia, ja toimitapoja tulisi kehittää
5. Tiedon varmuuskopiointi- ja palautusmenetelmiä tulisi kehittää ja testata
6. Maataloussektorin tulisi kehittää yhteistyötä muiden kriittisen infrastruktuurin sektoreiden kanssa

Cooperin suosituksista erityisesti ensimmäinen on kuvaava. Hän ei näe, että maataloussektorilla olisi riittävää kyberturvallisuuden kulttuuria, ja täten resursseja tulisi ohjata kyberturvallisuustietämyksen levittämiseen ja turvallisuustietoisuuden parantamiseen. Cooper puhuu koko maataloussektorin tasolla, mutta asia koskee niin ruokateollisuuden suuryrityksiä kuin myös alkutuottajia. Turvallisuuskulttuurin luominen voi olla erityinen ongelma maatiloilla, joiden henkilöstöresurssit ovat jo muutenkin rajalliset. Tämän takia maatilojen voi yksin olla käytännössä mahdotonta noudattaa Cooperin toista suositusta, koska tiloilla ei ole riittäviä resursseja ammattimaisen kyberturvallisuuskulttuurin käyttöönottoon ja vaalintaan.

Cooperin suositukset 3-5 voivat olla haastavia noudattaa maatilatasolla, koska ne käytännössä vaativat ensimmäisten kahden suosituksen noudattamista. Arvioita, strategioita, tai menetelmiä on vaikeaa kehittää ilman riittävää ymmärrystä ja asiantuntemusta. Kuudes suositus on lähinnä koko sektorin tasolla tehtävää toimintaa, jossa yksittäisen maatilan osuus on luultavasti vähäinen.

Cooperin kaikkien suositusten noudattaminen on jotain, mitä maataloussektorin tulisi tehdä kokonaisvaltaisesti. Kaikkien toimijoiden tulee olla mukana, jotta maatalouden kyberturvallisuutta on mahdollista parantaa. Kuten Viiol ym. (2016) huomauttavat, on kyberturvallisuus vain niin hyvä kuin sen heikoin lenkki.

Kyberturvallisuustutkimus ymmärrettävästi keskittyy ensisijaisesti sektoriin itseensä kohdistuviin kyberuhkiin. Maataloudessa kuitenkin käytetään yhä enemmän erilaisia verkkoon kytkettyjä laitteita, kuten antureita, sensoreita, valvontajärjestelmiä, ja automaatiojärjestelmiä. Jokainen laite, johon on mahdollista muodostaa yhteys maatilan oman tietoverkon ulkopuolelta, on mahdollinen heikkous paitsi maatilan omalle kyberturvallisuudelle, myös yleiselle kyberturvallisuudelle. Maatilan laitteisiin tunkeutumisen motiivina ei läheskään aina ole halu hyökätä maatilan omaa kyberympäristöä vastaan. Laitteita voidaan saastuttaa haittaohjelmilla tarkoituksena käyttää saastutettua laitetta kyberhyökkäykses-

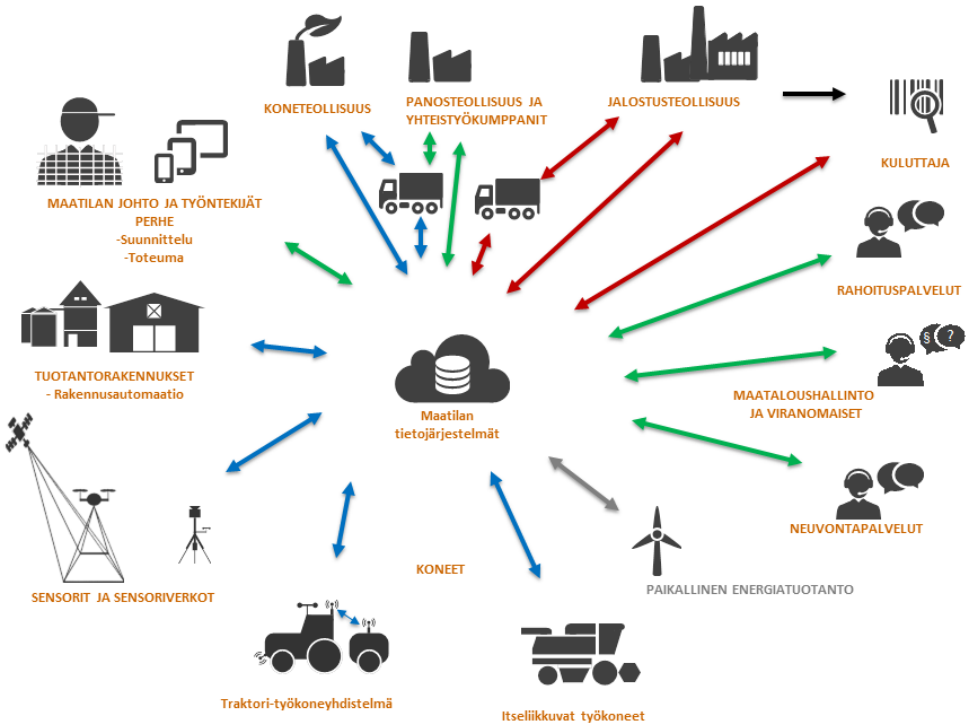
sä jotain toista kohdetta vastaan. Esimerkiksi lokakuussa 2016 Internetin domain-osoitteistoa vastaan tehtiin laajamittainen hajautettu palvelunestohyökkäys, jossa käytettiin ainakin 100 000 kaapattua laitetta (Hilton, 2016). Hyökkäys tehtiin erilaisilla verkkoon liitetyillä laitteilla, jotka oli kaapattu käyttäen Mirai-nimistä haittaohjelmaa.

Huono kyberturvallisuus ei siis aiheuta haittaa vain yritykselle itselleen, vaan mahdollistaa yrityksen laitteiston käytön hyökkäyksissä muita tahoja vastaan.

4. Alkutuotannon fyysinen ja digitaalinen toimintaympäristö

Maatalouden alkutuotannon toimintaympäristö on tyypillisesti maatila. Alkutuotannon mekanisoituminen ja automatisoituminen on vähitellen luomassa myös toimintaympäristöjä, jotka muistuttavat enemmän tehdasympäristöä kuin perinteistä maatilaa, mutta niitä ei tässä selvityksessä ole käsitelty erikseen.

Maatilan fyysinen toimintaympäristö koostuu vähintäänkin tilan rakennuksista, kiinteistä laitteista ja rakennelmista, liikkuvista ja vedettävistä työkoneista, työkaluista, sekä pelloista ja muusta tilan omistamasta maa-alasta. Fyysisen toimintaympäristön yhteydessä on myös maatilan kybertoimintaympäristö, joka tyypillisesti koostuu yhdestä tai useammasta fyysisesti tai loogisesti erillisestä tietoverkosta, toimistotietokoneista, kiinteistä oheislaitteista, kannettavista laitteista, sekä rakennelmiin, kiinteisiin laitteisiin, työkoneisiin ja muihin tiloihin liittyvistä ja niihin erikseen rakennetusta tietotekniikasta.



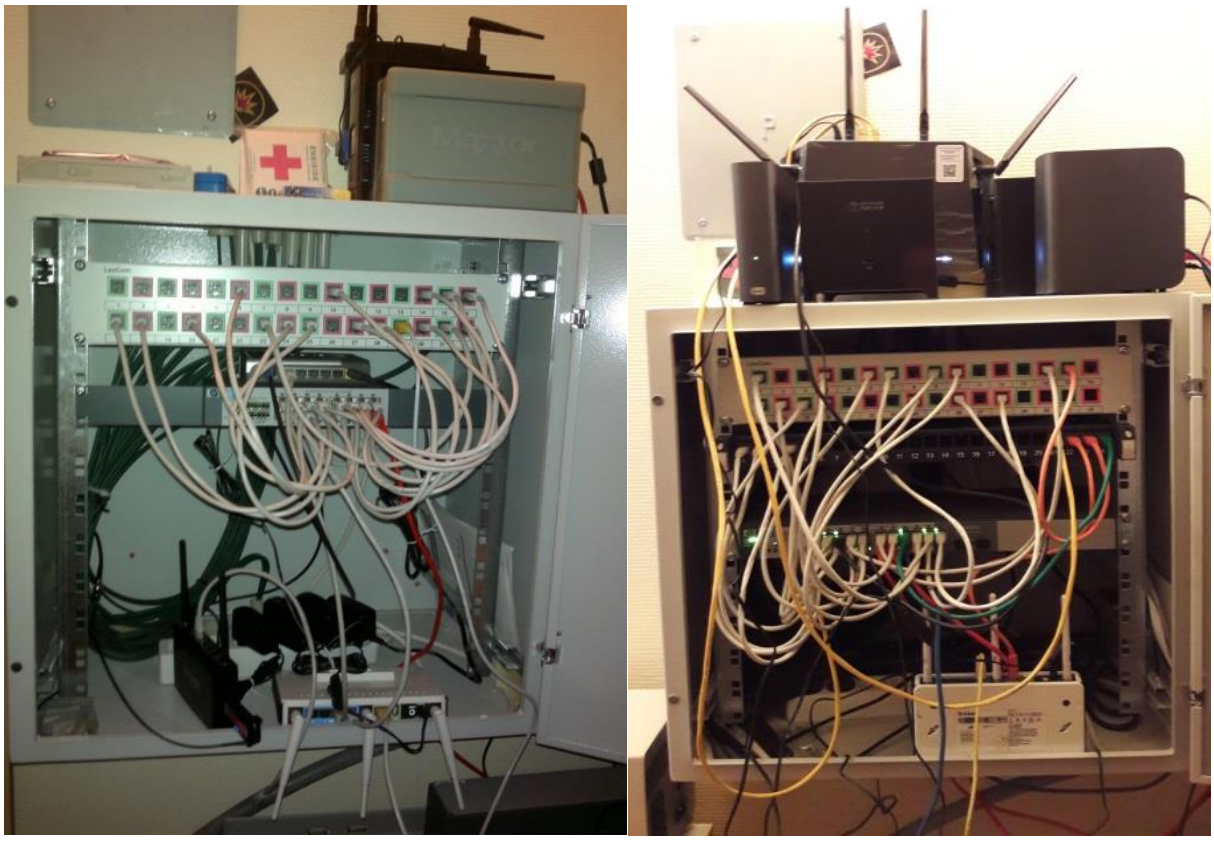
Kuva 1. Maatilan toimintaympäristössä on perinteisiä koneita, koneita automaatiolaajennuksilla ja uusia automaattisia toimilaitteita. Maatilan tietojärjestelmä on usein jakaantunut useampaan erilliseen kokonaisuuteen.

4.1. Maatilan digitaalinen toimintaympäristö ja sen yleiset heikkoudet

Maatilan tietotekninen toimintaympäristö on harvoin etukäteen kokonaisuutena suunniteltu ja tämän suunnitelman mukaan rakennettu. Tavallisempaa on, että tietotekninen toimintaympäristö on rakentunut orgaanisesti vuosien saatossa, kun tilan fyysistä toimintaympäristöä on kehitetty ja tätä kautta on noussut uusia tietoteknisiä tarpeita. Tällöin digitaalista toimintaympäristöä on laajennettu ja muutettu uusia tarpeita vastaavaksi. Lopputuloksena on usein kokonaisuus, jonka ymmärtäminen, ylläpito ja päivittäminen on voi olla haastavaa.

4.1.1. Maatilan digitaalinen toimintaympäristö

Tyypillinen maatilan digitaalinen toimintaympäristö perustuu maatilan lähiverkkoon, jonka rungon muodostaa maatilan ulkoverkkoon kytkevä reititin, sekä siihen liitetyt laitteet. Riippuen maatilasta, ulkoverkkoon kytketyssä reitittimessä voi olla kiinni useita muitakin reitittimiä, ja osa lähiverkosta voi toimia langattomasti. On myös mahdollista, että tilalla on useita eri lähiverkkoja esimerkiksi tilan eri osissa. Maatilan lähiverkko voi olla fyysisesti tai loogisesti erotettu pienemmiksi aliverkoiksi, tai sitten se voi olla reititetty yhdeksi kokonaisuudeksi. Mikäli tässä dokumentissa ei erikseen toisin sanota, oletetaan että joko maatilan lähiverkko on yhtenäinen kokonaisuus, tai että verkon fyysisellä tai loogisella rakenteella ei ole väliä. Tämän lisäksi maatilalla voi olla suuriakin määriä laitteita, joita ei ole kiinnitetty maatilan lähiverkkoon. Nämä laitteet ovat kiinni tietoverkossa matkapuhelinverkon kautta, ja kommunikoivat keskenään sekä maatilan muiden laitteiden kanssa julkisen tietoverkon läpi. Maatiloilla on myös paljon käytössä laitteita, jotka lähettävät tietoa SMS-viestien avulla.

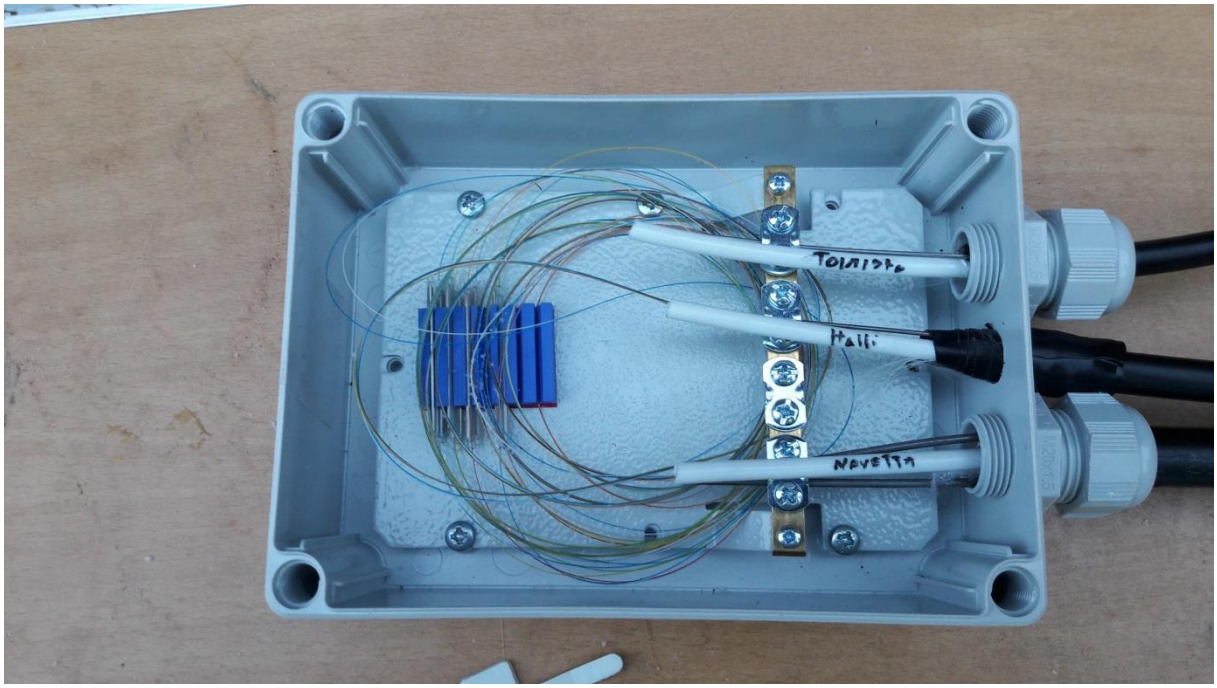


Kuva 2. Esimerkki maatilan ristikytkentäkaapin kehittymisestä. Laitemäärä on kasvanut tarpeiden kehittymisen mukana. Useimmat maatilojen verkoissa käytetyt laitteet ovat koti- tai harrastekäyttöön tarkoitettuja.

Maatilan asuinrakennuksen tietoverkko on yleensä samankaltainen kuin muidenkin asuntojen sisäiset tietoverkot. Siinä on kiinni maatilan toimistokäyttöön tarkoitettuja tietokoneita, oheislaitteita, ja muita maatilan toimintaan liittyviä asuintilassa sijaitsevia laitteita. Asuinrakennuksen tietoverkossa on myös yleensä kiinni maatilayrittäjän perheenjäsenten tietokoneita ja mobiililaitteita, sekä talon muita laitteita, kuten televisioita tai muuta viihde-elektroniikkaa. Samaan verkkoon kytkeytyvät usein myös tilalla vierailevat henkilöt kuten myyjät, neuvojat, eläinlääkärit, asentajat ja tuttavat.

Maatilan talouskeskuksen tietoverkko kattaa tilan ulkorakennukset tyypillisesti tarpeen mukaan. Lyhyillä etäisyyksillä voidaan käyttää wlan-tekniikkaa. Pidemmille matkoille ja rakennusten välille joudutaan yleensä rakentamaan erillinen verkko käyttäen valokuitua. Valokuituverkkoa tilan sisällä tarvitaan tyypillisesti yli 100m etäisyyksillä.

Tyypillisimmin tietotekniikkaa on lisätty eläintuotantotilojen eläinsuojiin, kuten kanaloihin, sikaloihin, tai navetoihin. Eläinsuojissa oleva tietotekniikka liittyy tyypillisesti eläinrekisterien ylläpitoon, eläinsuojan automatiikan valvontaan ja ohjaukseen. Riippuen käytetystä automaatioteknologiasta, voi eläinsuojassa olla yksi tai useampia automaatiojärjestelmiä, sekä niiden toimintaa valvovia ja ohjaavia tietokoneita. Eläinsuojan automatiikka on yhä enenevässä määrin tietoverkkoon kytkettyä, mutta osa automaatiojärjestelmistä voi myös olla eristettyjä. Erilaisia automaatiojärjestelmiä on lukuisia, ja niihin liittyy yhä suurempi määrä erilaisia sekä järjestelmätoimittajan, että heidän yhteistyökumppaniensa, tarjoamia palveluita. Täten automaatiojärjestelmien kytkeytyminen maatilan tietoverkkoon riippuu tilanteesta ja järjestelmän valmistajasta. Tyypillisesti uudemmat ratkaisut sisältävät verkkoyhteyden jo pelkästään siksi, että järjestelmätoimittaja haluaa tarjota järjestelmän ylläpitoon liittyviä palveluita.



Kuva 3. Maatilan rakennusten väliset yli 100m pituiset kaapeloinnit rakennetaan valokuituverkkona.

Maatilan tietoverkkoon voidaan myös kytkeä erilaisia sensorijärjestelmiä ja muita sulautettuja laitteita, jotka voivat tuottaa ja käyttää dataa. Tällaisia laitteita ovat esimerkiksi sääasemat, maaperäanturit, eläimiin kiinnitetyt anturit, valvontakamerat ja muu kulunvalvontalaitteisto, sekä modernit liikkuvat maataloustyökoneet. Koska erilaisia laitteita ja valmistajia on lukemattomia, riippuu täysin tilanteesta miten nämä erilaiset laitteet on liitetty maatilan tietoverkkoon.

Maatilan tietoverkkoon voi siis olla kytkettynä suuri määrä erilaisia laitteita, ja tietoverkon rakenne ja toiminnallisuus on täysin riippuvainen tilanteesta.

4.1.2. Haasteita ja heikkouksia toimintaympäristössä

Maatilan tietoverkko voi olla hyvinkin monimutkainen kokonaisuus, jossa on kiinni useita erilaisia laitteita. Verkon rakenne syntyy yleensä vaatimusten kehittymisen mukana, varsinaista verkkorakenteen suunnittelua ei yleensä ole ennakkoon tehty. Laitekannan monipuolisuus tekee verkosta haastavan ylläpitää. Tyypillinen suomalainen maatila on pien- tai mikroyritys, jolla ei välttämättä ole kovinkaan syvällistä tietoteknistä osaamista. Maatalous on liiketoimintaa, jota teknologia avustaa, joten maatilan henkilöstön ydinosaaminen liittyy nimenomaan maataloustuotantoon. Tämä on valtava haaste erityisesti pienille tiloille pakollisen teknologian lisääntyessä ja toimintaympäristön muuttuessa monimutkaisemmaksi. Tarve ammattimaiselle teknologiaosaamiselle ja tekniikan ylläpidolle kas-

vaa, ja maatilan käytössä olevat resurssit eivät välttämättä kasva tarpeen tahdissa. Haasteita aiheuttavat esimerkiksi laitteiden elinkaaren hallinta, ohjelmistojärjestelmien ylläpito ja tekninen tuki, käytössä olevat tietoverkkoratkaisut, sekä enenevässä määrin digitalisoituva maatilaa ympäröivä liiketoimintaekosysteemi.

Monien maatilan laitteiden elinkaari on hyvin pitkä. Esimerkiksi traktoria voidaan käyttää tilalla erilaisiin työtehtäviin jopa 20-30 vuotta, ja rakennusten käyttöikä on tyypillisesti 30-50 vuotta. Laitteiden pitkä elinkaari aiheuttaa vaatimuksia huollolle; vanhoihinkin laitteisiin on saatava varaosia, ja laitteissa olevaa tietotekniikka täytyy olla mahdollista päivittää siten, että sitä voi käyttää yhdessä tilan uudempien laitteiden kanssa. Pitkäikäisten laitteiden ja tietotekniikan välillä on erittäin voimakas kontrasti. Tyypillinen tietokoneen tai mobiililaitteen elinkaari on noin 5 vuotta, ja vaihtelee noin kahden ja kymmenen vuoden välillä. Elinkaarien pituuden erosta tulee erityisen suuri ongelma, kun maatilan pitkäikäisiin laitteisiin ja koneisiin lisätään tietotekniikkaa, ja kone kytketään osaksi maatilan tietoverkkoa ja sitä kautta internetiä. Jokainen verkkoon kytketty laite vaatii säännöllisiä tietoturvapäivityksiä, jotta siitä ei muodostuisi turvallisuusuhkaa. Päivitysten loppuminen tekee laitteesta tietoturvariskin, koska ohjelmistossa olevia vikoja ei enää korjata. Täten laitteeseen on mahdollista tunkeutua ja sitä kautta esimerkiksi käyttää sitä osana kyberhyökkäystä. Sulautettujen laitteiden kanssa ongelma voi olla esim. sopivien liitäntöjen puuttuminen uudemmista tietokoneista.

On myös tärkeää saada viljelijät tietoiseksi tarpeesta pitää ohjelmistot ajan tasalla. Päivittämätön laite ei ole uhka pelkästään maatilan omalle tietoturvalle, vaan se voidaan myös kaapata muualle tarkoitettuja hyökkäyksiä varten. Laitteiston ohjelmisto tulee pitää ajan tasalla koko laitteen elinkaaren ajan.

Monilla maatiloilla ei ole käytettävissä ammattimaista IT-tukea. Tietotekniikkaa hoidetaan ja ylläpidetään itse. Usein käytössä oleva ulkopuolinen apu on teknologiasta jossain määrin perillä oleva tuttava, esimerkiksi naapurin lapsi. Ammattimaisen tuen puuttuessa koneita ei välttämättä ole alun perinkään asennettu ja alustettu oikein. Täten maatilan tilanne saattaa olla sellainen, että laitteilla ei ole teknistä tukea, niitä ei pidetä yllä, eikä maatilalla ole myöskään kykyä havaita tietoturvahyökkäyksiä.

Maatiloilla käytössä olevat internetliittymät ovat monesti kotikäyttöön tarkoitettuja. Kuitenkin, maatilan tietotekniikan lisääntyessä ja monimutkaistuessa, maatilan verkkoliittymän läpi kulkevat palvelut muuttuvat yhä monipuolisemmiksi. Monet tilalle asennetut laitteet vaativat toimiakseen sovelluksia, joiden takia maatilan tietoverkkoon joudutaan tekemään asetuksia joiden luonnetta, tai olemassaoloa, ei ole etukäteen suunniteltu ja joiden vaikutusta tietoturvaan ei välttämättä ymmärretä. Kotiverkkoliittymät, jollaisia suuri osa maatilojen verkkoliittymistä on, on usein suojattu ulkopuolelta. Maatalouskäytössä liittymiin joudutaan avaamaan palvelujen toimimista varten TCP/IP portteja. Tarpeettomat avatut portit ovat tietoturvariski, ja palveluntarjoajan liittymään tarjoama tuki ja palvelut eivät välttämättä enää kata maatilan tarpeita riittävästi.

Maatilan tietojärjestelmien varmistukset ovat usein puutteellisia. Maatilalla tuotettavasta ja säilytettävästä tiedosta ei välttämättä oteta säännöllisiä varmuuskopioita, jolloin konerikon tai vastaavan sattuessa voi esimerkiksi viljelyhistoriatietoa hävitä. Ja, vaikka varmuuskopioita otettaisiin, ei tietojen palautusta varmistuksista luultavasti harjoitella. Asia on osittain korjautumassa maatilan ohjelmistojen muuttuessa paikallisessa tietokoneessa käytettävistä toimisto-ohjelmistoista enemmän pilvipalveluiksi. Pilvipalvelussa tiedon säilytys ja varmuuskopiointi on palveluntarjoajan vastuulla. Esimerkiksi viljelysuunnitteluohjelmat ovat siirtymässä yhä enemmän pilvipalveluihin.

Maatilan sähkönsaannin varmistukset ovat usein puutteellisia, eivätkä kata maatilan tietojärjestelmiä. Tämä voi aiheuttaa tilanteen, jossa sähkönjakeluhäiriön sattuessa maatilan laitteet pysyvät toiminnassa varavirralla, mutta laitteita ei enää ole mahdollista valvoa tai ohjata, koska niiden ohjaamiseen käytettävät tietokoneet sammuvat.

Useasti maatilojen tietojärjestelmien käyttäjien hallintaa ei ole kunnolla suunniteltu ja toteutettu. Maatilan tietojärjestelmä voi esimerkiksi olla toteutettu siten, että kaikilla käyttäjillä on pääsy kaikkeen dataan. Tämä voi tapahtua vaikkapa siten, että maatilan jokaisessa tietokoneessa on käy-

tössä vain yksi käyttäjätunnus, jota kaikki koneen käyttäjät käyttävät. Tällöin saman käyttäjätunnuksen takana on sekä maatilan kirjanpitotieto, että päivittäiseen toimintaan liittyvä analyysidata, että kaikki muukin tietokoneella oleva tieto. Kaiken datan säilyttäminen samassa paikassa johtaa siihen, että tietoturva-aukkojen avulla on helpompi päästä käsiksi maatilan datan kokonaisuuteen. Samoin kaikki maatilan työntekijät, sekä kunnallisen lomitusjärjestelmän kautta tilalle tulleet lomittajat, pääsevät käsiksi kaikkeen maatilan tietoon. Tämä on ongelma erityisesti lomittajien tapauksessa, koska heillä ei ole työsuhdetta maatilaan.

Maatilojen kyberturvallisuus ei tänä päivänä rajoitu pelkästään tilaan itseensä ja sen hallinnoimiin järjestelmiin. Maatilojen tietoja on tilan omien ja sen yhteistyökumppaneiden tietojärjestelmien lisäksi myös huomattavia määriä erilaisissa laitevalmistajien ja viranomaisten järjestelmissä. Laitevalmistajien järjestelmiin tieto saattaa mennä, koska laite on toimiakseen kytkettävä tietoverkkoon ja lähettää dataa automaattisesti, tai koska laitevalmistaja ja tila ovat tehneet sopimuksen datan käytöstä. Monien viranomaisjärjestelmien käyttö on maatiloille pakollista johtuen joko laeista ja säädöksistä, tai sitten esimerkiksi tarpeesta hakea viljelytukia. Täten maatilan kyberturvallisuus voi olla uhattuna myös sellaisten järjestelmien kautta, joihin maatilalla itsellään ei ole mahdollisuuksia vaikuttaa. Esimerkkinä tällaisesta järjestelmästä voidaan käyttää esimerkiksi Viljavuuspalvelun tulospalvelua, johon kirjauduttiin tietoturvallisesti hyvin heikolla menetelmällä. Täten ulkopuolisen tahon on helppo saada selville tietyn maatilan palvelutunnukset ja sitä kautta päästä käsiksi tilan tietoihin.

Tilalla vierailevat toimijat voivat myös kytkeytyä tilan verkkoon erillisen vierasverkon puuttuessa. Samassa verkkoympäristössä ollessa on mahdollista että laitteet vaihtavat tietoja tai verkko tai kytkeytynyt laite voivat saastuttaa toisensa. Olisi perusteltua tarjota vierasverkkoratkaisu myös maatilaympäristössä.

Verkkopalveluita tarjoavilla toimijoilla on myös oma vastuunsa palveluiden toimivuudesta ja turvallisuudesta, ja heidän tulisi myös kehittää palveluitaan maatilojen ja muiden pien- ja mikroyritysten tarpeita vastaaviksi. Nykytilanteessa on kuitenkin epäselvää miten vastuu tietoturvasta jakautuu palvelun tarjoajan käyttäjän kesken. Esimerkiksi vastuu tietojen varmuuskopioinnista ja saatavuudesta voi olla puutteellista. Jatkossa on kyettävä selkeämmin jakamaan tämä vastuu, missä tarvitaan luultavasti ulkopuolisten toimijoiden apua.

4.2. Maatilan johtaminen ja taloushallinto

Tyypillinen suomalainen maatila on mikro- tai pienyritys, jonka palveluksessa on hyvin vähän henkilöstöä. Henkilömäärä tosin vaihtelee suuresti riippuen tuotantomuodosta ja tilan koosta. Tilan johtaminen täten keskittyy tilan toiminnan suunnitteluun ja valvontaan, kirjanpitoon, investointeihin, sekä tuotteiden myyntiin. Työnjohtaminen ja henkilöstöhallinto ovat tyypillisesti vähäisemmässä osassa. Johtamisessa ja taloushallinnossa käytetään työkaluna pääasiassa tietokonetta, joskin tietojärjestelmien siirtyminen pilvipalveluihin mahdollistaa nykyään ainakin joidenkin asioiden tekemisen myös kannettavilla laitteilla.

4.2.1. Haasteita ja heikkouksia tilan johtamis- ja taloushallintojärjestelmissä

Maatilan johtamisessa keskeisin käytössä oleva ohjelmistotyökalu on kirjanpito-ohjelmisto. Tilan kannalta ohjelmiston keskeisin osa on veroilmoituksen laatimiseen liittyvä kirjanpito-osio. Kirjanpidon lisäksi ohjelmistoon kuuluvat yleensä ostoreskontra, laskutus ja palkanlaskenta. Perinteisesti maatiloilla käytössä olleet kirjanpito-ohjelmistot ovat olleet yhden käyttäjän, yhdelle koneelle asennettuja sovelluksia. Kehitys on kuitenkin viemässä näitäkin sovelluksia verkkopohjaiseen suuntaan. Ohjelmistoista on jo pitkään ollut liittymiä verkkopalveluihin, kuten pankkien sovellukset ja verotukseen ja palkanlaskentaan liittyvät tiedonsiirrot. Tulevaisuudessa itse ohjelmatkin voivat osittain tai kokonaan siirtyä pilvialustoilla toimiviksi, jolloin ne eivät enää olisi tiettyyn tietokoneeseen sidottuja.

Pankkiyhteyksien hoitamiseen on perinteisesti käytetty erillisiä sovelluksia maksatusaineistojen siirtoon. Pankkiyhteyksien käytössä ollaan myös siirtymässä selainpohjaisiin sovelluksiin.

Maatilojen tietojärjestelmien käytössä voidaan tunnistaa useampi henkilöryhmä. Näitä ovat esimerkiksi maatalousyrittäjä, hänen perheensä, tilan palkattu henkilöstö, maatalouslomittajat, ja maatalousneuvojat. Eri henkilöryhmillä on maatilan tietoverkkoihin ja tietoihin erilaiset tarpeet, oikeudet ja velvollisuudet. Monissa maatilan tietojärjestelmissä ei kuitenkaan ole valmiutta eriyttää käyttöoikeuksia henkilöstöryhmän perusteella. Esimerkiksi maatalouslomittaja, joka ei ole työsuhteessa maatalousyritykseen, tarvitsee pääsyn lomitustyöhön liittyviin tietoihin, kuten maitoanalyyseihin. Lomittajalla ei kuitenkaan ole tarvetta päästä esimerkiksi maidon tilitykseen liittyviin tietoihin. Ilman mahdollisuutta antaa käyttäjille käyttöoikeuksia henkilöstöryhmän mukaan ei tietoteknisesti ole mahdollista estää lomittajaa tarkastelemasta tietoja, jotka eivät hänelle kuuluisi.

Erityisen ongelmallinen on luottamuksellinen tieto, kuten henkilöihin liittyvät tiedot. Henkilötietojen säilyttäminen on henkilötietolakien mukaan järjestettävä tietyllä tavalla, ja henkilötiedot ovat luottamuksellisia. Täten henkilötietoihin tulisi päästä käsiksi vain niiden henkilöiden, joilla on siihen tarve.

Yksi suuri ongelma ovat tilan ulkopuoliset järjestelmät, joihin kirjaudutaan vahvan henkilötunnistautumisen kautta käyttämällä esimerkiksi pankkitunnuksia. Vahva henkilötunnistus on aina sidottu johonkin luonnolliseen henkilöön, eikä kyseistä tunnusta saisi luovuttaa kenellekään toiselle. Tietojärjestelmät tulee aina suunnitella niin että käyttöoikeuksia voidaan määritellä tarpeen mukaan henkilökohtaisesti. On tietoturvan kannalta erittäin arveluttavaa jos järjestelmän käytöstä sopimuksen tehnyt joutuu luovuttamaan omat tunnukset toiselle henkilölle järjestelmän käyttämistä varten. Henkilötunnistukseen perustuvia palveluita ovat esimerkiksi pankki-, vakuutus- ja tukihakemuspalvelut.

Maatalouden tietojärjestelmien ylläpitoon liittyvä tuki järjestää tyypillisesti itselleen etäkäyttömahdollisuuden järjestelmiin, joiden ylläpito kuuluu tuen piiriin. Ongelmana on että etäkäyttöohjelmien tietoturva voi olla puutteellinen tai että etäkäyttöä voidaan käyttää myös väärin.

4.3. Rakennukset ja muut pysyvät rakennelmat

Maatalouden rakentamisessa käytetään hyvin samantyyppistä tekniikkaa kuin muussakin teollisuusrakentamisessa. Talotekniikan laitteet verkottuvat ja myös niiden tuottama uhka on otettava huomioon. Maatilan rakennusten tietoverkon perusteet on selostettu yleisellä tasolla raportin osiossa 4.1.1. Rakennuksista tietotekniikkaa on erityisesti tilan asuinrakennuksessa sekä kotieläintuotantoon liittyvissä rakennuksissa. Tekniikkaa voi olla myös tilan muissa rakennuksissa riippuen tilan teknologiatasosta ja harjoitetusta maataloustoiminnasta. Huomattavia määriä automaatiojärjestelmiä ja sen takia myös tietotekniikkaa on käytössä kotieläintuotannossa sekä kasvihuonetuotannossa. Peltoviljelyssä automaatio on tekemässä läpimurtoa, mutta siellä lähinnä liikkuvissa työkoneissa eikä niinkään rakennuksissa.

Kotieläintuotannon rakennuksissa automaation avulla usein hallitaan rakennuksen sisäilmastoa. Esimerkiksi siipikarjantuotannossa rakennuksen sisäolosuhteita muutetaan päivittäin kasvatettavien eläinten kehittyessä. Automaatiota käytetään myös eläinten ruokinnassa, tarkkailussa, jätösten keräämisessä ja poistossa, sekä lehmien lypsyssä. Automaatiota hallitaan tyypillisesti tietokonesovelluksilla, joiden toiminta on oltava jatkuvaa ja katkotonta.

Kasvihuoneissa on usein sisätilan lämpötilaa ja kosteutta valvovia ja hallinnoivia järjestelmiä. Kasvihuoneen sisätilaa voidaan hallinnoida ilmanvaihdon ja sadetusjärjestelmien avulla. Koneellisen ilmanvaihdon lisäksi käytössä on myös tuuletusluukkujen automaattisia säätöjärjestelmiä, sekä erilaisia verhoratkaisuja liiallisen auringonvalon heijastamiseksi pois. Automaatiojärjestelmä voi hallinnoida myös kasvihuoneen valoja sekä automaattisia ruokintalaitteistoja. Kasvihuoneista pisimmälle automaatio on edennyt kasvuhuoneissa, joissa kasvatus on hyvin pitkälle automatisoitua.

4.3.1. Haasteita ja heikkouksia tilan rakennuksiin liittyen

Maatilan asuinrakennuksessa on tilan johtamiseen ja hallinnointiin liittyvää tietotekniikkaa sekä maatalousyrittäjän ja hänen perheensä henkilökohtaista tietotekniikkaa ja viihde-elektroniikkaa. Tietokoneisiin kohdistuvia haasteita ja uhkia käsitellään tarkemmin raportin osioissa 4.7.

Eläinsuojien sisäolosuhteet vaativat jatkuvaa valvontaa ja säätöä, ja olosuhteiden on pysyttävä eläimille suotuisina. Jo muutaman tunnin katkos tai virheellinen toiminta ilmastoinnissa ja lämmönsäätelyssä voi aiheuttaa merkittävää haittaa eläinten hyvinvoinnille. Mikäli ilmastoinnin ja lämpötilan hallintajärjestelmään on liitetty maatilan tietoverkkoon, on se myös haavoittuva mahdollisille kyberhyökkäyksille. Verkkoon liittäminen kuitenkin mahdollistaa laitteiston etävalvonnan- ja hallinnan, joten se usein koetaan hyödylliseksi, ja verkkoon liitettyjen laitteiden määrä eläinsuojissa on lisääntymässä.

Kasvihuoneen automaation valvonta- ja hallinnointijärjestelmä voi olla etäkäytettävä samalla tavoin kuin eläinsuojan, jolloin siihen kohdistuu samanlaisia kyberuhkia. Myös kasvihuoneessa voi jo muutaman tunnin katkos tai virheellinen sisätilan säätö aiheuttaa haittaa kasvien hyvinvoinnille.

Kotieläintuotannossa ja kasvihuonetuotannossa käytettävät automaatiojärjestelmät tarvitsevat jatkuvaa valvontaa ja säätöä. Täten järjestelmän tulisi kyetä ilmoittamaan ongelmista ja tarpeista viljelijälle ajasta ja paikasta riippumatta. Järjestelmien etävalvonta, ja erityisesti etähallinta, vaatii kuitenkin järjestelmien välistä integraatiota. Tämä taas on mahdollinen kyberuhkien lähde, mikäli ulkopuolinen taho pääsee käsiksi valvonta- ja hallinnointisovelluksiin. Automatiikan väärä säätö voi aiheuttaa vahinkoja hyvinkin nopeasti. Lisäksi, mikäli eri automaatiojärjestelmiä voi etähallinnoida samalla laitteella, mahdollistaa kyseiseen laitteeseen tunkeutuminen kaikkiin järjestelmiin tunkeutumisen.

Kuva 4. Maatilan toimintaympäristössä lämpötilan vaihtelut, pöly, kosteus ja eläinten kontaktit asettavat suuret vaatimukset asennusten toteuttamiselle ja laitteiden rakennevaatimuksille.

4.4. Peltoviljelyn järjestelmät

Peltoviljelyssä tärkeimpiä digitaalisia järjestelmiä ovat viljelysuunnitteluohjelmisto ja siihen liittyvät muut ohjelmistot ja palvelut. Tämän lisäksi pelloilla voi olla käytössä sensoreita, ja liikkuvista työkoneista voi myös olla mahdollista saada dataa. Tämän lisäksi viljakuivureissa ja –siiloissa on käytössä automatikkaa.

Peltoviljelyn keskeisin järjestelmä on viljelysuunnittelu- ja muistiinpano-ohjelmisto. Viljelysuunnitteluohjelmasta on hyvin yleisesti yhteyksiä erilaisiin ulkopuolisiin palveluihin, kuten esimerkiksi tukihakemuksiin ja tarvittavien tietojen noutamiseen. Tietoja noudetaan mm. viljavuustutkimuksista.

Peltojen sensoroinnin myötä käyttöön on tulossa myös peltojen reaaliaikaiseen valvontaan liittyviä sovelluksia. Sensoreiden avulla mittaustietoa kerätään ainakin säähän, maaperään ja vesitalouteen liittyen. Näiden laitteiden mittaustiedot välittyvät tyypillisesti langattomassa verkossa joko suoraan maatilan oman langattoman lähiverkon kautta, tai mobiiliverkon avulla. Usein sensoritiedot kerätään ensin sensorivalmistajan palvelimelle, josta viljelijä voi sitten hakea ne omaan käyttöönsä sovelluksen avulla.

Viljakuivureissa on tyypillisesti automaattinen järjestelmä, joka ohjaa kuivausprosessia. Nämä järjestelmät ovat perinteisesti olleet eristettyjä, mutta nekin ovat kehittymässä verkkopohjaisiksi. Automaatiojärjestelmien toteutukseen käytetään teollisuudessa yleisesti käytettyjä komponentteja.

Peltoviljelyssä käytettävät liikkuvat ja vedettävät työkoneet käsitellään osiossa 4.6.

4.4.1. Haasteita ja heikkouksia peltoviljelyn järjestelmissä

Viljelysuunnitteluohjelmistojen ongelmat ovat hyvin samantyyppisiä kuin muissa tilan johtamiseen liittyvissä ohjelmistoissa. Mikäli ohjelmisto on paikallinen, siihen kohdistuvat kyberuhat ovat hyvin riippuvaisia käytetyn koneen tietoturvan tasosta. Tyypillisiä ongelmia ovat esimerkiksi sähkökatkot sekä konerikon tapahtuessa ajantasaisten varmuuskopioiden puute, jonka takia voidaan menettää tärkeitä tietoja. Verkon läpi käytettävää ohjelmistoa taas uhkaavat samat kyberuhat kuin muitakin tilan ulkopuolisia palveluita, kuten esimerkiksi verkkoyhteyden katkeaminen. Tietokoneisiin liittyviä kyberuhkia käsitellään tarkemmin osiossa 4.7.

Tilalla käytettävät sensorit ovat myös mahdollinen kyberuhka. Niiden sulautettuja järjestelmiä uhkaavat samat asiat kuin muitakin verkkoon kytkettyjä laitteita. Samoin tilan eri automaatiojärjestelmien sulautetut laitteet ovat mahdollisia kyberuhkia. Tosin automaatiojärjestelmät voivat olla helpompi suojata ulkopuolisilta tunkeutujilta kuin sensorijärjestelmät, koska ne ovat suuremmalla todennäköisyydellä kiinni vain maatilan sisäverkossa.

Viljakuivaamoita käytetään vain kausiluontoisesti, mikä aiheuttaa ylimääräisiä ongelmia niiden automaatiojärjestelmien kyberturvallisuuteen. Kausittainen käyttö saattaa viivästyttää tärkeiden päivitysten asentamista, kun laite ei ole päällä päivityksen ilmestyessä, ja sitä kautta huonontaa järjestelmän turvallisuutta. Tämän takia kausikäyttöiset laitteet tulisi tarkistaa ja päivittää aina ennen käyttöönottoa, mikäli ne ovat kytkettynä internetiin. Kuivaamo voi myös olla kaukanakin tilan talouskeskuksesta, joten fyysinen tunkeutuminen rakennukseen voi olla suurempi uhka kuin talouskeskuksen välittömässä läheisyydessä olevissa rakennuksissa. Mikäli hyökkääjä pääsee fyysisesti käsiksi tietokoneeseen, on hänellä yleensä huomattavasti helpompi vaikuttaa siinä oleviin tietojärjestelmiin.

4.5. Kotieläintalouden järjestelmät

Karjataloudessa on käytössä suunnittelu- ja valvontaohjelmia samalla tavoin kuin peltoviljelyssäkin. Tämän lisäksi karjatalouden järjestelmiin kuuluvat erilaiset eläinten hoitoon liittyvät tietojärjestelmät. Käytettävien järjestelmien tyyppi riippuu kasvatettavista eläimistä.

Karjataloudessa on erilaisia automaatiojärjestelmiä käytetty jo pitkän aikaa. Eläinsuojien ilmanvaihtoa ja lämpötilaa säätävien automaatiojärjestelmien lisäksi järjestelmiä voidaan käyttää eläinten ruokintaan ja valvontaan, jätteiden poistoon, ja eläinten puhdistukseen, sekä lypsykarjalla lypsämi-

seen. Eläinsuojien automatiikkajärjestelmät koostuvat tyypillisesti kiinteästi asennetuista laitteista ja näiden valvontaan ja ohjaukseen käytetyistä tietokoneista. Koneet on myös mahdollista liittää verkkoon etäyhteyksiä varten. Tyypillisesti moderni kotieläintalouden automaatiojärjestelmä vaatii etäyhteyksiä esimerkiksi järjestelmän toimittajan ylläpitoa tai laitteen etävalvontaa ja ohjausta varten. Eläinten etävalvontajärjestelmät liittyvät tyypillisesti eläinten hyvinvoinnin ja hoidon tarpeisiin. Etävalvontaa tarvitaan esim. poikimistapahtumissa tai eläinten vapaaksi pääsyn seurannassa. Valvontaan käytetyt laitteet ovat usein sulautettuja laitteistoja jotka sisältävät pienen palvelinlaitteiston.

Kotieläintalouteen liittyy myös viranomaisjärjestelmiä, joita on käytettävä säännöllisesti osana tilan jokapäiväistä hallinnointia. Esimerkiksi karjataloudessa kotieläimiin liittyvät muutokset on rekisteröitävä valtakunnallisiin rekistereihin 7 vuorokauden sisällä. Väärästä ja viivästyneestä ilmoituksesta määrätään sanktioita. Ilmoitukset tehdään sähköisillä järjestelmillä, jolloin maatilan digitaalisen järjestelmän toimimattomuus esimerkiksi kyberhyökkäyksestä johtuen voi estää ilmoituksen teon. Myös paperisten rekisteröintikorttien ja ilmoitusten käyttö edellyttää yleensä niiden tulostamista verkosta. Näissä ylivoimaisen esteen tilanteissa tuottajan tulee tehdä kirjallinen ilmoitus 15 päivän kuluessa kuntaan. Tuottajasta riippumaton ennalta arvaamaton tilanne ja ylivoimainen este ilmoituksen tekemiseen eivät johda tuenmenetykseen.

Kotieläintaloudessa käytetään myös samanlaisia liikkuvia työkoneita kuin peltoviljelyssä. käytettävät liikkuvat ja vedettävät työkoneet käsitellään osiossa 4.6.

4.5.1. Haasteita ja heikkouksia kotieläintalouden järjestelmissä

Karjatalouden tietojärjestelmien kyberturvallisuutta uhkaavat samankaltaiset uhat kuin muitakin maatalouden tietojärjestelmiä riippuen siitä onko järjestelmä kytketty tietoverkkoon vai ei. Johtuen etävalvonnan tarpeista yhä suurempi määrä tietojärjestelmiä on verkkoon kytkettyinä ja täten niitä uhkaavat tietoverkosta tulevat kyberuhat.

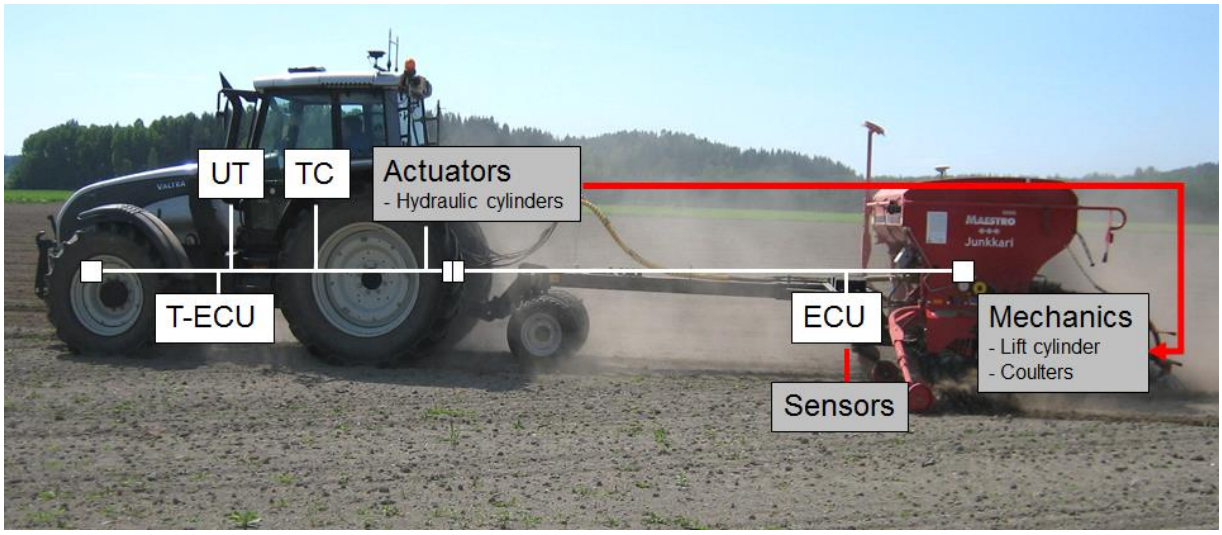
Kotieläintalouden automaatiojärjestelmiä liitetään tietoverkkoihin yhä enenemässä määrin, jotta järjestelmiä voidaan valvoa, säätää, ja ylläpitää etänä. Laitteet voivat kuitenkin olla huonosti suojattuja, varsinkin jos kyseessä on järjestelmä jota ei ole alun perin suunniteltu verkkoon liitettäväksi. Täten automaation kyberturvallisuus voi maatilan olla kannalta erittäin tärkeä ja haastava asia. Laitteen kaappaamalla voidaan aiheuttaa vahinkoa ja vaarantaa eläinten hyvinvointia esimerkiksi sotkemalla ruokinnan. Automaatiojärjestelmät ovat myös haavoittuvia sähkönjakelun häiriöille, koska lyhyetkin katkokset eläinten hyvinvoinnista huolehtivassa automatiikassa voivat aiheuttaa suurta haittaa.

Eläinten päivittäiseen hoitoon liittyvä tieto tulisi olla käytettävissä myös tietoliikenneverkon häiriötilanteissa. Ruokintaa ja lypsyä ei voida jättää suorittamatta puuttuvan tietoliikenteen takia. Eläinten jalostustiedot ja eläinrekisteri on tyypillisesti sijoitettu verkkopalveluihin. Esimerkiksi eläinten myyntiin tarvittavat dokumentit tulostetaan myyntitilanteessa verkosta. Jos verkkopalveluun pääsy on estynyt, voidaan joutua tilanteeseen, jossa tarvittavaa asiakirjaa ei voida tuottaa eläimen mukaan toimitettavaksi.

4.6. Maatalouden ajoneuvot

Maatilalla yleisimmin tunnettuja ajoneuvoluokkia ovat traktorit ja leikkuupuimurit. Tilakoon kasvaessa käyttöön tulee yleensä suuri joukko erilaisia itsekulkevia työkoneita; ajosilppurit, rikkaruohoruiskut, ajettavat lietteenlevityslaitteet ja sadonkorjuukoneet. Modernit maatalousajoneuvot ovat tyypillisesti väyläohjattuja, ja siten niiden on mahdollista sekä käyttää että tuottaa dataa. Väylää käytetään traktorin sisäiseen ohjaukseen ja enenevässä määrin työkoneiden hallintaan.

Toimialan kehittämä ISO11783 eli ISOBUS -standardi mahdollistaa eri valmistajien traktorien ja työkoneiden yhteen liittämisen väylätasolla. Yhteen liittäminen on erityisen haastavaa, koska kaikkia laiteyhdistelmiä ei voida toiminnallisuuden ja turvallisuuden osalta erikseen testata. Yhteensopivuus määritellään standardia vastaan tehtävällä yhteensopivuustestillä.



Kuva 5. ISOBUS ohjattu traktori ja työkone. Väylä mahdollistaa työkoneyksikön automaattisen ohjaamisen. Automaattinen järjestelmä voi pyytää kohottamaan konetta esimerkiksi esteen tai maalajin vaihtumisen takia. Myös ajo-uran merkintään käytettävät sitkaimet liikkuvat automaattisesti päisteissä. Häiriöt tai haittaohjelmat väylässä voivat aiheuttaa odottamattomia liikkeitä koneessa.

4.6.1. Traktorit

Maatalous- ja metsäkoneiden käyttämä CAN -väyläratkaisu on määritelty standardissa ISO 11783, joka tunnetaan kaupallisesti nimellä ISOBUS. Traktorin moottorin ja vaihteiston ohjaus noudattaa standardia SAE J1939, jota käytetään yleisesti raskaan kaluston väyläratkaisuissa. ISOBUS on laajennus tähän standardiin ja toteuttaa traktorin ja työkoneen välisen tiedonsiirron.

4.6.2. Traktoriin kytkettävät työkoneet

Traktoriin liitettävissä työkoneissa elektroniikka ja automaattiset toiminnot ovat lisääntymässä. Ensimmäisen sukupolven automaatioratkaisut ovat olleet valmistajakohtaisia ja niissä ei yleensä ole ollut liitäntää ulkoiseen verkkoon. Uudemmat koneet noudattavat ISO11783 standardia. Tämän avulla työkone voi liittyä traktorin väylään ja olla edelleen saavutettavissa. Työkoneiden ylläpitoon ollaan kehittämässä myös verkkopohjaisia ratkaisuja.

4.6.3. Maatalouden itsekulkevat koneet

Maatalouden itsekulkevat koneet kootaan yleisesti käytössä olevista komponenteista joita käytetään yleisesti teollisuudessa ja raskaassa kalustossa. Itsekulkevien koneiden ohjausväylän perustekniikka on yleensä SAE J1939 standardin mukainen. Itsekulkevissa koneissa varsinainen toimilaitteiden ohjaus voidaan toteuttaa valmistajakohtaisilla ratkaisuilla. Itsekulkevissa laitteissa voi olla tuki myös ISO11783 standardin mukaiselle tiedonsiirrolle, jolloin laitetta voidaan verrata traktori-työkoneyhdistelmään vaikka kone olisi yksi kokonaisuus.

4.6.4. Muut ajoneuvot

Maataloustyökoneiden lisäksi maataloudessa käytetään autoja ja muita ajoneuvoja, joita ei ole suunniteltu erityisesti maatalouskäyttöön. Niiden kyberuhkia ei tässä raportissa käsitellä.

4.6.5. Haasteita ja heikkouksia maatalouden ajoneuvoissa ja koneissa

ISO11783 (ISOBUS) -standardin nykyiset toteutukset eivät rajoita työkoneen väylälle pääsyä. Täten mikä tahansa traktoriin liitetty laite voi ottaa traktorin ohjauksen haltuunsa. Tämä mahdollistaa lait-

teen etäohjauksen, mutta tällä hetkellä suurin osa liikkuvista työkoneista ei ole kiinnitettynä tietoverkkoon. Tarve verkkoyhteyksille on kuitenkin kasvamassa, ja jo lähitulevaisuudessa suoraan verkossa olevien työkoneiden määrä voi kasvaa nopeastikin. Yleiseen tietoverkkoon ja traktorin väylälle liitetty laite kuitenkin myös mahdollistaa etähyökkäykset, joissa traktoria ohjataan tekemään ei-toivottuja toimintoja. Maatalouskonetoimiala työstää toiminnalliseen turvallisuuteen liittyen ISOBUS -standardiin ratkaisuja, joiden avulla voidaan varmistua että traktorin saamat ohjauskäskyt tulevat luotetulta toimijalta. Järjestelmä tunnetaan nimellä TIM (= tractor implement managment).

Myös maatalousajoneuvojen datan käyttö on nopeasti kehittyvä ala ja standardeja kehitetään voimakkaasti. Uusimmat versiot ISOBUS -standardista mahdollistavat traktorin toimintojen automaattisen ohjaamisen, mikä on tuonut maatalousajoneuvoihin enenevässä määrin automatiikkaa, kuten peltotöiden automaattiohjauksen. Väyläohjaus mahdollistaa myös sen, että esimerkiksi vedettävä työkone ohjaa traktorin kulkua työtehtävän aikana. Täysautomaattiset liikkuvat työkoneet ovat tällä hetkellä kaupallisten konseptiajoneuvojen tasolla. Teollisuudessa on valmius ruveta rakentamaan maatalouden täysautomaattiajoneuvoja välittömästi kun lainsäädäntö sallii niiden käytön maataloustyössä.

EU asetuksessa N:o 167/2013 määritellään mm. traktoreista koskevasta liitännästä minkä avulla traktorin väylää ja ohjausjärjestelmää voidaan lukea ja suorittaa tarvittavia huoltotoimenpiteitä. Tätä liitäntää on myös mahdollista käyttää erilaisten mittauslaitteiden liitäntäpisteenä. Tulevaisuudessa ajoneuvojen väyliin liitetään myös erilaisia mittaus- ja seurantalaitteita ja ne voivat olla myös yhteydessä erilaisiin verkkopalveluihin, kuten sääpalveluihin. Koska ajoneuvojen väylän arkkitehtuuri on alkujaan suunniteltu niin, että kaikki väylään kiinni pääsevät laitteet voivat kommunikoida ja vaihtaa tietoja ilman rajoituksia, tämä kehitys voi tulevaisuudessa huonontaa maatalousajoneuvojen kyberturvallisuutta. Väylän heikko tietoturva ja ajoneuvoon liitettävät verkkoyhteydet mahdollistavat ajoneuvon toimintaan vaikuttamisen etäyhteydellä.

4.7. Maatilan tietokoneet

Maatilalla tietokoneita on vähintäänkin tilan asuinrakennuksessa. Koneita voi olla myös eläinsuojissa, kasvihuoneissa, sekä muissa tilan ulkorakennuksissa. Ulkorakennusten tietokoneet ovat tyypillisesti kyseisen rakennuksen automatiikan ohjaus- ja valvontakoneita, tai liittyvät muuten kyseisessä rakennuksessa tehtävään työhön. Tämän lisäksi maatilalla on tyypillisesti kannettavia laitteita, kuten älypuhelimia ja tablettitietokoneita. Maatilan tietokoneet voidaan jakaa kahteen eri luokkaan: tilan hallinnointiin käytettävät työtietokoneet, ja maatilan asukkaiden henkilökohtaiset tietokoneet.

4.7.1. Työtietokoneet

Tilan johtamisen ja viestintään käytetyt tietokoneet ovat tyypillisesti kotikäyttöön tarkoitettuja tietokoneita, eivätkä siten eroa tilan asukkaiden henkilökohtaisista koneista. Monesti voi itse asiassa olla niin, että viljelijä käyttää samaa tietokonetta sekä tilan hallinnointiin, että henkilökohtaiseen käyttöön. Hallinnointi ja henkilökohtainen käyttö voivat jopa olla samalla käyttäjätunnuksella. Hallinnointityöhön käytettäviä tietokoneita koskevat täsmälleen samat kyberuhat ja riskit kuin muitakin työtietokoneita. Täten niiden tietoturvasta on huolehdittava samalla tavalla. Paras tapa koneen tietoturvan varmistamiseksi on kaikkien käytettyjen ohjelmien päivityksistä huolehtiminen, sekä hyvän tietoturvaohjelmiston käyttäminen. Lisäksi työtietokoneella olisi syytä välttää epäluotettavien verkkopalveluiden käyttöä, jotta kone ei turhaan altistu tietoturvaongelmille.

Maatilan työtietokoneiden suurin kyberuhille altistava tekijä voi olla laitteiden ammattimaisen ylläpidon puuttuminen, mitä käsiteltiin tarkemmin osiossa 4.1.2. Täten laitteiden ohjelmistot eivät välttämättä ole ajan tasalla, laitteita ei ole varmistettu sähkönjakelun häiriöiden varalta, ja laitteiden varmuuskopiot eivät ole ajan tasalla.

Automaatiojärjestelmiä valvovia tietokoneita uhkaavat samanlaiset kyberturvallisuusriskit kuin muitakin maatilan koneita. Tämän lisäksi ulkorakennuksissa olevat tietokoneet voivat altistua lialle, pölylle, ja kosteudelle huomattavasti asuinhuoneistossa käytettäviä tietokoneita enemmän. Täten ne ovat alttiimpia laitteiston hajoamiselle, koska kuluttajatietotekniikkaa ei ole suunniteltu likaisissa olosuhteissa käytettäväksi.

4.7.2. Henkilökohtaiset tietokoneet

Suuri osa suomalaisista maatiloista toimii perheviljelmämallilla. Täten monilla tiloilla sama tietoverkko, jota käytetään tilan johtamiseen, hallinnointiin ja automaatiojärjestelmien valvontaan, on myös perheen käytössä. Tämä yhteiskäyttö on osaltaan riski maatilan tietoturvalle, koska samassa lähiverkossa tilan työtietokoneiden kanssa on myös koneita, joilla voidaan esimerkiksi käydä erilaisilla viihdesivustoilla, olla yhteydessä vertaisverkkoihin, tai käyttää muita verkkopalveluita jotka saattavat altistaa käytetyn koneen kyberuhille. Tämä puolestaan aiheuttaa suuremman vaaran muiden tilan verkossa olevien tietokoneiden saastumiseen. Olisi perusteltua jakaa tilan tietoverkko useampaan aliverkkoon, vaikka liittymä olisikin sama. Näin mahdollinen hyökkäys esim. viihdelaitteisiin rajautuisi sisäverkossa osaan, jossa tilan työtietokoneet ja muut laitteet eivät ole.

4.8. Alkutuotannon harjoittama jatkojalostustoiminta

Alkutuotannon harjoittamalla jalostustoiminnalla tarkoitetaan tilalla tuotettujen tuotteiden edelleen jalostamista. Alkutuotannon jalostustoiminta käyttää yleensä samaa tietotekniikkaan kuin tilan muukin liiketoiminta.

Jatkojalustukseen käytettävät tekniset ratkaisut ovat pienen mittakaavan tehtaita. Tehdasmainen toimintatapa tuo automaation myös pienjalostustoimintaan enenevässä määrin. Laitteita ei kuitenkaan usein hankita kokonaisuuksina vaan ostamalla isomman teollisuuden käytöstä poistamia laitteita ja sovittamalla ne pienimuotoiseen tuotantoon. Kun jalostustoimintaa laajennetaan, hankinnat kohdistuvat teollisuuden käyttämiin pieniin järjestelmiin missä tietoturva on huomioitu yleensä järjestelmätoimittajan ratkaisuilla.

Jalostustoimintaan liittyy usein suoramyyntiä ja vähittäiskauppaa. Vähittäiskaupan harjoittaminen edellyttää melkein aina maksujärjestelmien käyttöön ottamisen. Käytössä ovat myös markkinointiin liittyvät nettisivustot ja mahdollisesti verkkokauppa-alusta. Tällaiset tilojen käytössä olevat verkkopalvelut kattavat kaikki vaihtoehdot harrastepohjaisista viritelmistä ammattimaisesti valmistettuihin sivustoihin. Verkkokaupan tietoturva noudattaa alan yleisiä periaatteita. Suoramyyntiä varten yrityksissä otetaan käyttöön myös sähköisiä maksujärjestelmiä sekä verkkomaksamiseen että korttimaksuun.

4.8.1. Haasteita alkutuotannon harjoittamassa jalostustoiminnassa

Pienimuotoisen jalostustoiminnan kustannuksia pidetään kurissa hankkimalla käytettyä teknologiaa. Laitteet voivat olla käyttökuntoisia osakokonaisuuksia joiden ylläpitoon alkuperäisen valmistajan tukea ei ole saatavissa. Laitteistoja myös kunnostetaan ja muutetaan omatoimisesti käyttötarkoitukseen sopivaksi. Laitteiden automaatiolle ei välttämättä ole jatkossa saatavissa yläpitoa ja päivityksiä. Näin laitteiden tietoturva laskee ajan myötä.

Maksujärjestelmät ovat yleensä toimittajan ja maksuliikennettä tarjoavien yritysten ylläpidossa koko elinkaaren ajan. Näihin laitteisiin kohdistuvat uhat ovat hallittavissa tätä kautta. Omiin verkkopalveluihin lisättävät maksujärjestelmät ovat myös yleensä jonkun toimittajan hallinnassa. Uhka nettisivustoissa liittyy lähinnä siihen, että sivusto kaapattaisiin ja tilaus- ja maksuliikenne ohjattaisiin väärään paikkaan.

5. Maatalousympäristön kyberuhkia

Maatiloihin voidaan katsoa kohdistuvan ainakin kolmenlaisia erilaisia kyberuhkia. Ensinnäkin, maatilan digitaalista toimintaympäristöä uhkaavat erilaiset onnettomuudet ja vahingot, kuten laitteiden vikaantuminen tai rikkoutuminen, sääilmiöiden aiheuttamat kybervahingot, eläinten aiheuttamat vahingot, sekä ohjelmistojen ja palveluiden ei-tarkoitushakuinen väärinkäyttö. Toiseksi, maatilaa vastaan voidaan tehdä kyberhyökkäys, jolla pyritään tunkeutumaan johonkin tai joihinkin maatilan järjestelmiin, ja sitä kautta joko varastamaan maatilan digitaalista omaisuutta, tai vaikuttamaan maatilan toimintaan. Kolmanneksi, maatilan laitteita voidaan kaapata johonkin muuhun tarkoitukseen, kuten esimerkiksi kyberhyökkäysalustoiksi jotain muuta kohdetta vastaan.

Näistä uhista ensimmäinen ja toinen vaikuttavat maatilan toimintaan. Kolmas kyberuhka tyypillisesti ei aiheuta mitään vaikutuksia ennen kuin kaapattua alustaa käytetään luvatta. Tosin kyberuhkaa ei välttämättä huomata edes silloin, kun kaapattua laitetta käytetään osana hyökkäystä, mikäli sillä ei ole näkyvää vaikutusta tilan omaan toimintaan.

5.1. Vahingot ja onnettomuudet

Maatila on fyysisesti monille tietoteknisille laitteille vaativa toimintaympäristö. Laitteita käytetään ulkona monenlaisissa sääolosuhteissa, ja niitä voi olla pysyvästi sijoitettu tiloihin, joissa lämpötila ja ilmankosteus vaihtelevat huomattavasti. Maatila on myös toimintaympäristönä likainen, jolloin koneisiin nopeasti kertyy mm. pölyä, eläinten karvoja, ja muuta likaa. Laitteet voivat myös helposti altistua rajuillekin iskuille esimerkiksi pudotessaan. Koska monet maatiloilla käytetyt tietokoneet ja muut tietotekniset laitteet ovat ensisijaisesti kuluttajakäyttöön tarkoitettuja, ne kestävät yleensä huonosti likaa ja iskuja, ja täten laitteen rikkoutumisen vaara on olemassa.

Kuva 6. Kotieläintalouden automaatio on usein sijoitettu haastavaan ympäristöön. Kosteus, pöly ja eläinten kontaktit saattava aiheuttaa laitteiden rikkoontumisia.

Sääilmiöt voivat myös rikkoa laitteita. Tietokoneet tarvitsevat sähköä, eivätkä kestä jännitepiikkejä. Koska haja-asutusalueella sähköjohdot menevät usein maan pinnalla, ovat esimerkiksi ukkosen aiheuttamat vauriot yleisempiä kuin tiheästi asutetuilla alueilla.

Maatilan tietoverkon maadoittaminen ja liittäminen muuhun sähköverkkoon tulisi selvittää. Olemassa olevat käytännöt ja ohjeet eivät anna ilmeisesti riittävää suojaa ylijännitetilanteissa. Haja-asutusalueella yleisesti annettu suositus irrottaa laitteet sähköverkosta ukonilmalla on vaikea toteuttaa verkotetussa toimintaympäristössä. Laitteita ja liityntäpisteitä on lukuisia, ja monet laitteista eivät ole sellaisia että ne voidaan noin vain sammuttaa. Asennukset ovat monesti kiinteitä. Esimerkiksi eläinsuojan ilmastoinnin valvonta- ja ohjauslaitteiden on oltava päällä jatkuvasti. Näistä seikoista johtuen laitteiden järjestelmällinen irrottaminen sähköverkosta on käytännössä mahdotonta. Ylijännitesuojaukseen olisi löydettävä parempia rakenteellisia ratkaisuja sekä suunnittelu- ja asennusohjeita.

Maatilan sijainti vaikuttaa suuresti siihen, kuinka altis tila on sääilmiöille. Esimerkiksi rannikolla ja sisämaassa tuuli vaikuttaa eri tavoilla, ja tuulten pääasiallinen suunta ja ukkosmyrskyjen yleisyys vaihtelevat maan eri osissa. Sääilmiöitä vastaan suojautuminen perustuu ensisijaisesti ennalta varautumiseen. Tilan on tehtävä pitkän aikavälin varautumista erilaisiin sääilmiöihin esimerkiksi rakenteellisilla ratkaisuilla, jotka tekevät tilan tietoverkosta mahdollisimman säänkestävän. Maadoittamisratkaisut, ylijännitesuojaukset, varavirtalähteet ja vastaavat kuuluvat tähän varautumiseen, kuten myös herkkien laitteiden sijoittaminen paikkoihin, joissa sää ei pääse niihin suoraan vaikuttamaan. Lyhyen aikavälin varautumista taas on tehtävä silloin, kun sääennusteen mukaan sään ääri-ilmiö saattaa vaikuttaa tilaan. Tällöin esimerkiksi on syytä sammuttaa ei-kriittiset tietojärjestelmät, tarkastaa varavoiman saatavuus, valmistautua korjaamaan mahdollisia vahinkoja, ja niin edelleen.

Kuva 7. Salaman aiheuttama ylijännite valokuituliittymässä. Liittymän asennuksesta puuttunut potentiaalintasaus muuhun sähköverkkoon aiheutti virtapiikin useaan eri laitteeseen. Salaman on tullut ulos mustan laitteen kulmasta ja maadoittunut valkean kytkentärasian ja valokuidun suojalankojen kautta maahan. On hyvin todennäköistä että valokuitukaapelin suojakuori on jostakin vaurioitunut salamaniskun seurauksena. Vaurion takia vettä ja likaa voi päästä kuitukaapelin sisään ja aiheuttaa myöhemmin kaapeliin vaurion.

Maatalouden tuotantorakennuksiin sijoitetuilla laitteille tulee myös kosteusvaurioita suhteellisen kosteuden noustessa. Laitteiden riittävä kotelointiluokka (SFS-EN 60529) suojaa pölyltä ja kosteudelta. Kuitenkin, mikäli laitteen lämpötila on sama tai alempi kuin ympäristössä olevan ilman lämpötila, alkaa kosteus tiivistyä laitteiden pinnalle suhteellisen kosteuden noustessa yli 90%. Sähköisten laiteiden olisi parempi olla koko ajan päällä, jolloin laitteen tuottama hukkalämpö estää kastepisteen ylittymisen laiteessa. Myös laitekotelon tai tilan lisälämmitys varmistaa riittävän kuivat olosuhteet.

Pölyltä suojaaminen on usein haastavaa koska laitteita on jäähdytettävä. Aktiivijäähdytys, kuten esimerkiksi jäähdytystuuletin, kerää pölyä ja kerryttää sitä laitteiden sisään. Pölyisissä oloissa tulisi ensisijaisesti valita laite, jossa on passiivinen jäähdytys. Mikäli on käytettävä aktiivijäähdytystä vaativia laitteita, tulisi niiden olla pölyisissä olosuhteissa käytettäviksi suunniteltuja, tai laitteen puhtaudesta on pidettävä jatkuvasti huolta.

Maatalouden toimintaympäristössä myös eläimet voivat vaikuttaa laitteistojen toimintaan. Kaapeloinnit kulkevat usein paikoissa, jotka ovat myös jyrsijöiden liikkumisreittejä, jolloin kaapelit voivat vaurioitua jyrsijöiden hampaissa tai kynsissä. Täten syntyvät vauriot voivat tulla esille vasta pitkänkin ajan kuluttua esim. ilman kosteuden muuttuessa, ja usein vaurioituneen kohdan löytäminen voi olla haastavaa. Kaapelivaurioita voi syntyä niin rakennuksissa kuin ajoneuvoissa. Syntynyt vaurio estää tai vähintäänkin haittaa laitteen toimintaa.

Hyötyeläinten aiheuttamia vahinkoja ovat tyypillisesti eläinten normaaliin käyttäytymiseen liittyvät kuormitukset johtoihin, antureihin ja toimilaitteisiin. Laitteet on suojattava niin että eläin ei voi niitä rikkoa eikä itse vahingoittua esim. sähköiskun seurauksena. Erityisesti ruokintalaitteet ovat eläinten mielenkiinnon kohteena.

Hyötyeläimet tuottavat likaa ja kuona-aineita, jotka vähitellen myös kerrostuvat eläinsuojiin. Suojissa olevat laitteet ovat täten erittäin vaativassa toimintaympäristössä, mikä on otettava huomioon niitä valittaessa ja sijoitettaessa. Kaapelointireittien suunnittelussa on huomioitava lian kertyminen rakenteiden päälle. Myös säännöllinen puhdistaminen laitetiloissa ja myös laitteiden sisällä on perusteltua.

Maatilan verkkoyhteydet voivat myös katketa. Syynä voi olla fyysinen vika, virhe maatilalla, tai virhe verkkopalvelun tarjoajan palvelussa. Laitteiden on syytä olla sellaisia, että ne kykenevät suoriutumaan ainakin perustoiminnallisuuksista myös ilman verkkoyhteyksiä.

5.2. Kyberhyökkäykset maatilaa vastaan

Erilaisia tahoja, jotka voivat pyrkiä hyökkäämään maatilaa vastaan, on useita. Lehto *ym.* (2017) listaavat mahdollisina hyökkääjinä sisäpiiriläiset, kybervandaalit, kybervakoilijat, sekä kyberterroristit ja sotilaat. Näiden lisäksi ainakin kyberrikolliset ovat mahdollisia hyökkääjiä, jotka saattavat toimia myös maatiloja vastaan. Normaalin yhteiskuntajärjestyksen ja rauhantilan vallitessa sotilaat eivät ole aktiivinen uhka ja tässä yhteydessä sisäpiiriläisten aiheuttamia uhkia ei käsitellä erikseen. Raportin osiossa 4.2.1 käsitellään mahdollisia ongelmia, joita maatilan tietojärjestelmiä käyttävät eri ihmisryhmät voivat aiheuttaa. Tosin minkä tahansa alla kuvatun hyökkäyksen voi tehdä myös sisäpiiriläinen. Kuitenkin, koska suomalaiset maatilat ovat kohtuullisen pieniä, on sisäpiiriläisten määrä yleensä rajallinen ja täten heidän aiheuttamansa ongelma myös rajallinen.

Kyberhyökkäyksillä voidaan pyrkiä vaikuttamaan suoraan maatilan toimintaan jollain tavalla. On ainakin kolme suoraa tapaa pyrkiä vaikuttamaan maatilan toimintaan: maatilan datan tuhoaminen, maatilan datan pahantahtoinen salaaminen, ja maatilan laitteiden ja tuotantoprosessien häirintä. Lisäksi maatilaan voidaan vaikuttaa varastamalla maatilan dataa ja käyttämällä sitä tilaa vastaan. Kyberhyökkäyksen tarkoituksena voi myös olla mahdollistaa tai peittää fyysinen tunkeutuminen maatilalle. Kaikki nämä vaikutusmekanismit vaativat hyökkääjältä pääsyä maatilan tietojärjestelmiin ja sitä kautta maatilan laitteisiin, dataan ja toiminnanohjaukseen.

Datan tuhoaminen vaatii hyökkääjältä pääsyn tietojärjestelmään, jossa dataa säilytetään. Tiedon voi tämän jälkeen tuhota helpoiten tuhoamalla kaiken tietojärjestelmässä säilytettävän tiedon. Mikäli

hyökkääjä haluaa jostain syystä tuhota vain tietyt tiedot, tai aiheuttaa haittaa tietoja muuttamalla, on hänen tiedettävä missä tietoa säilytetään ja miten siihen voi vaikuttaa. Esimerkiksi erilaiset kybervandaalit voivat olla kiinnostuneita tiedon tuhoamisesta. Motiivi voi olla esimerkiksi kokeilunhalu, hauskanpito, kiusanteko, tai eläinaktivismi. Myös terroristit voivat tuhota dataa.

Datan pahantahtoinen salaaminen tyypillisesti tehdään käyttämällä ns. kiristyshaittaohjelmaa. Näitä ohjelmia levitetään esimerkiksi sähköpostin välityksellä, mutta on olemassa menetelmiä, joilla haittaohjelmia voidaan levittää myös verkkosivustojen kautta. Tyypillisesti kiristyshaittaohjelma toimii käyttäjän käynnistäessä sen epähuomiossa, jonka jälkeen ohjelma salaa tietokoneen tiedot ja vaatii käyttäjältä lunnaita niiden palauttamiseksi. Kiristyshaittaohjelmat ovat tyypillinen kyberrikollisten käyttämä hyökkäyskeino.

Tilan datan tuhoamisen tai salaamisen voi mieltää tuotantoprosessien häirinnäksi, mutta tuotantoprosesseja voi häiritä myös aiheuttamalla ei-toivottua toimintaa tilan käyttämään laitteistoon ja automatiikkaan. Erityisesti kotieläintalouden ja kasvihuonetilat voivat olla haavoittuvia tämän kaltaisille hyökkäyksille. Eläinten valvontalaitteistojen, ruokintalaitteistojen, tai eläinsuojien sisäolosuhteita säätävien laitteistojen vääränlainen toiminta voi sekoittaa maatilan toimintaa, ja pahimmassa tapauksessa huonontaa eläinten hyvinvointia ja aiheuttaa tilalle huomattavia tappioita. Vastaavasti myös kasvihuoneen valvonnan ja säädön rikkominen voi haitata kasvien hyvinvointia ja aiheuttaa huomattavia tappioita. On myös mahdollista hyökätä tilan satoa vastaan tietyissä tilanteissa, kuten esimerkiksi vaikuttamalla viljan kuivaussiilon toimintaan. Liikkuvien työkoneiden liittäminen tietoverkkoon voi myös tehdä mahdolliseksi niitä vastaan hyökkäämisen, joka voi aiheuttaa suuriakin uhkia liikenne- ja työturvallisuudelle esimerkiksi ohjaamalla työkone väärään paikkaan. Tällaisia hyökkäyksiä voivat tehdä vandaalit ja terroristit, sekä poikkeusolojen vallitessa myös kybersotilaat.

Datan varastaminen vaatii hyökkääjältä pääsyn tietojärjestelmään, jossa dataa säilytetään, sekä tiedon siitä, missä tietoa säilytetään. Tällöin hyökkääjä voi tehdä datasta itselleen kopion. Tietojärjestelmiin tallennetun datan lisäksi hyökkääjä voi pyrkiä varastamaan dataa suoraan dataa tuottavasta järjestelmästä. Hyökkääjä voi esimerkiksi tunkeutua tilan valvontakameroihin ja pyrkiä sitä kautta hankkimaan itselleen videomateriaalia tilan toiminnasta. Tilan tietojen luvaton kopiointi on tyypillistä kybervakoilua, mutta taustalla oleva motiivi voi vaihdella aktivismista taloudellisen hyödyn tavoitteluun tai valtiolliseen tiedusteluun.

Kyberhyökkäyksillä voidaan myös pyrkiä mahdollistamaan fyysinen tunkeutuminen maatilalle, tai peittää fyysisen tunkeutumisen jälkiä. Tällöin hyökkääjän kohteena on esimerkiksi maatilan kulunvalvonta ja hyökkäys voi kohdistua vaikkapa valvontakameroita vastaan. Mikäli tilalla on sähköiset lukot, voidaan niihin pyrkiä vaikuttamaan. Tämä tosin voi vaatia huomattavasti enemmän tietoa hyökkääjältä kuin esimerkiksi kuluttajaelektroniikkatasoisiin webbikameroihin perustuvaan valvontakamerajärjestelmään tunkeutuminen. Motiiveja fyysiseen tunkeutumiseen voi olla useita. Eläinaktivismi, varkaudet ja vahingonteko ovat näistä muutamia.

Maatilan tietojärjestelmiin tunkeutuminen voi olla joko opportunistinen hyökkäys haavoittuvaiseksi huomattua järjestelmää vastaan, tai sitten suunnattu juuri kyseistä kohdetta vastaan.

Opportunistiset hyökkääjät etsivät automatisoidusti tietoverkoista haavoittuvia tietojärjestelmiä, sekä levittävät erilaisia hyökkäykseen käytettäviä haittaohjelmia esimerkiksi sähköpostin välityksellä. Varsinainen hyökkäys kohdistuu sitten niitä kohteita vastaan, joilta sattuu löytymään heikkouksia, tai jotka sattuvat aktivoimaan haittaohjelman.

Kohdistetut hyökkäyksen takana on taho, joka haluaa vaikuttaa nimenomaan valittuun kohteeseen. Tiettyä maatilaa vastaan tällaisen hyökkäyksen motiivina voisi toimia esimerkiksi eläinaktivismi. Kohdistetussa hyökkäyksessä voidaan käyttää samoja menetelmiä kuin opportunistisessa, mutta käytettäviä työkaluja saattaa olla enemmän käytössä. Lisäksi kohdistetussa hyökkäyksessä voidaan pyrkiä pääsemään fyysisesti käsiksi maatilan tietokoneisiin.

5.3. Maatilan laitteiden kaappaus

Maatilojen tietojärjestelmissä voi olla useitakin haavoittuvia laitteita. Koska tietoturva ei tyypillisesti kuulu maatilan ydinosaamiseen, voi turvallisuus olla huonolla tasolla niin tilan tietokoneissa kuin muissakin tietoteknisissä laitteissa.

Haavoittuva, internetiin näkyvä laite, voidaan nykyään kaapata osaksi kyberhyökkäyksiin käytettävää ns. bottiverkkoa. Haavoittuvien laitteiden etsintä on automatisoitua toimintaa, jossa jo kaapatut laitteet satunnaisesti etsivät verkosta haavoittuvia laitteita ja sellaisen löytäessään kaappaavat sen. Esimerkiksi mirai-haittaohjelma leviää verkkoon kytkettyihin, suojaamattomiin laitteisiin erittäin nopeasti. Haavoittuva laite voi nykyään saastua oltuaan verkossa vain minuutteja. Ohjelmaa käytettiin esimerkiksi syksyllä 2016 suuressa palvelunestohyökkäyksessä useita verkkopalveluita vastaan (Hilton 2016).

Kyberhyökkäysalustojen etsinnän automatisoituminen tarkoittaa sitä, että jokainen maatila, siinä missä jokainen muukin verkkoon kytketty järjestelmä, on jatkuvan kyberuhan alla. Uhka on kuitenkin vaikeasti havaittava, koska se ei kohdistu maatilaan itseensä ja kaapattu laite toimii normaalisti silloin, kun sitä ei käytetä osana hyökkäystä. Hyökkäyksen aikana maatilan tietoverkko voi puuroutua, varsinkin jos tilalla on suuri määrä kaapattuja laitteita. Lisäksi tilan palveluntarjoajan järjestelmät voivat huomata tilan laitteiden olevan osa palvelunestohyökkäystä, jolloin palveluntarjoaja voi joutua itse rajoittamaan tilan tietoliikennettä.

Maatilan laitteita voidaan kaapata myös muihin tarkoituksiin kuin kyberhyökkäysalustoiksi, vaikka tarkoituksena ei olisi vaikuttaa suoraan maatilan toimintaan. Yhä useammat laitteet ovat yhteydessä internetiin mobiiliverkon välityksellä. Maatilalla esimerkiksi erilaiset peltosensorit tai viljelijän puhelimeen hälytyksiä lähettävät järjestelmät voivat käyttää mobiiliverkkoa, ja nopeiden, neljännen sukupolven mobiiliverkkojen yleistyessä voidaan maatilan kaikki verkkoyhteydet järjestää mobiiliverkon kautta. Mobiili tiedonsiirto ei kuitenkaan välttämättä ole kiinteähintaista, varsinkin mikäli siirrettävän datan määrä on erittäin suuri. Täten, mikäli kaapattua laitetta käytetään suurten datamäärien siirtoon, voi tästä tulla maatilalle iso ylimääräinen kulu.

Mobiiliverkkoa käyttävä laite on jatkuvassa yhteydessä langattomaan puhelinverkkoon, joten sitä voidaan käyttää myös puheluiden soittamiseen. Mikäli kaapatulla laitteella soitetaan puheluita esimerkiksi maksullisiin palvelunumeroihin, voi tästäkin tulla maatilalle iso ylimääräinen kulu.

6. Tietojärjestelmät ja tietosuoja maatalouden liiketoiminnassa

Modernit maatilat tuottavat ja käyttävät monenlaista tietoa, ja tilaan liittyvä tieto on tallennettu useisiin eri tietojärjestelmiin. Maatilalla on tyypillisesti käytössä viljelysuunnitteluohjelmisto, jonka avulla maatilan viljelytoimintaa johdetaan. Suomessa on yleisesti käytössä neljä viljelysuunnitteluohjelmistoa: Datatechin PeltoW, MTechin WebWisu, SoftSalon Peltotuki ja Suonentiedon AgriNeuvos. Viljelysuunnitteluohjelmistossa on maatilan peltojen tiedot, viljelyhistoriatiedot, sekä muuta maatilan tuotantoon liittyvää tietoa, riippuen käytetystä ohjelmistosta, viljelytoiminnasta, ja muista tilasta riippuvaisista tekijöistä. Käytännössä jokainen suomalainen maatila käyttää myös Maaseutuviraston Vipu-palvelua, jonka avulla tehdään esimerkiksi maataloustukihakemukset. Tyypillisesti Viljelysuunnitteluohjelmistoissa on rajapinta Vipuun, jolloin ohjelmistoa voi käyttää tukihakemuksen teossa.

Viljelyohjelmistojen lisäksi eläintiloilla on lisäksi käytössä eläinkasvatukseen liittyviä järjestelmiä, kuten esimerkiksi nautakarjatilojen Minun maatilani ja Naseva, lammastilojen WebLammas, sekä sikatilojen Sikava. Näihin järjestelmiin tallennettaan tiedot tilan eläimistä ja niihin liittyvistä toimenpiteistä, kuten esimerkiksi syntymistä, ostoista ja myynneistä, teurastuksista, ja sairauksista. Lisäksi tiloilla on käytössä erilaisia eläinten ruokintaan, eläinsuojien olosuhteiden hallintaan, ja muuhun eläinten hoitoon liittyviä tietojärjestelmiä. Nämä järjestelmät seuraavat eläinten ja eläinsuojien tilaa, ja monia niistä voidaan käyttää myös eläinten hoidossa käytettävien automaatiojärjestelmien ohjauksessa. Järjestelmien ohjauksessa käytettävät sovellukset toimivat tyypillisesti paikallisverkossa. Kotieläintalouden eläintietoihin liittyvät sovellukset ovat perinteisesti hyödyntäneet keskitettyä palvelua. Palvelujen käyttö on siirtymässä selainpohjaisiksi.

Seuranta- ja ohjausjärjestelmät tuottavat ja käyttävät erilaisten sensoreiden mittaamaa dataa. Esimerkiksi lehmiä voidaan valvoa märehdintää ja liikettä mittaavilla sensoreilla, jotka tuottavat jatkuvaa dataa lehmän käytöksestä, ja kasvihuoneen lämpötilaa ja kosteutta mittaamalla ohjataan huoneen sisäolosuhteiden säätöä. Eri sensorijärjestelmien tuottama data voidaan käyttää suoraan ja sen jälkeen tuhota. Data, tai siitä jalostettu tieto, kuitenkin usein tallennetaan, tyypillisesti järjestelmän omaan tietokantaan.

Maatilalla on myös paljon tietoa, jota kertyy maatilan toiminnasta esimerkiksi tositteiden, sopimusten, raporttien, kuittien ja muiden dokumenttien muodossa. Näistä muodostuu maatilan digitaalinen arkisto, jossa on tilan digitaalisessa muodossa olevat dokumentit. Maatilan digitaalista arkistoa käsitellään tarkemmin dokumentin osiossa 8.

Tilojen toiminnasta kertyy yhä enenemässä määrin dataa, jota on tyypillisesti tallennettuna eri paikkoihin. Vipu-palvelussa on tietoa käytännössä jokaisesta suomalaisesta maatilasta, ja meijereiden järjestelmissä on suuria määriä dataa jokaisesta meijerille maitoa tuottavasta tilasta. Suuri osa tästä datasta sisältää tietoja, jotka liittyvät maatilan toimintaan.

Maatalousyrityksen tuottama tieto on samalla tavalla luottamuksellista kuin minkä tahansa muunkin alan yrityksen tuottama tieto. Esimerkiksi tilan digitaalisessa arkistossa oleva sopimustieto on luottamuksellista, ja sitä väärinkäyttämällä voidaan esimerkiksi vaikuttaa kilpailutilanteeseen; maatilalla työskenteleviin henkilöihin liittyvät tiedot, kuten palkanmaksu ja tarkat henkilötiedot, ovat myös luottamuksellisia. Usein, kun erilaisia asiakirjoja käsitellään eri tietokoneilla, jää asiakirjoista useita kopioita eri tietokoneisiin. Mikäli maatilan tietokoneella on käsitelty luottamuksellista tietoa, tulee koneen asiallisesta hävittämisestä huolehtia sen elinkaaren päättyessä. Asiallisessa hävittämisessä tärkeintä on huolehtia siitä, että koneen kiintolevy tyhjennetään tai toimitetaan hävitettäväksi niin, että tiedot eivät sitä kautta voi joutua vääriin käsiin.

Maatilan on myös syytä ottaa huomioon kuinka henkilöihin liittyvistä tiedoista, kuten työsopimuksista, terveystiedoista, ja palkkalaskelmista, saattaa syntyä henkilörekisteri. Henkilörekisterin ylläpidosta aiheutuu tiettyjä velvoitteita, jotka tulee myös ottaa huomioon maatilalla. Tietojen tallentaminen on hoidettava siten, että tietoihin ei voi päästä käsiksi tarpeettomasti.

Tilan tietosuojan suhteen tukihakemukset ja niihin liittyvät valvontadokumentit voivat olla ongelma. Tukipäätökset ovat osittain julkisia. Viranomaiset julkaisevat nämä tukihakemusten julkiset tiedot. Maatilan on kuitenkin pidettävä omaa arkistoa myöhempiä selvityksiä silmälläpitäen myös jätetyistä tukihakemuksista ja tukipäätöksistä. Myös tukiehtojen mukaiset muistiinpanot tulee arkistoida. Valvontavelvollisuuteen kuuluvien tietojen lisäksi asiakirjoissa saattaa olla mukana valvontaan kuulumattomia tietoja tai yksityiskohtia. Nämä tiedot tulisi pystyä poistamaan asiakirjoista ja sähköisestä materiaalista mitä valvontaan toimitetaan. Esimerkkinä käyttäjätunnukset joita on välitetty viljavuusanalyysitulosten paperisissa dokumenteissa. Kun aineistoa toimitetaan sähköisesti, saattaa tiedoissa olla myös muuta luottamuksellista valvontaan kuulumatonta tietoa. Sähköisen aineiston luovuttamisessa käyttäjällä tulisi aina olla tieto siitä mitä luovutettava aineisto sisältää.

7. Materiaali- ja varaosahuolto

Maatilan tuotantotarvikehuoltoon on kehitetty järjestelmiä joiden avulla esim. rehutilaus voi syntyä automaattisesti. Automaattiset tilausjärjestelmät ovat vielä harvinaisia ja yleensä varmistetaan erillisellä tekstiviestillä. Kyberhyökkäystilanteessa rehutoimitusten hoitaminen voi olla toiminto, jossa tilapäisvälineet on otettava käyttöön. Tilausväli on tyypillisesti 2-3 viikkoa. Teollisia rehuja ei yleensä varastoida pidemmäksi aikaa tiloilla.

Maatalouden laitteiden vanheneminen on tulevaisuuteen katsottaessa merkittävä uhka. Laiteratkaisuista riippuen voi olla tarvetta useampaan elinkaaren aikaiseen päivitykseen. Jos käytetyt osat ovat hyvin erilaistettuja voi olla vaarana että varaosia ei ole saatavissa esim. valmistuksen päätyttyä. Yleinen varaosahuoltovelvollisuus, 10 vuotta, on merkittävästi lyhempi kuin maatalouskoneiden tyypillinen elinkaari. Varaosahuollon riskinä ovat myös komponentit, joiden valmistus päättyy ja joille ei ole saatavissa korvaavaa tuotetta. Esimerkiksi mikropiireissä uuden sukupolven käyttöön ottaminen voi vaatia koko ohjelmiston uudelleensuunnittelua.

Kuva 8. Maatalouden käyttöympäristö asettaa suuremmat vaatimukset käytettäville komponenteille. Laitteisiin kohdistuu myös iskuja ja normaalia suurempia kiihtyvyyksiä. Laitteiden suunnittelussa tulee komponenttien tukemiseen kiinnittää huomiota. Kuvassa piirilevyllä ollut kondensaattori on irronnut tuen puuttuessa. Kyberturvallisuuteen kuuluu myös käytettyjen osien varaosahuolto.

8. Varmuuskopiot ja digitaalinen arkisto

Yritystoiminnassa tietokoneiden varmuuskopiointi on yleensä hoidettu keskitetysti tai tiedot on tallennettu keskitettyyn palveluun joka varmuuskopioidaan. Maatalouden tietojärjestelmiä ei yleensä ylläpidetä ammattimaisesti ja myös varmuuskopiointi jää käyttäjäkohtaiseksi. Käytössä on usein sovelluskohtaisia varmuuskopiointi ohjelmia, joilla voidaan varmistaa yksittäisen sovelluksen tietosisältöä. Niiden käyttö jää käyttäjän vastuulle.

Varmuuskopiointi tulisi järjestää automaattisilla, ajoitetuilla sovelluksilla. Varmuuskopiointipaikka ja väline tulisi olla kiertävä niin että esim. tulipalossa tiedot eivät tuhoudu. Maatilan toimintaympäristössä ratkaisu voisi olla sijoittaa varmuuskopiointi eri rakennukseen kuin missä tietoja yleensä käytetään. Tällä saavutettaisiin korkeampi turvallisuustaso.

Sovellusten siirtyminen pilvipalveluiksi ratkaisee osittain varmuuskopiointiin liittyviä ongelmia. Pilvipalvelun tarjoaja vastaa yleensä aina varmuuskopioinnin järjestelyistä. Pilvipalvelun toimittajan luotettavuus ja jatkuvuus on merkittävä asia. Usein ilmaiset, tai johonkin tuotteeseen liittyvät, palvelut voivat sulkeutua yllättäen. Tällöin palveluun tallennettuihin tietoihin ei käyttäjällä ole enää pääsyä. Tämä uhka on myös otettava huomioon pilvipalveluita valittaessa.

Myös sopimusten ja muiden asiakirjojen säilyttäminen sähköisessä muodossa tulee turvata. Sopimusten kopioita voidaan tarvita uudelleen vuosienkin kuluttua. Sopimusoikeudellisesti maatalouden sopimukset voivat olla kestoltaan jopa useita vuosikymmeniä. Digitaalista arkistoa on esimerkiksi verotukseen liittyvä kirjapito, jolla on kuuden vuoden säilytysvelvollisuus. Digitaalinen arkisto on oltava avattavissa vielä ajankin kuluttua, joten käytettävien tiedostomuotojen tulisi olla yleisesti tuettuja. Vuosina 1990–2007 maatiloilla oli käytössä ohjelmistoja joiden tiedostoformaatin auki saaminen voi olla jo nyt haastavaa ohjelmistojen poistuttua markkinoilta. Tällaisia ohjelmia ovat esimerkiksi tuolloin yleinen toimisto-ohjelma Works, joka oli tietokoneissa valmiiksi asennettuna.

Varmuuskopiointia on seurattava ja on selvitettävä menetelmät, joilla varmuuskopioiden tiedot voidaan palauttaa. Vanhempien varmuuskopioiden tietojen palauttamiseen liittyy myös tietojen käyttöön tarvittavan sovelluksen palauttaminen. Tiedot on voitava päivittää uudemmille sovelluksille, tai vanhempi sovellus on voitava asentaa uudelleen käyttöön. Myös koko sovellus voi olla poistunut markkinoilta. Digitaalisen arkiston ylläpitoon kuuluu täten myös käytettyjen sovellusten arkistointi.

9. Maatalouden tietojärjestelmien kriisinkestävyys

Maatalouden käytössä olevia järjestelmiä ei yleensä ole suunniteltu kriisiaikojen toimintaa tukevaksi. Käytetyt laitteistot ovat yleensä koti- ja harrastekäyttöön tarkoitetusta laitteista koottuja. Kriisinkestävyyden kannalta keskeistä on yleensä sähkön saanti. Sähköverkon toiminta ja laatu erilaisissa kriisitilanteissa on ensimmäinen ratkaiseva tekijä. Paikallisesti tuotetun varavoiman heikko laatu voi vaikuttaa häiritsevästi tai jopa rikkoa puolijohdetekniikkaan perustuvia laitteita. Erityisesti alijännitteen on todettu vaikuttavan laitteiden toimintaan. Maatilojen varavoimaratkaisuissa tulisi kiinnittää huomiota riittävään kuormituksen kestoon mikä takaa laadukkaan sähkön häiriötilanteissa.

Paikallisesti toimivat järjestelmät voidaan ottaa käyttöön yleensä heti kun sähkönsaanti on toiminnassa. Verkkoon liitettyjen järjestelmien käyttö kriisitilanteissa edellyttää toimivia verkkoyhteyksiä. Valitettavasti tietoliikenneverkko on varmistettu yleensä vain muutamien tuntien varakäytöllä ja on samalla tavalla riippuvainen samasta alueellisesti sähkönsyötöstä kuin maatilat.

9.1. Vaikutuksen sähkönjakelun häiriöissä

Sähkönjakelun häiriön välitön vaikutus on laitteiden sammuminen. Varavoimaratkaisulla maatilan sisäinen toiminta voidaan palauttaa, ja kriittisten tietolaitteiden suojaaminen UPS-järjestelmillä ja ylivirtasuojilla on perusteltua. Usein lyhyt sähkökatkos on vahingollisin laitteelle varsinkin silloin, kun laite ei ole vielä palautunut edellisestä katkoksesta. Varavoima ei ole juuri koskaan tiloilla online-tyyppistä vaan käynnistyy vasta sähköjen jo katkettua.

Yleisesti sähkökatkoksen venyminen yli 3-5h tunnin mittaiseksi katkaisee myös puhelin- ja tietoliikenteen alueella. Tähän katkokseen yksittäisen tilan on vaikea vaikuttaa. Olisi perusteltua että hajaasutusalueen matkapuhelinverkkoihin vaadittaisiin pidempää varavoiman kestoa ja mahdollisuutta syöttää virtaa myös paikallisesti tuotettuna.

Sähkökatkot vaikuttavat myös alueen vesihuoltoon. Vesi on merkittävä tekijä juomavetenä ja myös prosessien kannalta esimerkiksi maidontuotannon laitteiden pesussa. Vesiverkoston lamauttaminen kyberhyökkäyksellä vaikuttanee tehokkaimmin esim. maidontuotannon toimintaedellytyksiin. Esimerkiksi automaattilypsy ei voi toimia ilman painevettä.

Myös sää voi vaikuttaa sähkönjakeluun. Alkutuotannon omissa sääriskeissä yli/alijännitteet ovat keskeinen uhka. Salamaniskut tai syöttöjohtojen yhdistyminen voivat aiheuttaa IVT laitteiden rikkoontumisen.

9.2. Tietoliikenteen häiriöiden vaikutukset

Tietoliikenteen välitön katkos vaikuttaa ensin yleiseen viestintään. Pitempiaikainen kesto estää etähuoltoon, valvontaan, tilauksiin ja viranomaistoimintaan liittyvät toiminnot. Tietoliikenteen häiriöt tulevat esiin heti sähkönjakeluun liittyvien häiriöiden kanssa. Tietoliikenteen omat häiriöt voivat olla säähän, laiterikkoihin tai järjestelmiin tehtyjen iskujen seurauksia. Tietoliikennehäiriöt myös estävät pilvipalveluiden käyttämisen, mikä voi tulevaisuudessa olla yhä suurempi haitta maatilan toiminnalle.

9.3. Laitteiston rikkoutuminen ja datan korruptoituminen

Laiterikko tyypillisesti joko haittaa tai estää jonkin tilan järjestelmän toiminnan. Riippuen rikkoutuneesta laitteesta, haitta voi kohdistua mihin tahansa osaan tilaa, ja aiheuttaa myös datan menetyksiä. Myös datan keruu esimerkiksi eläinten tai peltojen jatkuvasta seurannasta voi häiriytyä. Laiterikot myös haittaavat tilan jokapäiväisiä toimintaprosesseja.

Data voi korruptoitua joko dataa kerättäessä, mikäli keruuseen käytetty laite ei toimi oikein, tai varastossa datavaraston rikkoutuessa tai joutuessa kyberhyökkäyksen kohteeksi. Mikäli kadonnut tai

korruptoitunut data on varmuuskopioitu, voidaan se palauttaa varmuuskopioista. Keruun aikana kadonnut tai korruptoitunut data on monesti sellaista, ettei sitä voida palauttaa. Tällöin, riippuen tilanteesta, voidaan data pyrkiä korvaamaan toisesta lähteestä saadulla tiedolla, arviolla, tai voidaan joutua toimimaan ilman dataa.

9.4. Poikkeusolot

Poikkeusolo on tilanne, jossa suuresta häiriötekijästä johtuen sovelletaan valmiuslakia. Poikkeusoloja ovat Suomeen kohdistuva aseellinen, taloudellinen, suuronnettomuuden, luonnononnettomuus tai laajalle levinneen vaarallisen tartuntataudin aiheuttama laajamittainen uhka.

Poikkeusoloissa viranomaisilla on tavallista suurempia valtuuksia, jotka voivat vaikuttaa myös maatilojen toimintaan joko suoraan tai välillisesti. Tällaisissa oloissa maatilan perustuotannon ylläpitäminen voi olla haastavaa, eikä normaaleja käytäntöjä voi välttämättä soveltaa. Olot voivat vaikuttaa myös tilan kybertoimintaympäristöön esimerkiksi siten, että kaikki normaalisti käytössä olevat verkkoresurssit eivät ole saatavilla. Voi myös olla tarve eristää tilan kriittiset järjestelmät ulkoisesta tietoverkosta.

Kriisitilanteissa yhteiskunnan toiminta ja käytössä oleva resurssit, mukaan lukien ruuan alkutuotanto, saattavat joutua tietyiltä osin viranomaisten suoraan ohjaukseen. Esimerkiksi merkittävä osa uusimmasta ajoneuvokalustosta voidaan tarvittaessa ottaa puolustusvoimien käyttöön. Tilanteessa on huolehdittava siitä, että traktorikalustoa jää riittävästi tiloille ruuan alkutuotannon turvaamiseksi. Varaosahuolto vaatii kriisiaikana myös huomiota. Sähköisesti ohjattujen laitteiden varaosien saatavuutta ja kohdistamista tarpeeseen tulisi myös varautumisessa selvittää.

On myös mahdollista, että maatilan koko kybertoimintaympäristö halvaantuu samalla kertaa. Tällaisen tapauksen voi aiheuttaa esimerkiksi laajamittainen elektromagneettinen pulssi, joka vaurioittaa puolijohdetekniikkaa sisältäviä laitteita. Tällainen ilmiö on erittäin epätodennäköinen, mutta sellaisen voi aiheuttaa esimerkiksi voimakas aurinkopurkaus tai yläilmakehässä tapahtuva ydinräjähdys.

10. Kyberuhilta suojautuminen

Selkeimmät yleispätevät ohjeet maatalouden kyberturvallisuuden parantamiseksi löytyvät Cooperilta (2015). Hän antaa kuusi suositusta maataloussektorin kyberturvallisuuden parantamiseksi:

1. Maataloussektorille tulisi luoda kyberturvallisuuskulttuuri
2. Sektorille tulisi saada enemmän kyberturvallisuuden asiantuntijoita
3. Kyberturvallisuuden arvioimiseksi tulisi kehittää menetelmiä
4. Maatalouden kyberturvallisuusstrategioita, suunnitelmia, ja toimitapoja tulisi kehittää
5. Tiedon varmuuskopiointi- ja palautusmenetelmiä tulisi kehittää ja testata
6. Maataloussektorin tulisi kehittää yhteistyötä muiden kriittisen infrastruktuurin sektoreiden kanssa

Ensimmäisen suosituksen mukaan koko toimialan tulee olla mukana kyberuhilta suojautumisessa. Uhkien hallitsemiseksi tarvitaan toimialan koulutusta ja tiedottamista, jotta toimialalle syntyy riittävän hyvä kyberturvallisuuskulttuuri, ja jotta hyvät turvallisuuskäytännöt saadaan käyttöön koko toimijaketjussa. Tässä työssä keskeinen asema on alan suurilla toimijoilla, joita viljelijät kuuntelevat, ja jotka saavat viljelijät mukaan työhön.

Toinen suositus vaatii myös työtä koko toimialalta. Yksittäisillä viljelijöillä ei ole resursseja kyberturvallisuusasiantuntijoiden hankkimiseksi. Täten, mikäli tätä suositusta halutaan seurata, resurssit on hankittava esimerkiksi keskusjärjestöjen tai neuvontajärjestöjen kautta. Järjestöillä on riittävästi resursseja ja rahaa, jotta alalle voitaisiin saada houkuteltua asiantuntijoita, jotka voisivat auttaa kyberturvallisuuden parantamisessa.

Kolmas, neljäs ja viides suositus ovat kaikki hyvin pitkälti riippuvaisia ensimmäisen kahden suosituksen toteutumisesta. Mikäli alalle saadaan riittävästi asiantuntijoita, on mahdollista kehittää menetelmiä, strategioita ja toimitapoja. Mikäli taas saadaan luotua alan kattava kyberturvallisuuskulttuuri, on mahdollista saada nämä menetelmät käyttöön maatilatasolle. Kuudes suositus on jälleen toimintaa, jota on tehtävä koko toimialan tasolla. Kriittisten sektoreiden yhteistyötä on Suomessa mahdollista kehittää esimerkiksi huoltovarmuuskeskuksen johdolla.

FBI (2016) antaa myös suosituksia kyberuhkia vastaan suojautumiselta, mutta nämä suositukset eivät ole läheskään yhtä yleisiä kuin Cooperin. Esimerkiksi ensimmäinen FBI:n suositus on seurata työntekijöiden kirjautumisia, erityisesti mikäli ne tapahtuvat työajan ulkopuolella. Tämä, kuten muutkin FBI:n suositukset olettavat selvästi, että maatilalla on ammattimainen tieturva, jolla on riittävästi resursseja verkkoliikenteen seuraamiseen. Tämä ei tyypillisesti pidä paikkaansa suomalaisella maatilalla.

Mahdollisia toimenpiteitä, mitä koko toimialan tasolla voitaisiin tehdä kyberturvallisuuden parantamiseksi on kerätty taulukkoon 1.

Taulukko 1. Toimenpide-ehdotukset kyberturavallisuuden kehittämiseksi.

Toimenpide	Toimenpiteen kuvaus	Huomioita toimenpiteen aloittamisesta
Kyberturvallisuuskulttuurin luonti	Maatalouden alkutuotannon toimijoiden tietoisuutta ja ymmärrystä kyberturvallisuudesta tulee lisätä, toimialan toimijoille tulee saada organisatorista ymmärrystä asian tärkeydestä	Jatkuva prosessi, joka tulisi aloittaa mahdollisimman pian
Kyberturvallisuuden koulutus viljelijöille	Viljelijöiden ammattitaidon kehittämiseen ja ylläpitoon tarkoitettuun koulutukseen tulee lisätä kyberturvallisuuden koulutusta	Mahdollisimman pian
Neuvontapalvelu kyberturvallisuudesta	Perustetaan ensisijaisesti viljelijöille suunnattu palvelu tai joukko palveluita, jotka antavat apua ja neuvoa kyberturvallisuusasioissa	Järkevää pystyttää kun koulutus on alkamassa
Maatilojen sähköturvallisuuden kehittäminen	Maatilojen sähköverkkojen kytkennät, varmistukset, yms. tulee kehittää siten, että tilat pystyvät jatkamaan toimintaa sähkönjakeluhäiriöiden aikana	Mahdollisimman pian
Maatilojen tietoturvan kehittäminen	Maatilojen tietoverkot ja niissä kiinni olevat laitteet tulee suojata haittaohjelmia vastaan	Kyberturvallisuuskoulutuksen jälkeen
Tulevat maatalouden järjestelmät tulee kehittää kyberturvallisiksi	Maatalouden ohjelmisto- ja laitevalmistajien kanssa tulee kehittää ohjelmistoja ja laitteita kyberturvallisiksi. Vaatii huomattavasti toimialan sisäistä turvallisuuskulttuurin kehittymistä, jotta valmistajille saadaan riittävä paine	Järkevää aloittaa, kun kyberturvallisuuskulttuurin luonti on saatu hyvään alkuun
Kyberturvallisuuden ylläpito osaksi tilan ylläpitoa	Sähköisten järjestelmien huolto tulisi saada osaksi tilan normaalia huoltosykliä	Valistus tehtävä koulutuksen yhteydessä – tukea annettava neuvontapalvelussa
Järjestelmällinen varmuuskopiointi	Tilojen tietojärjestelmistä tulisi ottaa säännöllisesti varmuuskopioita, joiden palauttaminen tulisi olla myös varmistettua	Valistus tehtävä koulutuksen yhteydessä

Kyberturvallisuuskulttuurin kehittämiseksi on mahdollista tehdä lukuisia eri toimenpiteitä. Tärkein käytännön toimenpide voisi olla kyberturvallisuuden perusteiden opetuksen sisällyttäminen osaksi maanviljelijöille tarjottavaa koulutusta siten, että se sulautuisi luonnolliseksi osaksi viljelijän ammattitaidon opetusta. Turvallisuuskoulutus sopisi esimerkiksi maatilan hallinnon koulutuskokonaisuuteen. Koulutuksen tarkoituksena olisi ennen kaikkea lisätä viljelijöiden tietoisuutta siitä, että kyberturvallisuus on aihe, jonka tärkeys on koko ajan kasvamassa. Mitä enemmän tilalla on moderneja, erityisesti verkkoon yhteydessä olevia laitteita, sitä tärkeämpää on huolehtia tilan kyberturvallisuudesta. Tietoisuuden lisäksi koulutuksessa olisi tärkeää myös iskostaa viljelijöiden päähän ajatus siitä, että kyberturvallisuuteen on mahdollista saada apua ja neuvoja, eikä viljelijän ole pakko pähkäillä asiaa yksin.

Viestintäviraston kyberturvallisuuskeskus on Suomen tärkein julkinen toimija yleisessä kyberturvallisuusvalmiuden ylläpitämisessä sekä tietoisuuden levittämisessä ja ylläpidossa. Toimialan tulisi pyrkiä hyödyntämään keskuksen asiantuntemusta ja valmiutta, sekä erityisesti palveluita, joita keskus tarjoaa pien- ja mikroyrityksille. Erityisesti, mikäli kyberturvallisuuskeskus parantaa pienille yrityksille tarjoamiaan palveluita tulevaisuudessa, on toimialan syytä vaalia yhteyksiä.

Tärkeää on myös käytössä olevien ja jatkossa kehitettävien järjestelmien kyberturvallisuus. Ohjelmistot, laitteet ja niistä muodostuvat järjestelmät tulisi alusta pitäen rakentaa siten, että ne tukevat kyberturvallista toimintaa. Tässä asiassa vastuu on ennen kaikkea laitevalmistajilla ja ohjelmistotuottajilla, mutta asiakkaiden on myös osattava vaatia näitä ominaisuuksia tuotteilta ja palveluilta. Tätäkin asiaa voidaan edistää tietoisuutta kasvattamalla ja kouluttamalla viljelijöitä.

Maatilan kyberturvallisuuteen kuuluu kuitenkin paljon muutakin kuin tietojärjestelmien turvaaminen haittaohjelmilta ja hyökkääjiltä. Maatilojen ottaessa käyttöön yhä enemmän automatiikkaa ja tietojärjestelmiä korostuu myös maatilan sähköverkon ja tietoliikenneyhteyksien kestävyys. Maatilojen on kyettävä jatkamaan toimintaansa myös sähkönjakeluhäiriöiden tai tietoliikennehäiriöiden aikana. Automaatiojärjestelmien suojaamisen ja toimivuuden kannalta on myös tärkeää, että maatilan käyttämä sähkö on riittävän tasalaatuista. Jännitepiikit voivat rikkoa laitteita, ja liian huonolaatuinen sähkö voi sotkea tietokoneiden ja automaatiojärjestelmien toimintaa. Täten on tärkeää huolehtia, että tiloilla on mahdollista saada käyttöön hyvälaatuista sähköä myös poikkeustilanteissa.

10.1. Käytännön toimia maatilalla

Vahingoilta ja onnettomuuksilta suojautuminen tapahtuu ensisijaisesti hyviä ja turvallisia työtapoja noudattamalla. Tilan ulkopuolisilta ilmiöiltä tai onnettomuuksilta suojautuminen vaatii varautumista. Sähköjakeluhäiriöitä vastaan voi suojautua ylijännitesuojilla sekä varavoimalla, ja lialta voi suojautua sopivilla laitevalinnoilla, laitteiden oikealla asentamisella ja säännöllisellä siivoamisella. Lämpötilan ja kosteuden vaihteluiden aiheuttamilta ongelmilta voi suojautua sopivilla laitevalinnoilla ja asentamalla laitteet sopiviin paikkoihin. Eläinvahingoilta suojautuminen vaatii järjestelmän rakentamista alun perin sellaiseksi, että eläinten on vaikea sitä vahingoittaa. Esimerkiksi johdotukset tulisi tehdä siten, etteivät eläimet pääse niihin kiinni.

Verkkoyhteyksien katkeamiselta voidaan suojautua varayhteyksien avulla. Esimerkiksi älypuhelimia voidaan nykyään käyttää liikkuvina internet-tukiasemina. Tällöin maatilan ensisijaisen verkkoyhteyden katketessa voidaan yhteys muodostaa älypuhelimen kautta.

Varsinaisia kyberhyökkäyksiä vastaan tulee myös varautua etukäteen. Tärkein varautumiskeino on kaikkien laitteiden kaikkien ohjelmistojen pitäminen ajan tasalla, sekä tietoturvaohjelmien käyttäminen kaikissa tärkeissä laitteissa, joihin sellainen on mahdollista asentaa. Laitteiden ajan tasalla pitäminen ei rajoitu pelkästään tietokoneisiin, vaan myös kaikki muutkin laitteet, kuten reitittimet, automaatiojärjestelmät, älypuhelimet ja muut tulee pitää päivitettyinä.

Toinen yhtä tärkeä varautumiskeino on ottaa kaikesta tärkeästä tiedosta säännöllisiä varmuuskopioita. Tämän lisäksi tilalla tulee olla selkeät käytännöt miten kopiot otetaan ja miten tiedot palautetaan tarvittaessa.

Maatilan tietoverkko tulee rakentaa siten, että mahdollisimman suuri osa siitä ei näy sisäverkon ulkopuolelle. Mikäli verkkopalvelun tarjoajan antamassa päätelaitteessa on palomuuri, tulee palomuuri asentaa mahdollisimman suojaavaksi. Vain ne laitteet ja palvelut, joiden täytyy näkyä internetiin toimiakseen, näkyvät sisäverkon ulkopuolelle. Mahdollisesti haavoittuvia sulautettuja laitteita, varsinkin sellaisia joita on vaikeaa päivittää, tulee välttää. Mikäli niitä täytyy käyttää, tulee ne asentaa siten, etteivät ne näy tilan sisäverkon ulkopuolelle.

Mobiiliverkkoon kiinnitetyt laitteet tulee myös pitää ajan tasalla, jotta niitä ei voida väärinkäyttää. Väärinkäyttöä, ja ennen kaikkea väärinkäytöstä koituvia kuluja, voidaan myös estää tiedonsiirtokatoilla ja kieltämällä puheluiden soittaminen liittymällä. Tällöin tosin maatilan oma tiedonsiirto voi häiriytyä, mikäli mobiililiittymän tiedonsiirtokatto tulee vastaan.

Maatilan tietoturvatason seuraaminen ei ole toiminto, jota viljelijä kykenee noin vain jatkuvasti tekemään. Täten olisi hyvä, että viljelijöillä olisi käytössään esimerkiksi muistilista, jonka avulla käydä läpi tilan kyberturvallisuuden ydinasiat. Lista toimisi muistin tukena, ja sen avulla voitaisiin varmistua, että viljelijällä olisi työväline, jonka avulla ylläpitää kyberturvallisuutta. Etelä-Savon ammattiopiston opettaja Jorma Flinkman on laatinut tällaisen muistilistan. Lista on liitetty raporttiin Flinkmanin suostumuksella liitteenä A.

11. Yhteenveto

Maatalouden kyberuhkat ovat yleisesti hyvin samankaltaisia kuin muussakin yhteiskunnassa jos tarkastellaan viestintää ja tietokoneiden käyttöä. Toimialan tyypilliset uhat liittyvät laitteiston vanhenemiseen ja päivitysten laiminlyöntiin. Myös järjestelmien kokonaissuunnittelun puuttuminen voi aiheuttaa tarpeettomia uhkatilanteita. Laitteistojen pitkät elinkaaret aiheuttavat jatkossa entistä suurempia haasteita niiden turvalliseen ylläpitoon. Voidaan odottaa että esim. Navetan n. 30 vuoden elinkaaren aikana tietojärjestelmät tullaan uusimaan 4-6 kertaan. Tämä uusiminen voi tapahtua liukuvasti aiheuttaen yhteensopimattomuuksia ja tieturvaheikkouksia. Sama ongelma on jatkossa myös ajoneuvoissa. Maatalouden erikoisajoneuvojen, kuten traktorien, leikkuupuimurien, ja kurottajien, tyypillinen elinkaari on ollut useita vuosikymmeniä. Nyt käyttöön tulevat ajoneuvot sisältävät melkein poikkeuksetta CAN -väylään perustuvan ohjausratkaisun, johon tullaan myöhemmin lisäämään työkoneitten ja etämittauslaitteiden tiedonsiirtoa. Tämä avaa reitin alun perin suojaamattomiin väyläratkaisuihin, ja on merkittävä kyberuhka tulevaisuudessa, jos ratkaisuja ei suojata asianmukaisesti. Väylään perustuvat ratkaisut ovat kuitenkin merkittävässä osassa tehostettaessa traktorien ja työkoneiden tuottavuutta. Tämä tuottavuuslisäystä ei pidä estää ja hidastaa huonolla tietoturvalla vaan ratkaisut on aina tehtävä turvallisuus huomioiden. Tietoturva on keskeinen osa laitteiden käyttöturvallisuutta.

Henkilökohtaisten tietokoneiden ja älypuhelinten turvallisuudessa on noudattava yleisiä tietoturvakäytäntöjä. Alan tiedotusvälineissä tulisi huomioida alkutuotannon toimialalla toimivat siten, että uutisiin nostettaisiin ne tietoturvaan liittyvät ohjeet joita noudattamalla päästään parempaan tietoturvallisuuteen.

Alkutuotanto voi olla kohteena tilanteessa missä kyberhyökkäyksellä on tarkoituksena lamaannuttaa yhteiskunnan keskeisiä toimintoja. Alkutuotannon pieni yksikkökoko ja hajautettu tuotanto tekee kuitenkin hyökkäyksen tehokkaan toteuttamisen haastavaksi. Yksittäisten laiteperheiden kautta toteutettu hyökkäys voi kuitenkin aiheuttaa vakavan häiriön toimialalle. Hyökkäys yksittäistä tilaa vastaan voi kuitenkin aiheuttaa tilan taloudelle merkittävää vahinkoa.

Viitteet

Bunge, Jacob (2015): Agriculture Giants Boost Cybersecurity to Shield Farm Data. The Wall Street Journal, helmikuu 2015. http://www.wsj.com/articles/agriculture-giants-boost-cybersecurity-to-shield-farm-data-1424380098

Cooper, Christina (2015): Cybersecurity in Food and Agriculture. Kirjassa Protecting Our Future, Volume 2: Educating a Cybersecurity Work Force.

FBI (2016): Smart Farming May Increase Cyber Targeting Against US Food and Agriculture Sector. Private Industry Notification, PIN 160331-001.

Flinkman Jorma, Esedu, puhelinkeskustelu 16.3.2017

Heinänen Petteri Aidon Oy, Puhelinkeskustelu 20.1.2017

Hilton, Scott (2016): Dyn Analysis Summary of Friday, October 21 Attack. Company News, Dyn. http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

Kaarlonen Jussi, Valtra Oy, Puhelinkeskustelu 12.1.2017

Kauhanen Jari, MTK Pohjois-Savo ry, Puhelinkeskustelu 15.3.2017

Kauppinen Kimmo, Kaisanet Oy, Puhelinkeskustelu 13.1.2017

Lehto, Martti, Limnell, Jarno, Innola, Eeva, Pöyhönen, Jouni, Rusi, Tarja, ja Salminen, Mirva (2017): Suomen kyberturvallisuuden nykytila, tavoitetila, ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017

Manning, Lauren (2016): What is the Cybersecurity Threat in Agriculture. Agfunder News, https://agfundernews.com/what-is-the-cybersecurity-threat-in-agriculture.html

SFS-EN 60529 (IEC 60529) standardi.

Tikkanen Tuomo Viljelijä, Puhelinkeskustelu 12.1.2017

Valtioneuvosto (2013): Suomen kyberturvallisuusstrategia. Saatavilla http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit

Viool, Vincent, van Zuidam, Evelien, Poppe, Krijn ja Bogaardt, Marc-Jeroen (2016): Cybersecurity in the Agrofood sector. Capgemini Consulting.

Zorz, Zeljika (2016): FBI warns farming industry about equipment hacks, data breaches. Helpnet Security, https://www.helpnetsecurity.com/2016/04/21/farming-cyber-risks/

Maatilan tietoturvakartoitus

Tilan nimi	

Päiväys	

		Rastita nykytilanne (X)			
		Tilanne			
Nro	Tarkastuskohta	ON Kunnossa	EI OLE Kunnossa	EI KOSKE tilaa	Mahdolliset toimenpiteet
1	Laitteet on suojattu salasanalla, pin koodilla tms.				
2	Laitteiden huolto on systemaattista				
3	Laitteita uusitaan säännöllisesti / tarvittaessa				
4	Mobiililaitteiden tiedot varmuuskopioidaan myös				
5	Ohjelmien asennus tietokoneelle on hallittua				
6	Ohjelmistopäivitykset ovat ajan tasalla				
7	Tietokoneen eri käyttäjillä on omat profiilit / tunnukset				
8	Tietokoneiden käyttötila on suojattu pölyltä ja kosteudelta				
9	Tietokoneissa on virus ja haittaohjelmasuojaus				
10	Varmuuskopiointi on säännöllistä				
11	Varmuuskopiot säilytetään turvallisessa paikassa				
12	Käyttäjille on luotu tarvittavat ohjeet tietoturvaan				
13	Käyttäjillä on omat salasanat				
14	Tietokoneen ja ohjelmien käyttöön on saatu koulutusta (on osaamista)				
15	Puhelimen käytön ja jutustelun vaarat tunnetaan				
16	Tietototurvalla on nimetty vastuuhenkilö				
17	Tärkeät paperit on luokiteltu ja palosuojattu				
18	Vieraat ohjataan ja ohjeistetaan asianmukaisesti				
19	Ulkopuoliset tietojen käyttäjät on tunnistettu				
20	Ulkopuoliset tietojen käyttäjät ovat luotettavia				
21	Henkilötietoja käsitellään asianmukaisesti				

		Rastita nykytilanne (X)			
		Tilanne			
Nro	Tarkastuskohta	ON Kunnossa	EI OLE Kunnossa	EI KOSKE tilaa	Mahdolliset toimenpiteet
22	Ongelmatielanteissa saadaan apua nopeasti				
23	Kulunvalvonnasta on huolehdittu				
24	Puhelimen ja tabletin tietoturva on huomioitu				
25	Salasanat ym. tiedot (mm. tunnuslukulistat) säilytetään oikein				
26	Sähkökatkoihin on varaudutte UPS laitteilla				
27	Tiedot ja tietokoneet ovat lukitussa tilassa				
28	Tietoliikenne on turvattu häiriöiden varalta				
29	Tietoturvauhat on kartoitettu / tunnistettu				
30	Vanhentuneet tiedot (myös paperit) tuhotaan asianmukaisesti				
31	Käytämme luotettavia pilvipalveluita				
32	Tietotekniset laitteet on luetteloitu				
33					
34					
35					
36					
37					
38					
39					
40					
	Rastit yhteensä				

Tarkastuksen teki _____

Seuraavan tarkastuksen ajankohta _____

Luonnonvarakeskus
Latokartanonkaari 9
00790 Helsinki
puh. 029 532 6000