KYBERIN TASKUTIETO MAATILOILLE

TYÖRYHMÄ
Markus Lassheikki
Juha Niemi
Jussi Nikander
Mikko Laajalahti
Kalle Luukkainen
Panu Moilanen
Juha Mantila
Ossi Hietala
Jarkko Ilomäki
Juha Nuutila
Tuomo Tikkanen
Jussi-Pekka Kotilainen

KUVITUS
Linda Saukko-Rauta
Redanredan Oy

TAITTO
Ossi Hietala

JULKAISIJAT
Jyväskylän yliopisto ja
Maanpuolustuskoulutus-
yhdistys 2018

PAINO
Sata-Seri, Rauma

ISBN
978-951-39-7639-2
(painettu)
978-951-39-7640-8
(verkkojulkaisu)

MAHDOLLISTAJAT
Huoltovarmuusorganisaatio
ICT-Suomi ry
Maatalouskoneiden tutkimussäätiö

CREATIVE COMMONS -LISENSSI
Tämä opas on julkaistu
CC BY-NC-ND 4.0 -lisenssillä.

MIKSI MAATILOILLA TARVITAAN KYBERTURVALLISUUTTA?

Kybermaailma on tullut myös maatiloille. Maatilat ovat entistä enemmän teknistyneet ja digitalisoituneet.

Maatilojen tietojärjestelmät ovat elimellinen osa maatilojen toimintaa. Ilman tietojärjestelmiä maatilat eivät toimi. Eläinten hyvinvointi on riippuvainen toimivista laitteista. Ilman niitä ilmastointi ei toimi, ruokinta ei onnistu, vedensaanti voi vaarantua ja lypsäminenkään ei onnistu. Laitteet sisältävät tietotekniikkaa ja ovat yhteydessä tietojärjestelmiin internetin kautta. Tämä altistaa myös maatilat kybermaailman uhkille.

Maatiloilla syntyy paljon arvokasta tietoa. Tieto on talennettava turvallisesti. Tiedon säilyminen on varmistettava ja asiattomien pääsy tietoon ja tiedon väärinkäyttö on estettävä.

Maatilojen hankinnat ovat usein pitkäaikaisia. Laiteiden ja järjestelmien toimivuus, yhteensopivuus ja tietoturva kannattaa tarkistaa jo ostovaiheessa.

Maatilojen tuotanto on tärkeää Suomen huoltovarmuudelle.

Tämän oppaan tarkoitus on antaa sinulle käytännön tietoa ja vinkkejä, jotta pystyt paremmin huomioimaan kybermaailman haasteet ja mahdollisuudet maatilasi arjessa.

Tämän oppaan lisäksi sinun kannattaa tutustua Maanpuolustuskoulutusyhdistyksen (MPK) ja Jyväskylän yliopiston julkaisemaan KYBERIN TASKUTIETO: KESKEISIN KYBERMAAILMASTA JOKAISELLE -oppaaseen.

KYBER- JA INFORMAATIORISKEJÄ MAATILOILLA

Kyberriskienhallinta alkaa riskien tiedostamisesta. Maatiloihin useimmin vaikuttavat kyberuhat ovat säätilojen aiheuttamat häiriöt ja tilan henkilöstön tekemät virheet.

Myrskyjen aiheuttamat sähkökatkot sammuttavat laitteita, jolloin tilan tietojärjestelmät on osattava käynnistää uudelleen. Ukkonen ja vesivahingot taas voivat rikkoa laitteita. Laiterikkoja voi tulla myös muista syistä, esimerkiksi jyrsijt voivat aiheuttaa yllättävääkin vahinkoa.

Käyttäjille sattuu myös vahinkoja, jotka varsinkin huonosti suunnitellussa kyberjärjestelmässä voivat aiheuttaa suuriakin ongelmia. Aina kun tietojärjestelmiin tekee muutoksia, on syytä tietää mitä tekee, jottei epähuomiossa aiheuta itselleen ongelmia. Varovaisuutta kannattaa käyttää myös silloin, kun pyytää tai

palkkaa apua tietojärjestelmien kanssa. Yhteistyötahon tulee olla asiansa osaava ja tuntea tilan kyberympäristö. Asiantuntijakin voi tehdä helposti virheitä tuntemattomassa ympäristössä.

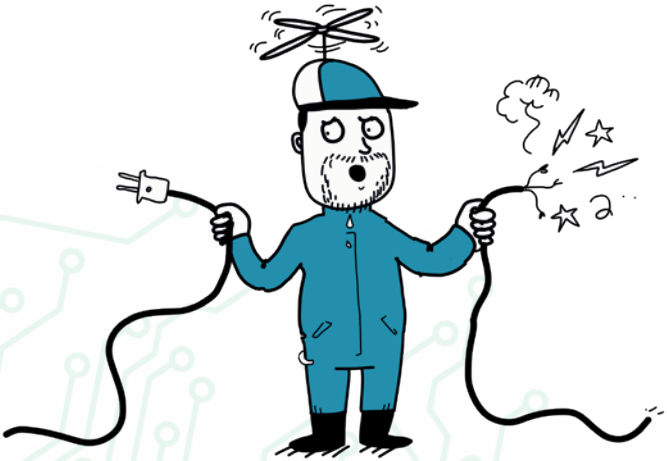
Maatilaan voi myös kohdistua erilaisia kyberhyökkäyksiä. Usein tila itsessään ei ole hyökkäyksen kohde, vaan esimerkiksi haittaohjelma pääsee sattumalta tunkeutumaan riittämättömästi suojattuihin tilan tietojärjestelmiin. Hyökkäys voi tietenkin olla suunnattu myös tilaa vastaan. Esimerkiksi eläinsuojiin asennettujen valvontakameroiden kuvat voivat kiinnostaa ulkopuolisiakin.

On myös syytä miettiä, mitä kaikkea itse kertoo maatilasta sosiaalisessa mediassa. Asioita on helppo erottaa asiayhteydestä, ja erityisesti mielipitetä jakavissa aiheissa itse julkaistujakin valokuvia voidaan yrittää käyttää myös tilaa vastaan.

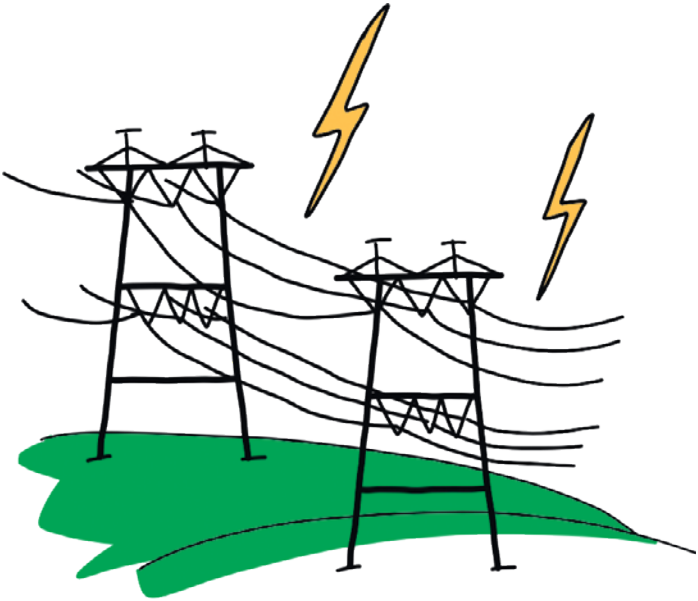
SÄHKÖN SAANTI JA SÄHKÖTURVALLISUUS: KAIKKI RIIPPUU SÄHKÖSTÄ!

Kyberlaitteet tarvitsevat sähköä toimiakseen, ja toimiakseen luotettavasti ne vaativat laadukasta sähköä. Maaseutualueella sähkökatkot ja jännitteenvaihtelut vaativat huomiota. Laitteita voidaan suojata välittömiltä sähkökatkoilta ja ylijännitteiltä varavirta- eli UPS-laitteilla. Ylijännitesuoja pitää rakentaa sähköverkkoon monivaiheiseksi, jotta saavutetaan riittävä suojaustaso. Sähköturvallisuusmääräykset antavat hyvän perustan myös kyberturvalliselle toiminnalle. Tietoverkkojen kannalta keskeistä on kaapelointi ja laitetilojen maadoittaminen samaan potentiaalitasoon muun laitteiston kanssa. Sähköturvallisuustarkastuksessa on hyvä kiinnittää huomiota myös tietoverkon kuntoon.

Varavoimaratkaisu pitää mitoittaa tuotannon ja olosuhteiden



tarpeiden mukaiseksi. Polttomoottorikäyttöinen varavoimalaite tarjoaa riittävän tehon. Jatkuvassa käytössä polttoaineen tarve on kuitenkin merkittävä. Varavoimaratkaisun mitoituksessa kannattaa tavoitella riittävää tehoa ja rajoittaa käyttöaikaa polttoaineen kulutuksen minimoimiseksi. Tämä tarkoittaa sitä, että kun varavoima on päällä voidaan kaikkia tarvittavia kulutuskohteita käyttää. Esimerkiksi lypsyaikaan on maito saatava jäähtymään, tarvittava pesuvesi lämpiämään ja laitteiden akut varautumaan. Varavoimaa on saatava kyberlaitteiden kaikkiin käyttöpisteisiin.



TIETOLIIKENNE JA TIETOVERKOT

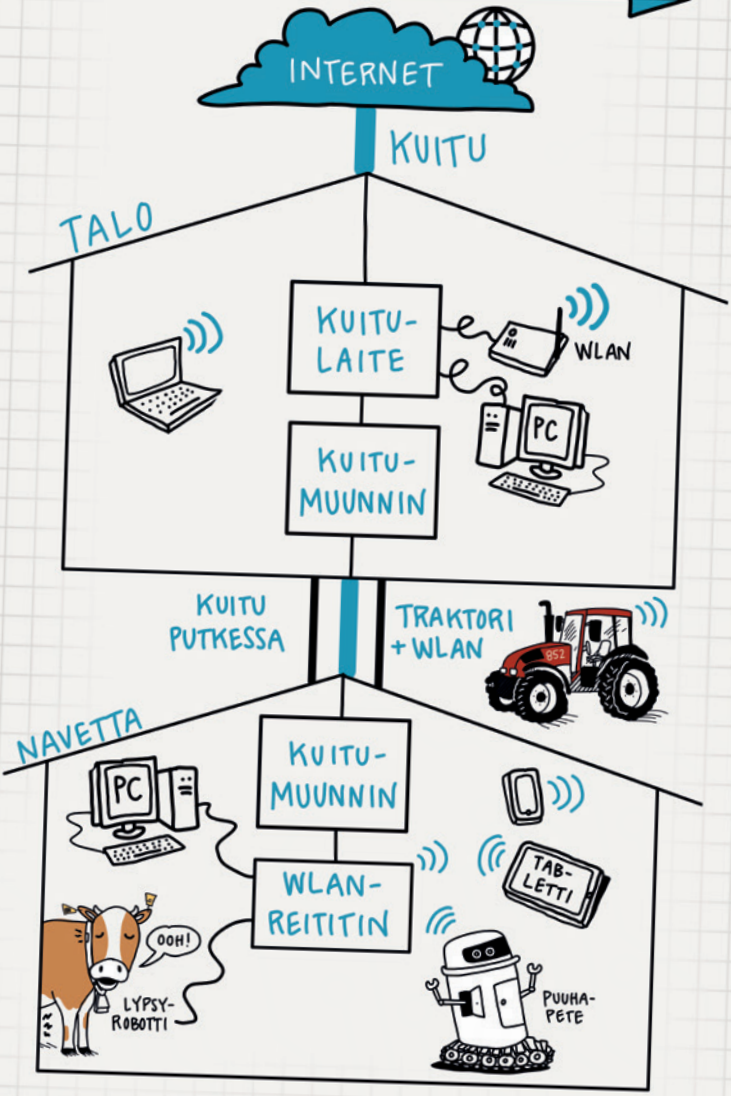
Maatilan tietoverkon suunnittelussa on kiinnitettävä huomiota verkon saavutettavuuteen. Asuinrakennuksen verkon suunnittelulle annetaan tarkat ohjeet rakennusmääräyksissä. Keskeinen asia on yleiskaapelointi kaikkiin asuinhuoneisiin. Samaa ohjetta voi noudattaa tuotantorakennuksissa; verkkoliitäntöjä on oltava kattavasti niissä tiloissa, joihin laitteita ollaan sijoittamassa. Rakennusten väliin kannattaa sijoittaa riittävän iso putkitus (110 mm) myöhempiä tarpeita varten erikseen tietoliikennettä ja käyttösähköä varten. Yli 100 m matkalle tarvitaan kuparikaapeliin vahvistin. Suositeltavaa on käyttää valokuitua rakennusten välisiin vetoihin.

Verkon rakenne kannattaa dokumentoida. Uusrakentamisessa dokumentti syntyy sähkösuunnitelman osana. Koko maatilan tietoverkon voi dokumentoida yksinkertaisella piirroksella, jossa laitteet ovat laatikoita ja niiden väliset johdot viivoina laatikoiden välillä. Tämä kuva auttaa yleensä ratkaisemaan verkossa olevia ongelmia, kun tiedetään miten laitteet sijoittuvat verkossa.

Maatilan verkko koostuu lähiverkosta, joka voi olla langallinen (LAN) tai langaton (WLAN). Se voi olla yhteydessä internetiin joko mobiiliyhteydellä (2G, 3G, 4G, 5G) tai kiinteällä yhteydellä, jonka voi toteuttaa usealla eri tavalla. Laitteissa, koneissa ja ajoneuvoissa on sisäisiä verkkoja, esim. CAN- ja ISOBUS-väyliä, jotka myös voivat liikennöidä ulkoisiin verkkoihin ja palveluihin.

Maatilan verkon rakenteeseen tulisi sisällyttää palomuuriratkaisuja. Palomuuri on erillinen verkon laite tai tietokoneessa oleva ohjelmisto, jolla hallitaan niin tietokoneiden kun verkkojen välistä liikennettä. Kun siirretään tietoa tietokoneelta toiselle kaikkiin palomuureihin on määriteltävä yhteydet tietojen siirtämiseksi. Myös nämä yhteydet on suojattava huolellisesti.

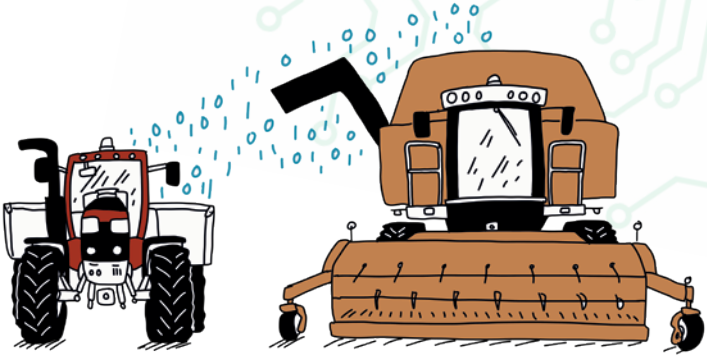
MAATILAN TIETOVERKKOKARTTA 11/2018



TILAN SISÄISET JA ULKOISET JÄRJESTELMÄT

Maatila tuottaa paljon tietoa, josta myös ulkopuoliset ovat kiinnostuneita. Kerättävää tietoa käytetään tuotannon ohjaukseen ja tuotteiden kaupalliseen sertifiointiin. Hankittaessa järjestelmiä pitää huolehtia siitä, että tietojen omistus- ja käyttöoikeudesta on sovittu kaikkien osapuolien oikeuksia kunnioittaen. Maatilan pitää päästä omistamaansa tietoon tarkoituksenmukaisilla välineillä. Yrittäjän on myös oltava tietoinen siitä, mihin tietoja edelleen käytetään. Maatilalla syntynyt tieto voi olla luottamuksellista, ja se voi olla myös EU:n tietosuoja-asetuksen eli GDPR:n tarkoittamaa tietoa, jota tulee osata käsitellä oikein.

Tietokone on jo pitkään ollut peruslaite verkossa, mutta useiden sovellusten päivittäinen käyttö on siirtymässä älypuhelimiin ja muihin mobiililaitteisiin. Älypuhelimen käytössä on huomioitava tapa, jolla se liittyy tilan tilan sisäverkkoon ja tietokoneisiin, joko tilan verkkoliittymän tai paikallisen langattoman verkon kautta.



Maatilan verkkoliittymä on usein ominaisuuksiltaan vastaava kuin kuluttajaliittymä. Siinä operaattori on huolehtinut tietyistä perustietoturvaratkaisuista. Kun liittymään tarvitaan ohjata ulkopuolelta tulevaa liikennettä, kuten valvontakameroita tai älypuhelimella suoritettavaa etäohjausta, joudutaan liittymää avaamaan. Yleensä operaattori siirtää vastuuta silloin liittymän haltijalle. Liittymään tarvitaan tarkoituksenmukainen palomuuri suojaamaan liikennettä.

Nykyaikainen maataloustraktori CAN-väyläohjauksella ja ISOBUS-varustuksella on hyvinkin itsenäinen tietolaite. Traktori mittaa ja kerää tietoa toimintaansa varten. Lisäksi valmistajat keräävät tietoja tuotekehitykseen ja traktorin ylläpitoon liittyviin tarkoituksiin. Valmistajat suunnittelevat laitteet lähtökohtaisesti turvallisiksi. Traktorin väylään liittyvät laitteet voivat kuitenkin vaikuttaa ohjaukseen. Näissä laitteissa on aina huomioitava mahdollinen turvallisuusriski. ISOBUS-väylä on tarkoitettu traktorin ulkopuolisten laitteiden liittämiseen turvallisesti.

Rakennusautomaatiolla ohjataan ilmastointia, valaistusta ja muita laitteita. Automaatio liittyy verkkoihin yleensä etävalvonnan ja ohjauksen tarpeista. Tämän automaation verkkoliitynnän yhteyden turvallisuus tulee muistaa varmistaa.

Kyber- ja informaatio-riskejä maatiloilla 4

Sähkön saanti ja sähköturvallisuus 6

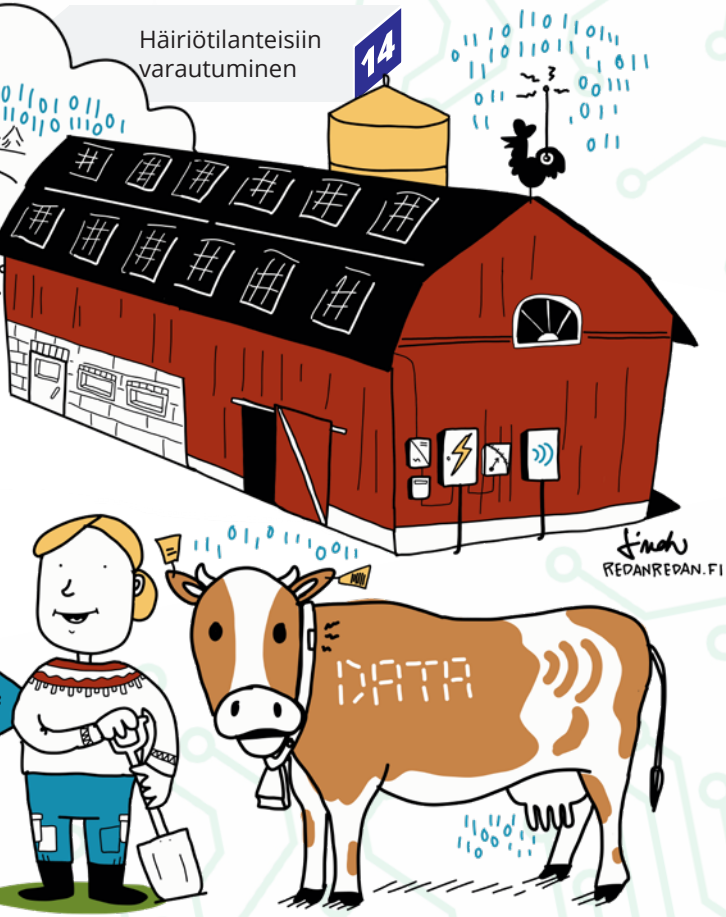
Turvallinen tunnistautuminen ja hyvät salasanat 16

Tiedon varmentaminen tuo turvallisuutta 1

Tietoliikenne ja tietoverkot 8

Tilan sisäiset ja ulkoiset järjestelmät 10

Häiriötilanteisiin varautuminen 14



8

Ovatko hankintasi kyberturvallisia? 20

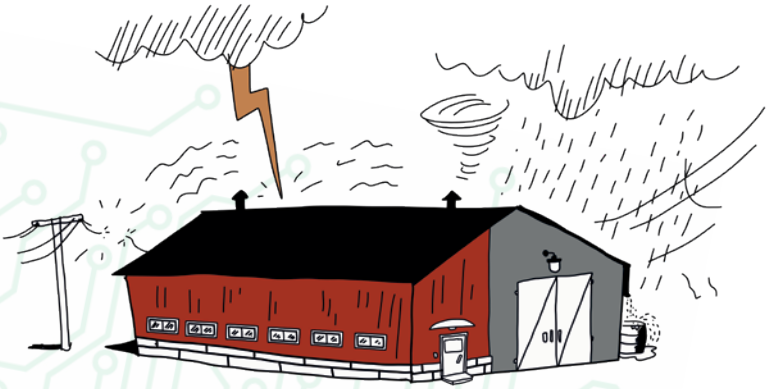
Päivittäminen on paras turva 22

MITEN VARAUTUA ERILAISIIN HÄIRIÖIHIN?

Tietojärjestelmien häiriöt ovat vähintäänkin harmittavia. Niistä voi myös aiheutua isoja taloudellisia menetyksiä tai vaaratilanteita. Häiriöstä riippuen vaikutukset tuntuvat maatilalla joko heti tai vasta jonkin ajan kuluttua. Monipuolinen varautuminen parantaa tilan kriisinsietokykyä ja häiriötilanteesta palautumista.

Häiriötilanteen alkaessa sen ajallinen kesto, maantieteellinen laajuus ja alkusyy ovat harvoin tiedossa. Tämä lisää epävarmuuden tunnetta. Häiriöiden aiheuttamaa henkistä rasitusta voi vähentää pohtimalla ja varautumalla etukäteen, miten kustakin tilanteesta selviää. Laadi esimerkiksi yksityiskohtaiset tarkistuslistat erilaisten häiriötilanteiden varalle.

Sähkönjakelun häiriö näkyy välittömästi laitteiden sammumisena. Sähkökatkot ovat tyypillisimmin lyhyitä räpsyjä, mutta ne voivat kestää tunteja, päiviä ja pisimmillään jopa viikkoja. Äkilliset virtapiikit voivat rikkoa laitteita. Lisäksi sähkökatkoilla on välillisiä vaikutuksia, esim. mistä eläimet ja laitteet saavat vettä pitkitty-



neessä häiriötilanteessa.

Sähkölinjojen vierimetsien hoidolla, varavoimakoneella ja varavirtalähteillä/akuilla on mahdollista torjua sähkökatkon aiheuttamia vaikutuksia. Pitkien sähkökatkojen varalta kannatta sopia etukäteen öljy-yhtiön kanssa polttoaineen tilaus- ja toimitusmenettelystä tilatankkiin. Hanki herkkien tietoteknisten laitteiden suojaksi UPS-laite. Sen tehtävä on taata tasainen virransyöttö lyhyissä katkoksissa ja syöttöjännitteen epätasaisuuksissa.

Jo 3-5 tunnin mittainen sähkökatko katkaisee myös tieto- ja puhelinliikenteen mobiiliverkossa. Tällöin laitteiden etähuolto, tilaukset ja sähköiset viranomaisilmoitukset eivät toimi. Kiinteä liittymä on mobiiliverkkoa toimintavarmempi sähkökatkossa. Paikallisesti toimivaa tietojärjestelmää on mahdollista käyttää silloinkin, kun pilvipalveluiden varassa olevat järjestelmät ja tietokannat eivät ole käytettävissä.

Sopimuksia tehtäessä on tärkeää ottaa huomioon, että sähkö- ja tietoliikennekatkot saattavat vaikuttaa myös tilan ulkopuolisten kumppaneiden ja palveluiden tuottajien toimintaan.

TURVALLINEN TUNNISTAUTUMINEN JA HYVÄT SALASANAT

Maatilalla yhteisessä käytössä oleville tietokoneille tulee luoda jokaiselle käyttäjälle oma käyttäjätunnus, salasana sekä perustaa tarvittavat oikeudet eri ohjelmiin ja palveluihin. Ohjelmien asentamista, huoltoja ja käyttäjätilien luontia varten tulee olla erillinen järjestelmänvalvojan tai pääkäyttäjän tili, jota ei käytetä muuhun tarkoitukseen. Tällä tilillä tulee olla erityisen vahva salasana.

Korkean suojaustarpeen palveluissa, kuten sähköpostissa, pilvipalveluissa ja eläinrekisterissä, tulee käyttää vahvoja salasanoja. Vahvat salasanat ovat yli 15 merkin pituisia lause- kirjain-, ja numeroyhdistelmiä. Omasta näkymästä löytyy hyviä salasanoja: esimerkiksi **PunainenValtraTalonEdessä_852** on jo vahva verkkosalasana. Salasanan pituus on pääasiallinen turvallisuutta lisäävä tekijä. Lyhyemmän salasanan voi tarvittaessa luoda katkaisemalla sanoja: **PuVaTaEd_852**.

Tärkeimmät salasanojen ja kirjautumisten turvallisuutta lisäävät käytännöt ovat henkilökohtaiset ja palvelukohtaiset salasanat, riittävän pitkät salasanat ja kaksivaiheinen tunnistus , kuten pankkitunnus ja mobiilivarmennus.

Tärkein salasanojen tietoturvakäytäntö on kuitenkin käyttäjä itse. Älä asenna mitään tuntematonta sovellusta. Salasanoja ei saa tallentaa koneen muistiin. Älä anna henkilökohtaista salasanaasi kenellekään.

Sähköpostiosoite on avain pääsylle moniin palveluihin, ja sen avulla on mahdollista vaihtaa ja varmentaa uusi salasana. Sähköpostissa tulee olla vahva salasana ja se on vaihdettava säännöllisesti, esimerkiksi puolivuosittain. Sähköpostissa on suositeltavaa käyttää kaksivaiheista tunnistusta, kuten puhelinvarmistusta.

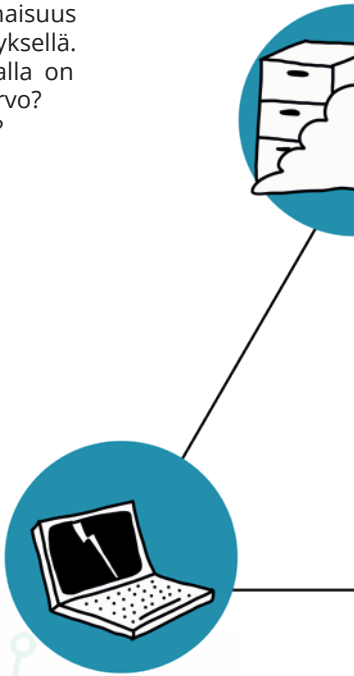
Samaa salasanaa ei saa käyttää monessa eri järjestelmässä. Salasanasta voi luoda erilaisia variaatioita: **PunainenValtraTalonEdessä_852**, **PunainenValtraLadonEdessä_852**, **PunainenValtraVerkkokaupassa_852**, ja niin edelleen. Salasanojen käyttöä voi helpottaa erityisillä salasanojen hallintaohjelmilla.

TIEDON VARMENTAMINEN TUO TURVALLISUUTTA

Maatilan tietojen varmentaminen vaatii suunnittelua. Maatilan tiedonhallinnan kokonaisuus on kartoitettavissa kolmella peruskysymyksellä. Millaista ja missä tallennusmuodossa tilalla on tietoa olemassa? Mikä on kunkin tiedon arvo? Mikä on tietojen menettämisen uhkakuva?

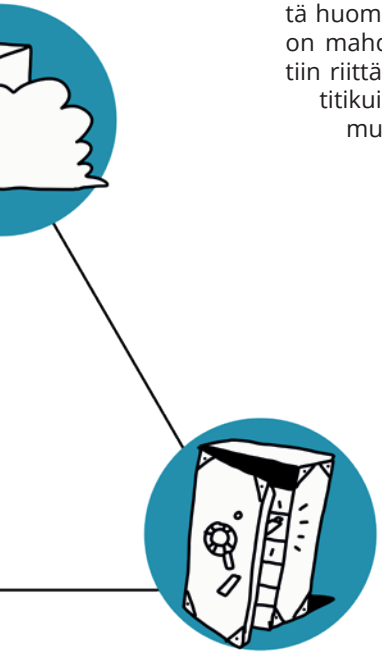
Valokuvilla on erilainen rahallinen arvo verrattuna kirjanpitoaineistoon. Lisäksi erilaisia ovat niiden tilantarve varmuuskopioinnissa ja palauttamisen mahdollisuus. Uhkakuvia ovat mm. laitteiden rikkoutuminen tai vaihtaminen uusiin, palo, salamanisku, varkaus, tietomurto ja verkko-ongelmat.

Puhelimien ja tablettien yksinkertaisin varmuuskopiointi tapahtuu laitteiden kanssa tarjotun pilvipalvelun avulla. Maksuton tallennustila riittää laitteen asetusten ja yhteystietojen varmuuskopiointiin, ja muun muassa valokuville on ostettavissa lisätilaa.



Maatilan tietokoneiden sisältämä tieto on yleensä tilan tuottamaa aineistoa. Sähköpostin tiedot voi tallentaa paikallisesti, jos käytössä ei ole verkkosähköpostia. Verkkosovellusten ja -palveluiden varmuuskopioinnista huolehtii yleensä palvelun tarjoaja, ja tämä tulisi mainita palvelun sopimuksessa.

Lypsyrobotin kaltaisen tuotantoautomaation



tietojen varmentamiseen tulee kiinnittää erityistä huomiota, jotta vikatilanteesta palautuminen on mahdollisimman helppoa. Varmuuskopiointiin riittää säännöllinen varmuuskopiointi muistitikuille tai automaattinen, säännöllinen varmuuskopiointi verkkolevylle.

Totaalisen tuhon, kuten tulipalon, varalle on hyvä, että tärkeimmät tiedot olisivat olemassa tilan ulkopuolella pilvitallennuspalveluissa. Tietojen siirto ja ajantasaisuus tulee automatisoida, mutta sen toimivuutta tulee myös seurata.

Tärkeintä on, että ajantasainen tieto on olemassa muuallakin kuin yhdellä laitteella ja yhdessä rakennuksessa. Tietojen palauttaminen perustuu ennakolta suunniteltuun prosessiin, jonka toimivuus pitää myös testata.

On myös oleellista tietää missä kunkin sovelluksen tai palvelun tiedot sijaitsevat, ja ovatko ne käytettävissä verkkoyhteyden katketessa.

Oletko varmuuskopioinut tärkeät tietosi?

Osaatko palauttaa tiedot varmuuskopiosta?

Missä säilytät tärkeitä tietojasi?

Mitkä tiedot ovat **pilvessä** ja mitkä **paikallisina**?

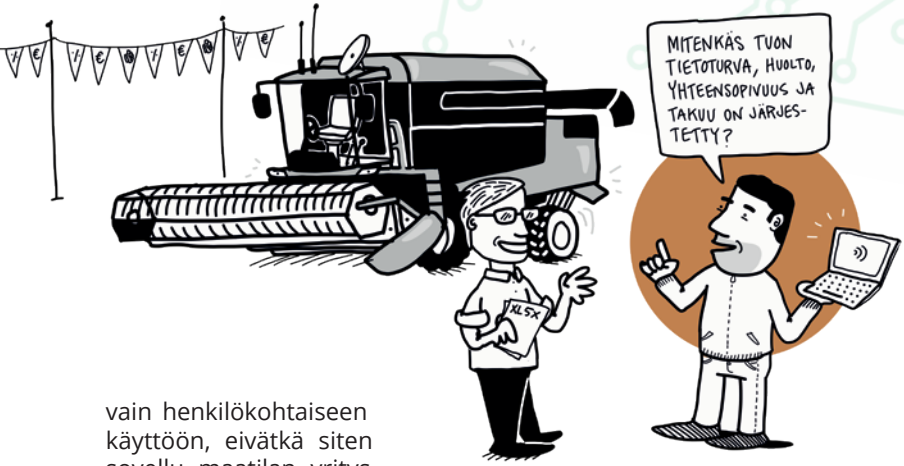
OVATKO HANKINTASI KYBERTURVALLISIA?

Laitteiden hankinta on aloitettava käyttötarpeen suunnittelulla. Valintaan vaikuttavat tilan järjestelmät, oli sitten kyse tilan työkoneista tai tietoteknisistä laitteista. Huomioitava on myös, tuleeko laite vain paikalliseen tai henkilökohtaiseen käyttöön, vai liittyykö laite maatilan omaan tietojärjestelmäkokonaisuuteen?

Isompia kone- tai laitehankintoja tehdessä tulee selvittää, millainen laitteen valmistajan automaatiojärjestelmä on. Onko se suljettu vai yhteensopiva muiden laitteiden ja maatilan olemassa olevan järjestelmän kanssa? On syytä pohtia, miten laite tai huolto ja korjaus toimii hankinnan jälkeen ja jopa kansainvälisessä kriisitilanteessa.

Henkilökohtaisen laitteen hankinnassa käytettävyydellä on suuri painoarvo. Oleellista on, miten laite soveltuu olemassa olevien muiden järjestelmien kanssa yhteen. Kuinka helposti muissa laitteissa tai järjestelmissä olevaa tietoa voi käyttää, tai tämän laitteen tietoja jakaa muiden käyttöön. Tietojen jakamisessa oleellista on kuitenkin tietoturvallinen käyttö, eli kenellä on oikeus näihin tietoihin.

Maatilan kasvaessa yksinyrittäjää suuremmaksi on tietoteknisissä laitteissakin siirryttävä yrityslaitteisiin, sovelluksiin ja palveluihin. Koti- tai kuluttajalaitteet ovat tarkoitettuja



vain henkilökohtaiseen käyttöön, eivätkä siten sovellu maatilan yrityskokonaisuuteen. Yrityslaiteille on saatavilla laajennettuja takuita, jolloin asentaja tulee 1-2 vuorokauden sisällä paikalle ja huoltaa laitteen siten, että kaikki tiedot säilyvät.

Laitteiden hankinnassa ja käyttöönotossa kannattaa käyttää maatilakokonaisuuden ymmärtäviä asiantuntijoita. Tietojen siirto aikaisemmista järjestelmistä, ohjelmistojen ja oheislaitteiden asennus, käyttäjäoikeuksien määrittely, liittyminen maatilan tietoverkkoon, tietoturva sekä varmuuskopioinnin määrittely on mittava projekti. Asiantuntija voi opastaa myös laitteiden ja ohjelmien uusien ominaisuuksien hyödyntämisessä, joka helpottaa jokapäiväistä käyttöä.

Kyberturvallisuus ja tietoturva ovat maatilan toiminnalle tärkeitä. Ne kannattaa suunnitella jo maatilan tietojen käsittelyjärjestelmän perustamisvaiheessa ja uusien laitteiden käyttöönotossa, sekä tarkistaa vuosittain.

PÄIVITTÄMINEN ON PARAS TURVA

Helpoin tapa ylläpitää maatilan tietoturvaa ja kyberturvallisuutta on muistaa pitää kaikki tilan järjestelmät päivitettyinä. Ajan tasalla oleva järjestelmä on turvallisuuden ja toimivuuden tae. Uudemmat tietojärjestelmät ja laitteet tarkistavat säännöllisesti niihin saatavat päivitykset.

Monilla tiloilla on kuitenkin käytössä vanhempia järjestelmiä, joissa käyttäjän on huolehdittava päivityksistä. Tilalla käyttäjän tulee olla tietoinen, mitä toimenpiteitä eri laitteet vaativat pysyäkseen ajan tasalla, ja huolehtia ohjelmistojen ajantasaisuudesta osana tilan koneiden ja laitteiden huoltoa.

Tärkeää on myös selvittää milloin laitteita tai ohjelmistoja pitää uusia. Tietoteknisen laitteen tyypillinen elinkaari on 3-5 vuotta. Tilan toimintaan tulee huomattavasti pienempiä ja lyhyempiä häiriöitä, mikäli laitteet uusitaan ennen niiden rikkoutumista, tai jos tilalla on selkeä toimintasuunnitelma miten rikkoutuneet laitteet korvataan. Varautuminen maksaa itsensä takaisin laiterikon sattuessa!

Tärkeä osa tilan kyberturvallisuutta on myös palomuurien käyttäminen. Palomuuri on tietokoneen ohjelmisto tai verkon laite, joka valvoo tietoliikennettä, ja päästää läpi vain sallitun liikenteen. Palomuurin avulla on mahdollista rajoittaa valvontakameroiden kuvien tai muun arkaluontoisen tiedon vuotamisen tilan tietoverkon ulkopuolelle. Lisäksi palomuureilla voidaan rajoittaa myös haittaohjelmien leviämistä.

Palomuurien asentaminen ja ylläpito vaatii tietoteknistä osaamista, joten asiassa on hyvä turvautua asiantuntijan apuun. Palomuureja voi olla tilalla myös useita; esimerkiksi erillinen palomuuri joka valvoo kaikkea tilan verkkoliikennettä ja lisäksi tilan kaikilla tärkeillä tietokoneilla omat palomuurit jotka suojaavat kyseisiä koneita.

HALUATKO TIETÄÄ LISÄÄ?

Viranomaisilla ja järjestöillä on lukuisia kyberturvallisuutta edistäviä verkkosivustoja ja -aineistoja. Ne tarjoavat tietoa ja uutisia kybermaailman tilanteesta myös maatiloille.

Viestintäviraston kyberturvallisuuskeskus
WWW.VIESTINTAVIRASTO.FI/KYBERTURVALLISUUS

Kyberin taskutieto
URN.FI/URN:ISBN:978-951-39-7589-0

Kodin turvaopas: Kyberturvallisuus
KODINTURVAOPAS.FI/KYBERTURVALLISUUS

Alkutuotannon kyberuhat
JUKURI.LUKE.FI/HANDLE/10024/539088

Tämä opas on ladattavissa sähköisenä osoitteista
- URN.FI/URN:ISBN:978-951-39-7640-8
- MPK.FI/KOULUTUKSET/KYBERTURVALLISUUS/

Tutustu myös Luonnonvarakeskuksen, Huoltovarmuusorganisaation sekä Maa- ja metsätaloustuottajain keskusliiton verkkosivuihin:
LUKE.FI · HUOLTOVARMUUS.FI · MTK.FI

MAATILAN 10 KYBERKYSYMYSTÄ

		KYLLÄ	EI
1	Oletko varmuuskopioinut omat tietosi, mukaan lukien käyttäjätunnukset ja salasanat? Osaatko palauttaa varmuuskopiot?	☐	☐
2	Teetkö järjestelmällisesti saatavissa olevat ohjelmistopäivitykset kaikkiin laitteisiin?	☐	☐
3	Toimiiko tila-automaatio (ilmanvaihto, vesi, lämpötila ja ruokinta) myös sähkökatkon tai laiterikon sattuessa?	☐	☐
4	Saatko painevettä lypsyrobotille sähkökatkossa?	☐	☐
5	Ovatko varavoima ja sen polttoainehuolto kunnossa?	☐	☐
6	Onko kaikilla käyttäjillä henkilökohtaiset ja riittävän pitkät salasanat?	☐	☐
7	Onko henkilötietojen käsittely turvallista? (ks. EU:n yleinen tietosuoja-asetus eli GDPR)	☐	☐
8	Tiedätkö, mitä tietoja tilastasi kerätään palveluiden tuottajien järjestelmiin? Voitko saada tietosi palveluntuottajalta käyttökelpoisessa muodossa?	☐	☐
9	Arvioitko kaikkien hankintojesi kyberturvallisuuden ja yhteensopivuuden?	☐	☐
10	Onko tilalle laadittu tietoverkkokartta?	☐	☐