Maatilan kyberturvallisuus -infopaketti

jamk | Jyväskylän ammattikorkeakoulu

Maa- ja metsätalous-ministeriö

Digitalisaatio tuo uusia uhkakuvia maatiloille

Maatalouden digitalisaation kiihtyessä maatilat ovat entistä riippuvaisempia digitaalisista palveluista ja järjestelmistä. Samalla kun uusien järjestelmien käyttöönotto helpottaa monia työvaiheita, se voi myös lisätä internetin kautta tulevia uhkia.

Infopaketista löydät vastauksen kysymyksiin:

- Mitä huomioida kehittäessäsi tilasi digitaalisen ympäristön turvallisuutta?
- Millainen on mallitila kyberturvallisuuden näkökulmasta?

Mallitila kyberturvallisuuden näkökulmasta

Päärakennus

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

Tuotantotilat

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

Tilan tietoverkko

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

Pilvipalvelut

Vipu, Wisu, Wakka, Google Drive ym.

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

Anturit ja työkoneet

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

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

Kyberturvallisuuden tarkistuslista tilallisille

Kunnossa

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

- [ ] Tunnista kriittiset toiminnot ja suunnittele, miten toimitaan, jos järjestelmät eivät toimi, esimerkiksi mitä töitä voidaan tehdä manuaalisesti.
- [ ] Sähkökatkon varalta varmista tuotantolaitteiden varavoima ja tarvittaessa painevesi.
- [ ] Varmista, että myös tuotantoa ohjaavat tietokoneet ovat varavirtalähteen perässä.
- [ ] Pidä varalla kiinteän nettiliittymän lisäksi mobiililiittymää.
- [ ] Järjestä tietojen säännöllinen varmuuskopiointi ja useiden kopioiden säilyttäminen fyysisesti eri paikoissa, kuten ulkoinen kiintolevy, DVD, pilvipalvelu. Varmista myös, että osaat palauttaa tiedot varmuuskopioista tilanteen niin vaatiessa.
- [ ] Varmista henkilötietojen ja muiden arkaluontoisten tietojen asiallinen käsittely niiden koko elinkaaren ajalta.
- [ ] Asenna ja päivitä säännöllisesti virus- ja haittaohjelmien torjunta, mieluiten automaattisesti.
- [ ] Jos mahdollista, laita sähköpostisovelluksissa viestien sisältämät linkit ja kuvat pois käytöstä.*
- [ ] Mieti etukäteen poikkeustilanteen viestintä.

Seuraavat suositeltavat toimenpiteet saattavat vaatia asiantuntijan apua:

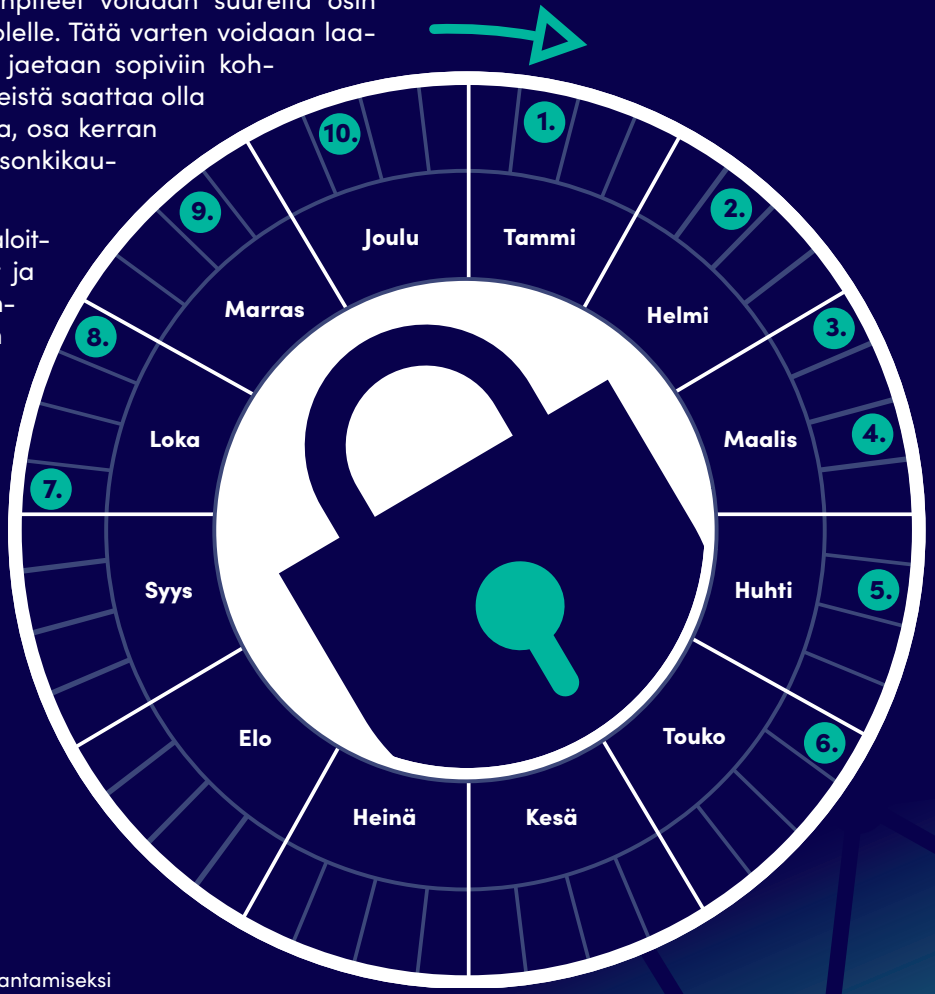
- [ ] Käytä palomuureja, estä kaikki paitsi välttämätön liikenne oman verkon ja internetin välillä.
- [ ] Salli liikenne valvontakamerajärjestelmiin vain niistä IP-osoitteista, joille se on välttämätöntä.
- [ ] Toteuta verkon segmentointi, edellytä segmentoinnin järjestämistä esimerkiksi laitetoimittajalta uusia järjestelmiä asennettaessa.
- [ ] Tee vain yhdet järjestelmänvalvojan tunnukset ohjelmistojen asentamista varten. Luo peruskäyttöön jokaiselle omat tunnukset, joissa ei ole järjestelmänvalvojan oikeuksia.
- [ ] Poista tarpeettomat etäyhteysohjelmat ja etäyhteyteen käytettävät RDP-portit käytöstä.*
- [ ] Ota käyttöön lokien kerääminen ja niiden seuranta. Vinkkejä: www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

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

Kyberturvallisuuden vuosikello

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

Vuosikellon tekeminen kannattaa aloittaa listaamalla kaikki toimenpiteet ja jatkaa sijoittamalla ne sopiviin ajankohtiin. Esimerkiksi kausikäyttöisten laitteiden tarkistus ja päivittäminen kannattaa ajoittaa tehtäväksi aina ennen niiden käyttöönottoa.**



Toimenpidelista voi näyttää esimerkiksi tältä:

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

*Lähde: 10 kohtaa kyberturvallisuuden parantamiseksi matkailualalla. 2021. Matkailun vastuullisuus näkyväksi Keski-Suomessa-hanke. Viitattu 6/2022. https://visitjyvaskyla.fi/professionals/wp-content/uploads/sites/2/2021/09/10-kohtaa-kyberturvallisuuden-parantamiseksi-matkailualalla.pdf

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

Haluatko tietää enemmän kyberturvallisuudesta alkutuotannossa?

Kyberturvallisuus alkutuotannossa
– käsikirja kyberpoikkeamien hallintaan

Lataa maksuton käsikirja!

Käsikirjan avulla alkutuottaja:

- ✓ Laajentaa ymmärrystään kyberturvallisuuden merkityksestä digitaalisessa toimintaympäristössään.
- ✓ Ymmärtää ajankohtaisia toimialaan kohdistuvia kyberuhkia.
- ✓ Saa konkreettisia ohjeita kyberpoikkeamien hallintaan.

Infopaketti ja käsikirja ovat Kyberpoikkeamanhallinnan prosessit ja toimintaohjeet elintarviketuotannossa ja –jakelussa –projektin tuotoksia. Projektin on rahoittanut Maa- ja metsätalousministeriö ja toteuttanut Jyväskylän ammattikorkeakoulun IT-instituutti.

Lisätietoa aiheesta
www.jyvsectec.fi/elintarvikeketju

jamk | Jyväskylän ammattikorkeakoulu

Maa- ja metsätalous-ministeriö