Mtech
Digital Solutions

Maatilan kyberturvallisuus

Suojaa tilasi ja tietosi digitaalisilta uhkilta

Toni Haapanen | Mtech Digital Solutions

Mtech
Digital Solutions

Miksi tämä koskee maatilaa

Maatalouden digitalisaatio ja automaatio ovat muuttaneet tilojen toimintaa pysyvästi. Nykyinen maatila on yhtä aikaa tuotantolaitos, datakeskus ja verkottunut ympäristö.

Maatiloilla käytetään yhä enemmän automatisoituja ja IoT (esineiden internet)-pohjaisia järjestelmiä kuten sensoreita, automaattilypsy- ja ruokintajärjestelmiä, kastelun ja ilmanvaihdon ohjausta, sekä eläinten hyvinvoinnin ja tuotosseurannan etävalvontaa.

Nämä järjestelmät tekevät arjesta tehokkaampaa, mutta samalla ne avaavat myös uusia riskejä.

- Verkkoon kytketyt laitteet voivat olla alttiita tietomurroille ja haittaohjelmille.
- Hyökkäys tai vika voi pysäyttää tuotannon, heikentää eläinten hyvinvointia ja aiheuttaa taloudellisia tappioita.
- Pahimmillaan se voi vaikuttaa koko elintarvikeketjun huoltovarmuuteen.

Digitalisaatio tuo tehokkuutta ja tarkkuutta, mutta myös uusia riskejä, jotka eivät katso tilan kokoa

Mtech
Digital Solutions

Kyberturvallisuuden tulevat haasteet maataloudessa

Teknologinen riippuvuus kasvaa, ja automaatio, anturit, pilvipalvelut ja liikkuva data edellyttävät lähes 100% toimintavarmuutta. Nykyään kymmeniätuhansia automaattilypsyrobottia ympäri maailmaa kerää jatkuvasti tietoa tuotannosta, eläinten terveydestä ja käyttäytymisestä – tieto, jonka varaan koko toiminta rakentuu.

Kyberuhkien määrä kasvaa nopeasti:

- Kyberturvayritykset raportoivat 30 %:n vuosittaisen kasvun hyökkäysten määrässä
- Yhdysvalloissa FBI raportoi 8,2 % kasvun kiristyshyökkäyksissä maataloussektorilla.
- Joissakin kyselyissä lähes puolet viljelijöistä pitää kyberturvallisuushuolia suurimpana esteenä digitalisaation edistymiselle.
- Ohjelmistojen haavoittuvuudet ja vanhentuneet järjestelmät lisäävät riskejä – erityisesti prosessinohjausjärjestelmissä, joita on vaikea päivittää. Monet automaatiojärjestelmät ovat verkossa jatkuvasti ilman tehokasta päivitys- ja tietoturvakäytäntöä.
- Kyberrikolliset ja valtiolliset toimijat ovat entistä ammattimaisempia ja kohdistavat hyökkäyksiä ruokaketjuihin ja kriittiseen infrastruktuuriin.
- Inhimilliset virheet ja tekniset viat (sähkökatkot, laitteistoviat, ohjelmistovirheet) ovat yhä yleisimpiä häiriöiden syitä.
- Maatalous on yksi vanhimmista elinkeinoista, mutta nyt sen on sopeuduttava digitaaliseen aikaan.

Tietoturva on koko ketjun yhteinen vastuu – ja tuotantoketju on yhtä vahva kuin sen heikoin lenkki.

Mtech
Digital Solutions

Miltä uhka näyttää ja mitä se voi viedä mukanaan

Maatilalla on samat kyberriskit kuin millä tahansa digitaalisella organisaatiolla. Ei tarvitse olla suuri yritys ollakseen houkutteleva kohde vaan riittää, että käytetään verkkoa.

Nykyinen maatila on täynnä verkottuneita järjestelmiä ja jokainen yhteys on mahdollinen hyökkäyspinta.

Kun yksikin digitaalinen järjestelmä pysähtyy, sen vaikutus tuntuu nopeasti koko tilan toiminnassa – tuotannossa, taloudessa ja maineessa.

- Automaattilypsy tai ruokintaohjelma lukkiutuu – lypsy ja ruokinta pysähtyvät, eläinten hyvinvointi vaarantuu ja maitotuotanto lamaantuu hetkessä. Jokainen hetki ilman toimivia järjestelmiä merkitsee taloudellista tappiota.
- Haittaohjelma pysäyttää kirjanpidon, laskutuksen tai lohkokirjaukset – arjen hallinta keskeytyy, tärkeät tiedot voivat kadota, vääristyä ja tilan taloudellinen raportointi ja viranomaisvelvoitteet viivästyvät.
- “Pankista” tai “asiakkaalta” tullut viesti kalastelee tunnuksia – kun käyttäjätunnukset tai maksutiedot päätyvät rikollisille, seurauksena voi olla taloudellisia menetyksiä, ja tilin tai tiedon väärinkäyttöä.
- Kadonnut puhelin, tietokone tai massamuisti sisältää tilan ja asiakkaiden tietoja – jos laite joutuu vääriin käsiin, se voi johtaa tietovuotoon, henkilötietojen väärinkäyttöön ja luottamuksen menettämiseen.

Maatilan tärkein omaisuus ei ole vain eläimet ja koneet vaan myös tieto, joka ohjaa kaikkea niiden ympärillä.

Mtech
Digital Solutions

Esimerkki - Kyberhyökkäys lypsytilalle Sveitsissä

Sveitsissä vuonna 2024 tehty kiristyshyökkäys lamautti automaattilypsyjärjestelmän kokonaan. Rikolliset pääsivät tilan verkkoon, salakirjoittivat tietokoneet ja lypsyrobotit, ja vaativat 10 000 dollarin lunnaita saadakseen järjestelmät takaisin käyttöön.

Seuraukset olivat vakavia ja välittömiä:

- Lypsyrobotit pysähtyivät, ja 70 lehmän tila jäi ilman automaattista lypsyä.
- Koska osa järjestelmästä oli onneksi irti verkosta, osa lehmistä voitiin lypsää manuaalisesti, mutta tuotanto hidastui ja eläinten hyvinvointi vaarantui.
- Tila menetti pääsyn kaikkiin keskeisiin tietoihin - eläinten terveystietoihin, tiineys- ja siemennystietoihin, sekä tuotantohistoriaan.
- Kun viljelijä ei enää tiennyt, mitkä eläimet olivat tiineitä, hän joutui turvautumaan eläinlääkärin arvioon.
- Tapaus johti lisäkuluihin ja myös yhteen eläimen menetykseen.

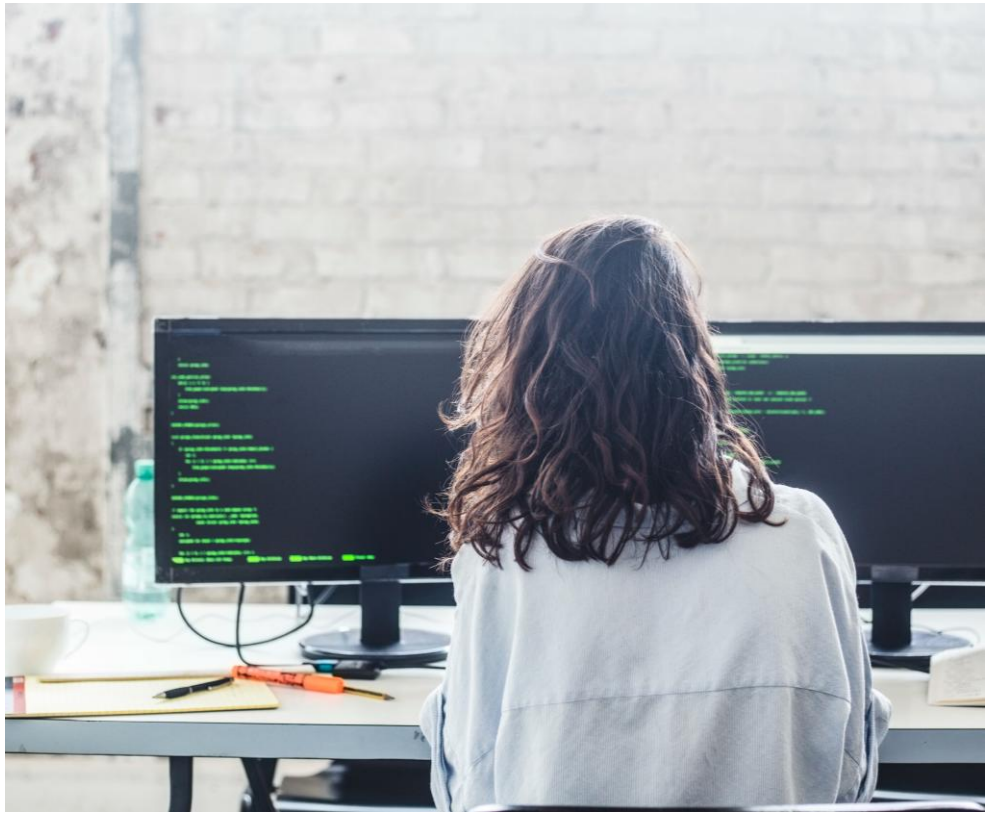
Asiantuntijat pystyivät lopulta palauttamaan osan tiedoista vanhoista varmuuskopioista, mutta tuotanto oli pysähdyksissä useita päiviä, aiheuttaen merkittäviä taloudellisia tappioita.

Kyberhyökkäys ei vaikuta vain tietokoneisiin – se voi suoraan uhata eläinten terveyttä, tuotannon jatkuvuutta ja koko ruokaketjun luotettavuutta.

Lähde: The Bullvine, 2024 – “Cybercriminals Hijack Milking Robots, Swiss Farmers’ Data Held Ransom”

Mtech
Digital Solutions

Ihminen tietoturvan ytimessä



Teknologia on vain puolet tietoturvasta ja toinen puoli on ihminen. Suurin osa tietoturvaloukkauksista ei johdu ohjelmiston virheestä, vaan tavallisesta toiminnasta: kiireestä, luottamuksesta ja huolimattomuudesta.

Jokainen meistä on osa tietoturvaa ja se syntyy arkisista tavoista ja valinnoista.

- Tunnista uhat ja ole tietoinen siitä, millaisia huijauksia ja haittaohjelmia liikkuu maailmassa.
- Älä klikkaa epäilyttäviä linkkejä tai avaa liitteitä, jos viesti vaikuttaa oudolta.
- Älä jaa salasanoja tai tunnuksia, ei edes tuttujen kanssa. Käytä mieluiten salasanojen hallintaohjelmaa.
- Pidä laitteet ja ohjelmistot ajan tasalla.
- Säilytä tietoja vain siellä, missä ne kuuluvat.
- Suojaa verkkosi ja varmista, että Wi-Fi on salattu ja salasana riittävän vahva.
- Pidä varmuuskopiot kunnossa.

Mtech
Digital Solutions

Fyysinen turvallisuus ja toimintavarmuus

Kyberturvallisuus ei ole vain ohjelmia ja salasanoja, mutta myös fyysinen ympäristö vaikuttaa tietoturvaan.

Fyysinen turvallisuus

- Suojaa tilat ja laitteet lukituksilla, kulunvalvonnalla ja ohjeilla.
- Älä jätä arkaluonteisia papereita tai IT-laitteita valvomatta.
- Varaudu varkauksiin ja pahantahtoisiin toimijoihin.
- Älä koskaan käytä tuntemattomia tai “löydettyjä” USB-tikkuja tai muita massamuisteja.
- Käytä vain luotettuja, virustarkastettuja laitteita.
- Salaa ulkoiset kovalevyt ja muistit, joissa on tilan tai asiakkaiden tietoja.

Sähkön saanti ja varavoima

- Sähkökatko pysäyttää kaiken, myös tietoturvan.
- Käytä automaattista varavoimaa turvaamaan verkkojen ja laitteiden toiminta.
- Tarkista säännöllisesti, että varavoima kytkeytyy päälle automaattisesti.

Fyysinen turvallisuus on osa kyberturvaa se pitää tietojärjestelmät ja tuotannon käynnissä myös poikkeustilanteissa.

Mtech
Digital Solutions

Tekoäly - uudet haasteet

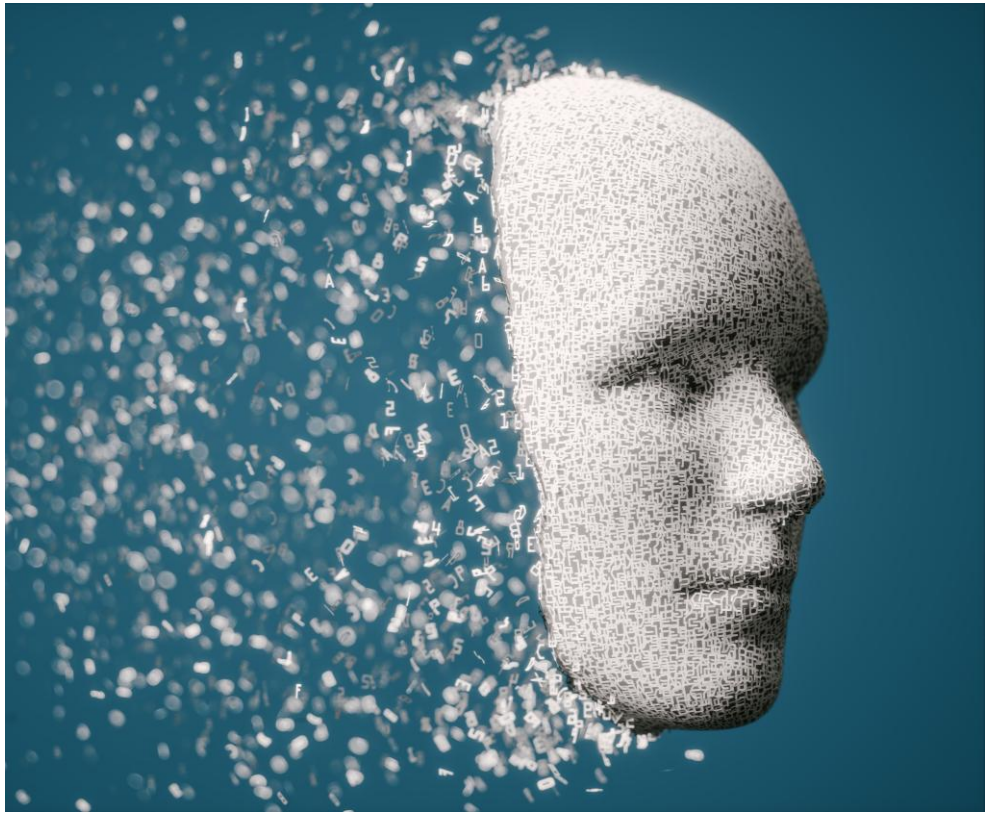
Tekoäly tuo valtavia mahdollisuuksia, mutta myös uudenlaisia riskejä.

AI tekee hyökkäyksistä älykkäämpiä, uskottavampia ja helpommin automatisoitavia. Rikollisille tekoäly on työkalu aivan kuten muulle.

Näin se näkyy arjessa:

- Väärennetyt viestit ja puhelut täydellisellä suomen kielellä, jopa tutun ihmisen äänellä.
- ”Deepfake”-videot ja kuvat, joilla luodaan uskottavia valeuutisia tai “toimeksiantoja.”
- Tekoälyn kirjoittamat huijausviestit näyttävät entistä aidommilta.
- Automaattiset hyökkäykset etsivät heikkoja salasanoja ja avoimia laitteita.

Suomeksi kirjoitetut ja tyyliltään uskottavat viestit tekevät huijausten tunnistamisesta vaikeampaa kuin koskaan. Siksi on tärkeää, että tärkeät päätökset vahvistetaan toista kanavaa pitkin – puhelimitse, kasvotusten tai sovitun prosessin kautta.



Mtech Digital Solutions

Yhteenveto

- Maatalous ei ole poikkeus
  - Samat kyberuhat, jotka kohdistuvat pankkeihin, teollisuuteen ja kuntiin, koskevat myös maatiloja ja automaattilypsyjärjestelmiä
- Teknologian kasvu lisää vastuun tarvetta
  - Jokainen verkkoon kytketty laite, pilvipalvelu ja sovellus avaa uuden oven ja vaatii tietoisuutta ja osaamista tietoturvasta.
- Tietoturva on yhteinen asia
  - Tila, neuvoja ja toimittajat muodostavat yhden ketjun. Jos yksi lenkki pettää, vaikutus tuntuu kaikissa
- Ihminen ratkaisee enemmän kuin teknologia
  - 95 % loukkauksista alkaa inhimillisestä virheestä, mutta samat ihmiset voivat myös estää ne
- Pienet teot vievät pitkälle
  - Päivitykset, varmuuskopiot, vahvat salasanat ja terve epäluulo suojaavat tehokkaammin kuin moni kallis ohjelma.

Mtech
Digital Solutions

Kysymykset

www.mtech.fi

Mtech Digital Solutions

MtechDigi

Mtech Digital Solutions

Mtech Digital Solutions

Lähteet

- https://www.threatvirus.com/2025/07/deepfake-cyber-attacks-2025-guide
- https://www.maaseuduntulevaisuus.fi/mainos/0f809933-831a-4c8c-adc1-f43fcd473a29
- https://maaseutuverkosto.fi/wp-content/uploads/2023/01/maatilan_kyberturvallisuus-infopaketti.pdf
- https://www.frontiersin.org/journals/sustainable-food-systems/articles/10.3389/fsufs.2022.884187/full
- https://www.thebullvine.com/news/cybercriminals-hijack-milking-robots-swiss-farmers-data-held-ransom
- https://www.siberoloji.com/cybersecurity-in-agriculture-protecting-smart-farms-and-food-supply-chains
- https://www.ncsc.gov.uk/files/NCSC_Cyber%20Security%20Guide%20for%20Farmers-%20digital.pdf