

# **O**SAAVA FARMARI

## Maatilan kyberturvallisuus

Maatilojen riskienhallinta -koulutus

Jyväskylän ammattikorkeakoulu, Biotalousinstituutti



# MAATILAN RISKIENHALLINTA KOULUTUS

## Kyberturvallisuus

21.11.2022

Klo 12.05 – 13.00 Maatilan kyberturvallisuus ja siihen liittyvät riskit

Jyrki Kataja

Biotalousinstituutti / AB SmartDIH

Elintarviketuotannon ja –jakelun kyberturvallisuus / Älymaatila / Energiatehokkuus, energiantuotanto ja –käyttö tulevaisuudessa

Elintarviketuotannon ja -jakelun toimijoiden Kyberharjoittelukyvykkyyden kehittäminen (EKK)



Vipuvoimaa  
EU:lta  
2014–2020



jamk

## Kyberturva

datan/tiedon - siirto – varastointi – käyttö; järjestelmien ja laitteiden toimivuus

## Tietoturva

datan/tiedon – saatavuus – luottamuksellisuus - eheys



JYVSECTEC  
by jamk

SERVICES · CYBER RANGE · TOPICS · R&D · NEWS AND INSIGHTS

ACTIVE

### Food Chain Cyber Resilience

Digitalization and technological advances are bringing lots of changes in food production and its technical environment. Systems and processes in the field are evolving at an increasing pace. Thus, we need to be prepared for cyber threats and disruptions targeted to different sections of the food chain.

*A capability for a food chain cybersecurity exercise will be developed together with the actors in the food supply chain.*

#### Yhteistyökumppanit

Atria DeLaval SOK Perinteinen Maito Oy RUOKLAVARMAUSKESKUS  
NATIONAL EMERGENCY SUPPLY AGENCY

Telia netum TRAFICOM National Cyber Security Centre Cinia

Valio elisa Fazer K jamk | Jyväskylän ammattikorkeakoulu  
University of Applied Sciences

jamk

<https://jyvsectec.fi/2021/09/food-chain-cyber-resilience/>

# Kyberturvallisuuden näkökulmia

## Kyberturvallisuuden määrittelyä

- Kyberturvallisuus on turvallisuuden osa-alue, jolla pyritään sähköisen ja verkotetun yhteiskunnan turvallisuuteen.
- Kyberturvallisuudessa tunnistetaan, ehkäistään ja varaudutaan sähköisten ja verkotettujen järjestelmien häiriöiden vaikutuksiin yhteiskunnan kriittisiin toimintoihin.
- Kyberturvallisuusajattelussa yhdistyy tietoturvallisuuden, jatkuvuuden hallinnan ja yhteiskunnan kriisivarautumisen ajattelua.
- Kyberturva <-> Tietoturva; erona fyysiset vaikutukset -> lehmien tunnistaminen, lypsyrobotin toiminta, lehmien tuotostiedot.

# Kyberturvallisuuden näkökulmia

## Kyberuhkien ja -riskien hallinta perustuu niiden tiedostamiseen

- Lähestymistapoja;
  - Perusprosessin poikkeama; esim. jännitepiikki sähköverkossa.
  - Laitteen rikkoontuminen; esim. anturin komponentti.
  - Tahattomasti aiheutettu tilanne; esim. osaamattomuus, väsymys.
  - Tahallaan aiheutettu tilanne; esim. hyötymistarkoitus.
- Ihmiset
- Anturit ja mittalaitteet
- Tuotantoa tekevät laitteet.
- Yrityksen sisäinen johtamisjärjestelmä.
- Yrityksen tuotantodatan merkitys kilpailijoille, markkinoille, tuotantopanoksien toimittajilla.



# Kyberuhkien ja -riskien hallinta perustuu niiden tiedostamiseen

- Sähkö on avainasemassa.
  - Lähes kaikki laitteen tarvitsevat sähköä ja toimiakseen luotettavasti ainakin tieto- ja mittaustekniikka sekä tiedonsiirto tarvitsevat laadukasta sähköä.
    - UPS-laitteet; riittävä kapasiteetti, monivaiheisuus (varavoimalan riittävä teho)
    - Investointien yhteydessä uusien ja vanhojen tilojen, kaapelointien ja järjestelmien yhteistarkastelu myös kyberuhkien kannalta.
    - Sähkön laatuun vaikuttamalla voidaan vaikuttaa myös maatalan fyysisiin toimintoihin. (esim. taajuusmuuntimiin)





# Kyberuhkien ja -riskien hallinta perustuu niiden tiedostamiseen

- Tiedot ovat avainasemassa.
  - **Turvallisuus lähtee tiedon varmentamisesta = varmuuskopioiti**
- Kuinka usein varmuuskopiointi tehdään
  - Missä varmuuskopiot fyysisesti ovat?
  - Missä tallennusmuodossa kriittiset tiedot ovat?
  - Mikä on kunkin tietoaineiston arvo?
- **Tietojen palauttaminen perustuu suunniteltuun ja testattuun toimintatapaan.**
- Tietojen käytettävyys verkkoyhteysongelmien aikana;
  - Paikallisella asemalla
  - Pilvipalvelussa
  - Varavirran todellinen käyttöaika (akut, polttoaine)



# Kyberuhkien ja -riskien hallinta perustuu niiden tiedostamiseen

- Maatilan erityispiirteitä.

1. Tärkeimmät kyberuhkien syyt:

- a) Säätilojen aiheuttamat häiriöt
- b) Tilalla työskentelevien inhimilliset virheet
- c) Tahalliset / tarkoitukselliset häiriötilanteet

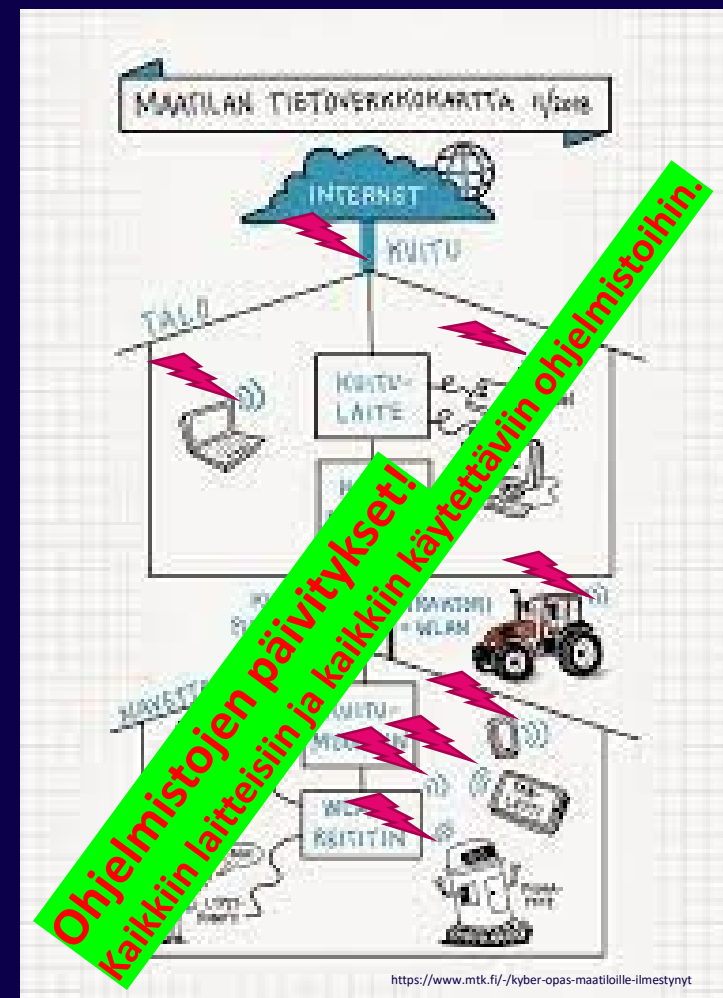
2. Tietotekniikkaa uusittava useammin kuin koneita ja rakennuksia

- a) Tietotekniikan elinkaari 3-5 vuotta (- 10 vuotta)
- b) Koneisen ja laitteiden elinkaari 10 – vuotta (10 – 30 vuotta)
- c) Rakennusten elinkaari 20 – vuotta (30 – 50 vuotta)

**(ainakin 2 kertaa ja parhaimmillaan jopa 20 kertaa elinkaaren aikana)**

- Maatilan tietoverkkokartta (tietovirrat)

- Monestako pisteestä maatilasi näkyy ulospäin tietoverkkoihin?



# Kyberuhkien ja -riskien hallinta perustuu niiden tiedostamiseen

- Ihmiset ovat avainasemassa.
  - Yrityksen tietokoneille luodaan jokaiselle käyttäjälle;
    - Käyttäjätunnus
    - Salasana
    - Perustetaan tarvittavat oikeudet eri ohjelmiin ja palveluihin.
  - Pääkäyttäjän tili (järjestelmänvalvoja) vain;
    - Ohjelmien asentamiseen ja päivittämiseen
    - Huoltotoimenpiteitä varten
    - Käyttäjätilien luontia varten
    - Vahva salasana
  - Sähköpostiosoite on avain moniin palveluihin;
    - **Vahva salasana** (vaihdettava usein)
    - Ainakin pääkäyttäjän tilin toiminnoissa kaksivaiheinen tunnistus (esim. puhelinvarmennus)

**Yrittäjät**

**Vakituinen henkilöstö**

**Kausityöntekijät**

**Kotimainen**

**Ulkomainen**



**Osaaminen**

**Ammattitaito**

**Ehtimien**

**jamk**



# Kyberturvallisuuden näkökulmia kasvihuoneyrityksille

Yksityiset henkilöt, yritykset ja organisaatiot voivat ilmoittaa Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle niihin kohdistuneista tietoturvaloukkauksista, kuten tietojen kalastelusta tai palvelunestohyökkäyksistä, sekä näiden loukkausten yrityksistä.

**Etukäteisen varaudutaan.**

**Jälkikäteen selvitetään sotkuja ja etsitään syyllisiä.**

**Kiitos ajastanne!**

Elintarviketuotannon ja -jakelun toimijoiden Kyberharjoittelukyvykkyyden kehittäminen (EKK)



Vipuvoimaa  
EU:lta  
2014-2020

