KOMIO
Koulutusyhteistyöllä kohti parempaa maankäyttösektorin ilmasto-osaamista

# Maatalouden kyberturvallisuus

Kuula Juha

Jamk 2024



Nappaa hiilestä kiinni
MAANKÄYTTÖSEKTORIN ILMASTORATKAISUT

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

HAMK Hämeen ammatti-korkeakoulu

jamk | Jyväskylän ammattikorkeakoulu

Karelia

LAPIN AMK
Lapland University of Applied Sciences

YRKESHÖGSKOLAN NOVIA

OAMK

SAVONIA

XAMK
Kaakkois-Suomen ammattikorkeakoulu

# Digitaalinen turvallisuus

KOMIO
Koulutusyhteistyöllä kohti parempaa maankäyttösektorin ilmasto-osaamista

- **Tietosuoja**: Jokaisen oikeus henkilötietojensa suojaan
- **Tietoturva**: Toimia, joilla varmistetaan tiedon
  - **luottamuksellisuus** -> tieto käytettävissä vain sen käyttöoikeuden haltijoille
  - **eheys** -> tiedon muutosoikeus sen käyttöoikeuden haltijalla
  - **käytettävyys** -> tiedot ja tietojärjestelmät ovat käytettävissä (järjestelmät toimivat ja tieto on saavutettavissa)
- **Kyberturvallisuus:** Tavoitetila, jossa digitaaliseen ympäristöön voidaan luottaa
- **Riskienhallinta:** Tiedostetaan olemassa olevat riskit. Voidaan jakaa neljään toimintatapaan, riski poistetaan, sen todennäköisyyttä tai vaikutusta pienennetään tai se voidaan hyväksyä
- **Jatkuvuus ja varautuminen:** Pidetään turvallisuustoimia yllä ja varaudutaan mahdollisiin uhkiin

Lähde: Tuni – Kyberturvallisuus kurssimateriaali

# Kyberturvallisuus

KOMIO
Koulutusyhteistyöllä kohti parempaa maankäyttösektorin ilmasto-osaamista

- ”Kun digitaalisia tietojärjestelmiä sisältävä toimintaympäristö, eli kybertoimintaympäristö on luotettava ja sen toiminta turvattua voidaan puhua kyberturvallisuudesta.” (Suni ym. 2020)
- Kolme tukipilaria
  - Ihmiset: Toimintaan liittyvät henkilöt koulutetaan toimimaan oikein. Näin voidaan välttyä esimerkiksi henkilö- tai käyttäjätunnusten joutuminen vääriin käsiin.
  - Prosessit: Kehitetään turvallisuutta lisääviä prosesseja ja käytänteitä. Prosesseja kehittämällä voidaan välttyä esimerkiksi kulunvalvonnan aiheuttamista heikkoukista.
  - Teknologia: Suunnitellaan ja toteutetaan turvallisuutta parantavaksi. Esimerkiksi varmistetaan kriittisten järjestelmien (maitotankki, lypsyrobotti, lämmityskeskus…) virransaanti häiriötilanteessa.
- Kybertuvallisuus käsittää siis koko toimintaympäristön, sen sovellukset, laitteet

Lähde: Elintarviketeollisuuden kyberturvallisuus opas

# Verkon kyberuhat

KOMIO
Koulutusyhteistyöllä kohti parempaa maankäyttösektorin ilmasto-osaamista

- **Haittaohjelmat**:
  - **Virus** tallentaa laitteeseen haitallista koodia
  - **Kiristysohjelma** lukitsee tiedot siten, ettei niihin pääse käsiksi
  - **Mato** kykenee monistamaan itseään ja voivat levittää esimerkiksi kiristysohjelmaa
  - **Vakoiluohjelma** kerää tietoja (web-kamera, henkilötiedot, tunnukset…)
  - **Troijalainen** pyrkii naamioimaan itsensä oikeaksi sovellukseksi
- **Haitalliset sähköpostit ja tekstiviestit** ovat massaviestejä (spam), joilla yritetään saada käyttäjä avaamaan viestin haitallinen liite tai linkki.
- **Haitalliset verkkosivut** voi olla naamioitu näyttämään aidolta sivulta ja kykenevät asentamaan haittaohjelmia tai varastamaan laite-/verkkotietoja.
- **Haitalliset sovellukset** ja niiden käyttöoikeudet pyytävät liikaa käyttöoikeuksia laitteelle kerätäkseen ylimääräistä tietoa käyttäjästään esimerkiksi markkinoinnin tai tietojen eteenpäin myynnin vuoksi.
- **Haitalliset laitteet:** Verkkoyhteyttä tarvitsevan laitteen tietoturva voi olla kyseenalainen tahallisesti tai tahattomasti

Lähde: Yksinyrittäjän ja mikroyrityksen Kyber- ja tietoturvaopas

# Maatilan kyberturvallisuus 1/2

KOMIO
Koulutusyhteistyöllä kohti parempaa maankäyttösektorin ilmasto-osaamista

- Hyökkäyksen kohde
  - Uhriksi voi joutua kuka tahansa esimerkiksi haitallisen verkkosivun tai haavoittuvuuksia etsivän skannauksen lopputuloksena
  - Hyökkääjää ei välttämättä kiinnosta yksittäiset maatilan tiedot, vaan verkkoon kytketyt laitteet ylipäänsä tai esimerkiksi tunnukset ja henkilötiedot
- Maatilaa koskevat samat verkon kyberuhat kuin ketä tahansa
- Maatilaympäristön ero taajaman yrityskiinteistöihin
  - Kosteat ja pölyiset tilat
  - Eläimet
  - Sähkökatkot
  - IT-ympäristö usein yrittäjän harteilla
  - Johtamiseen liittyviä tehtäviä hoidetaan usein muiden töiden ohella -> Kesken muun työn tullut haitallinen sähköposti tai tekstiviesti voi saada virheellisen reagoinnin aikaiseksi

Lähde: Kyberturvallisuus alkutuotannossa

# Maatilan kyberturvallisuus 2/2

KOMIO
Koulutusyhteistyöllä kohti parempaa maankäyttösektorin ilmasto-osaamista

- Tiedonkeruu
  - Anturiteknologiassa, samoin kuin kaikissa IoT-laitteissa on tärkeä huomioida laitteiden ajantasaisuus
  - Huolehdi kerätyn datan varmistamisesta
- Verkkoon kytkettävät laitteet ovat usein oletustietoturva-asetuksiltaan vaatimattomia. Vaihda laitteiden oletusasetukset!
- Varmista onko verkkoon kytkettävällä tiedonkeruulaitteella mahdollista käyttää tiedonsiirron salausta
- Varmista kriittisen automaation (lämmitys, jäähdytys, lypsyrobotti…) toiminta tai vaihtoehtoinen toimintapa häiriötilanteessa kuten sähkökatko tai palvelunestohyökkäys, joka on anturiteknologiassa yksi suurimmista riskeistä.
- Etähallittavat laitteet (esimerkiksi lämmitys, valaistus, kamera- tai kulunvalvonta)
  - Varmista, että hallintasovelluksen ja laitteen välinen tiedonsiirto tapahtuu suojatusti.
  - Anna pääsyoikeus vain niitä tarvitseville henkilöille.
  - Estä päättyneen työsuhteen jälkeen henkilön pääsy järjestelmiin.

# Miten tunnistaa huijaus? Pysähdy miettimään ja arvioimaan!

KOMIO
Koulutusyhteistyöllä kohti parempaa maankäyttösektorin ilmasto-osaamista

- Viestissä tiedustellaan luottokortti- tai henkilökohtaisia tietoja
- Viestissä on kirjoitusvirheitä tai outoja termejä, viestin ulkoasu ei muutoinkaan noudata ”oikean” lähettäjän tyyliä
- Viestiin vaaditaan reagoimaan nopeasti
- Tarjotaan epäilyttävän halpoja tuotteita
- Lähettäjän osoite on epämääräinen
- Nettiosoite ei vastaa mainitun yrityksen osoitetta
- Viesti on lähetetty esim. yöllä tai muuhun epätavalliseen aikaan
- Viestissä on outo, esimerkiksi kirjaimista ja numeroista koostuva, linkki
- Nettiosoitteen alku on muotoa ”http”, vaikka pitäisi olla suojatusta yhteydestä kertova ”https”
- Pyydetään lataamaan jokin ohjelmisto
- Ilmoitetaan paketista, jota ei ole tilattu

Lähde: Kyberturvallisuus alkutuotannossa

# Jos huijaus osui kohdallesi

KOMIO
Koulutusyhteistyöllä kohti parempaa maankäyttösektorin ilmasto-osaamista

- Vaihda salasana(t)
- Ole tarvittaessa yhteydessä pankkiin
- Tee rikosilmoitus [1]
- Ilmoita kyberturvallisuuskeskukselle [2]
- Jos epäilet tulleesi huijatuksi voit ottaa yhteyttä rikosuhripäivystykseen [3]
- Jos epäilet asentaneesi haittaohjelman:
  - Palauta laite tehdasasetuksiin
  - Jos palautat varmuuskopiota, varmista että se on ajalta ennen haittaohjelman asentamista
  - Jos kyseessä on SIM-kortillinen laite, ota yhteys operaattoriin. Liittymästä on voinut lähteä maksullisia viestejä

Lähde: Kyberturvallisuus alkutuotannossa

# Varautuminen

KOMIO
Koulutusyhteistyöllä kohti parempaa maankäyttösektorin ilmasto-osaamista

- Vaihda verkkolaitteiden (reititin ym.) oletusasetukset
  - Ylläpitäjän salasana
  - WiFi:n pääsykoodi
  - Jos tarvetta avoimelle verkolle, tee sitä varten vierailijaverkko
- Älä käytä tuotannon tietokonetta (esim. lypsyrobotin kone) muuhun kuin tuotannonohjaukseen
- Pidä tietokoneiden, mobiililaitteiden ym. päivitykset ajan tasalla
- Huolehdi, että virusohjelmat ovat ajan tasalla ja suorittavat tarkistukset säännöllisesti
- Luo tietokoneille käyttäjätunnukset sen eri käyttäjille
- Salasanat
  - Käytä vahvoja salasanoja
  - Älä käytä selaimen salasanojen tallentamista (automaattinen kirjautuminen)
  - Käytä salasanojen hallintasovellusta [4], kun kirjautumiskohteita on useita
- Varmuuskopiot säännöllisesti
  - Kaikista tuotannon sovelluksista
  - Käyttöjärjestelmän palautuspiste
  - Säilytä varmuuskopioita ainakin kahdessa sijainnissa, huomioi myös palo ym. Riski
- Varmista kriittisten laitteiden sähkön saanti, käytä vara-akku ja/tai varavirtalähdettä
- Järjestä tuotannon laitteille sopivat olosuhteet (kosteus, pöly…)

# Materiaalin tuotanto

KOMIO
Koulutusyhteistyöllä kohti parempaa maankäyttösektorin ilmasto-osaamista

*Materiaali on tuotettu KOMIO-hankkeessa, jossa koostetaan opintomateriaaleja ammattikorkeakoulujen luonnonvara-alan TKI-toiminnan, erityisesti Hiilestä kiinni -kokonaisuudesta rahoitettujen hankkeiden tuloksista. Hanke rahoitetaan Maa- ja metsätalousministeriön Hiilestä kiinni- maankäyttösektorin ilmastotoimenpidekokonaisuudesta ja sitä toteuttavat yhteistyössä Seinäjoen ammattikorkeakoulu SeAMK (projektin vetäjä), Hämeen ammattikorkeakoulu HAMK, Jyväskylän ammattikorkeakoulu Jamk, Kaakkois-Suomen ammattikorkeakoulu Xamk, Karelia-ammattikorkeakoulu, Lapin ammattikorkeakoulu Lapin AMK, Yrkeshögskolan Novia, Oulun ammattikorkeakoulu Oamk ja Savonia-ammattikorkeakoulu.*

# Materiaalin sisältämät linkit

1. Tee rikosilmoitus: https://poliisi.fi/tee-rikosilmoitus
2. Ilmoita kyberturvallisuuskeskukselle: https://www.kyberturvallisuuskeskus.fi/fi/ilmoita
3. Rikosuhripäivystys: https://www.riku.fi/palvelut/rikosuhripaivystys-116-006/
4. Salasanojen hallintasovellus: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon

# Lähteet

KOMIO
Koulutusyhteistyöllä kohti parempaa maankäyttösektorin ilmasto-osaamista


- Traficom – Kyberturvallisuuskeskus https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva (viitattu 23.11.2023)
- Tampereen yliopisto -kurssimateriaali https://plus.tuni.fi/comp.sec.100/fall-2021/m01_introduction/cybersecurity/?hl=fi (viitattu 23.11.2023)
- XAMK – Yksinyrittäjän ja mikroyrityksen Kyber- ja tietoturvaopas https://www.xamk.fi/tutkimus-ja-kehitys/kyberturvallisuuden-abc-yrittajille/ (viitattu 23.11.2023)
- Jamk, Suni ym. – Kyberturvallisuus alkutuotannossa – käsikirja https://urn.fi/URN:ISBN:978-951-830-677-4 (viitattu 23.11.2023)
- Poliisi, tee rikosilmoitus sivu: https://poliisi.fi/tee-rikosilmoitus (viitattu 23.11.2023)
- Kyberturvallisuuskeskuksen ilmoitussivu: https://www.kyberturvallisuuskeskus.fi/fi/ilmoita (viitattu 23.11.2023)
- Rikosuhripäivystys: https://www.riku.fi/palvelut/rikosuhripaivystys-116-006/ (viitattu 23.11.2023)
- Kyberturvallisuuskeskus – Ohjeita salasananhallintaohjelman käyttämiseen: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon (viitattu 24.11.2023)
- Jamk Suni ym. Kyberturvallisuus elintarviketeollisuudessa – käsikirja: https://urn.fi/URN:ISBN:978-951-830-679-8 (viitattu 24.11.2023)