MPK

MAANPUOLUSTUSKOULUTUSYHDISTYS
FÖRSVARSUTBILDNINGSFÖRENINGEN

Kyberturvallisuus maatiloilla

Maatalouden varautuminen - 2021

ILTALEHTI

liSa: Lypsyrobotti sai aikaan yli tonnin puhelinlaskun - soitteli viihdelinjoille

19.05.2015 klo 21:57

Maitotilan isäntä ja emäntä saivat yllättävän puhelinlaskun, kertoo lisalmen Sanomat.

Kiuruvetisen maitotilan pitäjät hämmästyivät perin pohjin tarkastellessaan puhelinlaskua, joka oli peräisin navetan lypsyrobotin ja isännän välisestä hälytyslinjasta. Tapauksesta uutisoi lisalmen Sanomat.

https://www.iltalehti.fi/uutiset/a/2015051919720798

MPK

Kyberin taskutieto maatiloille

Miksi maatiloilla tarvitaan kyberturvallisuutta?

- Maatilojen kasvanut teknisyys, digitalisaatio
- Tietojärjestelmät ovat maatilojen elinehto
- Laitteissa tietotekniikkaa ja internetyhteys
  - Altistuminen uhkille
- Arvokasta dataa
- Hankintojen pitkäaikaisuus
- Tuotannon tärkeys Suomen huoltovarmuudelle

Kyber- ja informaatioriskejä maatiloilla

- Säätilojen häiriöt, luonnonilmiöt
  - Sähkökatkot
  - Vesivahingot
  - Jyrsijät
- Inhimilliset virheet
  - Henkilöstön osaaminen
  - Tietojärjestelmien muutokset (tahalliset / tahattomat)
  - Pätevä alihankinta
- Puutteellinen suojaus
- Sosiaalinen media

Sähkön saanti ja sähköturvallisuus: kaikki riippuu sähköstä!

- Tietojärjestelmät vaativat laadukasta sähköä
- Huomioi sähkökatkot ja jännitevaihtelut
  - Varavirtalaitteet (UPS)
  - Monivaiheinen ylijännitesuoja
  - Sähköturvallisuusmääräyksistä apua myös kyberiin
- Kaapeloinnin merkitys
- Laitetilojen maadoitus
  - Sama potentiaalitaso muun laitteiston kanssa
- Sähköturvallisuustarkastuksessa tietoverkko mukaan
- Varavoimalaitteen oikea mitoittaminen
  - Polttoaineen tarve!

Tietoliikenne ja tietoverkot

- Suunnittelun keskiössä verkon saavutettavuus
- Verkkoliitännät siellä missä laitteetkin
- Rakennusten välinen riittävä putkitus
- Kuparikaapeliin vahvistin yli 100 m matkalle
- Valokuitu rakennusten välille suositeltavaa
- Verkon rakenteen dokumentointi
  - Osana sähkösuunnitelmaa
  - Langaton, langallinen, mobiili, kiinteä
  - Laitteiden ja koneiden sisäiset verkot ja väylät
- Muista palomuuri!

Tilan sisäiset ja ulkoiset järjestelmät

- Maatilan datan määrä huomioitava
- Data kiinnostaa myös ulkopuolisia
- Omistus- ja käyttöoikeuksien kunnioittaminen
- Luottamuksellisuus ja tietosuoja (GDPR)
- Älypuhelinten/tablettien liityntä verkkoon
- Verkkoliittymän vastuut
- Maatalouslaitevalmistajien tiedonkerääminen
- Rakennusautomaation verkon turvallisuuden varmistaminen

Miten varautua erilaisiin häiriöihin?

- Varautuminen
  - Häiriöiden vähentäminen = taloudellisen vahingon minimointi
- Vahinko ei tule kello kaulassa
  - Pohdi ja varaudu etukäteen
- Yksityiskohtaisen tarkistuslistan laatiminen
- Sähkökatkot, jännitehäiriöt
  - Linjojen hoito, varavoimakone, varavirtalähde, akut
  - Polttoaineen tilaus- ja toimitusmenettelyt
  - UPS-laite

Miten varautua erilaisiin häiriöihin?

- Kiinteäliittymä tietoverkossa on mobiilia varmempi
- Paikallinen tietojärjestelmä toimii kun pilveen ei saa yhteyttä
- Huomioi katkot myös sopimuksissa
  - Ulkopuoliset kumppanit ja palvelun tuottajat

Turvallinen tunnistautuminen ja hyvät salasanat

- Joka käyttäjälle ohjelmiin ja palveluihin oma:
  - Tunnus
  - Salasana
  - Tarvittavat oikeudet
- Erillinen järjestelmänvalvojan tunnus!
- Vahvat ja palvelukohtaiset salasanat
  - Yli 15 merkkiä
- Kaksivaiheinen tunnistus
  - Esimerkiksi puhelinvarmennus

Turvallinen tunnistautuminen ja hyvät salasanat

- Salasanoja ei saa tallentaa koneen tai selaimen muistiin
- Älä anna henkilökohtaista salasanaasi kenellekään
- Käytä salasanojen hallintaohjelmaa

Tiedon varmentaminen tuo turvallisuutta

- Varmentaminen vaatii suunnittelua
- Kolme kysymystä:
  - Millaista tietoa ja missä muodossa?
  - Mikä on tiedon arvo? Valokuva - kirjanpitoaineisto
  - Mikä on menetyksen uhkakuva? Rikkoutuminen - tietomurto
- Varmentaminen pilveen
  - Esim. kuluttajamallin älypuhelimet ja tabletit
- Tuotannon sovellusten ja palvelujen varmuuskopiointi toimittajan vastuulla
  - Vai onko? Mitä sanoo sopimus?

Tiedon varmentaminen tuo turvallisuutta

- Tuotantoautomaation tietojen palautuksen varmistaminen
- Säännöllinen kopiointi tikulle vai automaattinen verkkolevylle?
  - Muista seurata, tarkistaa ja koeponnistaa varmistettu tieto
- Palautusprosessin ennalta määrittely ja testaaminen
- Oleellista tietää missä mikäkin tieto sijaitsee
  - Onko käytettävissä jos verkkoyhteyttä ei ole?
- Tärkeitä kysymyksiä:
  - Oletko varmuuskopioinut tärkeät tietosi?
  - Osaatko palauttaa tiedot varmuuskopiosta?
  - Missä säilytät tärkeitä tietojasi?
  - Mitkä tiedot ovat pilvessä ja mitkä paikallisina?

Ovatko hankintasi kyberturvallisia?

- Hankinta alkaa tarpeen suunnittelulla
  - Olemassa olevilla järjestelmillä vaikutusta
  - Paikallinen? Henkilökohtainen? Tilan käyttöön?
- Isompien automaatiojärjestelmähankintojen kohdalla selvitä:
  - Paikallinen vai yhteensopiva jo hankittujen kanssa?
  - Huolto ja korjaus elinkaaren aikana sekä poikkeusoloissa
- Henkilökohtaisessa laitteessa käytettävyys ja yhteensopivuus ratkaisevat
- Tietojen jakamisessa oleellista on tietoturvallisuus
  - Kuka pääsee ja mihin tietoon?

Ovatko hankintasi kyberturvallisia?

- Tila kasvaa → kuluttajatuotteista yritystuotteisiin
  - Yritystuotteiden laajemmat takuut
- Hyödynnä asiantuntijoita hankinnoissa
  - Tiedon siirto vanhasta järjestelmästä uuteen
  - Asennukset
  - Käyttöoikeuksien määritys
  - Verkkoon liittyminen
  - Tietoturva ja varmuuskopiointi
- Tarkista säännöllisesti
  - Ns. vuosikello

Päivittäminen on paras turva

- Helpoin tapa ylläpitää kyberturvallisuutta on järjestelmien päivittäminen
- Uudet laitteet ja järjestelmät tarkistavat päivitysten saatavuutta automaattisesti
  - Vanhempien laitteiden kohdalla vastuu jää käyttäjälle
- Tietoteknisten laitteiden elinkaari 3-5 vuotta
- Varautuminen maksaa itsensä takaisin laiterikon sattuessa
- Palomuuria ei saa unohtaa
  - Rajaa mm. valvontakamerat sisäverkkoon

Maatilan 10 kyberkysymystä

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?

MPK

Kysymyksiä ja vastauksia

Mihin kysymykseen haluaisit kurssilla saada vastauksen?

- Jos kyberhyökkäyksellä saadaan tärkeät järjestelmät kuten pankkitoiminnot pois toiminnasta pidemmäksi ajaksi, onko mitään varajärjestelmiä?
  - Varajärjestelmistä vastaa palveluntuottaja itse
  - Vrt. palvelunestohyökkäykset suomalaisia pankkeja vastaan vuoden 2014 lopulla
    - https://yle.fi/uutiset/3-9258886
- Tilan oman tietokannan turvaaminen?
  - Kuten minkä tahansa yrityksen tietokannan toimenpiteet
    - Fyysinen pääsy, käyttäjätunnukset, yhteyksien suojaaminen, varmuuskopiot, palautussuunnitelma
- Mitä kaikkia asioita varautumisessa pitää muistaa ottaa huomioon?
  - Kyberin taskutieto maatiloille kertoo jo paljon.
  - Ylätasolla ainakin näitä asioita:
    - Ennakointi, suunnittelu, priorisointi, testaaminen, harjoittelu, palautuminen

Mihin kysymykseen haluaisit kurssilla saada vastauksen?

- Voiko lehmien putkilypsyjärjestelmän kautta ulkopuolinen salakuunnella
  - Vaatinee ”jalansijan” järjestelmässä
    - Jos laitteessa ei ole mikrofonia niin puhetta/ääntä ei.
    - Jos laite on kytketty verkkoon ja sinne on mahdollista asentaa sovelluksia niin tietoliikennettä kyllä
- Kuinka suuri kyberturvallisuusuhka langattomat laitteet (pad, laptop, puhelin) ovat?
  - Mikä laite? Miten suojattu? Onko päivitetty? Mitä laitteella voi tehdä? Kuka pääsee laitteelle? Mitä tietoja laitteella on? Mihin tietoon laitteella pääsee käsiksi?
- Miten suojautua Googlelta?
  - Lyhyesti: Ei käytä yrityksen palveluita
  - Pitkästi: Suojauskeinot riippuvat uhkamallista ja riskin sietokyvystä.
- Laitteiden internet ja laitteilta suojautuminen (esim. robotti-imuri).
  - IoT-laitteet omaan verkkoon ja hankinta vaiheessa valitsee tietoturvallisia laitteita

Mihin kysymykseen haluaisit kurssilla saada vastauksen?

- Verkkotiedustelun käytännön uhat
  - Tietovuodot: (yritys)salaisuudet, tunnukset, salasanat, maksutiedot, sopimukset
    - Mikä on uhkamalli maatiloille?
- Tietoturva
  - Peruselementit: luottamuksellisuus, eheys, saatavuus
  - Lisäelementit: kiistämättömyys, tunnistaminen, todentaminen, luvittaminen, kirjaaminen
- Mitä tehdä kun kyberhyökkäys on onnistunut esim. tilan tietokoneisiin?
  - Toimia palautumissuunnitelman mukaan.
    - Hyökkäyksen pysäyttäminen, vahingon rajaaminen/eristäminen, järjestelmän palauttaminen

Mihin kysymykseen haluaisit kurssilla saada vastauksen?

- Riittääkö tavalliset virusturvaohjelmat tilan tietojärjestelmän turvaamiseen?
  - Suojaaman haittaohjelmilta kyseisellä laitteella? Kyllä
  - Yksinään koko tilan turvaamiseen? Ei
- Miten suojautua kyberhyökkäyksiä vastaan?
  - Ennakoimalla, varautumalla, suunnittelemalla
  - Ei kytketä Internetiin laitteita, jotka eivät sinne kuulu ja joita ei ole kunnolla suojattu
  - Laittamalla tunnukset, salasanat ja pääsyoikeudet kuntoon
- Tietoliikenne
  - OSI-malli: https://fi.wikipedia.org/wiki/OSI-malli
    - (Open Systems Interconnection Reference Model)
  - Mikroaaltouuni ja Bluetooth voivat häiritä WLAN/WIFI-signaalia

Mihin kysymykseen haluaisit kurssilla saada vastauksen?

- Miten suojata oma lähiverkko ja laitteet.
  - Palomuuri, anti-virussovellus, verkon segmentointi, laitteiden ja sovellusten ”koventaminen”, varmuuskopiointi, pääsynhallinta
- Millaisen turvallisuusuhan internettiin kytkeytyvät laitteet voivat tulevaisuudessa muodostaa maatilojen näkökulmasta?
  - Lyhyesti: Jo nyt ovat suurehko ongelma. Esim. voidaan valjastaa palvelunestohyökkäyksiin
    - Esim. Mirai bottiverkko (https://en.wikipedia.org/wiki/Mirai_(malware))
- Miten turvallisuusuhkaan pitäisi varautua?
  - Riippuu pitkälti uhasta
    - Tietoturvalliset laitteet, laitteiden suojaaminen (palomuuri, segmentointi, koventaminen), tietoliikenteen ja sähkönsaannin varmistaminen

Mihin kysymykseen haluaisit kurssilla saada vastauksen?

- Miten entistä enemmän automatisoituvan maataloustuotannon tulisi varautua kyberturvallisuusriskeihin?
  - Yrittäjät: Tietoisuuden ja osaamisen kehittäminen
  - Maatalouskauppa: Sidosryhmien kanssa turvallisesti toimiminen
  - Teollisuus: Automaatio-osaajien pitää oppia tietotekniikkaosaajien virheistä
  - Järjestöt: Yhteistyö, tiedotus, osaamisen jakaminen, opastaminen
- Mikä nähdään maatilojen suurimpana haittavaikuttajana kyberympäristössä?
  - Esineiden Internet

Kiitos