

Kyberturvallisuuden vahvistaminen maatiloilla käytännön keinoin

Matti Saari

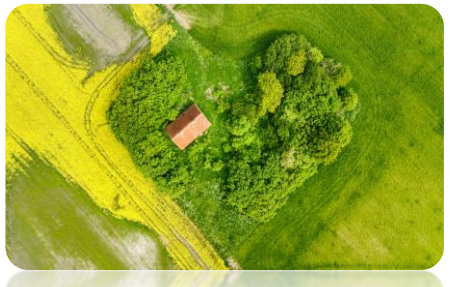
Seinäjoen ammattikorkeakoulu | Seinäjoki University of Applied Sciences

Mitä on kyberturvallisuus?

Kyberturvallisuus keskittyy tietojärjestelmien, tiedon ja laitteiden turvallisuuden takaamiseen **verkkoympäristöissä.** Kyberturvallisuus on tietoturvallisuuden yksi osa-alue. Tietoturvallisuus kattaa tiedon turvaamisen laajemmin.

Mistä maatilojen kyberturvallisuus koostuu?

Maatilojen kyberturvallisuus koostuu laajasta joukosta erilaisia osa-alueita. Aihetta käsitellään usein vain teknisestä näkökulmasta, mutta kokonaisuuteen nivoutuu paitsi **teknologia, myös henkilöstön osaaminen ja toimintatavat, organisaatiokulttuuri sekä kumppanuusverkoston toiminta.**



Miksi kybertuvallisuus on tärkeää maatiloilla?

- Maatiloilla käytetään nykyään monenlaisia automatisoituja järjestelmiä, kuten kotieläintuotannon etävalvontaa ja -hallintaa, automaattisia kastelujärjestelmiä sekä erilaisia IoT-pohjaisia laitteita.

  → laitteet ja järjestelmät voivat olla alttiita erilaisille kyberhyökkäyksille, kuten tietomurroille ja haittaohjelmille

  → kyberhyökkäykset saattavat aiheuttaa merkittävää vahinkoa tuotannolle: aiheuttaen erilaisia häiriöitä, taloudellisia tappioita ja maineen vahingoittumista, vaikuttaen koko ruokajärjestelmän huoltovarmuuteen

- Maatalous on usein erittäin **kausiluonteista** - **alkutuotannossa on kesäisin noin 16 000 kausityöntekijää**
  → näin suuri määrä kausityöntekijöitä aiheuttaa kyberuhan.



Miten kyberturvallisuutta voi itse parantaa – käytännön keinoja

1. Käyttäjätunnukset

Käyttäjätunnusten hallinnassa tulee käyttää **segmentointia,** eli välttää avaamasta kaikille täyttä pääsyä kaikkiin palveluihin, jos se ei ole tarpeen.
Jaettuja tunnuksia (kuten ”admin” tai ”ylläpito”) ei kannata käyttää, vaan jokaisella käyttäjällä tulee olla oma tunnus järjestelmään.

Perusmuotoiset salasanat ovat tietoturvariski ja kaikki vakiosalasanat tulee vaihtaa.
Tilien turvaaminen tulee tehdä turvallisilla salasanoilla ja monivaiheisella tunnistautumisella.

Monivaiheinen tai kaksivaiheinen (MFA tai 2FA) tunnistautuminen tarkoittaa sitä, että järjestelmä kysyy salasanan lisäksi tunnistautumista jollain toisella tavalla – esimerkiksi tekstiviestikoodilla tai mobiilisovelluksella. Näin pelkällä salasanalla ei voi kirjautua järjestelmään.

2. Salasanat

Samaa salasanaa ei tule käyttää useaan paikkaan. Salasana on vain niin turvassa kuin heikoin paikka, jossa sitä on käytetty.

Laitteiden tehdasasetusten vakiosalasanat ovat yleisesti tiedossa, joten niiden vaihtaminen on erityisen tärkeää.

Käyttäjillä tulisi olla **henkilökohtaiset salasanat eri palveluihin, eikä yhtä yhteistä salasanaa.**

Salasana on sitä turvallisempi mitä pidempi se on. Hyvä salasana voi olla pitkä erikoismerkkejä sisältävä **salalause,** joka on helppo itse muistaa, esimerkiksi: KeltainenPuimuriPellolla_2065

Monen eri salasanan muistaminen on käytännössä hankalaa.
Yksi hyvä vaihtoehto on käyttää **salasanojen hallintasovelluksia, esimerkiksi Bitwarden ja NordPass -ohjelmat.**

→ Salasanojen hallintatyökalu vaatii yhden salasanan muistamisen – ohjelma muistaa loput salasanat.

3. Päivitykset

Suurin osa tietokoneista ja älypuhelimista päivittää itsensä automaattisesti, kunhan varmistaa että **päivitysten haku on päällä.**

Erityistä huomiota tulee kiinnittää **laitteistoihin, palvelimiin ja erityisohjelmiin, sillä niiden päivityksistä saattaa joutua huolehtimaan itse.**

Mikäli päivitettäviä laitteita ja ohjelmia on suuri määrä, kannattaa miettiä **ohjelmistorekisterin** perustamista → lista käytössä olevista **laitteista, niiden käyttäjistä ja viimeisimmästä päivityspäivämäärästä.**

Mikäli laitteelle **ei enää ole valmistajan tukea eikä sille tehdä tietoturvapäivityksiä, on vain ajan kysymys, milloin se lakkaa olemasta turvallinen**. Tällainen laite kannattaa korvata uudemmalla tai vähintään eristää verkosta.

Työkoneilta kannattaa poistaa kaikki tarpeettomat ohjelmistot - mitä enemmän ohjelmia on koneella, sitä enemmän on myös tietomurtomahdollisuuksia.

4. Varmuuskopiointi

Yleisohje: säilytä kaikki tieto vähintään kahdessa paikassa.

Liiketoimintakriittisen tiedon tallennuksessa kannattaa käyttää 3-2-1-sääntöä
Tee tiedosta kolme kopiota, kahdelle erityyppiselle medialle (DVD, kovalevy, pilvi), joista yksi on fyysisesti eri paikassa kuin muut.
Huom! Varmuuskopiot tulee myös salata

Joissakin tapauksissa (esim. suuri datamäärä, josta vain osa muuttuu) kannattaa varmuuskopioida vain ne tiedostot tai tiedostojen muutokset, jotka ovat tapahtuneet edellisen varmuuskopioinnin jälkeen.

Yleisesti suositellaan säilyttämään **vähintään 3–7 varmuuskopioversiota**
→ antaa riittävän puskurin mahdollisia virheitä ja vioittuneita tietoja vastaan.

Testaa tietojen palautus varmuuskopioista!

5. Antivirusohjelma / Palomuuri

Antivirus- ja palomuuriohjelmat ovat tarpeellisia työkaluja tietokoneen turvaamiseksi, mutta ne **eivät vielä varmista tietoturvaa kokonaisuutena.**

Ohjelmien käytön lisäksi on tärkeää **olla avaamatta tiedostoja, jotka eivät ole tulleet luotettavista lähteistä.**

Ajankohtaista tietoa viruksista ja haavoittuvuuksista löytyy Traficomin kyberturvallisuuskeskuksen verkkosivuilta**: www.kyberturvallisuuskeskus.fi**

6. Tietojen kalasteluyritykset (phishing)

Nykyisin ei enää pysty erottamaan ulkonäön perusteella väärää sisäänkirjautumissivua oikeasta. Selaimen osoitekentän vasemmalla puolella on yleensä **lukon kuva,** joka tarkoittaa, että yhteys avatulle sivulle on salattu, eli tietoja ei pysty helposti lukemaan välistä.
Se ei kuitenkaan tarkoita, että sivun sisältö olisi luotettava.

Etenkin **verkkopankki kannattaa avata kirjoittamalla osoite itse selaimen osoiteriville ja tallettaa se kirjanmerkkeihin** + kirjautua verkkopankkiin jatkossa kirjanmerkin kautta**.**

Pankkitunnusten lisäksi **erilaiset sosiaalisen median tunnukset ja sähköpostitilit kannattaa suojata hyvin**. Identiteettivarkaus voi johtaa maineen menetykseen, ja yrityksen virallista sähköpostia voidaan käyttää eteenpäin asiakkaiden tai yrityskumppanien huijaamiseen.

Sähköpostilinkkien kanssa tulisi toimia varoen. Linkit saattavat ohjata käyttäjän esimerkiksi väärennetylle sivustolle.

Kalastelua tapahtuu nykyisin myös muilla tavoin, kuten **puhelimen välityksellä.** Esimerkkinä ”Avulias asiakaspalvelija” yrityksestä X soittaa ja pyytää kohdetta kirjatumaan tunnuksillaan verkkosivulle, joka on väärennetty → tunnukset hyökkääjälle.

Tekstiviestihuijaukset ovat tekstiviestejä, joiden lähettäjätieto on yleensä väärennetty esimerkiksi samaksi kuin pankki tai posti**.** Viesti sisältää linkin, jota klikkaamalla käyttäjä päätyy huijaussivustolle.

Eri tilanteisiin on hyvä olla ohjeistus siitä, miten viestijän henkilöllisyys todennetaan ja mitä kautta palveluihin kirjaudutaan sisään.

7. Fyysinen turvallisuus

Fyysinen turvallisuus on tarkalleen ottaen osa yleistä tietoturvaa, mutta se on hyvä linkittää myös kyberturvaan.

Erilaisiin fyysisen maailman uhkiin voi varautua monella tasolla – **(sähkö)lukot, kulunvalvonta, vartiointi ja ohjeistus siitä mitä tavaroita saa ja ei saa jättää valvomatta, tietojen salaus ja varmuuskopiointi.**

Kuten kyberturvassa yleisesti, fyysisessä turvassakin **tärkein näkökulma on riskien pienentäminen:**

- älä jätä sensitiivisiä papereita tai IT-laitteita sinne tänne
- mieti kuinka avoin pääsy on tarpeellinen eri tiloihin
- miten varkauksiin tai pahantahtoisiin toimijoihin varaudutaan
- kuinka tarkka turvallisuus tunnistettujen riskien valossa riittää

SEAMK
Seinäjoen ammattikorkeakoulu
Seinäjoki University of Applied Sciences

8. Massamuistit, kovalevyt ja usb-tikut

Suojaamattomissa laitteissa olleita massamuisteja tai löydettyjä usb-tikkuja ei tule käyttää. Saattavat saastuttaa oman laitteen / koko verkon.

9. Sähkön saanti

Sähkön saannin turvaaminen on keskeistä kyberturvallisuudessa, sillä tietoverkkojen, tietojärjestelmien ja erilaisten laitteiden toiminta perustuu sähkön jatkuvaan saatavuuteen.

Sähkön saannin varmistamisessa voidaan käyttää **automatisoituja varavoimajärjestelmiä ja UPS-laitteita (**UPS, Uninterruptible Power Supply).

Vinkkejä kyberturvallisempaan arkeen

1.) Turha kiire pois

- Valtaosa virheistä tulee kiireessä
  – tutkimusten mukaan n. 95 % ongelmista aiheutetaan omalla toiminnalla.

  → Verkkorikolliset käyttävät hyväkseen hyvin usein uhkailua ja kiirettä.
  Esim. verkkohuijarit voivat väittää, että tilisi lukitaan, jos et toimi välittömästi tai käytetään erilaisia ”toimi heti” tarjouksia.

- Kun tunnistat vaaran paikan, **pidä tauko ja mieti hetki mitä olet tekemässä ja miksi kyseitä asiaa pitää tehdä.** Vaaran paikka on esimerkiksi käyttäjätunnusten tai pankkitunnusten antaminen, kirjoittaminen verkkosivuille tai linkin klikkaaminen.

2.) Aina kun syötät tietojasi nettisivulle tai palveluun, pysähdy ja mieti miksi olet päätynyt kyseiseen tilanteeseen ja kuka prosessin käynnisti.

- Jos itse on käynnistänyt prosessin, sen on todennäköisesti turvallista, mutta ole silti varovainen!

- Jos sinut on ohjattu tekstiviestillä, pikaviestillä, somessa, sähköpostilla, nettisivuilta, jne. jonnekin satunnaiselle sivulle, ei kannata syöttää omia tietoja ellei ole 100 % varma, että sivusto on turvallinen.

3.) Keskustele perheen, ystävien ja työkavereiden kanssa kyberturvallisuudesta ja jaa omia hyviä kokemuksia ja toimintatapoja sekä havaitsemiasi uhkia.

Euroopan unionin osarahoittama

FarmGuard

SEAMK
Seinäjoen ammattikorkeakoulu
Seinäjoki University of Applied Sciences

jamk | Jyväskylän ammattikorkeakoulu

Huoltovarmuusorganisaatio
Försörjningsberedskapsorganisationen
National Emergency Supply Organisation

FarmGuard-hanke

Maatilojen ja puutarhojen kyberturvallisuuden vahvistaminen käytännön keinoin

Euroopan unionin osarahoittama

FarmGuard

SEAMK Seinäjoen ammattikorkeakoulu Seinäjoki University of Applied Sciences

jamk Jyväskylän ammattikorkeakoulu

Huoltovarmuusorganisaatio
Försörjningsberedskapsorganisationen
National Emergency Supply Organisation

Hankkeen toteuttajat ja toteutusaika

- Hankkeen päätoteuttajana ja koordinaattorina toimii Seinäjoen Ammattikorkeakoulu
- Osatoteuttajana Jyväskylän Ammattikorkeakoulu
- Huoltovarmuusorganisaation Alkutuotantopooli toimii kumppanina ja konsultoi työpakettien tehtäviä
- LähiTapiola, Maitosuomi, A-Tuottajat, ProAgria, Kauppapuutarhaliitto ry, Hämeen Ammattikorkeakoulu/Lepaan kampus, Keski-Pohjanmaan koulutusyhtymä, Pohjoisen Keski-Suomen ammattiopisto/Tarvaala, Jokilaaksojen koulutuskuntayhtymä/Haapajärvi, Keski-Uudenmaan koulutuskuntayhtymä/Saaren kartano, Mäntsälä, Ojanperän tila/Ilmajoki
- Toteutusaika: 1.9.2024-31.8.2026

Euroopan unionin osarahoittama

FarmGuard

SEAMK Seinäjoen ammattikorkeakoulu Seinäjoki University of Applied Sciences

jamk Jyväskylän ammattikorkeakoulu

Huoltovarmuusorganisaatio
Försörjningsberedskapsorganisationen
National Emergency Supply Organisation

Hankkeen tavoite

- Tavoitteena on **vahvistaa maatilojen ja puutarhojen kykyä varautua kyberuhkiin ja lisätä niiden resilienssiä.**
- Hankkeessa toteutetaan kuusi kokeilua hyödyntäen opetustiloja eri alueilla.
  - Näin saadut kokemukset ja hyvät käytänteet dokumentoidaan ja viestitään maatila- ja puutarhayrittäjille.
  - Hankkeessa tuotettavia aineistoja käytetään myös agrologien koulutusmateriaalien laatimisessa ja tuloksia hyödynnetään TKI-toiminnassa.
- Lisäksi hankkeessa luodaan jatkuvan kehittämisen malli kyberturvallisuuden ylläpitoon ja kehittämiseen maatiloilla ja puutarhoilla.
- Hankkeen avulla alan toimijat voivat verkostoitua ja hankkeen kokemukset jalkautetaan hyödyntäen eri sidosryhmiä sekä AgriHubi-foorumia.

Euroopan unionin osarahoittama

FarmGuard

SEAMK Seinäjoen ammattikorkeakoulu Seinäjoki University of Applied Sciences

jamk Jyväskylän ammattikorkeakoulu

Huoltovarmuusorganisaatio
Försörjningsberedskapsorganisationen
National Emergency Supply Organisation

Tulokset

- Kuusi dokumentoitua esimerkkitapausta maatilan tai puutarhan kyberturvallisuuden parantamisesta, kyberuhka-arvio ja koulutus.
- Arvioinneista saatavat kyberturvalliset toimintatavat ja hyvät käytänteet jalkautetaan maatiloille ja puutarhoille, teoriasta käytäntöön.
- Jatkuvan kehittämisen malli kyberturvallisuuden kehittämiseen.
- Opetusmateriaalia ja ohjeistuksia.

Lisätietoja

- Matti Saari/SeAMK, matti.saari@seamk.fi, puh. 040 6807544
- Jyrki Kataja/JAMK, jyrki.kataja@jamk.fi, puh. 040 5661034

- https://projektit.seamk.fi/farmguard



Euroopan unionin osarahoittama

FarmGuard

SEAMK
Seinäjoen ammattikorkeakoulu
Seinäjoki University of Applied Sciences

jamk | Jyväskylän ammattikorkeakoulu

Huoltovarmuusorganisaatio
Försörjningsberedskapsorganisationen
National Emergency Supply Organisation

KIITOS!

Kysymyksiä - kommentteja