

Lounea



ProAgria – Varautumisen aamukahvit.

18.2.2026

Markku Ylitalo / Lounea Yritysratkaisut Oy

Agenda

- Yritys- ja henkilöesittely.
- Kyberturvan ajankohtaiset asiat.
- Yleisimmät uhat maataloilla.
- Käytännön vinkkejä kyberturvaamiseen.
- Lounea Yritysratkaisut Oy:n palveluvalikoima.
- Kysymyksiä ja vapaata keskustelua





Lounean liiketoimintarakenne

LOUNEA OY

Kiinteistöt ja
sijoitustoiminta

LOUNEA NET OY

Konsernipalvelut:
talous, tietohallinto
ja HR

LOUNEA PALVELUT OY

Kuluttaja- ja operaattori-asiakasliiketoiminta,
mastoliiketoiminta

LOUNEA YRITYSRATKAISUT OY

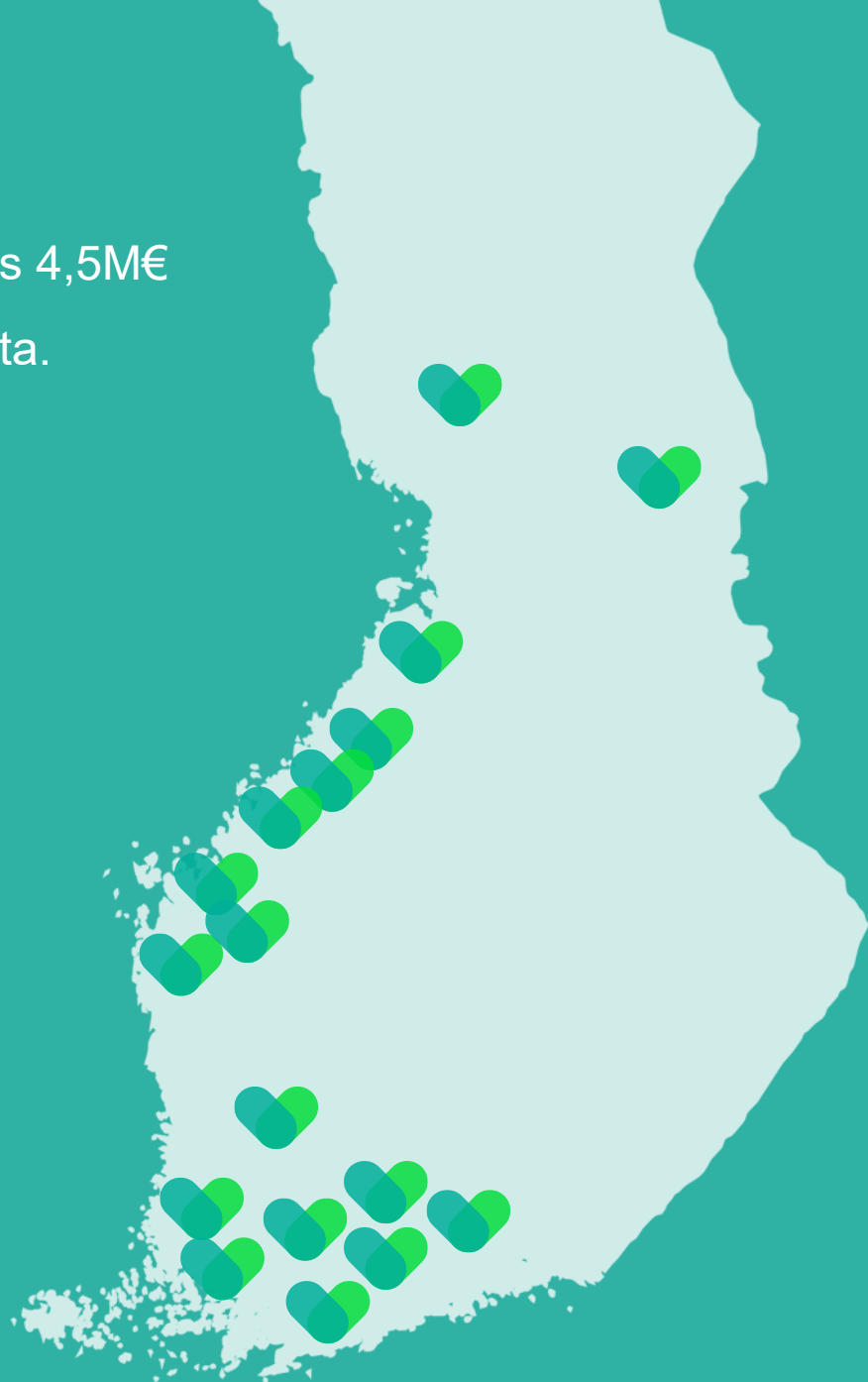
Yritysasiakasliiketoiminta

Lounea Yritysratkaisut Oy

- Liikevaihto 2024: 41 M €. Koko konserni 72,7M€ → tilikauden tulos 4,5M€
- Koostuu kahdesta liiketoiminnasta, valokuidusta ja ICT -ratkaisuista.
- Useita toimipisteitä ja noin 130 asiantuntijaa ympäri Suomea.
- Kotimaisessa omistuksessa oleva yli 130-vuotias yhtiö.
- Asiakastukemme palvelee 24/7.

Markku Ylitalo

- Yli 20 –vuoden kokemus IT –alalta useista eri rooleista.
- Nykyinen tehtävä: Kehityspäällikkö – Cyber & Cloud tiimin vetäjä.
- Todellisuudessa: Puhuva pää 😊



Iso 14001 ympäristösertifikaatti



- Lounea Yritysratkaisut Oy:lle on myönnetty ISO 14001 -ympäristösertifikaatti osoituksena panostuksesta kestävä kehityksen puolesta.
- ISO 14001 on maailman tunnetuin ympäristöjärjestelmän rakentamisen ja kehittämisen standardi, joka auttaa parantamaan ympäristöasioiden hallintaa ja ympäristönsuojelutoimien tuloksellisuutta organisaatioissa. Saamamme sertifikaatti todistaa, että ympäristöjärjestelmämme täyttää kaikki ISO 14001:2015 -standardin asettamat vaatimukset.
- ISO 14001 -standardin vaatimukset edellyttävät esimerkiksi, että tunnistamme toimintaamme liittyvät ympäristönäkökohdat, riskit ja mahdollisuudet sekä asetamme päämäärät ja tavoitteet ympäristönäkökohtien parantamiseksi. Me myös sitoudumme jatkuvaan parantamiseen sekä vastuulliseen toimintaan huolehtimalla, että täytämme meitä sitovat velvoitteet.



ISO/IEC 27001 tietoturvasertifikaatti



- Lounealla on ISO/IEC 27001 -tietoturvasertifikaatti, joka kattaa koko Lounea-konsernin toiminnan. Sertifikaatti vahvistaa, että tietoturvan hallintamme täyttää kansainvälisen standardin vaatimukset ja että toimintamme perustuu järjestelmälliseen riskienhallintaan, selkeisiin toimintamalleihin ja jatkuvaan kehittämiseen.
- Kyseessä on kansainvälisesti arvostettu standardi, joka osoittaa, että Lounealla on korkeatasoinen ja yhtenäinen tietoturvan hallintamalli. Sertifiointi vahvistaa myös Lounean valmiudet täyttää NIS2-direktiivin edellyttämät vaatimukset — erityisesti riskienhallinnan, prosessien dokumentoinnin ja toimintavarmuuden osalta.
- Tietoturva on olennainen osa Lounean vastuullisuusohjelmaa, jonka tavoitteena on varmistaa turvallinen, luotettava ja kestävä digi-infra suomalaisen yhteiskunnan tarpeisiin. Sertifiointi tukee missiotamme *muuttaa tapaa, jolla yhteiskunta toimii digitaalisessa maailmassa* — turvallisesti ja pitkäjänteisesti.
- Lounealla toimimme arvojemme mukaisesti: kohtaamme, välitämme ja toimimme. Nämä arvot näkyvät konkreettisesti myös tietoturvassa: kohtaamme asiakkaamme avoimesti, välitämme heidän tietoturvastaan ja toimimme läpinäkyvästi sekä standardien mukaan. ISO 27001 -sertifikaatti on lupaus siitä, että panostamme vastuulliseen, turvalliseen ja laadukkaaseen palveluun nyt ja jatkossa.

Lounea



Kyberturvan ajankohtaiset asiat.

- **0-päivähaavoittuvuudet ja kriittiset tietoturvapäivitykset.**
 - Uusia haavoittuvuuksia löydetään kokoajan joista ei vielä ole julkisesti tietoa esim. Valtori
 - Vanhat päivittämättömät laitteet joita hyväksikäytetään.
- **Ransomware –hyökkäysten kasvu**
 - Vuonna 2025 kasvu oli 52%.
 - OAPT –ryhmällä 144 uutta uhria 30pv aikana
- **AI –roolin kasvu hyökkäyksissä ja AI –käyttö normaalissa työssä.**
 - AI:lla tuotetut haittaohjelmat.
 - Organisaatioiden käyttämät AI –agentit lisäävät tietovuotoriskiä.
- **Geopoliittiset jännitteet ja kybersota**
 - Kyberhyökkäykset ovat yhä tiiviimmin sidoksissa geopoliittisiin kriiseihin ja valtioiden välisiin jänniteisiin.
 - Esim. Venäläisten operaatiot eurooppalaisiin energiasektorreihin ja valtionhallintoihin.
- **Resurssipula**
 - Säästöt henkilö- ja teknologiaresursseista heikentävät mahdollisuutta reagoida uhkiin.



Kyberturva ajankohtaiset asiat.

NIS2:

Uusi kyberturvallisuuslaki (124/2025), joka toimeenpani EU:n kyberturvallisuusdirektiivin (NIS2), astui voimaan Suomessa 8.4.2025. Laki asettaa erityisesti kriittisten toimialojen toimijoille **seuraavat velvoitteet**:

- Riskienhallinta
- Poikkeamien raportointi
- Toimijaluetteloon ilmoittautuminen
- Valvonta ja seuraamukset
- Dokumentointi
- Testaus
- Koulutukset
- Johdon vastuu
- Tarvittavat teknologiset ratkaisut



Kyberturvan ajankohtaiset asiat by Copilot.

🌟 Yhteenveto: Miltä maatilojen kybervuosi 2026 näyttää?

Ennustettu uhka	Kasvunopeus	Vaikutus maataloille
Ransomware-hyökkäykset	🔴 Erittäin korkea	Tuotannon seisaus, datan menetykset, palvelukatkot
IoT- ja laitehyökkäykset	🟡 Korkea	Automaation lamautuminen, valvontajärjestelmien häiriöt
AI-avusteiset hyökkäykset	🟡 Korkea	Huijausviestit, kehittyneet haittaohjelmat
Toimitusketjuhyökkäykset	🟡 Korkea	Epäsuorat häiriöt, palvelutoimittajien katkot
Geopoliittiset vaikutukset	🟡 Kasvava	Häiriöt infrastruktuureissa ja logistiikassa
Massahyökkäysten määrä	🟡 Tasainen kasvu	Lisää opportunistisia hyökkäyksiä tiloihin

✓ Johtopäätös

Vuonna 2026 maatalouden kyberuhat **kasvavat selvästi**, sekä määrällisesti että laadullisesti. Keskeiset syyt ovat:

- Ransomware-toiminnan tehostuminen ja uusien toimijoiden nousu
- IoT-laitteiden nopea yleistyminen
- AI:n tuoma hyökkäysten skaalautuvuus
- Toimitusketjujen haavoittuvuus
- Geopoliittisen kybertoiminnan lisääntyminen

Maatilojen onkin siirryttävä reaktiivisesta suojautumisesta **ennakoivaan kyberturvamalliin**, jossa keskiössä ovat päivitykset, IoT-verkkojen turvaaminen, kumppaniverkoston hallinta ja toimintasuunnitelmat häiriötilanteisiin.



Kyberturvan ajankohtaiset asiat by Copilot.

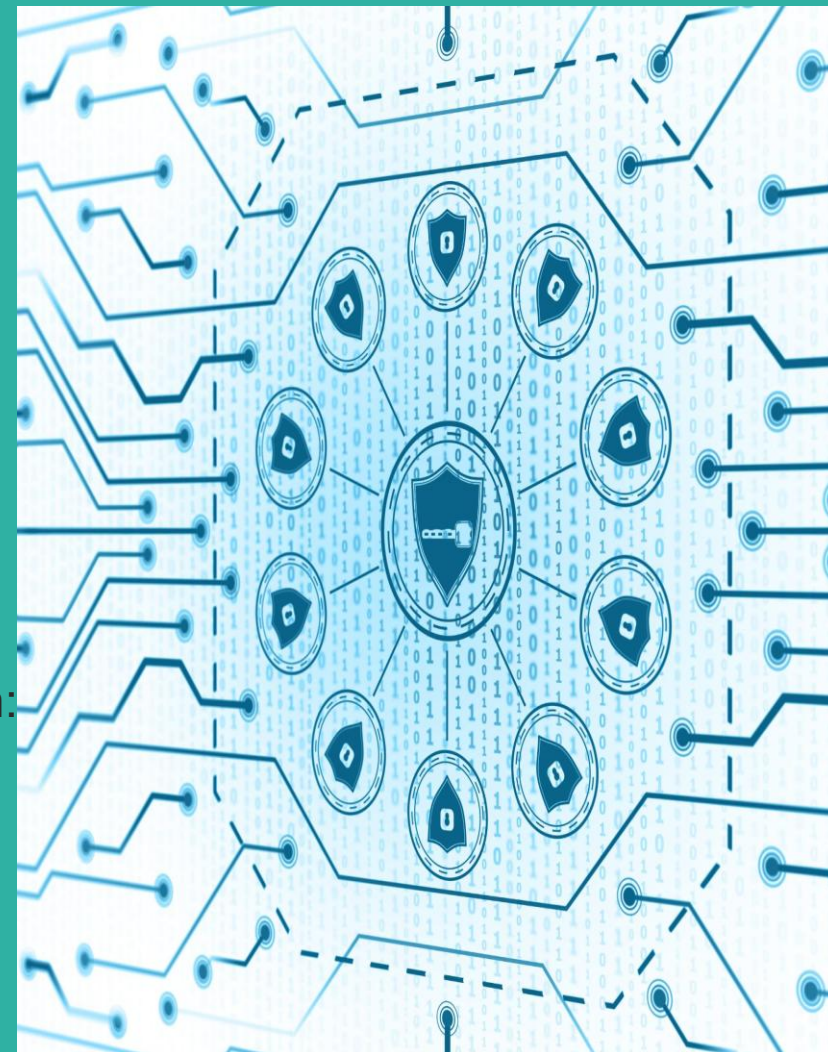
2) Kvantitatiivinen ennuste (Suomi: alkutuotanto, 2026)

Alla olevat arviot yhdistävät kansainvälistä trendidataa (hyökkäyskertymä, taktiikoiden muutos) maatalouden digitalisaatioasteeseen. Perustelut viittaavat mm. ransomware-volyymien kasvuun 2025→2026, "unmonitored devices" - ilmiöön sekä nollapäivien aktiiviseen hyväksikäyttöön. [techrepublic +3](#)

Riskikategoria	Todennäköisyys 2026	Odotettu muutos vs. 2025	Tyypillinen vaikutus
Ransomware/tuotannonohjaus	Korkea	+20–40 % tapausmäärissä	1–7 vrk seisokkiriski, tiedostojen salaus ja/tai tietojen vuoto
IoT-/reunalaitteiden väärinkäyttö	Korkea	+25–50 %	Sensoridatan luotettavuuden heikentyminen, automaattihäiriöt
Sähköposti-/viestintähuijaukset (AI-avusteiset)	Korkea	+30–60 %	Väärät tilitiedot, laskutushuijaukset, tunnusten kalastelu
Toimitusketju-incidentit (palvelu-/ohjelmistotoimittaja)	Keskikorkea→Korkea	+20–30 %	Maksu- tai logistiikkakatkäpäivityksen kautta leviävä haitakkeet
Mobiililaitteiden hyväksikäyttö	Keskikorkea	+10–20 %	Pääsyoikeuksien kaappausivukanavareitti muihin järjestelmiin

Yleisimmät kyberuhat maataloilla.

- Laitteet näkyvät Internetiin:
 - Esim. voidaan hyökätä ja kuormittaa ”Mansikin lypsyrobotia”.
 - Varastetaan ja tuhotaan jalostus- ja tuotantotiedot.
 - Kuormitetaan kuivaajaa: sammutus, ylikierrokset jne.
 - Häiritään vedenottoa porakaivoista.
- Sähkökatkoista johtuvat laite- ja ohjelmistorikot:
 - Tiedot korruptoituvat ja prosessit menevät sekaisin.
- Tahallinen järjestelmän väärinkäyttö:
 - Tahallinen tietojen muuttaminen, tuhoaminen varastaminen:
 - Antibioottiannostelu.
 - Eläintietojen muutos ruokinnan suhteen.
 - Kirjanpito.
- Käytetään haavoittuvia laitteita hyökkäykseen jotain muuta tahoa vastaan:
 - DDoS
- Vaikuttaminen / Toimitusketju:
 - Painostus tekemään jotain laitonta tai ohjata haluttuun päätökseen.
 - Kiristys.



Käytännön vinkkejä kyberturvallisuuden parantamiseksi

- Suojataan Internet –yhteys palomuurilla.
 - Verkon segmentointi.
 - Kotiverkko ja tuotantoverkko omanaan.
- Ohjelmistojen ja laitteiden päivityksistä huolehtiminen.
- IoT –laitteiden hallinta.
 - Vaihda oletussalasanat.
 - Laita laitteet omaan verkkoon.
- Kontrolloidaan ja vakioidaan etäyhteystavat ulkopuolisille toimijoille.
- Suojataan työasemat teknologialla jolla on kyky havaita ja reagoida poikkeamiin.
- Säännölliset tietoturvakannaukset verkkoon.
- Dokumentointi kaikista laitteista, ohjelmistoista, kumppaneista ja käyttäjistä.
- Kouluttautuminen.
- Velvoitta sidosryhmät toimimaan samalla tavalla.
- Varmuuskopiointi tärkeistä tiedoista.
- Suunnittele ja harjoittele kyberturvapoikkeamasta selviytymistä.
- UPSit takaamaan häiriötöntä sähköä ja virransyöttöä akkujen avulla.
- Selainten lisäosat. Minimoikaa käyttö ja ei salasanan tallennuksia selaimiin.

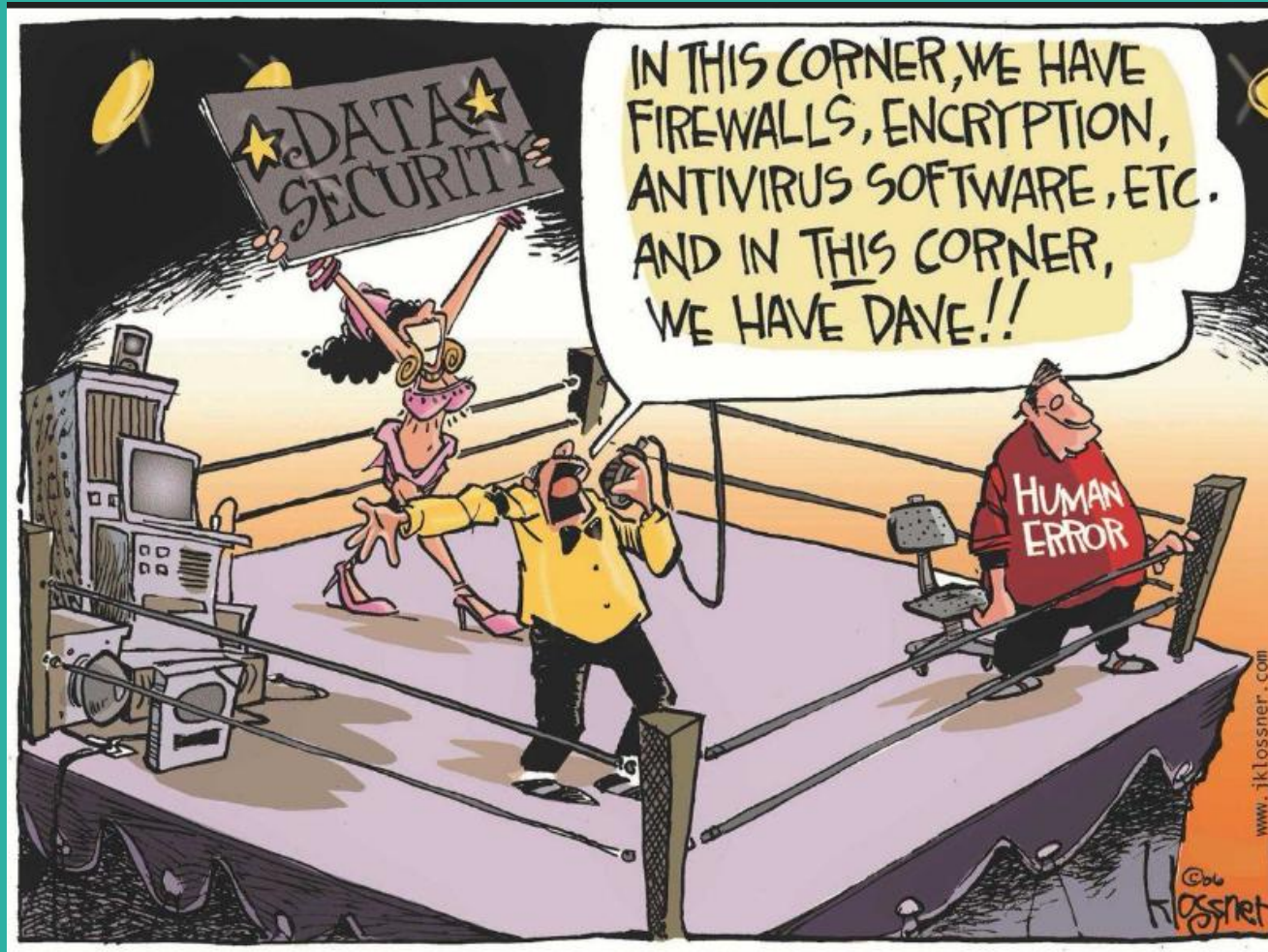


Käytännön vinkkejä kyberturvallisuuden parantamiseksi

- Ennakoi, estä, havaitse, reagoi.
 - Ennakoidaan ja arvioidaan mahdolliset kyberturvauhat:
 - Pääsynhallinta.
 - Laitteet.
 - Ohjelmistot.
 - Ulkopuoliset tahot.
 - Suojausteknologiat:
 - Palomuurit
 - Virustorjunta
 - Vahva tunnistautuminen
 - Havainnointikyky:
 - Jatkuva seuranta.
 - Logi –tiedot.
 - Reagointikyky.
 - Torjuminen.
 - Palautuminen.
 - Tiedottaminen.
 - Puutteiden korjaaminen.



Käytännön vinkkejä kyberturvallisuuden parantamiseksi



Lounea

YRITYSRATKAISUT

Palvelut yrityksille



Yhteydet

- ✓ Yritysyhteydet valokuidussa
- ✓ Yritysverkotukset
- ✓ Yritysmobiilikaistat
- ✓ Lähiverkkopalvelut
- ✓ Kytkin ja WLAN-palvelut
- ✓ Palomuuripalvelut
- ✓ Etätyöyhteydet



Viestintä

- ✓ Puhelinliittymät
- ✓ Viestintäratkaisut
- ✓ Lounea Mobiililiittymät
- ✓ Palvelu- ja yritysnumerot
- ✓ Web-palvelut
- ✓ Infonäytöt



Tietoturva

- ✓ Tietoturvapalvelut
- ✓ Pilvipalvelusuojuukset
- ✓ Päätelaitesuojaus
- ✓ Levynsalauspalvelu
- ✓ Varmistuspalvelut – ja palautuspalvelut
- ✓ Tietoturvakoulutukset
- ✓ Tietoturvatestaus



Ohjelmistot

- ✓ Microsoft 365 ohjelmistot
- ✓ Azure ja Sharepoint
- ✓ Muut Microsoft-lisenssit, SPLA
- ✓ Toiminnanohjaus
- ✓ Asiakkuudenhallinta
- ✓ Työajanseuranta
- ✓ Sähköinen allekirjoitus
- ✓ Integraatiot, raportointi, automatisointi



Tulostus- ratkaisut

- ✓ Toimistotulostaminen
- ✓ Suurkuvatulostus
- ✓ Tarra- ja etikettitulostaminen
- ✓ Tietoturvatulostus
- ✓ Tiedonhallintapalvelut
- ✓ Huolto- ja ylläpitopalvelut



Laitteet ja alustat

- ✓ IT-laitteet ja tarvikkeet
- ✓ Laitteiden elinkaaripalvelu
- ✓ Kierrätetyt laitteet palveluna
- ✓ Maksupäätteet
- ✓ Laitehallintapalvelut
- ✓ Konesalipalvelut
- ✓ Virtuaalipalvelimet
- ✓ Palvelinverkot



Asiantuntija- palvelut

- ✓ IT-tukipalvelut lähitukena
- ✓ IT-tukipalvelut etänä
- ✓ IT- ulkoistukset
- ✓ Asennus ja käyttöönottotyöt
- ✓ Koulutuspalvelut toimistosovelluksille

Lounea

Kysyttävää?

Miten ja minne käytöstä poistetut kännykät ja tietokoneet toimitetaan?

Kiitos.



Lounea