

Kyberturvallisuus 2025

Niko Candelin

"What comes to cybersecurity, you can only fail two ways, either you missed to identify the risk or opportunity and your time to exploit it."

- Chief Research Officer, Co-Founder, Netox
- Chairman of the Board, Finnish Information Security Cluster, FISC
- Vice Chairman, SOC / DFIR- ISAC, NCSC-FI
- Mentor, Defence Innovation Accelerator for the North Atlantic, NATO
- Member of Steering Group, Cyber Citizen, Aalto University / LVM



eMBA, CISM, CBM/C,
Management, University of Oulu
Cyber Risk Management, Harvard
Artificial Intelligence, MIT

TOTTA

- Maailman toiseksi vai kolmanneksi suurin kansantalous?
 - Suurin lyhyen aikavälin riski globaalisti (WEF 2025)
 - Monimutkainen (fyysinen, tekninen, kognitiivinen)
- 90 % tietomurroista johtuu inhimillisistä tekijöistä.
- Tekoälyn käyttö
- 100 % riskienhallintaa
- Johdon vastuu on aina olemassa



EI TOTTA

- Me ei olla kiinnostava kohde
- Vastuu voidaan ulkoistaa
- Meillä on kaikki kunnossa
- NIS2 suhtaudutaan kuin GDPR
- Vaatimustenmukaisuus riittää
- Ei voida tietää mitä tapahtuu
- Pilvipalvelut ovat turvallisia
- Ihminen on aina heikoin lenkki



Kiinteistöalan erityispiirteet

1. **Rakennusautomaatiojärjestelmät:** Kiinteistöjen hallinnassa käytetään yhä enemmän rakennusautomaatiojärjestelmiä, kuten lämmityksen, ilmanvaihdon ja valaistuksen ohjausta. Näiden järjestelmien haavoittuvuudet voivat altistaa kiinteistöt kyberhyökkäyksille.
2. **IoT-laitteet:** Kiinteistöissä käytetään paljon IoT-laitteita (Internet of Things), kuten älykkäitä termostaatteja, valvontakameroita ja ovilukkoja. Nämä laitteet voivat olla kyberrikollisuuden kohteena, jos niiden tietoturva ei ole riittävä.
3. **Tietojen hallinta:** Kiinteistöalan toimijat käsittelevät suuria määriä arkaluonteisia tietoja, kuten vuokralaisten henkilötietoja ja taloudellisia tietoja. Näiden tietojen vuotaminen voi aiheuttaa merkittäviä taloudellisia ja mainehaittoja.
4. **Geopoliittiset motiivit:** Valtiolliset toimijat voivat kohdistaa hyökkäyksiä toimialaan strategisista syistä, kuten poliittisen painostuksen tai taloudellisen vahingon aiheuttamiseksi. Tämä voi olla osa laajempaa geopoliittista konfliktia.
5. **Fyysisen ja kyberinfrastruktuurin yhteydet:** Kiinteistöjen järjestelmät ovat usein yhdistelmä fyysistä ja kyberinfrastruktuuria. Tämä tekee niistä alttiita hyökkäyksille, jotka voivat vaikuttaa sekä digitaalisiin että fyysisiin toimintoihin.



$$\text{Skull} \times \text{Power Line} + \text{Truck} \times (x/y \cdot z) = \text{Talvi 2025} / (-^{\circ}\text{C} \times \pi).$$

Hackers

don't give a shit:

- About your project's scope
- It's managed by a third party
- It's a legacy system
- It's "too critical to patch"
- About your outage windows
- About your budget
- You've always done it that way
- About your Go-Live Date
- It's only a pilot/proof of concept
- About Non-Disclosure Agreements
- It wasn't a requirement in the contract
- It's an internal system
- It's really hard to change
- It's due for replacement
- You're not sure how to fix it
- It's handled in the Cloud
- About your Risk Register entry
- The vendor doesn't support that configuration
- It's an interim solution
- It's [insert standard here] compliant
- It's encrypted on disk
- The cost benefit doesn't stack up
- "Nobody else could figure that out"
- You can't explain the risk to "The Business"
- You've got other priorities
- About your faith in the competence of your internal users
- You don't have a business justification
- You can't show Return on Investment
- You contracted out that risk

TULEVAISUUS

- Kaikkia resursseja hyödynnetään
- AI nopeuttaa prosesseja
- Uhkakenttä tulee tärkeämmäksi
- Kumppanuudet ovat keskeisiä
- Osaamisen kehittäminen on tärkeää
- Todentaminen on elintärkeää
- Läpinäkyvyys ja rehellisyys korostuvat
- Mitä odottaa Ukrainan rauhansopimukselta?

Kiitos!