



**Maanpuolustuslaitos**

**Savo-Karjalan maanpuolustuspiiri**

**DIGITAL TWIN SEMINAARI 15.03.2023**

**RAKENNETUN INFRAN KYBERTURVA**

Jari Raatikainen



”Ainoa turvallinen tietokone on sellainen, joka on lukittu kassakaappiin ja haudattu maan alle salaiseen paikkaan. Tästäkään en mene takuuseen.” Dennis Hughes (FBI)

Itse sanoin jo 1991, että PC tietokone on aivan liian monimutkainen laite, että sitä koskaan pitäisi edes saattaa normaalikäyttäjän ulottuville.

# RAKENNUKSEN TIETOVERKKO

- Ylläpitäjällä vähintään tietokone, jossa normaalisti; etähallinta, pankkiyhteydet, sähköposti jne
- Miten automatisoitu rakennus on ?
  - sähköiset lukot
  - hissi
  - lämmitys / ilmanvaihto
  - valvontakamerat

Onko verkko segmentoitu vai kaikki yhdessä ja samassa ?

# MISTÄ SE UHKA SITTEN TULEE ?

- Kalastelu (Phishing)
- Laitteen “kaappaus” osaksi bottiverkkoa (orjuuttaminen)
- Tiedon varastaminen
  - Jos Rakennuksessa on webbikamera ja sen kameran kuvaa voi kuka tahansa katsoa, syyllistytään GDPR myötä henkilötietojen käsittelyn rikkomukseen.
- Kiristys (ransomware)
- Harhaanjohtaminen (väärin uutisten tarjoaminen vaihtoehtoisena totuutena)
- Jos automaatio on osa rakennuksen verkkoa, voiko sitä ohjata tekemään väärin ? vrt STUXNET. Missä automaation kaapelit kulkevat ?

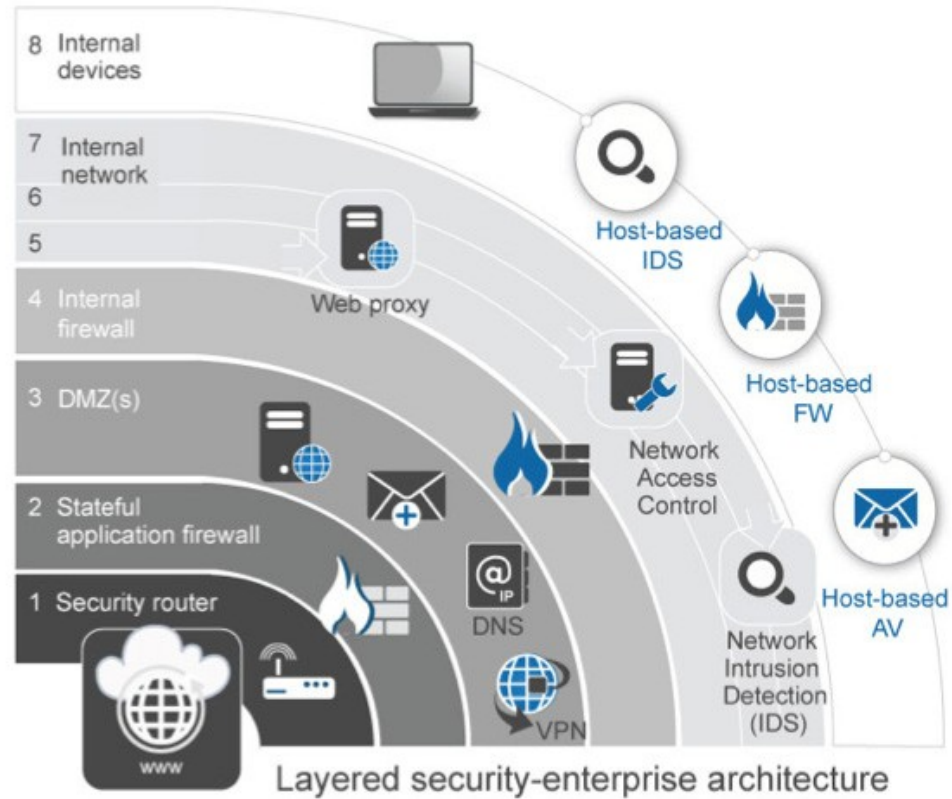
# OMAN TOIMINNAN TARPEELLISUUS

Ihminen on heikoin lenkki, se on fakta.

Jos mitenkään mahdollista, pidä rakennusverkko täysin erillään internetistä. Jos se ei ole mahdollista, käytä vähintään NAT palomuuria ja määrittele myös ulospäin sallitut yhteydet. Pyydä/hanki/osta apua jos et osaa.

Muista faktan tarkastus.

# KUMPI PETTÄÄ ENSIN?



# HYVÄ MUISTAA

Rikolliset ja valtiolliset toimijat muuttavat taktiikkaansa kokoajan. Mikä turvasi tänään, ei välttämättä enää huomenna toimi.

Yritä pitää työ ja huvi erillään.

Muista päivitykset !

Mieti, mitä tietoja julkaiset somessa / yleensä verkossa.



# MIKÄ MENI VIKAAN?



Lähde: <http://cdn1.smosh.com/sites/default/files/ftpuploads/bloguploads/0714/dumbest-twitter-credit-card-1b.jpg>



# LISÄTIETOA LÖYTYY

<https://jyx.jyu.fi/bitstream/handle/123456789/53510/978-951-39-7009-3.pdf?sequence=1&isAllowed=y>

Kyberin taskutietoa

<https://haveibeenpwned.com/>

Onko käyttäjätunnukseni/sähköpostiosoitteeni ollut mukana tietomurrossa

<https://www.pcmag.com/picks/the-best-password-managers>

Vertailu salasananhallinta ohjelmista

`nmap --script shodan-api --script-args 'shodan-api.apikey=<YOUR OWN API KEY>,shodan-api.target=194.157.253.10'`  
mitä shodan tietää yhteyspisteestäsi

KIITOS