

# Kyberturvallisuus yhteiskunnan selkärankana

Mihin varautua muuttuvassa  
toimintaympäristössä ja uhkakentässä?

19.5.2026

Kari Isokivijärvi  
Ratkaisuasiantuntija  
Elisa Kyberturvallisuuspalvelut

*elisa*

DIGITALISAATIOILLA  
KESTÄVÄ  
TULEVAISUUS



# Elisa turvannut suomalaisia organisaatioita jo yli 10 vuoden ajan

- Elisa Kyberturvakeskus ratkaisee asiakkaillemme +6000 kyberturvapoikkeamaa / kk
- Julkisen sektorin ja suomalaisten suuryritysten luottama
- +100 kyberintekijää palkkalistoilla
- Ammattilaisten arvostamat tapahtumat, keskustelu ja tutkimukset

KYBERINTEKIJÄT 2024



# Jos digitaaliset järjestelmät pettävät, meidän kaikkien arki pysähtyy

Nykyään kaikki pyörii järjestelmissä ja verkoissa. Yhtä lailla työmatka bussilla kuin tuotantolaitoksen tauoton liike vaativat toimiakseen yhteyksiä ja ohjelmistoja.

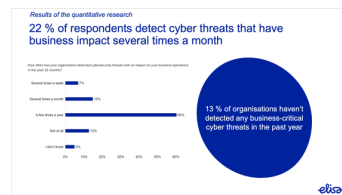
Entä kun näihin tulee häiriö vahingossa tai tarkoituksella?

## MIKSI ARKI PYSÄHTYY?

- Henkilökuntaa ja johtoa huijataan
- Enemmän järjestelmiä, enemmän haavoittuvuuksia
- Rikollisuus ja valtiollinen toiminta lisääntynyt
- Teknologinen kehitys tuo uusia uhkia

# 4/5

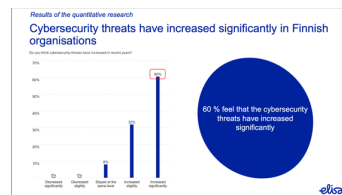
suomalaisista yrityksistä  
kärsii liiketoimintaan  
vaikuttavista  
kyberhyökkäyksistä  
vuosittain.



Lähde: *Understanding the cybersecurity landscape in Finland, 2025*, Noren (Elisan tilaama tutkimus).

# 9/10

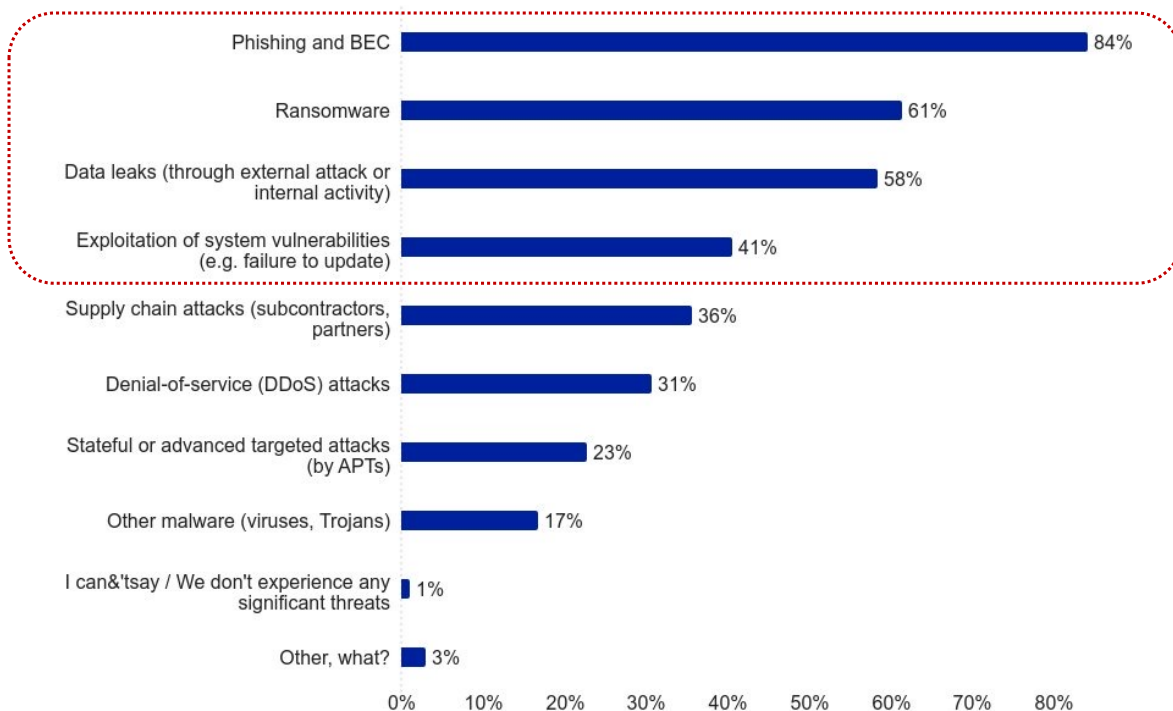
kokee, että kyberhyökkäysten määrä on lisääntynyt viimeisten vuosien aikana.



Lähde: *Understanding the cybersecurity landscape in Finland, 2025*, Noren (Elisan tilaama tutkimus).

# Suomalaisiin organisaatioihin kohdistuu jatkuvasti enemmän kyberuhkia

Which of the following cybersecurity threats do you currently see as the biggest risks to your organisation? Choose up to 5 of the most important.



Tietojenkalastelu, huijausviestit, kiristyshaittaohjelmat, tietovuodot ja tekniset hyökkäykset ovat yleisimpiä kyberhyökkäys tyyppisiä.

# Mitä on muuttunut?

1. Laajeneva hyökkäyspinta-ala
2. Uhkatoimijoiden kehitys
3. Geopoliittiset jännitteet ja resurssit
4. Tulevaisuuden uhkat ja ratkaisut



# Laajeneva hyökkäyspinta-ala

- Hyökkäysten määrä ja kehittyneisyys kasvavat nopeasti
- "Crime as a Service" madaltaa rikollisuuden kynnystä
- Murtautumisaika organisaatioihin lyhentynyt
- Haavoittuvuuksien hyväksikäyttö, erityisesti reunalaitteissa ja API-rajapinnoissa, kasvaa
- Identiteettipohjaiset hyökkäykset ja infostealer-haittaohjelmat yleistyvät
- Kiristyshaittaohjelmat "ammattimaistuvat", hyökkäykset kohdistuvat myös varmuuskopioihin
- IT & OT ympäristöt lähentyvät toisiaan

Keskimääräinen  
murtautumisaika 2024 62min  
vs 2025 48min

Verkon reunalaitteiden  
haavoittuvuuksien  
hyväksikäyttö 8x vuodesta  
2023

Vain 54% verkon  
reunalaitteiden  
haavoittuvuuksista saatiin  
korjattua vuoden sisällä,  
mediaani 32 päivää

2024 60% tietomurroista  
sisälsi identiteettielementin  
väärinkäytön

Infostealer mukana 24%  
kaikista havaituista  
tietoturvapoikkeamista

# Uhkatoimijoiden kehitys

- Rikollisryhmät ja valtiolliset toimijat kehittävät jatkuvasti uusia taktiikoita
- APT-ryhmien (Advanced Persistent Threat) hyökkäykset vaikeampia havaita
- Vakoilun osuus tietomurroista kasvaa
- Palvelunestohyökkäykset (DDoS) kasvaneet merkittävästi
- Kybervaikuttaminen osana valtiollista voimankäyttöä

89 % tietomurroista taloudellisesti motivoituneita

2023 vakoilun osuus 6 % kaikista tietomurroista vs 2024 17 %

Microsoftin seuraamien uhkatoimijoiden määrä 2023 300 ryhmää vs 2024 1500 ryhmää

Elisa havainnut 122% kasvun DDoS hyökkäyksissä vuoden aikana, Cloudflare 358% kasvun

# Geopoliittiset jännitteet ja resurssit

- Sääntelyn ja teknologian muutokset haastavat organisaatioita
- Budjettileikkaukset ja resurssien niukkuus heikentävät puolustuskykyä
- Pienet organisaatiot erityisen haavoittuvaisia
- Kasvava riippuvuus toimitusketjuista johtavaa entistä läpinäkymättömämpään ja arvaamattomampaan riskimaisemaan

WEF:n mukaan 71% kyberturvapäätäjistä eivät usko pienempien organisaatioiden kykenevän suojautumaan riittävän hyvin kasvavia kyberriskejä- ja hyökkäyksiä vastaan

Kolmansien osapuolien osuus tietomurroista 2023 15% vs 2024 30%

Toimitusketjujen haasteet suurin este kyberresilienssille 54% suurissa organisaatioissa

# Tulevaisuuden uhkat ja ratkaisut

- Uhkatoimijat hyödyntävät strategiaa "Kerää nyt, hyödynnä myöhemmin"
- Kvanttilaskenta uhkaa perinteistä kryptografiaa – post-quantum-ratkaisuiden aikajänne
- Tekoälyn (AI) rooli kasvaa: deepfake-hyökkäykset, AI-agentit, generatiivinen AI
- Zero Trust -arkkitehtuuri ja modernit todennusratkaisut (esim. Passkeys) keskiössä
- AI:n hallinta ja tiedon suojaaminen korostuvat

EU:n aikajänne PQC transitoon: implementoitu käyttöön korkean riskin kohteisiin 2030 ja keskitason riskin kohteisiin 2035

Gartnerin mukaan 2026 mennessä 30% yrityksistä pitää biometriaa epäluotettavana deepfake-hyökkäysten johdosta

15% työntekijöistä käyttää säännöllisesti GenAI alustoja yrityksen hallitsemilla laitteilla

Tällä hetkellä 30% Microsoftin koodista tuotetaan AI:lla ja 2030 ennusteiden mukaan jopa 95%

# Suosituksset organisaatioille

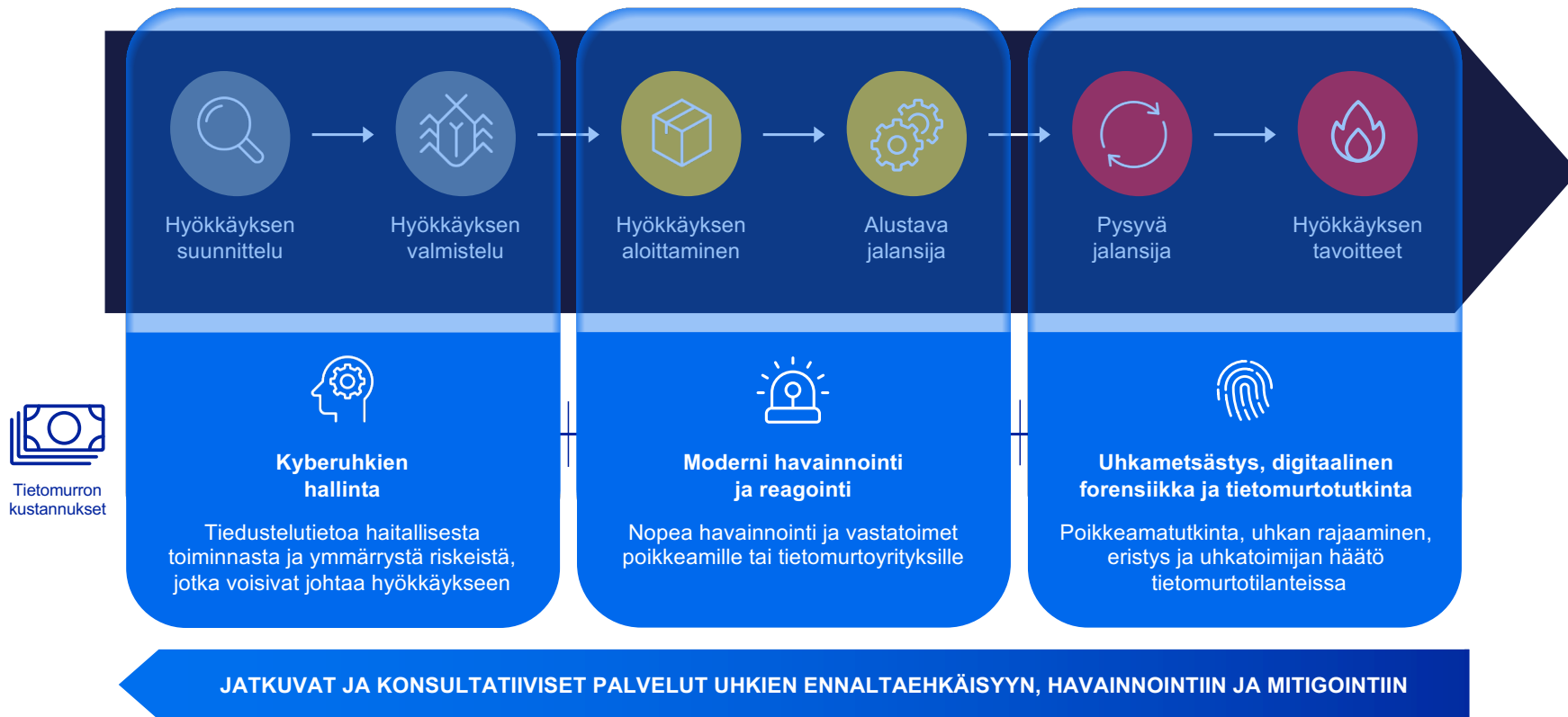
1. **Vahvista perustoimintoja** ja päivitä suojaustoimia jatkuvasti - Päivitysten hallinta, laitteiden suojaus, konfiguraatioiden kovennus...
2. Ota **hyökkäyspinta-alan valvonta** haltuun
3. Panosta **näkyvyyteen ja kykyyn reagoida** kyberpoikkeamiin
4. Ota käyttöön **monivaiheiset** todennustavat ja **Zero Trust** –malli vaiheittain kun arkkitehtuuria kehitetään
5. Kontrolloi AI-työkalujen käyttöä ja **kouluta henkilöstöä**



# Lievennä riskejä ja tietomurtojen aiheuttamia haittoja



## HYÖKKÄYKSEN ELINKAARI JA HAVAINNOINTIAIKA



Tietomurron kustannukset

*elisa*

**A SUSTAINABLE  
FUTURE THROUGH  
DIGITALISATION**

**Kiitos!**