Huoltovarmuuskeskus

Digitaalinen turvallisuus 2030

Valtioneuvoston periaatepäätös päivittyy – resilienssi, huoltovarmuus ja kyberturvallisuus 15.1.2025

Juha Ilkka
Ohjelmajohtaja

Uhkaympäristö muutoksessa

- Kriittisen infrastruktuurin suojaaminen
- Kyberuhat kehittyvät ja muuttuvat kiihtyvällä tahdilla
- Pitkät toimitusketjut ja kompleksinen arkkitehtuuri
- Digimurroksen eteneminen muuntaa riskejä
- Tekoälyn kehitys

Miten kyberturvallisuutta kehitetään huoltovarmuuden näkökulmasta?


Digitaalinen infrastruktuuri
Digiturvallisuuden tukipalvelut
Toimialojen ja kuntien osaaminen
Informaatioturvallisuus
Harjoittelu
Tilannetietoisuuden kehittäminen

Informaatio-turvallisuus

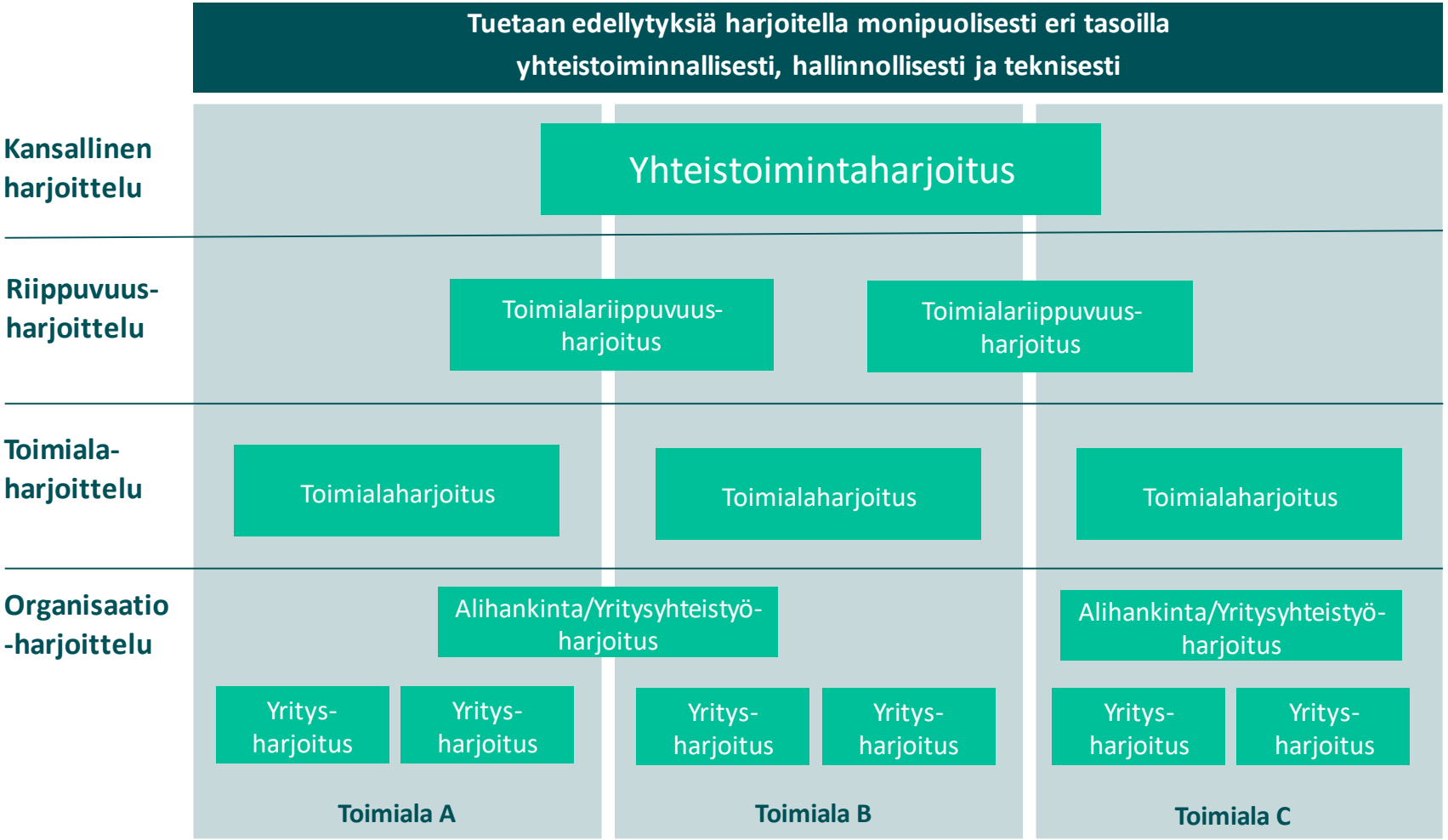
Informaatioturvallisuuden osaamiskeskus

- Tavoitteena on vahvistaa informaatioturvallisuuden osaamista kansallisesti ja kehittää toimintamalleja sekä työkaluja haitallisen vaikuttamisen torjuntaan.
- Osaamiskeskus toimii myös alan osaamisen solmukohtana kotimaassa ja luo verkostoja kansainvälisesti.
- Keskus tuottaa tietoa maahamme kohdistuvista tahallisista ja haitallisista informaatiokampanjoista sekä tukee elinkeinoelämää, kansalaisia ja viranomaisia informaatiovaikuttamisen tunnistamisessa ja torjunnassa.

HAVARO

- HAVARO on Liikenne- ja viestintävirasto Traficomin tuottama palvelu, joka havainnoi suomalaisiin yrityksiin kohdistuvia vakavia tietoturvauhkia ja varoittaa niistä.
- Palvelun tuottamisen perustana on kansallisen kyberturvallisuuden tilannekuvan ylläpitäminen ja huoltovarmuuden varmistaminen. Palvelu suunnataan ensisijaisesti huoltovarmuuskriittisille yrityksille ja organisaatioille, mutta palvelua voidaan tarjota muillekin organisaatioille.
- HAVARO tuottaa havainnointitietoa yleisistä ja vakavista tietoturvauhista maassamme. Kyberturvallisuuskeskus koostaa tietojen avulla kansallisen kyberturvallisuuden tilannekuvaa, jonka avulla kehitetään viestintäverkkojen ja -palveluiden toimintavarmuutta sekä turvallisuutta ja lisätään ymmärrystä tietoturvasta kaikkien verkoston organisaatioiden hyödyksi.

Kyberharjoittelu



Tilannetietoisuuden kehittäminen

- Kvanttilaskennan tietoturvavaikutukset - suositus varautua (Digipooli 2024)
- Tekoäly
  - Tekoälypohjaiset kyberturvallisuusratkaisut (2024)
  - Tekoälyn mahdollistamat kyberhyökkäykset (2022)
  - Tekoälyn soveltamisen kyberturvallisuus ja riskienhallinta (2021)
- 5G
  - 5G Hackaton
  - Hack the networks
  - 5G yksityisissä matkaviestinverkoissa
  - Toimenpideohje 5G-teknologian riskienhallintaan
- Toimialojen kyberkypsyyskartoitus
- Satelliittilaajakaistojen hyödyntäminen varautumisessa

Turvallinen ohjelmistokehitys

- Pohjalla Digipoolin toimialakartoitus
- Tietoa syvennettiin Traficomin selvityksellä 2023-2024
- Projekti käynnistyi Q2/2024
  - Sääntelyn vaikutus ohjelmistotoimialaan
  - Turvallisen ohjelmistokehityksen hankinta
  - Ohjelmistoturvallisuuden koulutus
  - Ohjelmistokehityksen ja –turvallisuuden johtaminen
  - Turvallisen ohjelmistokehityksen käytännöt

Yhteenveto

- **Digitaalinen turvallisuus 2030 –ohjelma** vie osaltaan Huoltovarmuuskeskuksen strategiaa eteenpäin. Strategiallaan HVK pyrkii vastaamaan kolmeen keskeiseen skenaarioon, joita ovat sotilaallinen uhka, laaja-alainen vaikuttaminen ja globaalin talouden vakavat häiriötilanteet.
- **Digimurroksen eteneminen muuntaa riskejä** - Yritysten käyttämät digitaaliset ratkaisut, kuten pilvipalvelut, tekoäly tai kvanttiteknologia kehittyvät vauhdilla. Samalla muuttuvat yritysten jatkuvuuden hallinnan keskeiset riskit, joihin ratkaisujen tunnistaminen on keskeinen osa huoltovarmuutta.
- **Huoltovarmuus tehdään yhdessä.** Suomen supervoima on hyvä yhteistyö viranomaisten, elinkeinoelämän ja kolmannen sektorin kanssa.

Huoltovarmuuskeskus

Fiksua huoltovarmuutta yhdessä.

Varmuuden vuoksi.

huoltovarmuuskeskus.fi varmuudenvuoksi.fi