HE 57/2024 Lausunto

Kyberturvallisuusdirektiivin täytäntöönpanoa koskevaksi lainsäädännöksi

Antti Laatikainen

Johtava tietoturvakonsultti, WithSecure Consulting

WITH secure | Consulting

Taustoitusta muistiosta

Nykyaikainen suomalainen yhteiskunta tarvitsee toimivia tietojärjestelmiä, joiden häiriönkesto, luotettavuus ja saatavuus ovat keskeisiä ihmisten turvallisuudentunteelle ja yhteiskunnan toimintakyvylle.

Kriittisen infrastruktuurin muodostavat tuhannet yritykset ja liikelaitokset, joiden kyberturvallisuuden minimitasot on määriteltävä yhteisesti.

WithSecuren mielestä ehdotettu kyberturvallisuuslaki on hyvin laadittu ja tarpeellinen, ja se tukee yhteiskunnan kybersietoisuutta.

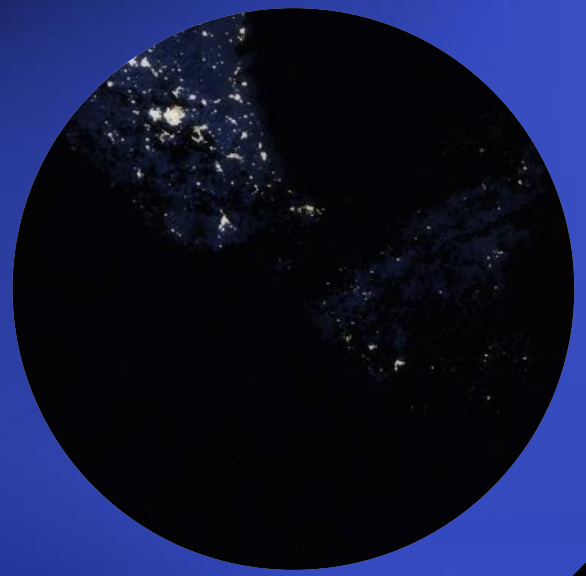
WithSecuren lausunnossa käsitellään riskienhallinnan käytäntöjä ja haasteita sekä sitä, miten käsittelyssä oleva laki voisi tukea näitä vielä tehokkaammin.



WITH secure | Consulting

Sisällys

- Riskienhallinnan merkitys ja haasteet
- Ohjeistuksen tarve
- Valvonta ja ilmoittaminen



WITH secure | Consulting

Riskienhallinnan merkitys ja haasteet



Kyberturvallisuuslaissa ei mainita yhteiskunnallisen vaikuttavuuden arviointia osana riskienhallintaa.

WithSecure korostaa, että riskienhallinnassa tulisi huomioida myös yhteiskunnallinen vaikuttavuus, ei pelkästään yrityksen omia liiketoimintariskejä.

Kokemuksemme mukaan monilla teollisuudenaloilla väärin ymmärretty riskienhallinnan lähtökohta johtaa kestämättömiin jäännösriskeihin ja riskien hyväksymisiin, mikä ei tue NIS2:n tavoitteita eikä toivotunlaisia yhteiskunnallisia vaikutuksia.





Ohjeistuksen tarve

Lain rinnalle tarvitaan konkreettista ohjeistusta, jotta organisaatiot ymmärtävät ja pystyvät tehokkaasti toteuttamaan riskienhallintakeinoja.

Tämä on erityisen tärkeää teollisuudenaloilla, joilla kyberturvallisuuden lähtökohdat ovat alhaiset.

Valvovien viranomaisten resurssointi kriittisen tärkeää jalkautukselle.

Mitä tehdä jos tunnistettuihin riskienhallinnan tarpeisiin ei löydy resursseja?





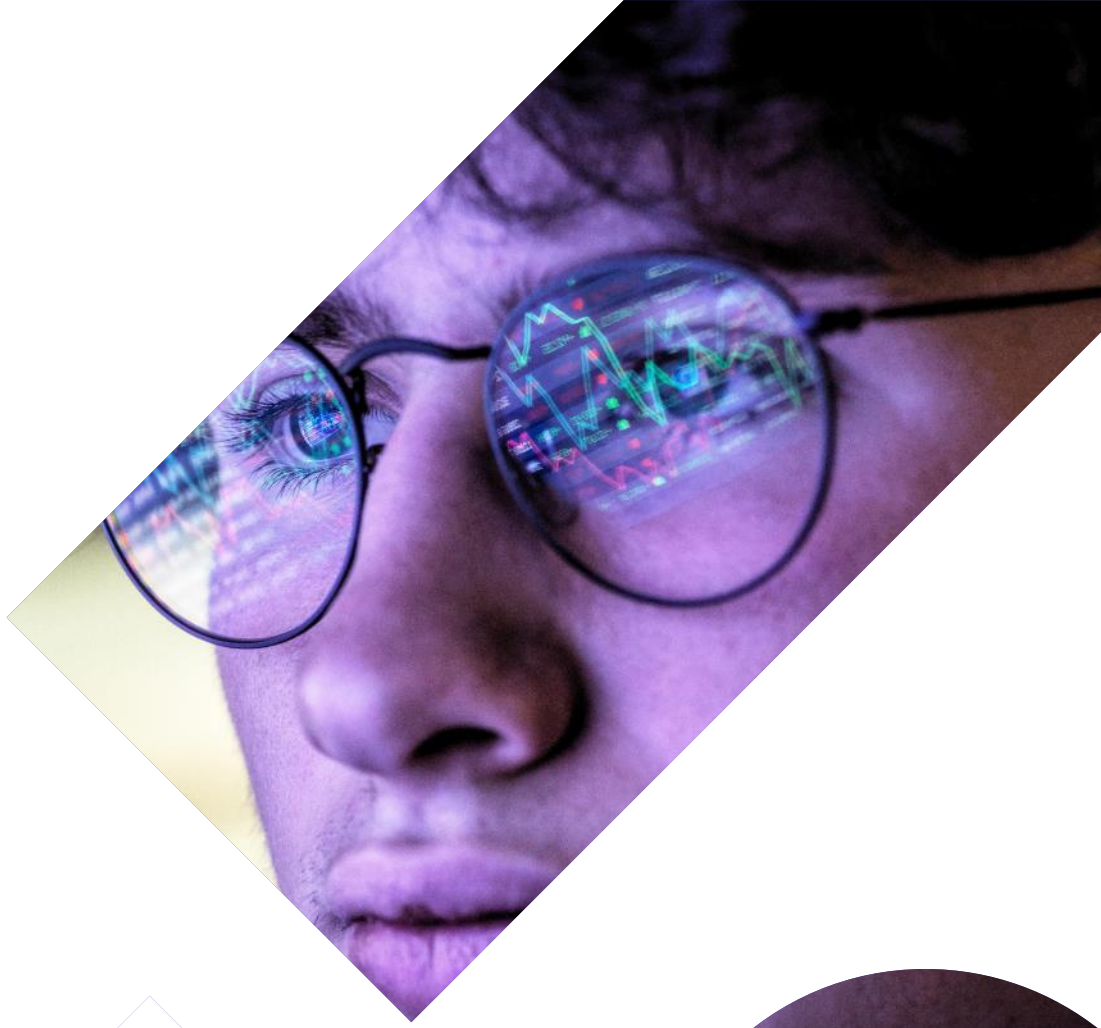


WITH secure | Consulting

Valvonta ja ilmoittaminen

WithSecure suosittelee, että lakiin lisätään toimintamalli whistleblower-kanavasta ja muista keinoista, joilla voidaan ilmoittaa yritysten riskienhallinnan puutteista valvoville viranomaisille.

Tämä auttaisi havaitsemaan ja käsittelemään merkittäviä riskejä ajoissa.







WITH®

secure