Tehokas menetelmä kyberturvallisuusriskien hallintaan teollisuudessa ja teollisuutta palvelevassa liiketoiminnassa

Kyberturvallisuusriskien hallinta teollisuuden tuotantoympäristöissä on erittäin tärkeää. **"Varaudu pahimpaan"** -menetelmä tarjoaa selkeän ratkaisun kyberturvariskien analysointiin. Se yksinkertaistaa kyberturvallisuuden riskiarvioinnin ja auttaa varautumaan uhkiin ajoissa.

Kenelle koulutus sopii?

Teollisuudessa tai teollisuuden palveluliiketoiminnoissa työskentelevät henkilöt, joiden täytyy huolehtia myös kybertuvallisuudesta.
Tietoturvan kehittämisestä vastaavat henkilöt, jotka suunnittelevat toimia, joilla estää kyberhyökkäykset
Hankinnan ja alihankintaverkoston vastuuhenkilöt
Teollisen tuotantoympäristön ja kunnossapidon johtohenkilöille,
Automaatio- ja järjestelmäasiantuntijoille
kyberturvariskeistä vastaaville.
Henkilöille, joiden vastuulla on turvallinen ja toimiva tuotantojärjestelmä.

Koulutuksen sisältö

Kyberturvallisuuteen liittyvät direktiivit ja määrykset
Varaudu pahimpaan -käsitteet
Varaudu pahimpaan – harjoituksia kyberuhkiin varautumisesta

"Varaudu pahimpaan" -menetelmä tarjoaa selkeän ratkaisun kyberturvariskien hallintaan. Se yksinkertaistaa kyberturvallisuuden riskiarvioinnin ja auttaa varautumaan uhkiin ajoissa.

Muuta tärkeää tietoa

Tunnista kriittisimmät uhat ennen kuin ne realisoituvat. Opi analysoimaan riskit ja varautumaan pahimpaan CER-direktiivin ja huoltovarmuuslain vaatimusten mukaisesti.

Perinteiset riskianalyysit ovat melko monimutkaisia ja siksi ne usein järjestelmien rakennusvaiheessa ohitetaan. Tämä altistaa yritykset tunnistamattomille kyberriskeille, joiden korjaaminen jälkikäteen kuluttaa yrityksen resursseja ja kasvattaa kustannuksia.

Suomalaisen kyberturvalain vaatimukset eivät suoraan sovellu tuotantoympäristöjen erilaisiin monimutkaisiin järjestelmiin, joten niiden käytännön toteuttaminen edellyttää räätälöityä, seuraamusperusteista riskianalyysiä aukkojen minimoimiseksi.

NIS 2 -direktiivin mukaiset velvoitteet tulivat voimaan 8.4.2025. NIS 2 on Euroopan unionin kyberturvallisuusdirektiivi.

HE 205/2024 | Hallituksen esitys eduskunnalle laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja eräiksi muiksi laeiksi | Hallituksen esitykset | Finlex

2.2.5 Kriittisten toimijoiden häiriönsietokyky

CER-direktiivin III luku sääntelee kriittisten toimijoiden riskiarviointia, toimijoiden toimenpiteitä häiriönsietokyvyn varmistamiseksi, taustantarkistuksia, poikkeamista ilmoittamista ja standardeja koskevia suosituksia.

CER-direktiivin III luvun 12 artiklassa säädetään kriittisten toimijoiden suorittamasta

riskiarvioinnista. Jäsenvaltioiden on varmistettava, että riskiarvioinnit on suoritettu määräajassa sen jälkeen, kun toimija on vastaanottanut ilmoituksen siitä, että se on määritetty kriittiseksi toimijaksi ja myöhemmin tarvittaessa ja vähintään neljän vuoden määrävälein. Riskiarvioinneissa on otettava huomioon artiklan 2 kohdan mukaan kaikki merkitykselliset luonnon ja ihmisten aiheuttamat riskit, jotka voivat johtaa poikkeamaan. Myös toimialojen ja rajat ylittävät riskit, onnettomuudet, luonnonkatastrofit, kansanterveydelliset hätätilanteet, hybridiuhat ja muut vihamieliset uhat on otettava huomioon. Riskiarvioinnissa on otettava huomioon se, missä määrin muut CER-direktiivin liitteessä tarkoitettujen toimialojen toimijat ovat riippuvaisia kriittisen toimijan tarjoamasta keskeisestä palvelusta. Tämä kattaa myös naapurijäsenvaltiot ja kolmannet maat.

Jos riskiarviointeja tai asiakirjoja on tehty muiden säädösten velvoitteiden perusteella, niitä voidaan käyttää 12 artiklassa säädettyjen vaatimusten täyttämiseen.

CER-direktiivin 13 artikla koskee kriittisten toimijoiden (alla tiivistetty lista) toimenpiteitä häiriönsietokyvyn varmistamiseksi.

Komissio on antanut delegoidun asetuksen (EU) 2023/2450 Euroopan parlamentin ja neuvoston direktiivin (EU) 2022/2557 täydentämisestä vahvistamalla ei-tyhjentävän luettelon keskeisistä palveluista seuraavasti:

energia-ala: johon kuuluu 8 alasektoria mm. Sähkön-, kaukolämmön-, öljyn, vedyn jakelu, tuotanto sekä ja varastointi
elintarvikealan tuotanto, jalostus ja jakelu (elintarvikeyritykset, jotka toimivat yksinomaan logistiikan ja tukkukaupan sekä laajamittaisen teollisen tuotannon ja jalostuksen alalla)
liikenneala: jossa 3 alasektoria mm. ilma-, raide ja vesiliikenne, lentokentät, satamat ja liikenteenhallinta
juomavesiala ja jätevesiala mm. jäteveden keruu, käsittely ja poistaminen.
terveysala: mm terveydenhuoltopalvelujen järjestäminen, lääkinnällisten laitteiden valmistaminen ja lääkkeiden jakelu
pankki- ja rahoitusala ala
digitaalisen infrastruktuurin ala, mm pilvipalvelujen ja internetin yhdysliikennepalvelujen tarjoaminen ja hallinnointi
julkishallinnon ala
avaruusala.

Ota yhteyttä

Margit Ojanen
koulutuskoordinaattori, teollisuus
050 374 2191
margit.ojanen@taitotalo.fi

Asiantuntijat

Teemu Kumpulainen
OT kyberturvallisuusasiantuntija
Kumpu Consulting Oy

Seuraavat koulutukset

Tehokas menetelmä kyberturvallisuusriskien hallintaan teollisuudessa ja teollisuutta palvelevissa toiminnoissa

Paikka: Taitotalo, Valimo, Valimotie 8, 00380 HELSINKI
Ajankohta: 7.10.2026
Ilmoittaudu viimeistään: 23.9.2026
Kesto: 1 päivä
Hinta: 950,00 € ALV 25,5 % Kokonaishinta sis. ALV 1 192,25 €

Lisätietoa

Tehokas menetelmä kyberturvallisuusriskien hallintaan teollisuudessa ja teollisuutta palvelevissa toiminnoissa
7.10.2026
Taitotalo, Valimo, Valimotie 8, 00380 HELSINKI

Keskiviikko 7.10.2026
Tehokas menetelmä kyberturvallisuusriskien hallintaan teollisuudessa ja teollisuutta palvelevissa toiminnoissa
Taitotalo, Valimo, Valimotie 8, 00380 HELSINKI
V423 ATK-luokka, Valimotie 8

9.00-9.45
Johdanto

Kumpulainen Teemu, Kumpu Consulting Oy

9.45-11.30
Direktiivit ja määräykset

Kumpulainen Teemu, Kumpu Consulting Oy

11.30-12.15
Lounas

12.15-14.00
Varaudu pahimpaan, käsitteet

Kumpulainen Teemu, Kumpu Consulting Oy

14.00-15.45
Harjoitukset

Kumpulainen Teemu, Kumpu Consulting Oy