Standardien ja sääntelyn kehitys OT-järjestelmissä

Henry Haverinen
Suomen Automaatioseuran webinaari
24.10.2023

CYBERISMO!

Taustaa

- Yleinen uhkatilanne on yhä kiristynyt
- OT-järjestelmät tarjoavat hyökkäyksille houkuttelevan kohteen mm. mahdollisen maksukyvyn, järjestelmien tärkeän tehtävän ja pitkien elinkaarien aiheuttaman haavoittuvuuden vuoksi
- IEC 62443 –standardisarja on onnistunut nousemaan merkittäväksi mittatikuksi tuotekehityksen, tuotteiden ja järjestelmien kyberturvallisuudessa
- EU-sääntelyllä halutaan varmistaa, että digitaaliset tuotteet ovat turvallisia ja että kriittiset toimijat suojautuvat

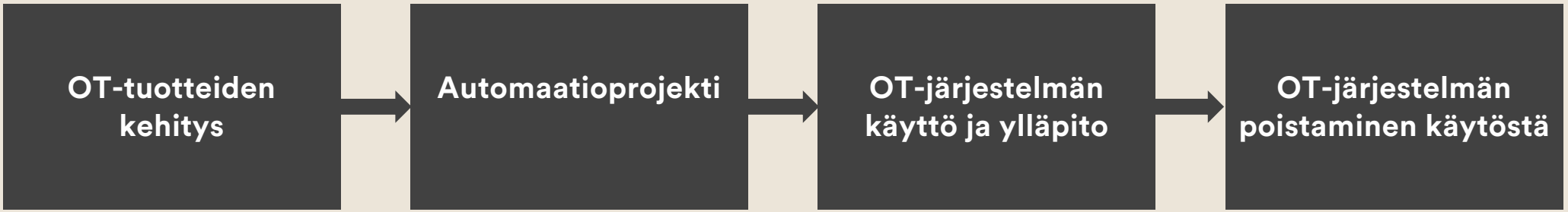
MISTÄ VAATIMUKSET TULEVAT

Vaatimukset kiristyvät

CYBERISMO!

LYHYT KERTAUS

Tärkeimmät IEC 62443 –standardit



IEC 62443-4-1: Turvallinen tuotekehitysprosessi

IEC 62443-4-2: Komponentin tietoturvakyvykkyydet

IEC 62443-2-4: Järjestelmäintegraattorin tietoturvallisuuden hallintajärjestelmä

IEC 62443-3-2: Järjestelmän riskienhallinta ja riskipohjainen segmentointi

IEC 62443-3-3: Järjestelmän tietoturvakyvykkyydet

IEC 62443-2-1: Toiminnanharjoittajan tietoturvallisuuden hallintajärjestelmä

IEC 62443-2-4: Elinkaaripalveluiden tarjoajan tietoturvallisuuden hallintajärjestelmä

CYBERISMO!

Tärkeimmät EU-säädökset

Kyberturvallisuusasetus
Cyber Security Act (CSA):
ENISA:n rooli ja EU-tason sertifiointiohjelmat

NIS2-direktiivi:
Varmistetaan kriittisten toimijoiden korkea kyberturvallisuuden taso

Myös esim:

Kriittisten toimijoiden häiriönsietodirektiivi eli Critical Entities Resilience Directive (CER)

Vaatimuksia kriittisille toimijoille EU:ssa

Vaatimuksia tuotteiden pääsemiseksi EU:n markkinoille

Radiolaitedirektiivi/
Radio Equipment Directive (RED):

Parannetaan verkon resilienssia, kuluttajien yksityisyyden suojaa ja vähennetään maksupetoksien riskejä

Kyberresilienssiasetus/
Cyber Resilience Act (CRA):

Parannetaan tietoturvan ja resilienssin tasoa tuotteissa, joissa on digitaalisia elementtejä

Myös esim:

Koneasetus eli Machine regulation

CYBERISMO!

NIS2-direktiivi

- Hyväksytty direktiivi, kansallinen lainsäädäntö meneillään
- Koskee kriittiseksi määriteltyjä organisaatioita EU:ssa
- Ei erittele OT-järjestelmiä erikseen, mutta koskee mm. energiasektoria, liikennettä, vesilaitoksia ja valmistavaa teollisuutta
- Paljon päällekkäisyyttä ISO 27001:n kanssa

NIS2-direktiivin sisältö

- Johdon rooli ja vastuu
- Riskienhallinta ja tietyt hallintakeinot, kuten järjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, kryptografia, jatkuvuudenhallinta, toimitusketjun turvallisuus, haavoittuvuuksien hallinta, poikkeamien käsittely
- Viranomaisille raportointi

Kyberresilienssiasetus (CRA)

- Ei vielä hyväksytty
- Koskee tuotteita, joissa on digitaalisia elementtejä. OT-tuotteet kuuluvat kriittisten tuotteiden luokkiin
- Sisältää vaatimuksia riskienhallinnasta, tietyistä teknistä kyvykkyyksistä, dokumentoinnista, haavoittuvuuksien hallinnasta, ja viranomaisille raportoinnista
- Paljon päällekkäisyyttä IEC 62443 osien 4-1 ja 4-2 kanssa – mutta myös uutta: esim. turvalliset oletusasetukset, SBOM:n tuottaminen, maksuton 5 vuoden tuki, ja poikkeamien raportointi viranomaisille

Tietoturvallisuuden hallintajärjestelmän perusteet

- ISO 27001
- IEC 62443:n osat 2-1 ja 2-4
- NIS2-direktiivi

Tavoitteet

Suojattava omaisuus

Riskien ja mahdollisuuksien hallinta

Tuotteiden ja projektien turvallisuus

Koulutus ja ihmisten tietoisuus

Poikkeusten hallinta ja liiketoiminnan jatkuvuus

Valvonta ja mittarit

Johtaminen ja johdon sitoutuminen

CYBERISMO!

OT

\+ Kyberstandardit ja -sääntely

= Vaikeaa!

Perusasioiden kautta!

Hallintajärjestelmä johdon tuella

Johdon tehtävä on järjestää aikaa ja rahaa, jotta organisaation tavoitteiden mukainen kyberturvallisuuden hallinta on mahdollista.

Yksinkertaistetaan organisaation omalle kielelle

Vaikka vaatimuksia tulee monesta lähteestä, rakennetaan vain yksi omaan toimintaan sisäänrakennettu kyberturvallisuusprosessi, organisaation omalla kielellä.

Yhteistyö ja avoimuus

Yhteistyö ja oppien avoin jakaminen on nyt entistä tärkeämpää. Esim. ISAC-tiedonvaihtoryhmät ja muut verkostot. Miksei hyödynnettäisi avointa kehitystä myös kyberturvallisuudessa!

RAKENTAVAA AKTIVISMIA

Cyberismo edustaa rakentavaa aktivismia, jonka tarkoitus on tehdä digitaalisesta maailmasta turvallisempi.

Meidän missiomme on rakentaa tätä muutosta yhteistyössä ja avoimuuteen perustuen.

CYBERISMO!

CYBERISMO!

> Make a difference in cybersecurity.