**Tietoturvan kehittäminen automaatioverkoissa**

Kalle Luukkainen, Head of Industrial Internet Security, Nixu Oyj

Modernit automaatiojärjestelmät ovat tänä päivänä pitkälle verkottuneita ympäristöjä. Teollisella internetillä haetaan merkittävää kilpailuetua, mutta samalla liiketoiminnasta tulee entistä riippuvaisempaa verkottuneiden järjestelmien turvallisuudesta.

Digitaaliseen liiketoimintaan kohdistuvat uhkakuvat kehittyvät kovaa vauhtia: Satunnaisesti leviävien haittaohjelmien rinnalle on tullut räätälöityjä ja kohdistettuja hyökkäyksiä. Motiivi on muuttunut rikolliseksi rahan tienaamiseksi, kiristykseksi ja valtiolliseksi tiedustelutoiminnaksi.

Myös kumppaneiden vastuulla olevat etäyhteydet, integraatiorajapinnat, pilvipalvelut ja esimerkiksi kumppaneilta tulevat ohjelmistopäivitykset voivat tarjota hyökkäysreitin automaatiojärjestelmään.

Nixun havaintoihin perustuen suurimmat teollisuuden haasteet tietoturvaan liittyen ovat: Tietoturvaan liittyvien vastuiden määrittely; tietoturvan hallinnan ja teknisen tason jatkuva kehittäminen; sekä tietoturvaan liittyvä havainnointi- ja reagointikyky.

Tietoturvaa arvioidessa on syytä tarkastella sekä  hallinnollista tietoturvaa (prosessit, dokumentointi, sopimukset, riskienhallinta), että teknistä tietoturvaa (verkot, laitteet ja ohjelmistot). Sopimuksiin kirjattujen vaatimusten toteutumista järjestelmätasolla ei voi tietää ilman tietoturvatestausta, ja testauksessa tehtyjen havaintojen säännönmukaisuus voidaan todentaa vain, jos siihen liittyvä prosessi on tarkastettu.

Tietoturvan hallinta järjestelmien elinkaaren aikana tuo omat haasteensa: Niin automaatioverkon suojaaminen elinkaaren kaikissa vaiheissa, kuin ”big datan” suojaaminen ja omistajuudesta sopiminen asiakassuhteen elinkaaren aika on välttämätöntä. Lisäksi on huomioitava mahdolliset elinkaaren aikana tapahtuvat muutokset vastuissa.

Hyvään tietoturvallisuuteen ei riitä pelkästään suojaavat kontrollit, vaan samalla on kehitettävä myös kykyä havaita läpi päässeet tietoturvaloukkaukset ja kykyä reagoida niihin.

Tietoturvan tilannekuva automaatiojärjestelmissä mahdollistaa tietoturvatapahtumien tehokkaan valvonnan, mutta voi myös parantaa prosessin toimintavarmuutta. Ongelmatilanteissa vaaditaan yhteistyötä ja harjoiteltuja toimintamalleja automaatiojärjestelmän operaattoreiden, tietoturvavastaavien, mahdollisen ulkoisen tietoturvakumppanin, sekä automaatiotoimittajan kesken. Esityksessä esitetään näkökulmia tietoturvan tilannekuvan kehittämisen ja ylläpitämisen toimintamalleista.