Avuksi tilannekuva koko laitoksesta

TEKSTI JARKKO BÖHM, MIPRO OY

Laaja-alaiset automaatiojärjestelmät yltävät verkon kautta jopa tuhansille koneille ja henkilöihin. Tietoturvariskien tunnistaminen on hankalaa mutta mahdollista, jos käytettävissä on tilannekuva koko laitoksesta.

Automaatio ja sen järjestelmät yhdistetään helposti pelkästään koneiden, laitteiden ja prosessien ohjaukseen ja valvontaan. Automaatiojärjestelmiin liittyy kuitenkin käyttökohteesta riippuen erinäinen määrä taustajärjestelmiä sekä valvomo- ja ohjausjärjestelmiä, jotka ovat välttämättömiä tuotantolaitoksen tehokkaan toiminnan kannalta.

Tietoturvan kannalta katsottuna kaikki nämä järjestelmät sekä niiden käyttäjät muodostavat kokonaisuuden, jonka osat ovat toisistaan riippuvaisia.

Tätä ei välttämättä tiedosteta yrityksissä. Automaatiojärjestelmän turvallisuus ulkoisia uhkia vastaan on kuitenkin yhtä hyvä kuin sen huonoimman osan tietoturva.

"TEKNISELLÄ SUUNNITTELULLA VOIDAAN RAJATA UHKIA JA NIIDEN VAIKUTUKSIA JÄRJESTELMÄÄN."

Automaatiojärjestelmän laajuus voidaan määritellä eri tavoin: teknisesti tarkasteltuna automaatiojärjestelmän laajuus määräytyy sen perusteella, kuinka suuri määrä laitteita pystyy kommunikoimaan tietoverkon avulla toistensa kanssa. Tämä on yleisin tapa rajata automaatiojärjestelmän koko.

Jos laajennetaan näkökulmaa, järjestelmän koko on yhtä kuin laitteiden määrä sekä ihmisten määrä, jotka pääsevät järjestelmään käsiksi.

Tarkastelussa on otettava huomioon myös etäyhteyksien kautta järjestelmään pääsevät henkilöt ja heidän käyttämänsä yhteydet. Jos etäyhteyksiä ei suojata asianmukaisesti, ajaudutaan ei-toivottuun tilanteeseen, jossa järjestelmän koko on yhtä kuin koko internet: tällöin järjestelmän voidaan kai katsoa olevan jo liian laaja.

Näitäkin tapauksia on maailmalta löytynyt useita. Wired-lehden tekemässä tutkimuksessa löydettiin 30 000 avointa järjestelmää, joista osa ei kysynyt edes salasanaa (www.wired.com/threatlevel/2013/11/internet-exposed).

Tietoverkkojen toiminnan turvaaminen ja turvallisuus

Tietoturvallisten verkkojen suunnittelu ja toteutus perustuu riskien ja uhkien arviointiin. Jos arviointia ei tehdä, tai se tehdään huolimattomasti, ei lopputuotekaan voi olla kovin tietoturvallinen tai luotettava.

Arvioinnissa on selvitettävä niin sisäiset kuin ulkoisetkin uhkat. Teknisen arvioinnin lisäksi on arvioitava myös käyttäjistä tai yhteistyökumppaneista aiheutuvat riskit.

Myös automaatiojärjestelmien pitkä elinikä aiheuttaa ongelmia tietoturvan ja luotettavuuden varmistamiseen. Järjestelmät saattavat olla uutena turvallisia ja luotettavia sen ajan mittapuun mukaan, mutta tilanne voi olla täysin toinen kymmenen vuoden päästä.

Sen vuoksi automaatiojärjestelmän ja sen taustajärjestelmien tietoturva- ja toiminnallisuusuhkia pitää kartoittaa koko järjestelmän elinkaaren ajan.

Tietoturvallisuudesta ovat vastuussa kaikki tahot, jotka liittyvät järjestelmään joko toimittajan, ylläpitäjän tai käyttäjän ominaisuudessa.

Turvallisuuskulttuuri tarkoittaa muun muassa tapaa, jolla automaatiojärjestelmien suunnittelu, toteutus ja ylläpito toteutetaan. Sitä tulee kehittää koko ajan, koska järjestelmät eivät ole koskaan täysin suojassa.

Tavoitteena turvallisuuskulttuurin luomisessa on lisätä tietoisuutta tietoliikenteeseen liittyvistä riskeistä, niin toteutuksen kuin myös ylläpidon aikana sekä sopia toimenpiteistä ja menettelyistä järjestelmän elinkaaren aikana. Turvallisuuskulttuu-

Automaatiojärjestelmä on kokonaisuudessaan laaja verkko erilaisia järjestelmiä ja käyttäjiä, joiden riippuvaisuudet toisistaan on huomioitava turvallisuuden ja tietoturvan hallinnassa.

rin avulla sitoutetaan myös muut järjestelmässä toimivat toimittajat samanlaiseen menettelyyn tietoturvan osalta.

Turvallisuuskulttuurin määrittelee järjestelmän loppukäyttäjä

Turvallisuuskulttuurin tulee olla yhteneväinen kaikkien järjestelmään liittyvien toimijoiden osalta; yksittäisen järjestelmän turvallisuuskulttuurin määrittelee järjestelmän loppukäyttäjä. Jos loppukäyttäjällä ei ole käytössään sopivaa turvallisuuskulttuuria, voi järjestelmän toimittaja suositella turvallisuuskulttuurin määrittelyä järjestelmän toimittamisen ohessa.

Jos kuitenkin järjestelmän toimittamisen aikana havaitaan, että tilaajalla ei ole kykyä tai halua toteuttaa toivottua turvallisuuskulttuuria, tulee tämä ottaa huomioon järjestelmän teknisessä suunnittelussa. Suunnittelulla voidaan rajata erilaisia uhkia ja niiden vaikutuksia järjestelmän toimintaan.

Turvallisuutta arvioitaessa on osattava tunnistaa automaatiojärjestelmän koko laajuus. Järjestelmän turvallisuuteen liittyvät esimerkiksi operaattoreiden tietoliikenneverkot.

Jos vaihdetaan tietoliikenneoperaattoria, on arvioitava myös operaattorin turvallisuuskulttuuri sekä verkon tekninen turvallisuus. Operaattorin kanssa on myös sovittava menettelyistä, miten operaattori huoltaa verkkoa ja ilmoittaa ennakkoon huoltokatkoista.

> “KAIKKIEN EI TARVITSE PÄÄSTÄ ETÄNÄ KÄSIKSI JÄRJESTELMÄÄN.”

Jokaisessa järjestelmässä on myös kunnossapitäjien yhteyksiä. Nämä ylläpitoyhteydet yleensä antavat oikeudet koko järjestelmän hallintaan ja muodostavat siksi merkittävän riskin järjestelmän toimintaan ja tietoturvaan.

On tärkeää, että yhteyden tekninen suojaus on kunnossa ja toteutettu esimerkiksi VPN-tekniikalla. Syytä on myös tehdä rajaus siitä, kuinka moni tarvitsee yhteyttä: kaikkien ei tarvitse päästä etänä käsiksi järjestelmään.

Järjestelmien keräämien tietojen tietoturva

Automaatiojärjestelmät tuottavat runsaasti informaatiota. Sen käyttö tai informaation merkityksen tunnistaminen ei kuitenkaan ole itsestään selvää.

Monesti tietojen tärkeyttä vähätellään ja ajatellaan, että esimerkiksi automaatiojärjestelmän lokitiedolla ei ole merkitystä tuotannon tehostamisessa, tuotantokatkojen estämisessä tai tietoturvamielessä yrityssalaisuuksien vuotamisessa ulkopuolisille.

Jos tietojen tärkeyttä ei tunnisteta, ei tietoja myöskään säilytetä tai kerätä järjestelmällisesti tai turvallisesti. Tiedot

voivat hävitä laiterikkojen takia, koska jos tietoja ei nähdä tarpeellisiksi, ei niitä myöskään yleensä varmuuskopioida tai säilytetä asianmukaisesti.

Automaatiojärjestelmän suunnittelussa tulisikin ottaa huomioon myös järjestelmän toiminnan seuranta ja seurannasta saatujen tietojen esittäminen erilaisina raportteina.

Tietoturvariskit voi selvittää lokitiedoista

Lokitietojen analysointi auttaa havaitsemaan myös ennen tunnistamattomia riskejä järjestelmän tietoturvassa. Epänormaalit toiminnot tai kirjautumiset voidaan havaita järjestelmästä ja niiden perusteella osataan ryhtyä selvittämään järjestelmän epänormaalia toimintaa.

Tietoturvariskien tunnistaminen lokitiedoista auttaa myös tunnistamaan uhkia, sillä yleensä tietoturvaan liittyvät uhkat, joita ei ole osattu ottaa huomioon suunnitteluvaiheessa, paljastuvat vasta hyökkäyksen tapahduttua. Jos analysointia ei tehdä, voi hyökkääjä jatkaa järjestelmän tutkimista, käyttämistä tai sabotoimista ilman vastatoimenpiteitä.

Jos kyseessä on haittaohjelma, jota suojausohjelmistot eivät tunnista, on erittäin tärkeää tietää, miten järjestelmä toimii optimaalisesti ja verrata sitä nykytilanteeseen.

Yleisimmin käytössä olevat valvomot esimerkiksi näyttävät prosessin sen hetkisen tilan ja vain kokenut käyttäjä, joka tietää, miten prosessi toimii optimaalisesti, voi havaita poikkeavia tapahtumia laitoksen tilassa.

Avuksi tilannekuva koko laitoksen toiminnasta

Vasta viime aikoina on havaittu, että automaatiojärjestelmien valvomot eivät välttämättä tarjoa riittävästi tietoa järjestelmää operoiville henkilöille. Valvomojärjestelmä saattaa välittää tietyn automaatiojärjestelmän tilatiedot, mutta muista automaatiojärjestelmistä ei välttämättä tule tietoja, ainakaan samalle työasemalle.

Tilannekuva koko laitoksesta toisi ongelmaan helpon ratkaisun. Tilannekuvassa ei tarvitsisi näyttää jokaisen automaatiojärjestelmän osan tilaa, vaan tuotantoon ja kunnossapitoon liittyvät olennaiset tiedot voitaisiin kerätä yhteen näyttöön, josta käyttäjät näkisivät yhdellä silmäyksellä, onko tarvetta toimenpiteisiin.

Tilannekuvaan voidaan myös liittää tietoja reaaliaikaisesta lokitiedon analysoinnista. Tällöin epänormaalit toiminnot voidaan ilmaista tilannekuvassa hälytyksenä. Tällaisia tietoja ovat esimerkiksi kirjautumiset järjestelmään, komentojen annot ja antajat sekä tiettyjen raja-arvojen ylitykset.

Tilannekuvanäytöt toisivat suuria hyötyjä erityisesti maantieteellisesti laajalle alueelle levittäytyneen automaatiojärjestelmän käyttöön ja ylläpitoon. Esimerkkinä sellaisista järjestelmistä ovat rautateiden turvalaitejärjestelmät sekä vesi- ja energiahuollon järjestelmät, joihin esimerkiksi myrskyt tai muut vastaavat luonnonilmiöt aiheuttavat vikatilanteita. AV