RENECO

Verkostoautomaatiojärjestelmien tietoturva

2013

Sisällysluettelo

VERKOSTOAUTOMAATIOJÄRJESTELMIEN TIETOTURVA

1 JOHDANTO

Tietoturvauhkat lisääntyvät riippumatta verkkoyhtiöiden toiminnasta. Julkinen media kirjoittaa nykyään varsin laajasti tietoturvarikkomuksista luoden uhkaavaa ilmapiiriä.

Kaikissa sähköyhtiöissä tietoturva on osana käytännön toimintaa ja järjestelmissä on huomioitu tietoturvan vaatimuksia. Nykyinen tietoturvan taso ei kuitenkaan ole riittävä, koska sähköverkon käytön toiminnat ja niitä tukevat verkostoautomaatiojärjestelmät monipuolistuvat nopeasti luoden niin toimintaan kuin järjestelmiin haavoittuvuuksia. Haavoittuvuuksia lisää myös tiedon määrän ja käsittelyn kasvu sähköverkkoliiketoiminnassa samoin kuin toiminnan tehostamisen edellyttämä tiedon avoimempi jakaminen. Vihamielisten tahojen aktiivisuus ja toimintatapojen monipuolisuus kasvavat lisäten painetta tietoturvallisuuden parantamiseksi sähköverkkojen yhteiskunnallisen kriittisyyden vuoksi.

Tietoturva käsitteenä ja toimintana ei ole kovin selkeä ja konkreettinen. Verkkoyhtiöiden johto kokee tietoturvallisuuden hieman hämäräksi, ”märäksi saippuaksi”, josta on vaikea saada kunnon otetta. Tietohallinnon ja tietoturvan ammattilaisten toimintaa puolestaan rajoittaa kustannusten kohtuullistamisen paineet. Selkeää tietoturvallisuuden tavoitetilaa ei ole juurikaan määritelty aiheuttaen jatkuvan keskustelun siitä, mitkä toimet ja ratkaisut ovat riittäviä. Järjestelmien toimittajat ja tilaajat eivät myöskään ole vielä löytäneet roolejaan ja vastuitaan tietoturvallisten ratkaisujen rakentajina ja ylläpitäjinä.

Monien maiden niin kuin Suomenkin viranomaiset ja alan järjestöt toimivat jo aktiivisesti yhteiskunnan huoltovarmuuskriittisten toimintojen tietoturvallisuuden parantamiseksi. Tästä on yhtenä osoituksena tämä Energiateollisuuden edistämä selvitys verkostoautomaatio-järjestelmien tietoturvasta.

Tässä selvityksessä on varsin laajasti perehdytty tietoturvauhkiin ja loukkausten syntymekanismeihin. Selvityksessä on kuvattu hyviä teknisiä ratkaisuja ja käytäntöjä, joita verkkoyhtiöt voivat hyödyntää omassa kehitystyössään. Samoin on hahmotettu tarvittavia toimenpiteitä, joilla verkkoyhtiö voi parantaa omaa tietoturvaansa lyhyellä, keskipitkällä ja pitkällä aikavälillä. Näiden haasteena on verkkoyhtiöiden erilaisuus niin koon kuin yritysrakenteen suhteen, jolloin ei ole olemassa ”one-size-fits-all”-ratkaisuja. Toteutettavat ratkaisut pitää rakentaa yhtiökohtaisesti.

Selvityksen yhteydessä tehdyssä kyselyssä verkkoyhtiöille samoin kuin avainhenkilöiden haastatteluissa kartoitettiin tietoturvan tasoa suomalaisissa verkkoyhtiöissä. Kaikissa yhtiöissä tietoturvaan kiinnitetään nykyään lisääntyvässä määrin huomiota. Taso ei kuitenkaan ole yhtenäinen vaan se vaihteli varsin paljon yhtiöittäin. Verkkoyhtiön koolla ja näkyvyydellä on huomattava vaikutus panostukseen tietoturvaan.

Hyvä tietoturva edellyttää yrityksen johdon sitoutumista turvallista toimintaympäristöä rakentavaan johtamismalliin – turvallisuusvastuuta ei voi ulkoistaa. Tietoturvan parantaminen ja ylläpitäminen ovat jatkuvaa tekemistä, joka pitää saada osaksi kaikkien jokapäiväistä työskentelyä ja toimintaprosesseja.

Tässä raportissa toimeksiannon tavoitteiden mukaisesti painopisteenä on tekninen tietoturva. Myös tietoturvan muita osa-alueita käsitellään niiltä osin kuin se on tarpeen painopisteen kattavan käsittelyn ja keskeisten käsitteiden selkeyttämisen vuoksi.

Osa tämän raportin ehdotuksista saattaa tuntua melko tiukilta vaatimuksilta nykyiseen tilanteeseen verrattuna. Tämä on mielestämme tarpeen, koska tietoturvauhkat ovat lisääntyneet nopeasti, haavoittuvuuksien määrä tuntuu pikemminkin kasvavan järjestelmäintegraatioiden ja toiminnan monipuolistumisen sekä toimintojen ulkoistamisen johdosta. Lisäksi rikollinen toiminta on tullut ammattimaisemmaksi ja yllätyksellisemmäksi. Toisaalta keinoja tietoturvan parantamiseksi on käytettävissä, toimenpidesuosituksia ja teknisiä ratkaisuja on koottu raportin loppupuolelle.

2 SELVITYKSEN TAUSTAT JA TEKOTAPA

2.1 Selvityksen taustaa

ICT-teollisuudessa viimeisen vuosikymmenen jatkunut internet- ja IP-teknologian kehitys näkyy vahvasti myös sähköverkkoyhtiöiden verkostoautomaatio- ja verkonhallinta-järjestelmien rakenteessa, ominaisuuksissa sekä niitä palvelevissa tietoliikenneratkaisuissa.

Internetin ja ethernet-pohjaisten lähiverkkojen sekä IP-protokollan kasvava rooli erilaisten automaatio-, hallinta- ja mittausratkaisujen rakennusosina sekä voimakkaasti lisääntynyt järjestelmien välinen tiedonsiirto ovat kasvattaneet tietoturvariskejä tuntuvasti myös sähköverkkoympäristössä.

Uudeksi kyberturvallisuusuhaksi perinteisten hakkereiden ja tietorikollisten rinnalle ovat nousseet valtiolliset tiedustelupalvelut ja kybersodankäyntiin erikoistuneet yksiköt. Sähköverkkojen keskeinen asema osana yhteiskunnan infrastruktuuria edellyttää verkkoyhtiöiltä entistä kattavampaa varautumista kasvaviin tietoturva- ja kyberturvallisuusuhkiin. Viranomaiset ja alan muut toimijat ovat seuranneet tilanteen kehittymistä pitkään ja käynnissä on useita hankkeita ja selvityksiä, joilla yhteiskunnan kriittisien toimintojen jatkuvuus pyritään varmistamaan uusien turvallisuusuhkien suhteen.

Reneco Oy on asiantuntijaorganisaatio, joka tuottaa palveluja energiayhtiöiden toiminnan kehittämiseen erityisenä vahvuutena sähköyhtiöiden ICT-järjestelmät. Energiateollisuuden tämän vuoden toimintasuunnitelmaan on kirjattu sähköverkkoyhtiöiden verkostoautomaatio- ja tietoliikennejärjestelmien tietoturvaan liittyviä tavoitteita. Tämän perusteella Renecon tekemä tutkimusehdotus hyväksyttiin Sähkötutkimuspoolin yhdeksi tutkimusaiheeksi ja rahoituksen piiriin. Hanketta rahoitti jossain määrin Renecon itsensä lisäksi myös alan teollisuus.

Selvityksen kohteeksi rajattiin sähköverkkoyhtiöiden verkostoautomaatiojärjestelmät ja niihin läheisesti liittyvät tietoliikennejärjestelmät ja -yhteydet. Työssä ei käsitellä sähkön toimitusmittauksiin liittyviä järjestelmiä (AMR).

2.2 Selvitykselle asetetut tavoitteet

Selvityksellä asetettiin seuraavat tavoitteet:

1. Arvioida sähköverkkoyhtiöiden verkostoautomaatiojärjestelmien tärkeimpiä turvallisuusuhkia painopisteen ollessa tietoturvassa
2. Kerätä kattava näkemys verkostoautomaatio- ja niihin liittyvien tietoliikennejärjestelmien tietoturvan nykytilasta
3. Kuvata järjestelmien kehittämistarpeita ja vaatimuksia tietoturvan suhteen
4. Koota käytännön suunnitteluohjeistoa ja hyviä käytäntöjä tietoturvallisen verkostoautomaatioympäristön rakentamiseksi
5. Kuvata periaateratkaisuja ja esittää järjestelmäesimerkkejä tietoturvallisen järjestelmäympäristön luomiseksi ja ylläpitämiseksi
6. Arvioida inhimillisen toiminnan ja menettelytapojen osuutta tietoturvallisen sähköverkkoympäristön toteuttamisessa ja ylläpitämisessä

2.3 Työn toteutustapa

Työ tehtiin suunnitteluvaiheen jälkeen seuraavasti:

1. Perehdyttiin aiheeseen liittyviin kansainvälisiin ja kansallisiin raportteihin, selvityksiin ja artikkeleihin (mm. Cigre-raportit, NIST- ja CPNI-aineisto, TITAN-käsikirja, alan standardit, normit ja ohjeistus), /1/ - /5/, /7/, /8/ ja /11 - /20/. Osion avulla selvitettiin verkostoautomaatiojärjestelmien tyypillisimpiä tietoturvauhkia sekä pyrittiin kokoamaan lista parhaista suosituksista ja sovellettavista standardeista.
2. Nettikyselyn avulla tehtiin luottamuksellinen kartoitus kohteena sähköyhtiöt. Erityisesti kyselyllä kartoitettiin verkostoautomaatiojärjestelmien tietoturvan nykytilannetta
    - Nettikyselyn tavoitteena oli saada vastaukset 25-30 sähköyhtiöltä ennalta laadittuihin kysymyksiin
    - Kysely lähetettiin kaikille sähköyhtiöille, jotka ovat Energiateollisuuden jäseniä
    - Vastaukset saatiin 28 yhtiöltä
3. Luottamukselliset haastattelut alan toimijoiden keskuudessa tavoitteena saada kattava yleiskuva verkostoautomaatiojärjestelmien tärkeimmistä uhista, kerätä tietoa hyvistä käytännöistä ja toimintamalleista

Haastatteluja tehtiin seuraavasti:

- Sähköyhtiöt 17 kpl
- Verkostoautomaatio- ja hallintajärjestelmien toimittajat 3 kpl
- Tietoliikennelaitteiden toimittajat ja teleoperaattorit 2 kpl
- Tietoturvaratkaisujen ja palvelujen tuottajat 3 kpl
- Viranomaiset 1 kpl

Työ tehtiin touko-syyskuun aikana 2013.

2.4 Projektin ohjausryhmä ja resurssit

Tämän selvitystyön ohjausryhmässä toimivat Kenneth Hänninen Energiateollisuus, Janne Stark ABB, Harri Nummenpää KSOY Verkko, Antti Vähälä Fortum Distribution sekä Jouko Tervo ja Jukka Perttala Reneco.

Työn päävastuullisena tekijänä toimi Jouko Tervo. Projektiaineistoa analysoi, kommentoi ja tarkasti Jukka Perttala.

Kiitokset ohjausryhmän jäsenille hyvistä neuvoista ja kommenteista.

3 SÄHKÖVERKKOJEN AUTOMAATIOJÄRJESTELMÄT

3.1 Verkostoautomaation sekä verkonkäytön järjestelmät

Tässä selvityksessä verkostoautomaatiojärjestelmällä tarkoitetaan tietojärjestelmää tai automaatiolaitetta, jolla suoraan ohjataan sähköverkon kytkentätilaa, säädetään verkon suureita tai suojataan sähköverkon toimilaitteita. Oleellisen osa verkostoautomaatio-järjestelmiä ovat erilaiset tiedonsiirtoyhteydet ja tietokannat, joita nämä järjestelmät tarvitsevat toimiakseen halutulla tavalla.

Sähköverkon käyttökeskuksen keskeiset tietojärjestelmät ovat käytönvalvonta- ja käytöntukijärjestelmät.

Käytönvalvontajärjestelmällä pidetään yllä ja valvotaan sähköverkon tilaa sähköasemilta kerättyjen mittausten ja tilatietojen avulla. Käytönvalvontajärjestelmällä voidaan ohjata sähköasemilla olevia katkaisijoita ja erottimia sekä muita toimilaitteita samoin kuin siirto- ja jakeluverkon keskeisiin kohteisiin rakennettuja maastoerottimia. Käytönvalvontajärjestelmä voi olla yhteydessä myös muiden sähköverkkoyhtiöiden käytönvalvontajärjestelmiin. Tällä yhteydellä välitetään mittauksia ja tilatietoja esimerkiksi yhteisiltä sähköasemilta tai rajapisteistä.

Käytöntukijärjestelmällä pidetään yllä sähköverkon kytkentätilaa. Käytöntukijärjestelmä saa toimilaitteiden tilatiedot ja mittaustiedot sähköverkosta käytönvalvontajärjestelmältä. Tämä tiedonsiirto on yksisuuntaista. Sähköt päällä -tiedot ja jännitetasotiedon etäluettavilta mittareilta on myös voitu liittää käytöntukijärjestelmään mittaustietojen keruujärjestelmästä. Kaiken kaikkiaan käytöntukijärjestelmä on liitetty hyvin moneen muuhun tietojärjestelmään joko sen tarvitsemien tietojen takia (esimerkiksi asiakastiedot) tai sen tuottamien tietojen takia (esimerkiksi sähkökatkot). Käytöntukijärjestelmä saa verkkotiedot verkkotieto-järjestelmästä. Käytöntukijärjestelmä ei ole varsinainen verkostoautomaatiojärjestelmä, mutta se on otettu tarkasteluun mukaan sen käyttötoiminnassa olevan keskeisen roolin ja uusien automaatiosovelluksia takia. Edelleen käytöntukijärjestelmällä on useita liityntöjä muiden sähköyhtiön tietojärjestelmien kanssa ja sillä on useita sekä sisäisiä että ulkoisille sidosryhmille tarkoitettuja web-sovelluksia.

Sähkönsiirto- ja jakeluverkko on suojattava vikatilanteiden, epänormaalien kuormitustilanteiden tai ulkoisten uhkien varalta automaattisesti toimivilla suojalaitteilla (suojareleillä). Verkon suojaustarve määräytyy pitkälle verkon rakenteesta. Silmukoitu kantaverkko tarvitsee kattavan ylivirta- ja jännitesuojauksen lisäksi diffentiaali- ja distanssisuojia. Kantaverkon erityisiä käyttötilanteita hallitsemaan on rakennettu hätäteho-yms. kuormien ohjaukseen käytettäviä ratkaisuja. Uudet suojausratkaisut, mm. verto- ja distanssisuojat alkavat yleistyä myös keskijänniteverkoissa. Sähköverkon rakenteen monimutkaistuessa, esimerkiksi hajautetun tuotannon takia, keskijännite- ja myös pienjänniteverkon suojaustarve kasvaa ja monipuolistuu entisestään.

Sähköasema-automaatio lisääntyy koko ajan tuoden erilaisia tukijärjestelmiä sähköasemille. Sähköasemille rakennetaan myös kasvavassa määrin erilaisia sähköisiä turvallisuusjärjestelmiä.

Yleisimpiä niistä ovat etävalvonnan mahdollistavat video- ja kulunvalvontajärjestelmät. Videojärjestelmiä voidaan käyttää myös käyttötoiminnassa sähköverkon tilan todentamiseen, esimerkiksi varmentamaan erottimien kytkentätila.

Kaikkia edellä mainittuja verkoston automatisointiin käytettäviä järjestelmiä on ylläpidettävä. Niihin tehdään ohjelmistopäivityksiä uusien ominaisuuksien saamiseksi, virheiden korjaamiseksi ja tietoturvan ylläpitämiseksi.

Kaikilla järjestelmillä on useita käyttäjiä, kuten käytönvalvojat, urakoitsijoiden henkilöstö ja valmistajien tukihenkilöt; Käytöntukijärjestelmää hyödynnetään asiapalvelun toteuttamisessa ja mahdollisesti myös viranomaisyhteistyössä. Osa näistä käyttäjistä voi liittyä järjestelmiin omilla työasemillaan.

Tietoturvan kannalta useat järjestelmien liitynnät muihin tietojärjestelmiin ja julkiseen tietoverkkoon ovat haasteellisia samoin kuin useat erityyppiset käyttäjätahot.

3.2 Tietoliikennejärjestelmät

Selvitystyössä rajauduttiin verkostoautomaation ja verkonkäytön järjestelmien tarvitsemien tietoliikenneyhteyksien toteuttamisessa käytettyihin tietoliikennejärjestelmiin ja –palveluihin. Käyttötoiminnan henkilöviestintään käytettäviä tietoliikennejärjestelmiä käsitellään niiltä osin kuin niitä käytetään verkostoautomaation yhteyksiin. Tässä selvityksessä on huomioitu seuraavat verkostoautomaatiossa yleisesti käytetyt tietoliikenneyhteydet:

1. Käytönvalvonnan tietoliikennejärjestelmät
    - Metallijohtimiin ja valokuituihin pohjautuvat kaapelijärjestelmät
    - Radiolinkit ja radiomodeemit
    - Matkaviestiverkot, omat suljetut radioverkot ja erillisverkot (VIRVE)
    - Julkiset kiinteät televerkot ja satelliittiyhteydet
    - Perinteinen piirikytkentäinen tietoliikenne ja IP-pohjainen tiedonsiirto
    - Tietoliikenneyhteyksien suojausmenetelmät
2. Suojausyhteydet ja niiden erityispiirteet
3. Sähköasemien sisäiset yhteydet, lähiverkot ja etätyöskentelyratkaisut
4. Yhtiön sisäiset lähi- ja laajaverkot soveltuvin osin
    - Käytön tietojärjestelmien ja niiden lähiverkkojen yhdyskäytävät sähköyhtiön muihin lähi- ja laajaverkkoihin
5. Extranet, internet ja julkiset tietoverkot niiltä osin kuin ne liittyvät verkkoyhtiön verkostoautomaatiojärjestelmiin
    - Yhdyskäytävien toteuttaminen, suojaaminen ja tietoturva

4 AUTOMAATIOJÄRJESTELMIEN TURVALLISUUSRISKIT JA –UHKAT

4.1 Yritys- ja tietoturvallisuudesta

Yritysturvallisuuden osa-alueita on havainnollistettu Elinkeinoelämän keskusliiton laatimassa oheisessa kuvassa.

Kuva 4-1. Elinkeinoelämän keskusliiton näkemys yritysturvallisuuden osa-alueista

Turvallisuusjohtaminen on osa normaalia yrityksen johtamista ja liiketoiminnan jatkuvuuden varmistamista. Yritysjohto määrittelee yritysturvallisuuden tavoitteet, toiminnan organisoinnin ja seurannan. Tästä käytetään yleisnimitystä turvallisuuspolitiikka. Turvallisuusnäkökohdat otetaan mukaan strategiseen suunniteluun ja päätöksentekoon.

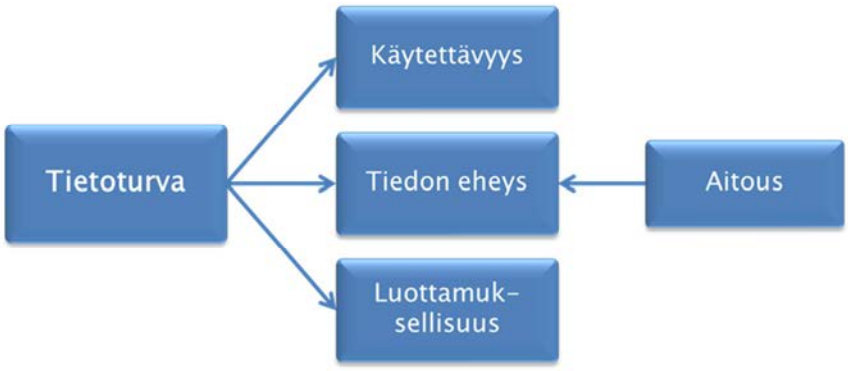
Turvallisuus ei ole erillinen toiminto vaan osa kaikkia yrityksen prosesseja. Turvallisuudelle tulee asettaa mittareita, joita seurataan ja raportoidaan säännöllisesti osana muuta toiminnan raportointia.

Turvallisuusvastuut on kohdennettava normaalin liiketoimintavastuujaon mukaisesti. Turvallisuushenkilöstö toimii asiantuntijoina tukien osaamisellaan toiminnasta johtamisvastuussa olevia esimiehiä ja muuta henkilöstöä.

Tieto- ja kyberturvallisuus

Tietoturva on varsin laaja käsite. Se kattaa kaikki keinot, joilla pyritään estämään tiedon tuhoutuminen, muuttuminen taikka joutuminen vääriin käsiin. Samalla kuitenkin tieto tulee pitää niiden saatavilla, joilla on siihen oikeus. Tieto voi olla sähköisenä, dokumentoituna tai puhuttuna.

Tietoturvaa arvioidaan usein kuvan 4-2 mukaisien informaation ominaisuuksien avulla (Sanastokeskus: Tiivis tietoturvasanasto).



Kuva 4-2 Tietoturvallisuuden ominaisuudet

Käytettävyydellä tai saatavuudella (availability) tarkoitetaan sitä, että tieto, järjestelmä tai palvelu on niihin oikeutettujen käyttäjien saatavilla ja hyödynnettävissä haluttuna aikana. Käytettävyys voidaan varmistaa huolehtimalla menetelmien ja järjestelmien luotettavuudesta, riittävällä järjestelmä- ja tiedonsiirtokapasiteetilla (ottamalla huomioon palvelunesto-hyökkäyksien mahdollisuus) sekä riittävillä varajärjestelmillä ja varmuuskopioilla.

Eheys (integrity) on tiedon ominaisuus, joka ilmentää sitä, ettei tiedon sisältöä ei ole luvattomasti muutettu tai se ei ole satunnaisten virheiden vuoksi muuttunut. Tyypillisiä ratkaisuja varmistaa tiedon eheys ovat pääsynhallinta, digitaaliset allekirjoitukset, tarkistussummat ja tarkistuskoodit.

Luottamuksellisuus (confidentiality) on tiedon ominaisuus, joka ilmentää sitä, että tieto on vain sen käyttöön oikeutettujen käytettävissä. Tietoliikenteen salausprotokollat kuten esimerkiksi HTTPS (Hypertext Transfer Protocol Secure) sekä järjestelmien pääsynhallintaan liittyvä vahva autentikointi ovat menetelmiä tiedon luottamuksellisuuden varmistamisessa.

Aitous tai kiistämättömyys (non-repudiation) on ominaisuus, joka ilmentää tiedon eheyttä ja sitä, että tiedon alkuperäinen lähde on se, joka sen väitetään olevan. Aitous voidaan todentaa muun muassa digitaalisin varmentein ja allekirjoituksin.

Tietoturvallisuuteen lasketaan muun muassa asiakirjaturvallisuus, sähköinen tietoturva, kilpailuherkkien menetelmien ja muun luottamuksellisen tiedon suojaaminen.

Kyberturvallisuus on käytännössä tietoturvallisuuden osa-alue, joka keskittyy sähköiseen tietojen käsittelyyn ja johon kohdistuu lähinnä vihamielisiä uhkatekijöitä. Kyberturvallisuus on ollut viimeaikoina medioissa paljon esillä Stuxnet- ja Flame-haittaohjelmien sekä valtiollisten vakoilu- ja turvallisuusorganisaatioiden toiminnan paljastusten ansiosta.

Tieto- ja kyberturvallisuudesta huolehtiminen on tärkeä osa riskien hallintaa ja liiketoiminnan jatkuvuuden varmistamista.

4.2 Tietoturvariskit ja kyberturvallisuusuhkat

4.2.1 Tietoturvauhkat

Verkostoautomaatiojärjestelmien tietoturvaa uhkaavat lukuisat tahot tai ei toivotut tapahtumat, onnettomuudet ja luonnonkatastrofit.

Yleisin tietoturvauhka on järjestelmien käyttäjät. Omat työntekijät tai ulkopuoliset palvelujen tuottajat voivat osaamattomuuttaan tai huolimattomuuttaan tärvellä tai tuhota tietoja. Harvinaisempaa on, että nämä henkilöt tahallisesti toimien sotkisivat tietoja, vaikka heidät tekee merkittäväksi uhkaksi osaaminen ja mahdollisuudet käyttää järjestelmiä ja voimajärjestelmän tuntemus.

Toisena varsin yleisenä uhkana tietoturvalle on järjestelmien laite- tai ohjelmistoviat. Varsinkin vasta käyttöönotetussa tietojärjestelmässä voi olla merkittävä määrä ohjelmistovirheitä, jotka paljastuvat vasta tuotannollisen käytön aikana. Tämän uhkan todennäköisyyttä lisää yhä monipuolistuvat järjestelmien toiminnallisuudet ja lisääntyvä järjestelmäintegraatio.

Taulukossa 4-1 on lueteltu tyypillisimpiä tietoturvauhkia aiheuttavia vihamielisiä tahoja. Taulukko perustuu pitkälle lähteen /7/ aineistoon.

Tietoturvaan vaikuttavia kehitystrendejä on taustoitettu hyvin esimerkiksi VTT:n TITAN-käsikirjassa, /8/.

Taulukko 4-1 Tunnistettuja uhkaavia tai vihamielisiä tahoja

Vihamielinen uhkaaja	Kuvaus
Hakkerit ja haktivistit	Hakkerit ja haktivistit pyrkivät murtautumaan tietojärjestelmiin urkkimalla käyttäjätunnuksia tai hyödyntämällä murtamiseen soveltuvia haittaohjelmia. Yleensä nämä haittaohjelmat ovat maksuttomasti internetistä saatavissa ja perustuvat tunnettuihin haavoittuvuuksiin. Hakkerit pyrkivät hankkimaan mainetta ja asemaa yhteisönsä keskuudessa. Haktivistit ajavat omia ideologioitaan ja levittävät propagandaa sijoittamalla niitä tukevia viestejä ilkivaltaisin tai rikollisin keinoin esim. yrityksen kotisivuille. Myös kohteen liiketoimintaa haittaavaa ilkivaltaa ja järjestelmien vahingoittamista esiintyy
Rikolliset	Rikollisten tavoitteena on taloudellisen hyödyn saaminen eri tavoin. Keinoina järjestelmiin murtautumisen avulla saatavat tietovarkaudet (esim. eri palvelujen tunnukset), joiden avulla tehdään taloudellisia tai aineellisia rikoksia. Tekijät voivat myös yrittää saada kohde tulemaan rikollisen omille huijaussivustoille. Järjestäytyneisiin luokiteltavat rikolliset käyttävät tyypillisesti myös tehokkaita maksullisia ja/tai heitä varten räätälöityjä haittaohjelmia
Terroristit	Terroristit voivat perinteisten omaisuutta tai ihmishenkiä uhkaavien fyysisten hyökkäysten lisäksi hyökätä erilaisilla murtumistyökaluilla kohteen kriittisiin järjestelmiin ja aiheuttaa niissä toimintahäiriöitä tai jopa pysyviä vaurioita
Bottiverkko-operaattorit	Bottiverkkojen ylläpitäjät ottavat haltuun kohteen tietojenkäsittelykapasiteettia rakentaakseen omia tarkoitusperiään palvelevia verkkoja. Näin saatuja verkkoja voidaan käyttää kohdennettuihin hyökkäyksiin, kuten esimerkiksi palvelunestohyökkäysiin (DoS-hyökkäys) ja roskapostin (SPAM) jakamiseen
Teollisuusvakoilijat	Teollisuusvakoilijat pyrkivät varastamaan taloudellisesti hyödynnettävää luottamuksellista tietoa kilpailijoiltaan tai tutkimuslaitoksilta keinoina murrot tietojärjestelmiin joko suoraan tai kohdeorganisaatiossa olevan myyrän avustuksella. Hyökkäystyökalut voivat olla tarkasti räätälöity kohteen erityispiirteiden perusteella. Sähköverkkoyhtiöille teollisuusvakoilu on pieni uhka
Valtiolliset tiedustelu- ja kybersodankäynnin organisaatiot	ICT-järjestemien roolin kasvaessa osana yhteiskunnan kriittistä infrastruktuuria on valtiollisten tiedusteluorganisaatioiden tärkeys ja resurssit kasvaneet huomattavasti. Lukuisat valtiot rakentavat tai jo omaavat kybertiedusteluun ja –sodankäyntiin erikoistuneita yksiköitä. Suurvalloilla niitä on lukuisia ja ne kukin ovat erikoistuneet erilaisiin kohteisiin ja toimivat hieman eri tavoin. Tiedustelutoiminnan tarkoituksena on hankkia kohteesta riittävästi tietoa kohdistetun hyökkäyksen toteuttamiseksi haluttaessa. Hyökkäyksellä pyritään lamaannuttamaan tai tuhoamaan kohdevaltion tieto- ja tietoliikennejärjestelmiä tai muuta tärkeää infrastruktuuria. Kybertyökalut voivat olla erittäin pitkälle kehitettyjä ja monimutkaisia ja niissä voidaan hyödyntää myös julkisesti tuntemattomia haavoittuvuuksia. Joidenkin tiedustelupalvelujen epäillään harjoittavan laajamittaista teollisuusvakoilua
Katkeroituneet henkilöt	Katkeroituneet henkilöt voivat olla yrityksen entisiä tai nykyisiä työntekijöitä, pettyneitä asiakkaita tai alihankkijoita. Ko. tahot pyrkivät eri keinoin esim. sabotoimaan kohdeyrityksen toimintaa tai saavuttamaan taloudellista etua laittomin keinoin. Avainasemassa olevien henkilöiden mielenterveys voi myös järkkyä. Sähköyhtiöissä tämä uhkakuva koetaan vähäiseksi.

4.3 Verkostoautomaatiojärjestelmien haavoittuvuudet

Kyberturvallisuusriskin toteutuminen edellyttää käytännössä haavoittuvuutta yrityksen tai sen henkilöstön toiminnassa tai tieto- tai tietoliikennejärjestelmissä.

Tässä luvussa käsitellyt haavoittuvuudet eivät ole tärkeysjärjestyksessä ja on luokiteltu haavoittuvuuden tunnistamis- ja eliminointimenetelmien perusteella seuraavasti:

1. Hallintoon ja johtamiseen liittyvät haavoittuvuudet
2. Varsinaisen verkostoautomaatiojärjestelmän (järjestelmäalusta ja sovellukset) haavoittuvuudet
3. Tietoliikenneverkon haavoittuvuudet

Haavoittuvuuden aiheuttaman uhkan vakavuuteen vaikuttaa uhkan toteutuessa lukuisat eri tekijät. Niitä ovat esimerkiksi seuraavat:

- Tietojärjestelmäarkkitehtuuri
- Käytössä olevat puolustusvälineet
- Hyökkäyksen edistyksellisyys
- Havaitsemiseen kulunut aika
- Tapahtuman välittömät vaikutukset
- Tapahtuman aiheuttamat taloudelliset ja muut vahingot

Jäljempänä olevissa taulukoissa on hyödynnetty lähteessä /7/ esitettyä aineistoa.

4.3.1 Hallintoon ja johtamiseen liittyvät haavoittuvuudet

Hallintoon ja johtamiseen liittyvät haavoittuvuudet johtuvat tyypillisesti puutteellisesta johtamisesta, huonosti toimivista prosesseista, heikoista tai puuttuvista ohjeista, kehnosta dokumentaatiosta ja henkilöstön puutteellisesta perehdytyksestä. Taulukossa 4-2 on lueteltu ja kuvattu tunnistettuja hallintoon ja johtamiseen liittyviä haavoittuvuuksia.

Taulukko 4-2 Hallintoon ja johtamiseen liittyviä haavoittuvuuksia

Haavoittuvuus	Kuvaus
Tietoturvapolitiikan ja johtamisen puutteet	Verkostoautomaatiojärjestelmien erityispiirteitä ei ole huomioitu tietoturvapolitiikkaa ja –ohjeistusta laadittaessa. Verkostoautomaatiojärjestelmien tietoturvan johtamista ei ole vastuutettu. Tietoturvan systemaattista seurantaa ja säännöllistä raportointia ei ole järjestetty tai vastuutettu.
Riskikartoituksen puutteet	Toiminnan jatkuvuutta uhkaavia riskejä ei ole tunnistettu riittävästi tai ennalta ehkäiseviin toimenpiteisiin riskien vaikutusten vähentämiseksi tai eliminoimiseksi ei ole ryhdytty
Henkilöstön tietoturvaosaaminen ja tietous puutteellista	Henkilöstön koulutus ja informointi on puutteellista. Ilman ajantasaista tietoturvapolitiikkaa ja –ohjeistusta, joihin henkilöstö on perehdytetty, ei todennäköisesti rakenneta ja ylläpidetä tietoturvallista verkostoautomaatioympäristöä
Haavoittuva tietojärjestelmäarkkitehtuuri	Verkostoautomaatiojärjestelmä on rakenteellisesti puutteellinen eikä sitä ole varustettu tietoturvauhkia estävällä, tunnistavilla ja eliminoivilla laitteilla ja ohjelmistoilla. Tietoliikenneverkkoa ei ole segmentoitu ja verkostoautomaatiojärjestelmien käyttöoikeuksien hallinta on leväperäistä tai muuten riittämätöntä. Ulkoisia tietoliikenneyhteyksiä ei ole suojattu riittävästi
Järjestelmien ja laitteiden rakentamisen ja häiriöpalauttamisen ohjeistus puutteellista	Järjestelmien suunnittelussa ja rakentamisessa käytettävää ohjeistusta tietoturvan huomioimisesta ei ole tai se on puutteellista. Jatkuvuussuunnittelun tuloksena syntyviä toipumissuunnitelmia ei ole tai ne ovat puutteellisia. Järjestelmien toipumissuunnitelman laadintaa ei ole vastuutettu.
Verkostoautomaatiojärjestelmän ja sitä tukevan tietoliikenneverkon konfiguraation hallinta puuttuu tai on riittämätön	Toimiva tietoturva edellyttää jatkuvaa ja ajantasaista järjestelmien ominaisuuksien ja parametroinnin hallintaa erityisesti tehtäessä järjestelmiin muutoksia. Parametroinnit ovat puutteellisia tai virheellisiä ja käytetään järjestelmien oletusasetuksia (tehdasasetuksia)
Puuttuvat auditoinnit tai katsastukset	Ulkopuolisten riippumattomien asiantuntijoiden on auditoitava säännöllisesti verkostoautomaatio- ja tietoliikennejärjestelmien rakenne, dokumentaatio, tietoturvapolitiikka/ohjeistus sekä käytön ja ylläpidon toimintatavat ja prosessit. Auditoijien on raportoitava vakavat löydökset ja tehtävä ehdotus niiden korjaamiseksi
Puutteellinen käyttöoikeuksien hallinta	Puutteet käyttöoikeuksien hallinnoinnissa ja autentikoinnin päivityksissä (esimerkiksi salasanojen vaihtaminen) lisäävät tunkeutumisriskiä tai antavat käyttäville liian laajoja oikeuksia tehdä järjestelmään haitallisia muutoksia

4.3.2 Verkostoautomaatiojärjestelmän haavoittuvuudet

Verkostoautomaatiojärjestelmäalusta muodostuu laitteista ja varusohjelmistosta (mm. käyttöjärjestelmä). Järjestelmäalustassa ajetaan toiminnallisuuden tuottavia sovellusohjelmia sekä mahdollisesti suojausohjelmia. Verkostoautomaatiojärjestelmän potentiaalisia haavoittuvuuksia on käsitelty seuraavasti:

1. Verkostoautomaatiojärjestelmän alustan rakenteen ja konfiguraation haavoittuvuudet
2. Verkostoautomaatiojärjestelmän fyysiset uhkat ja haavoittuvuudet
3. Varus- ja sovellusohjelmiston uhkat ja haavoittuvuudet

Seuraavissa taulukoissa kutakin haavoittuvuutta on käsitelty erikseen.

Taulukko 4-3 Verkostoautomaatiojärjestelmän alustan rakenteen ja konfiguraation haavoittuvuuksia

Haavoittuvuus	Kuvaus
Varus- ja sovellusohjelmistojen korjauspäivitykset puutteellisia	Automaatiojärjestelmiin tehtävät ohjelmistokorjaukset ja päivitykset ovat työläitä ja vaativat perusteellista testausta ennen tuotantoympäristöön asentamista. Tämä mahdollistaa haittaohjelmille laajan aikaikkunan tehdä hyökkäyksiä
Varus- ja sovellusohjelmistot vanhentuneita ja poistuneet ylläpidon piiristä	Ohjelmistot voivat olla niin iäkkäitä, että niitä ei enää ylläpidetä eikä korjauspäivityksiä ole saatavana, vaikka uusia haavoittuvuuksia löydettäisiin
Järjestelmän käyttöönotto ilman perusteellista testausta	Järjestelmän testaus voi olla puutteellista niin toimittajan kuin tilaajankin puolelta. Varsinkin tietojärjestelmissä voi olla paljon puutteita ja virheitä käytön alkaessa. Nämä voivat sisältää hyvin moninaisia uhkia tietoturvalle
Ohjelmistojen päivityksiä on toteutettu puutteellisin testauksin	Tietoturvapäivitysten puutteellisista testauksista johtuen järjestelmässä voi esiintyä toimintahäiriöitä tai se voi kaatua kokonaan. Ohjelmistopäivitysten ohjeistus tulisi laatia ja dokumentoida
Käytetään oletusparametrointia	Oletusparametrien käyttäminen varus- ja tietoliikenneohjelmistoissa jättää auki olevia tietoliikenneportteja sekä mahdollistaa haitallisten sovellusten ajamisen palvelimissa ja työasemissa
Kriittisistä järjestelmä-konfiguraatioista ja –parametreista ei ole varmuuskopioita	Järjestelmän haavoittuessa, kaatuessa tai toimiessa muutoin puutteellisesti järjestelmä palautetaan puutteellisilla tai vanhentuneilla asetuksilla ja tietomalleilla. Järjestelmä ei toimi oikein
Suojaamattomat kannettavat laiteet ja massamuistit	Luottamuksellinen aineisto tai muutoin sensitiivinen data voi joutua sopimattomalle taholle, mikäli niitä säilytetään huolimattomasti esimerkiksi salaamattomilla laitteilla tai muistivälineillä
Salasanat eivät ole käytössä	Verkostoautomaatiojärjestelmien osajärjestelmät ja työasemat tulee olla varustettu pääsyn ja käyttöoikeuksien hallinnalla asiattoman käytön estämiseksi
Salasanan paljastuminen	Salasanojen huolimattoman säilytyksen tai muun käsittelyn takia ne päätyvät asiattomiin käsiin aiheuttaen hyökkäysriskin
Salasanan riittämätön vahvuus	Hyökkääjä murtaa liian lyhyet, yksinkertaiset tai muutoin helposti johdettavat salasanat

Taulukko 4-4 Verkostoautomaatiojärjestelmä fyysisiä uhkia ja haavoittuvuuksia

Uhka / Haavoittuvuus	Kuvaus
Järjestelmälaitteiden riittämätön fyysinen suojaus	Valvomo- ja laitetilojen sekä sähköasemien fyysinen suojaus ja kulunvalvonta ovat riittämättömiä, mikä voi mahdollistaa asiattoman pääsyn laitetiloihin ja laitteisiin. Miehittämättömillä asemilla ei ole sähköistä video- tms. valvontaa. Riski laajalle kirjolle erilaisia haitallisia toimenpiteitä sekä uhka luonnonnettomuuksien ja poikkeuksellisten sääilmiöiden aiheuttamille vaurioille
Turvattomat ulkoiset yhteydet	Verkostoautomaatiojärjestelmien tietoverkkoon tulevat, huonosti suojatut ulkoiset yhteydet mahdollistavat asiattoman pääsyn laitteisiin/järjestelmiin. Palomuurit, DMZ-alueen välityspalvelimet etäkäytön RAS-palvelimet tms. ja IDS/IPS-järjestelmät ovat välttämättömiä turvallisen tietoverkon yhdysliikennekäytävissä. Suorat yhteydet julkiseen verkkoon automaatioverkosta eivät ole suositeltavia. Jos niitä on rakennettava pakottavista syistä, on niissä käytettävä lisäksi vahvaa salausta ja käyttäjien vahvaa autentikointia
Runsaasti järjestelmäliitäntöjä	Suuri määrä järjestelmistä lähteviä liityntöjä muihin järjestelmiin vaikeuttaa dataliikenteen hallinnointia ja se voi mahdollistaa asiattoman tiedonvälityksen järjestelmästä tai tietoverkosta toiseen
Dokumentoimattomat laite- ja ohjelmistokokoonpanot	Puutteellisesti dokumentoidut laite- ja ohjelmistokokoonpanot mahdollistavat asiattomien osien liittämisen järjestelmään sekä vaikeuttavat palauttamistoimenpiteitä kriisitilanteissa
EMC-häiriöt ja EMP-suojaus	Puutteellinen suojaus sähkömagneettisilta häiriöiltä voi aiheuttaa laitteiden toimintahäiriöitä ja virhetoimintoja erityisesti sähköasemilla kytkentätilanteissa ja ylivirtojen tai ylijännitteiden esiintyessä (esimerkiksi salamointi). Puutteellinen EMP-suojaus (Elektromagneettinen pulssi) altistaa elektroniset laiteet sähkömagneettiselle pulssille elektronisessa sodankäynnissä, seurauksena laitteiden tuhoutuminen
Varmentamaton tehonsyöttö	Kriittisten laitteiden varmentamaton tehonsyöttö tai riittämätön varakäyntiaika voi johtaa järjestelmän kaatumiseen tehonsyötön vikatilanteessa. Jotkin laitteet saattavat parametroitua virheellisesti tehonsyötön palauduttua tai laitteen elektroniset komponentit saattavat vioittua katkoksen yhteydessä
Puutteellinen ilmastointi ja kosteuden säätö	Elektroniset laiteet vanhenevat ja vikaantuvat ennen aikaisesti liian kuumassa ja/tai kosteassa käyttöympäristössä. Modernit prosessoripohjaiset laitteet voivat suojatoimenpiteenä sammuttaa itsensä tai siirtyä alennetun suorituskyvyn tilaan
Varmennusten puuttuminen	Kriittisten laitteiden tai tietoliikenneyhteyksien varmennusten puuttuminen voi johtaa järjestelmän toimimattomuuteen vikatilanteessa

Taulukko 4-5 Varus- ja sovellusohjelmistojen haavoittuvuuksia ja riskejä

Uhka / Haavoittuvuus	Kuvaus
Puskurin ylivuoto	Ohjelmistoissa voi olla puskureiden ylivuotohaavoittuvuuksia, joita hyökkääjät voivat hyödyntää, mikäli ne ovat tiedossa
Ohjelmistojen turvaominaisuudet eivät ole oletusarvoisesti päällä	Turvaominaisuudet voivat olla oletusarvoisesti pois päältä tai ne on voitu sulkea, kaikki tietoliikenneportit auki jne. Turvaominaisuuksista ei ole hyötyä, mikäli ne eivät ole käytössä
Palvelunestohyökkäykset (DoS)	Huonosti suojattuun verkostoautomaatiojärjestelmään voi kohdistua järjestelmäresursseja voimakkaasti kuormittava hyökkäys, joka estää tai hidastaa normaalia palvelutuotantoa. Tämä ei ole ongelma asianmukaisesti rakennetussa järjestelmäarkkitehtuurissa oleville verkostoautomaatiojärjestelmille, mutta hyökkäys voi kaataa esimerkiksi verkkoyhtiön nettisivut
Tietopakettien virheellinen käsittely	Joissain verkostoautomaatiojärjestelmissä voi esiintyä virhetoimintoja, mikäli ne vastaanottavat korruptoituneita tai tahallisesti virheellisenä lähetettyjä tietopaketteja sisältäen esimerkiksi ei sallittuja muuttujien arvoja
Turvattomien tietoliikenne-protokollien käyttäminen	Käytönvalvontajärjestelmissä yleisesti käytetyt protokollat (esimerkiksi IEC 60870-5-101 ja -104, DNP3 vanhemmat versiot ja Modbus) eivät rakenteellisesti sisällä tietoturvaominaisuuksia ja ovat siten hyvin haavoittuvia
Tarpeettomien prosessien ajaminen	Monissa yleisiä käyttöjärjestelmiä käyttävissä verkosto-automaatiojärjestelmissä tietoliikennepalvelut ovat päällä oletusarvoisesti ja aiheuttavat haavoittuvuusriskin
Avoimesti saatava järjestelmätietous	Yleisimpien järjestelmien järjestelmäspesifikaatiot ja ylläpitokäsikirjat ovat julkisesti saatavissa ja helpottavat hyökkäysten suunnittelua
Järjestelmävalvojan käyttöoikeuksien huolimaton hallinta ja käsittely	Järjestelmävalvojan ja –ylläpitäjän käyttöoikeuksien päätyminen asiattomiin käsiin altistaa järjestelmän väärinkäytöksille ja hyökkäyksille
IDS/IPS-hyökkäyksen-estojärjestelmää ei käytetä	Palomuurien lisäksi IDS/IPS-järjestelmät ovat tehokas keino suojata verkostoautomaatiojärjestelmien tietoverkkoja ei toivotulta liikenteeltä
Lokeja ei hyödynnetä tai seurata reaaliaikaisesti	Ilman ajantasaisia ja tarkkoja lokitietoja ei usein ole mahdollista selvittää tietoturvapoikkeaman aiheuttajaa. Sama koskee muita turvallisuusindikaattoreita
Virustorjunta- ja muita suojausohjelmistoja ei ole käytössä	Monet verkostoautomaatiojärjestelmät eivät toimi virheettömästi, mikäli virustorjuntaohjelmia otetaan käyttöön. Tästä aiheutuu merkittävä riski haittaohjelmien tunnistamiselle ja eristämiselle

4.3.3 Tietoliikenteen haavoittuvuudet

Verkostoautomaatiojärjestelmän toimivuuden elinehto on käytettävyydeltään ja siirron laadultaan korkeatasoiset tietoliikenneyhteydet riippumatta tietoliikenteen toteutustavasta. Tiedonsiirron korkea käytettävyys, eheys ja luotettavuus voivat vaarantua puutteellisella tietoliikenneverkon topologia- ja rakennesuunnittelulla, virheellisellä laiteparametroinnilla tai asiantuntemattomalla tai puuttuvalla ylläpidolla. Jäljempänä olevissa taulukoissa tietoliikenneverkon haavoittuvuuksia on käsitelty seuraavien näkökulmien suhteen:

1. Tietoliikenneverkon rakenteeseen ja fyysiseen suojaamiseen liittyvät haavoittuvuudet
2. Tietoliikenneverkon konfiguraation ja parametroinnin ja hallinnan haavoittuvuudet

Esitetyt haavoittuvuudet ovat satunnaisessa tärkeysjärjestyksessä ja luettelo uhista ja haavoittuvuuksista ei ole täydellinen.

Taulukko 4-6 Tietoliikenneverkon rakenteen tai fyysiseen suojaamisen haavoittuvuuksia

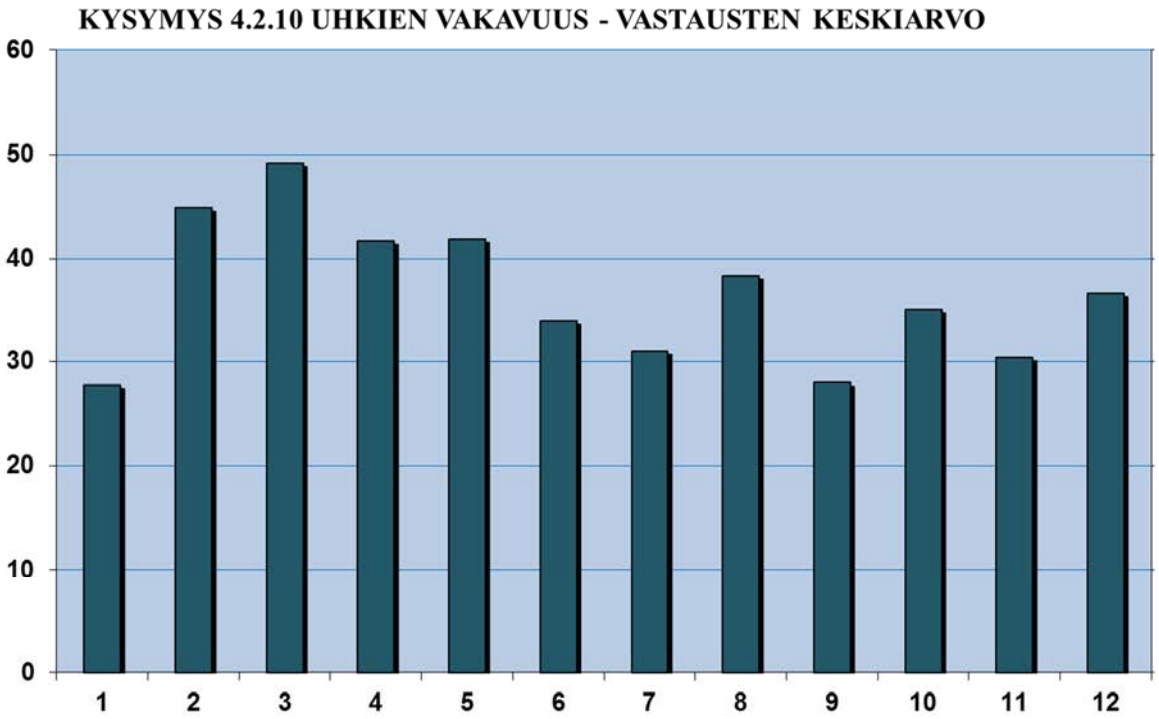
Haavoittuvuus	Kuvaus
Turvaton tietoliikeverkon rakenne ja siirtomedia	Tietoliikenneverkon rakenne on suunniteltu yleistä yritysteletoimintaa varten, eikä siinä ole huomioitu toimintakriittisten verkostoautomaatiojärjestelmien tietoliikenteen erityisiä turvallisuus-, luotettavuus ja laitevaatimuksia. Esimerkiksi valokaapeleiden avulla toteutetut siirtomediat ovat yleensä luotettavampia ja tietoturvallisempia kuin langattomat yhteydet
Tietoliikenneverkon ja sen laitteiden riittämätön fyysinen suojaus, esimerkiksi laitetilojen suojausluokitus ei ole riittävä, kuluvalvonta tai lukitus puutteellisia tai laitteita ei ole sijoitettu lukittuihin laitekaappeihin. Laitteiden portit ja liitännät fyysisesti ja loogisesti suojaamattomia	Telelaitetilojen, sähköasemien ja telelaitteiden riittämätön tai puuttuva fyysinen suojaus ja kulunvalvonta voi mahdollistaa huomaamattoman tunkeutumisen laitetiloihin ja laitteisiin. Miehittämättömillä asemilla ei ole esimerkiksi etävideo- tai sähköistä kulunvalvontaa. Riski kohdistuu laajalle kirjolle erilaisia haitallisia ja vihamielisiä toimenpiteitä. Uhka luonnononnettomuuksien ja poikkeuksellisten sääilmiöiden aiheuttamille vaurioille
Tietoliikenneyhteydet ovat varmentamattomia	Verkostoautomaatioyhteyksiltä edellytetään yleensä hyvin korkeaa käytettävyyttä, mikä vaati yhteyksien riippumatonta reitti- ja laitevarmennusta (esim. kahdennus). Myös tehonsyötöt ja kriittisten laitetilojen ilmastointijärjestelmät tulee kahdentaa tai niiden toimintaa tulee valvoa reaaliaikaisesti
Ulkoiset yhteydet ovat huonosti suojattuja	Ulkoiset yhteydet salaamattomia; ei käytetä VPN-tunnelointia tai vahvaa autentikointia
Puutteellinen tai tarkkuudeltaan riittämätön tietoliikenneverkon synkronointi	Puutteellisesti toimiva synkronointi voi aiheuttaa tiedonsiirtovirheitä tai kaataa tietoliikenneverkon tai sen solmuja erityisesti piirikytkentäisissä tietoliikenneverkoissa (esim. SDH- tai PDH-verkot). Myös paketti-kytkentäisissä verkoissa (mm. IP-verkot) synkronointi ja aikaleimojen siirto on toteutettava luotettavasti verkostoautomaatiojärjestelmän asettamien vaatimusten mukaisesti
Palomuureja, välityspalvelimia (proxy) tai IDS/IPS-järjestelmiä ei käytetä	Palomuurit sekä välityspalvelimet ja IDS/IPS- järjestelmät ovat oleellinen osa tietoliikenteen suojausta ja mahdollistavat liikenteen rajoittamisen sekä DMZ-alueiden rakentamisen
Tietoliikenneverkon salaus- ja suojausominaisuudet (laitteet ja ohjelmistot) puuttuvat kokonaan tai ovat puutteellisia	Tietoliikenneverkko ei mahdollista liikenteen salausta tai VPN-tunnelontia, jolloin turvallisuuskriittinen data, esimerkiksi salasanat, voivat joutua asiattomien käsiin

Taulukko 4-7 Tietoliikenneverkon konfiguraation, parametroinin ja hallinnan haavoittuvuuksia

Haavoittuvuus	Kuvaus
Puutteellinen tietoliikenteen reititys- ja access-parametrien hallinta sekä monimutkainen tai sekava verkkorakenne	Puutteellinen tietoliikenneverkon liikenteen hallinta mahdollistaa ei toivottujen järjestelmien/laitteiden kytkeytymisen verkostoautomaatiojärjestelmän laitteisiin, esim. puutteellisesti määritellyt palomuurisäännöt. Rakenteellisesti monimutkaisessa tai sekavassa verkossa ei aina hallita kaikkia tietoliikenteen mahdollisia reittejä
Laitteiden oletusparametrien käyttäminen	Asiattomat tahot pääsevät tunkeutumaan helposti tietoliikenneverkkoon tai sen laitteisiin käytettäessä käyttöoikeuksiin tai porttien aktivointiin yms. liittyvien tunnusten tai parametrien oletusarvoja
Tietoliikenneverkon konfiguraatioparametrien varmuuskopioinnin puuttuminen tai puutteet	Puuttuvat tai puutteelliset (esim. vanhentuneet) laite- ja järjestelmäparametrien varmuuskopiot voivat estää tietoliikenneverkon tai sen osan palauttamisen kriisitilanteessa
Tietoliikenneverkolla ei ole hallintajärjestelmää tai se on rakenteeltaan ja ominaisuuksiltaan puutteellinen	Tietoliikenneverkon hallintajärjestelmä mahdollistaa verkon keskitetyn ja reaaliaikaisen vikojen paikannuksen, verkon konfiguroinnin, siirronlaadun ja turvallisuus-parametrien seurannan sekä hallinnan
Tietoliikenneverkon hallintajärjestelmä tai verkon laitteiden hallintaliittymien käyttöoikeuksien riittämätön tai puuttuva hallinta	Tietoliikenneverkon hallintajärjestelmien tai –liittymien puutteellinen hallinta mahdollista asiattomien henkilöiden tai järjestelmien pääsyn tietoliikenneverkkoon ja voi johtaa tietoliikenneverkon rikolliseen haltuunottoon. Käyttöoikeuksiin liittyviä tunnuksia ja salasanoja ei vaihdeta säännöllisesti tai niiden rakenne on liian yksinkertainen
Hallintajärjestelmän ja/tai verkkolaitteiden lokeja ei hyödynnetä tai seurata systemaattisesti	Ilman ajantasaisia ja tarkkoja lokitietoja ei usein ole mahdollista selvittää laitteiden luvatonta käyttöä tai tietoturvapoikkeaman aiheuttajaa. Sama koskee muita turvallisuusindikaattoreita
Automaatiojärjestelmien vaatimaa turvallista verkkoa ei ole määritelty tai rajattu	Turvallisen verkon määrittely ja dokumentointi on edellytys verkon tehokkaalle suojaukselle
Turvallisessa verkossa siirretään turvatonta tai väärää liikennettä	Turvallista verkkoa käytetään myös muiden kuin verkostoautomaatiojärjestelmien tiedonsiirtoon, josta aiheutuu teknisiä ja turvallisuusriskejä
Avoimesti saatava järjestelmätietous	Suosittujen verkkolaitteiden rakennedata ja ylläpitokäsikirjat ovat julkisesti saatavissa ja helpottavat hyökkäysten suunnittelua

4.4 Nettikyselyssä tunnistetut uhkat ja haavoittuvuudet

Tietoturvaselvitykseen liittyvässä nettikartoituksessa kysyttiin myös vastaajien arvioita nimettyjen uhkien vakavuudesta, joka pyydettiin määrittämään vaikuttavuuden ja todennäköisyyden tulona. Vastauksissa oli jonkin verran hajontaa ja mitään uhkaa ei yhtiöissä koettu hyvin suureksi (max. 100). Suurimmaksi uhkaksi koettiin tietomurto käytönvalvontajärjestelmään.



KUVITELTU UHKA TAI HAAVOITTUVUUS

1 Palvelunestohyökkäys internet- tai extranet-sivuille
2 Tietomurto verkkoyhtiön tietojärjestelmiin (ei SCADA)
3 Tietomurto käytönvalvontajärjestelmään
4 Tietomurto sähköverkon suojauslaitteisiin (esim. suojarele)
5 Haittaohjelman tai haitakkeen pääsy verkkoyhtiön käyttökeskuksen sisäverkkoon riittämättömän tietoturvan takia
6 Oman henkilökunnan huolimaton tietovälineiden käyttö
7 Toimittajan tai palvelutuottajan huolimaton tietovälineiden käyttö
8 Asiakirjojen, salasanojen, avaimien tai muun luottamuksellisen materiaalin joutuminen asiattomien tahojen haltuun
9 Sähköpostin tai muun luottamuksellisen viestinnän päätyminen asiattomien haltuun
10 Sähkö- tai viestiasemien fyysisen suojaus ja valvonta puutteellista
11 Oman, toimittajan tai palvelutuottajan henkilökunnan palveluksessa olevan tai joskus olleen henkilön tahallisesti aiheuttama tietojärjestelmävaurio tai vikaohjaus
12 Kaikkien kysymyksien vastausten keskiarvo

Kuva 4-3 Nettikartoituksen uhkakuva-arvio

4.5 Haastatteluissa esiin nousseet uhkat ja tietoturvariskit

Haastatteluissa nostettiin esiin sangen laaja kirjo turvallisuusuhkia, joista osa liittyy suoraan ja osa epäsuorasti tietoturvaan. Oheisissa lainauksissa tunnistetut uhkat ja tietoturvariskit on pyritty ryhmittelemään aihealueen mukaan ja eivät ole tärkeysjärjestyksessä.

Vihamieliset tahot, joita ovat seuraavat:

- Sabotaasi, ääriliikkeet, hakkerit ja haktivistit koetaan selväksi riskiksi
- Verkkorikolliset ovat kasvava riski
- Tiedustelupalvelujen vakoilu on kyberuhkana käytännön todellisuutta
- Terroristien tekemät iskut ovat mahdollisia
- Ammattimaiset vihamieliset organisaatiot löytävät keinot, jos ne todella haluavat murtautua

Oman tai palvelutuottajan henkilöstön toiminta, osaaminen ja asenteet

- 80% uhkista realisoituu oman tai palvelutuottajan henkilökunnan kautta, koetaan isoksi ja haasteelliseksi riskiksi
- Oman henkilökunnan tahattomat virheelliset toiminnat johtuen osaamattomuudesta, kiireistä tai huolimattomuudesta
- Henkilöstö tuntee erinomaisesti laitteet, ohjelmistot ja järjestelmien heikkoudet, joihin perustuen hyökkäykset voidaan toteuttaa
- Ulkoiset tahot käyttävät yrityksen henkilökuntaa hyväksi sisään pääsyssä, esimerkiksi kiristämällä
- Henkilöstön ja johdon osaamisen ja tietoisuuden puute sekä väärät asenteet
- Oma henkilökunta voi ääritilanteissa aiheuttaa vahinkoa
- Henkilöstön huolimattomuuttaan tietojärjestelmiin tuomat haittaohjelmat, esimerkiksi muistitikulla

Tunnistettuja haavoittuvuuksia, uhkia tai puutteita:

- Sähköasemien fyysinen suojaus ja valvonta on hoidettu puutteellisesti
- Fyysinen ilkivalta on todennäköisintä. Toisaalta fyysisen turvallisuuden kanssa ei ole olut isompia ongelmia
- Suojauduttu väärällä tavalla eli yritetty rakentaa pelkästään vahva ja kova suojamuuri, jolloin ”sisus on pehmeä”. Jossain vaiheessa ”pöpöt” pääsevät joka tapauksessa suojatun alueen sisään, ja siihen ei olla riittävän hyvin varautuneita
- Usein haavoittuvin laite on se, jota ei edes ole osattu ajatella, esimerkiksi kulunvalvontalaite
- Verkostoautomaatiojärjestelmiä suunniteltaessa ei ole varauduttu ulkoisiin uhkiin ja järjestelmien rakenteellinen tietoturva on heikko
- Automaatiojärjestelmien protokollien häiritseminen on helppoa, koska niiden suojaus on puutteellista, ellei olematonta
- Eksoottiset protokollat eivät suojaa järjestelmiä, eivätkä ole kuin korkeintaan hidaste
- Viestiliikenne on ehkä heikoin lenkki, sovellukset on suojattu paremmin
- Käytetään täysin suojaamatonta, radiomodeemeihin perustuvaa ala-asemaliikennöintiä

- Tietoverkkojen arkkitehtuureissa on rakenteellisia heikkouksia. Tietoverkkojen segmentointi on puutteellista
- Ei seurata ”turvallisen” tietoverkon sisäistä liikennettä eikä ulos menevää liikennettä
- Tietämättömyys on uhista suurin
- Piirikytkentäisten laitteiden tarjonnan hiipuminen on tietoturvauhka
- IP-tekniikan lisääntyvä käyttö lisää haavoittuvuutta

Muita kommentteja

- Suomeen ei kohdistu merkittäviä tietoturvauhkia
- Smart Grid tuo lisää haavoittuvuuksia. Smart Grid on joidenkin sähköyhtiöiden mielestä kirosana
- Vihamieliset tahot voivat ottaa halutessaan sähköverkot hallintaansa
- Uhkien ja riskien ilmentyminen ja suunta voivat olla hyvinkin yllättäviä, minkä vuoksi varautuminen on hankalaa
- Julkisilla verkoilla toteutettujen automaatiojärjestelmien tietoturva on hyvä, mikäli ne on toteutettu vahvalla ammattitaidolla
- Sähköverkko on maantieteellisesti laajalle levittäytynyt ja suojaaminen siten vaikeampaa kuin teollisuusautomaatioverkoissa

4.6 Tietoturvaloukkausten syntymekanismeja

4.6.1 Kohdentamattomat hyökkäykset

Tietoturvaongelma syntyy periaatteessa kahdella eri tavalla: joko satunnaisen leviämisen seurauksena tai kohdennetun hyökkäyksen tuloksena. Ensin mainitussa hyökkääjä esimerkiksi asettaa haitta- tai hyökkäysohjelman odottamaan sopivaa uhria internetin websivujen mainosbanneriin tai johonkin sivujen kautta ladattavaan tiedostoon. Pahaa aavistamaton uhri klikkaa banneria tai avaa tiedoston, jolloin haittaohjelma saastuttaa uhrin työaseman. Haittaohjelma toimii ennalta ohjelmoidun kaavan mukaisesti uhrin tietoverkossa. Se voi olla esimerkiksi vakoiluohjelma, joka välittää rikollisen käyttämälle palvelimelle luottamuksellista, tietoturvahyökkäyksissä käytettävää tietoa.

Pääosin satunnaisiin, passiivisiin hyökkäystapoihin voidaan lukea myös erilaisten virusten, matojen ja muiden vastaavien haittaohjelmien levitys. Hyökkäykset eivät ole yleensä kohdennettuja ja uhriksi valikoituu satunnaisesti hyvin sekalainen joukko yrityksiä, yhteisöjä ja yksityisiä kansalaisia. Viruksia ja niiden kaltaisia haittaohjelmia on erittäin laaja kirjo, ja jotkin niistä voivat aiheuttaa tietojärjestelmille hyvinkin vakavia vaurioita ja voivat olla erittäin työläitä poistaa levitessään laajasti kohteen tietojärjestelmiin ja työasemiin tai naamioituessaan käyttöjärjestelmään (esimerkiksi rootkit-virukset).

Oma lukunsa on verkkokauppahuijausten tekijät, jotka houkuttelevat uhrin tekemään nettitilauksia luottokorttien avulla ainoana tarkoituksenaan saada uhrin luottokorttitiedot jatkopetoksien tekemistä varten. Näissäkin uhri valikoituu satunnaisesti ansan ollessa kuitenkin tarkoitettu jollekin tietylle, kyseisistä palveluista tai tuotteista kiinnostuneelle asiakaskunnalle.

Erilaisia kohdentamattomasti levitettäviä vakoiluohjelmia on myös laaja kirjo. Osa niistä on lähes harmittomia keräten esimerkiksi nettikäyttäjien käyttäjäprofiileja.

Vakavia ja todella vaarallisia voivat olla erilaiset käyttäjätunnuksia ja salasanoja urkkivat haittaohjelmat. Nettirikolliset voivat myydä saamaansa informaatiota eteenpäin, käyttää tietoa suoraan taloudellista vahinkoa aiheuttavien verkkorikosten tekemiseen tai valmistellakseen myöhemmin tehtävää kohdennettua hyökkäystä tarkemmin valitun uhrin tietojärjestelmiin.

4.6.2 Kohdennetut hyökkäykset

Kohdennettuja hyökkäystapoja on lukuisia ja yleensä ne ovat luonteeltaan aktiivisia. Näistä yksi näkyvimmistä on palveluestohyökkäykset (DoS), joilla halutaan lähinnä ruuhkauttaa tai kaataa kohteen julkiset internet-sivut ja samalla sen kautta tarjottavat palvelut. Hyökkäys tehdään aiheuttamalla kohdepalvelimelle niin suuri liikennekuorma, että palvelin ei suoriudu tehtävistään kohtuullisissa vasteajoissa. Hyökkäyksessä käytetään tyypillisesti haltuun otetuista tietokoneista muodostettuja bottiverkkoja ja hyökkäykset ovat yleensä tarkasti kohdistettuja tiettyihin yrityksiin tai julkisiin organisaatioihin. Palveluestohyökkäyksellä uhkailua voidaan käyttää myös kiristyskeinona.

Nettipalvelut voivat hidastua tai kaatua myös normaalista asiointiliikenteestä ja tällöin syynä on yleensä riittämätön tietoliikenne- tai palvelinkapasiteetti tai huonosti suunniteltu palvelu.

Hyökkääjä voi myös murtautua halutun kohteen nettisivun palvelimelle ja muuttaa niiden sisältöä tai laittaa sinne kuulumatonta informaatiota tai linkkejä. Tässä voidaan hyödyntää esimerkiksi nettisivujen hallintaominaisuuksia.

Yksi tapa tehdä kohdennettu hyökkäys on sähköpostipalvelun käyttäminen hyökkäysohjelman saamiseksi uhrin koneelle. Viesti voidaan naamioida uhrin yhteistyökumppanin, esimiehen tai kollegan nimissä lähetetyksi, jolloin pahaa aavistamaton uhri avaa viestin ja aktivoi sen mukana olevan haittaohjelman. Kohdennetut hyökkäykset edellyttävät kohdeorganisaation hyvää tuntemista ja niillä saattaa olla uhrin organisaation sisällä tarkoin määritelty loppukohde, esimerkiksi verkostoautomaatiojärjestelmän palvelin tai asiakaspalvelujärjestelmä. Sähköpostiviestin ensimmäinen vastaanottaja voi toimia vain välittäjänä haittaohjelman hakeutuessa toisen käyttäjän koneeseen, jolla ollaan yhteydessä tai joka on kiinteästi liitetty hyökkäyksen lopulliseen kohteeseen.

Kohdennettuihin hyökkäyksiin käytettäviä työkaluja on veloituksetta saatavissa julkisesta internetistä. Nämä ilmaisohjelmat käyttävät usein tunnettuja haavoittuvuuksia, joten asianmukaisesti suojattujen tietojärjestelmien torjuntaohjelmistot yleensä tunnistavat ja eliminoivat kyseiset hyökkäysohjelmat.

Kohdennettuihin hyökkäysiin on saatavissa myös maksullisia, tehokkaampia työkaluja. Epämääräiset ja puoli rikolliset tahot myyvät niitä voittoa tavoitellen. Nämä ohjelmat voivat perustua hyvin tuoreisiin, ns. nollapäivähaavoittuvuuksiin, joille ei ole vielä korjausta saatavilla.

Maksulliset tai valtiollisten tiedustelupalvelujen käyttämät hyökkäysohjelmat voivat perustua vielä täysin tuntemattomiin haavoittuvuuksiin tai jopa tahallisesti rakennettuihin tietoturva-aukkoihin. Näihin perustuvia haittaohjelmia voi olla erittäin vaikea tunnistaa tietojärjestelmistä niiden päästyä sisään yrityksen verkkoon.

Netistä löytyy lukuisia, helposti saatavissa olevia ilmaisia tai maksullisia vakoilu- ja murtotyökaluja sekä erilaisia haavoittuvuuksien analysointiohjelmia, esimerkiksi verkkosivut http://sectools.org/ , /23/.

4.6.3 Tahattomat tietoturvaloukkaukset

Yrityksen työntekijät voivat vahingossa huolimattomuuttaan tai taitamattomuuttaan aiheuttaa tietoturvavuodon tai ongelman toimintakriittiseen järjestelmään.

Tyypillinen esimerkki on saastunut tietomedia, esimerkiksi muistitikku, joka kytketään yrityksen verkossa olevaan työasemaan tai palvelimeen. Median sisältämä haittaohjelma saastuttaa yrityksen verkon aiheuttaen tietoturvatapahtuman.

Keinoja haavoittuvuuksien korjaamiseksi/eliminoimiseksi ja tietoturvahyökkäysten torjumiseksi tai vaikutusten pienentämiseksi esitetään lähinnä luvuissa 6 ja 7. Erityisen tärkeässä asemassa on tietoturvallisen järjestelmäarkkitehtuurin rakentaminen.

4.7 Esimerkkejä toteutuneista riskeistä ja uhkista

4.7.1 Tahalliset tapahtumat

Worcester ilmailun puhelinpalvelu, USA, 1997

Teini hakkeroi Worcesterissa, Massachusettissa julkisen puhelinjärjestelmän keskuksen ja kaatoi osan keskuksen puhelinpalveluista aiheuttaen paikallisen lentokentän lennonjohto- ja viranomaistoimintojen joutumisen puhelinmottiin. Vastaavista julkisen puhelinjärjestelmän keskusten hakkeroinnista on esimerkkejä myös Suomesta muun muassa 80-luvulta.

Maroochy Sire jätevesijärjestelmä, Australia, 2000

Katkeroitunut, hakuprosessissa hylätty työnhakija aiheutti tahallisesti useilla jätevedenkäsittelyjärjestelmään tekemillään hyökkäyksillä ja automaatiojärjestelmään virheellisesti syöttämillään järjestelmäparametreilla mm. jätevesivuodon. Paikalliseen jokeen ja puistoon pääsi yhteensä yli 1 000 m^3 jätevettä.

Useita muitakin vedenkäsittelyn automaatiojärjestelmiin kohdistuneita hyökkäyksiä on dokumentoitu.

Stuxnet-mato, mm. Iranin ydinmateriaalin käsittelyohjelma, 2010

Erittäin hienostunut ja monimutkainen mato levisi salakavalasti muistimedioiden välityksellä laajasti ja aktivoitui Iranin valtion käyttämissä, Siemensin valmistamassa teollisuusautomaatio järjestelmässä ilmeisenä tarkoituksenaan sabotoida Iranin ydinohjelmaa.

Yhdysvaltain turvallisuusviraston NSA:n ja brittiläisen GCHQ:n tiedustelutoiminta, 2013

The New York Times ja The Guardian -lehdet ovat julkistaneet lukuisia artikkeleita yhdysvaltalaisen NSA:n ja sen brittiläisen vastineen GCHQ:n harjoittamasta tiedustelu- ja vakoilutoiminnasta. Erittäin isoilla resursseilla toteutetussa laajassa tiedusteluhankkeessa on useita vuosia vakoiltu internet- ja puhelinliikennettä eri puolilla maailmaa.

Tiedusteluorganisaatiot ovat lehtitietojen mukaan murtautuneet myös salattuihin viesteihin ja muuhun sisältöön. Myös esimerkiksi Kiinan raportoidaan harjoittaneen laajamittaista vakoilutoimintaa, Mandiant-raportti 2013.

Julkisesti raportoimattomista hyökkäyksistä, Suomi

Myös suomalaisiin energiayhtiöihin kohdistuneita hyökkäyksiä on tiedossa, mutta luottamuksellisuudesta johtuen niitä ei voida kuvata tarkemmin. Eräässä tapauksessa edistyksellinen, energiayhtiön tietoliikenneverkon ja julkisen televerkon väliin asennettu erillinen havainnointijärjestelmä havaitsi yritysverkon sisälle jo päässeen meneillään olleen hyökkäyksen ennen laajamittaisten vahinkojen syntymistä. Yleisesti ottaen vihamielisistä hyökkäyksistä julkisuuteen tulee vain murto-osa.

4.7.2 Tahattomat tapahtumat

CSX Junaliikenteen ohjausjärjestelmät, USA, 2003

Sobig-virus saastutti CSX-yhtiön useita junaliikenteen ohjausjärjestelmiä eteläisessä Carolinan osavaltiossa elokuussa 2003. Virus pysäytti osan junaliikenteestä ja aiheutti lukuisia myöhästymisiä.

Davis-Besses ydinvoimala, USA, 2003

Microsoft SQL-palvelimen saastuttanut Slammer-virus esti turvallisuusjärjestelmän toiminnan Davis-Besse ydinvoimalassa Ohion osavaltiossa noin viiden tunnin ajan tammikuussa 2003. Sen lisäksi voimalan prosessiautomaatiojärjestelmä kaatui ja kesti yli kuusi tuntia ennen kuin se saatiin jälleen toimimaan. Slammer-viruksen tiedetään saastuttaneen ja aiheuttaen toimimattomuutta ainakin viiden voimayhtiön käytönvalvontaverkolle.

Voimayhtiön First Energy back-out USA, 2003

Tekninen vika käytönvalvontajärjestelmän tietokoneessa esti käyttökeskuksen operaattoria havaitsemasta sähköverkon käyttötilanteen muuttumista kriittiseksi. Lisäksi tapahtumaan liittyi informaatiokatkos aiheuttaen virheellisen tilannearvion verkon stabiilisuuden seurannassa. Useita tärkeitä 345 kV:n siirtolinjoja laukesi puiden aiheuttaman maasulun takia pohjoisessa Ohiossa. Tämä aiheutti ylikuorman muissa 345 ja 138 kV:n siirtolinjoissa seurauksena backoutiin johtanut ketjureaktio. Yhteensä 68 800 MW tuotantotehoa menetettiin 265 voimalaitoksen (yhteensä 508 generaattoria) erotessa verkosta.

Zotob-mato, USA, 2005

Zotob-mato saastutti useita Windows-pohjaisia teollisuusautomaatiojärjestelmiä elokuussa 2005 aiheuttaen tuotantokatkoksia tai -häiriöitä. Saastuneita järjestelmiä oli mm. seuraavissa yrityksissä: Daimler Chrysler, Caterpillar, Boeing ja useissa mediayhtiöissä.

Bellinghamin öljyputken vuoto, USA, 1999

Puutteellisesti toimineen öljyputken käytönvalvontajärjestelmän takia poikkeuksellisessa käyttötilanteessa putkesta pääsi virheellisten tilannetiedon seurauksena noin 900 m^3 bensiiniä ympäristöön. Seuranneessa räjähdyksessä ja tulipalossa kuoli kolme ja loukkaantui kahdeksan ihmistä.

Esimerkkien aineisto on pääosin peräisin NISTin julkaisusta, /7/. Dokumentissa esitettyjen linkkien takaa löytyy lisää esimerkkejä.

5 VERKOSTOAUTOMAATIOJÄRJESTELMIEN TIETOTURVAN NYKYTILANNE

5.1 Tietoturvan taso kansainvälisesti

Tietoturvan taso vaihtelee kansainvälisesti hyvin laajasti maan teollistumisasteen sekä taloudellisen ja poliittisen kiinnostavuuden perusteella. Alikehittyneiden maiden infrastruktuuri ja niiden verkostoautomaatiojärjestelmät ovat usein vanhanaikaisia ja puutteellisia. Toisaalta niissä ei ole internetin välityksellä helposti murrettavissa olevia rakenteita ja kohteet eivät kiinnosta tavanomaisia tietohakkereita ja -rikollisia. Edellä mainittujen maiden infrastruktuuria uudistettaessa käytetään yleensä modernia tekniikkaa ja tietoliikenne-verkkoja, jolloin näidenkin maiden kriittiset automaatiojärjestelmät voivat tulla vihamielisten tahojen ulottuville.

Teollistuneita maita pidetään tietoturvan edellä kävijöinä. Näiden maiden kriittisen infrastruktuurin ohjaus- ja hallinta on pitkälle automatisoitua ja vähällä henkilöstön määrällä toteutettua. Maissa on alan tutkimus ja teollisuus korkeatasoista ja viranomaiset aktiivisia. Tästä on esimerkkinä erilaisten CERT-toimintojen perustaminen, muun muassa kotimainen CERT-FI ja yhdysvaltalainen automaatiojärjestelmien tietoturvauhkiin erikoistunut ICS-CERT, /22/.

Eräissä Euroopassa maissa ja USA:ssa viranomaiset tai kantaverkkoyhtiöt ovat asettaneet perusvaatimuksia muun muassa sähköverkkoyhtiöiden verkostoautomaatiojärjestelmien tietoturvalle. Kantaverkkoyhtiöiden eurooppalainen kattojärjestö ENTSO-E on myös aktivoitunut aihealueen suhteen.

Raportin laatijalle on syntynyt alan kansainvälistä aineistoa tutkiessa käsitys, että ongelmat ovat pitkälle tiedostettuja ja asian kimpussa työskennellään. Paljon on jo tehty toimintakriittisten järjestelmien tietoturvan parantamiseksi, mutta paljon on vielä tekemättä. Tietoturvan taso on kirjava ja vaihtelee kovasti maittain ja yhtiöittäin. Yleisarvio tämän hetken tilanteesta on, että rikolliset ja muut tunkeutumista harjoittavat tahot johtavat kisaa valitettavan selvästi.

5.2 Verkostoautomaatiojärjestelmien tietoturvan taso Suomessa

5.2.1 Nettikyselyn tulokset ja havaintoja

Nettikysely tehtiin ainoastaan sähköyhtiöiden keskuudessa ja siihen vastasi 28 yhtiötä. Vastaajayhtiöt jakaantuivat kokonsa ja toimialueensa puolesta sangen tasaisesti ja edustavasti. Vastausprosentti jäi pienehköksi kyselyn laajuuteen nähden. Toivottavasti alhainen vastausprosentti ei kuvasta yhtiöissä vallitsevaa vakavuutta, jolla tietoturvaan suhtaudutaan. Tehdyn nettikyselyn tulokset on esitetty liitteessä 1.

5.2.1.1 Käytönvalvontajärjestelmiin liittyviä havaintoja

Oma henkilöstö/toimittajat ja palveluntuottajat

Osassa ainakin suurimpia sähköyhtiöitä on omat asiantuntijat, jotka ylläpitävät verkostoautomaatiojärjestelmiä ja tietoliikenneverkkoja. Pienemmissä yhtiöissä oman työn osuus on vähäisempi ja ulkopuolisia, toimittajien ja erillisten asiantuntijayritysten palveluja käytetään runsaasti.

Järjestelmien uusiminen tai päivittäminen

Valta osa vastaajista on uusimassa tai tekemässä muutoksia verkostoautomaatio-ympäristöönsä. Muutoksista suurin osa liittyy sähköverkon suojaukseen, käytönvalvontaan tai niiden tietoliikenteeseen tai sähköasemien video- ja kulunvalvontaan.

Käytönvalvonta- ja käytöntukijärjestelmät

Lähes kaikissa yhtiöissä on käytönvalvonta- ja käytöntukijärjestelmät. Suurin osa niistä perustuu standardeihin Windows-käyttöjärjestelmiin.

Käyttöoikeuksien hallinta

Järjestelmien käyttöoikeuksien hallinta on kirjavaa ja osin puutteellista. Sisäänkirjautumisessa vahvaa autentikointia ei edellytetty yhdessäkään yhtiössä ja käytönvalvontajärjestelmien osalta yhteinen salasana oli käytössä kymmenessä yhtiössä.

Käytönvalvontajärjestelmään kytkeytyminen

Käytönvalvontajärjestelmään pystyy kytkeytymään hyvin monipuolisesti käyttökeskuksessa olevien työasemien lisäksi, toimistossa ja kotona sijaitsevilta työasemilta. Myös toimittajalla tai palveluntuottajalla voi olla pääsy käytönvalvonta-järjestelmään. Tämä antaa joustavuutta rakentaa erilaisia ylläpito-, operointi- ja päivystysratkaisuja, mutta asettaa järjestelmien tietoturvaratkaisuille kovat vaatimukset. Vain kuudessa yhtiössä käytönvalvontajärjestelmää pystyy käyttämään ainoastaan käyttökeskuksesta.

5.2.1.2 Tietoliikenteen toteutukseen liittyviä havaintoja

Tietoliikenneverkon toteutus ja omistus

Suurin osa käytönvalvonnan ja sähköverkon suojauksen tarvitsemista tietoliikenneyhteyksistä on toteutettu omalla tietoliikenneverkolla, jota on täydennetty monessa yhtiössä ulkoisilla, yleensä teleoperaattorilta vuokratuilla yhteyksillä. Tämä mahdollistaa luotettavien, vahvasti eristettyjen vyöhykkeiden rakentamisen kriittisimpiä käytönvalvonta- ja suojaussovellutuksia silmällä pitäen. Sähköasemien yhteydet ovat usein myös varmennettuja, mikä lisää käytettävyyttä ratkaisevasti.

Tietoliikenneyhteyksien tyyppi

Verkostoautomaation tietoliikenteessä on käynnissä voimakas murros. Perinteisistä piirikytkentäisistä sarjaliikenneratkaisuista ollaan siirtymässä pakettikytkentäiseen, IP-pohjaiseen tietoliikenteeseen. Tekniikoita käytetään usein rinnakkain siirtymävaiheen aikana. IP-pohjaisiin järjestelmiin siirtyminen kasvattaa tietoturvariskiä, edellyttää turvallista verkkorakennetta ja vahvaa osaamista verkon laitteita parametroitaessa.

Tiedonsiirron tekninen toteutustapa

Eniten käytössä oli johtimiin perustuvia kupari- ja valokaapeliyhteyksiä. Näillä luotettavan tietoturvan rakentaminen on helpompaa kuin langattomissa siirtomedioissa. Erityisesti valokaapelin turvallisuusominaisuudet ovat korkeaa tasoa ja niillä voi toteuttaa sähköasemien vaarajännitesuojauksen usein vaatiman galvaanisen erotuksen.

Käytetyistä langattomista siirtomedioista erityisesti suojaamattomat analogiset radiolinkit ja radiomodeemiyhteydet vaativat erityishuomiota. Näistä tekniikoista tulisi luopua ripeällä aikataululla ja korvata järjestelmät moderneilla digitaalisilla ratkaisuilla. Myös yleisillä matkaviestinverkoilla toteutetut yhteydet sisältävät tietoturva- ja käytettävyysriskejä, jotka on osattava minimoida suojausratkaisuilla. Julkisia matkaviestinverkkoja käytetään yleensä onneksi lähinnä varayhteyksien toteuttamiseen tai yhteydet ovat muutoin vahvasti suojattu.

Tiedonsiirron digitalisoinnissa on vielä tekemistä. Muutamissa yhtiöissä sitä ei ole vielä aloitettu ollenkaan ja digitalisointiaste on alle 50 % yhdeksässä vastanneessa yhtiössä.

Käytönvalvontayhteyksien tiedonsiirtoprotokolla

Käytönvalvonnan yhteyksissä on käytössä vielä runsaasti analogisia tai hitaaseen sarjamuotoiseen datasiirtoon perustuvia yhteyksiä. Vastanneista ainakin 19 yhtiötä käyttää osaksi IP-pohjaisia protokollia ja uusien sähköasemien automaatio-väyläratkaisussa on ruvettu vahvasti käyttämään ethernet-pohjaista IEC 61850 väylästandardia.

Verkostoautomaatiojärjestelmien sisäisen tietoliikenteen suojaaminen

Valta osa verkostoautomaatiojärjestelmien sisäisestä tietoliikenteestä on toteutettu täysin suojaamatta. Pienellä osalla suojaus perustuu IP-verkon VLAN-ominaisuuksiin ja vain parissa tapauksessa on käytetty liikenteen salausta.

Käyttökeskuksen lähiverkko

Käyttökeskuksen lähiverkko perustuu yli puolessa yrityksistä ainoastaan yhteen loogiseen segmenttiin rakennetusta lähiverkosta. Verkkotekniikkana on käytetty lähinnä ethernet-tekniikkaa. Vain viidessä yhtiössä käyttökeskuksen lähiverkko on segmentoitu erillisiin alueisiin (aliverkkoihin).

Käyttökeskuksen lähiverkon ulkoiset yhteydet

Käyttökeskuksen lähiverkosta on rakennettu ulkoisia yhteyksiä lähinnä sähköyhtiön normaaliin yritysverkkoon (toimistoverkko) tai sen kautta tai suoraan toimittajan tai palvelutuottajan verkkoon. Neljässä tapauksessa ulkoisia yhteyksiä ei ollut ollenkaan.

Valtaosa käyttää palomuureja käyttökeskuksen verkon suojaamisessa myös yritysverkon suuntaan, mitä on hyvä käytäntö. Suorat yhteydet internet-verkkoon tai sen kautta ovat suuri riski ja vaativat huolellista suojaamista.

Sähköasemien kiinteät valvonta- ja muut yhteydet

Sähköasemille on rakennettu etäyhteyksiä sähköiseen kulunvalvontaan ja videovalvontaan vaihtelevasti. Kahdeksassa vastanneista yhtiöistä etävalvonta kattaa yli puolet asemista. Vain neljässä yhtiössä kaikki asemat ovat etävalvottuja.

Karkeasti arvioiden noin puolella sähköasemista on kiinteä puhelin- tms. yhteys yleiseen televerkkoon ja yhdessätoista yhtiössä asemilla oli etätyöskentelyn mahdollistavat kiinteät datayhteydet.

Suojareleiden etäyhteydet

Kuudessatoista yhtiössä etäyhteyksien avulla oli mahdollista päästä käsiksi suojareleiden tapahtumalokeihin tai asetteluihin. Mahdollisuus releiden asettelujen muuttamiseen etäyhteyttä käyttäen on merkittävä tietoturvauhka, ja toiminto pitäisi deaktivoida tai rakentaa siihen riittävän vahva suojausmenetelmä.

Käyttötoiminnan erillispuhelinverkko

Valta osalla yhtiöistä oli käytössään erillinen, sähköverkon käyttö- ja vikakorjaustoimintaa palveleva puhelinverkko, yleensä joko analoginen radiopuhelinverkko tai Suomen Erillisverkkojen VIRVE-palvelu. Vain neljässä tapauksessa erillistä puhelinverkkoa tai -palvelua ei ole käytössä ollenkaan.

Tietoliikenneverkon valvonta ja hallinta

Puolessa yhtiöitä tietoliikenneverkkoa valvotaan ja hallitaan erillisellä järjestelmällä. Puolessa näistä yhtiöistä tietoliikenneverkon hallinta on yhtiön omissa käsissä.

5.2.1.3 Turvallisuuden ja tietoturvan johtamiseen ja hallinnointiin liittyviä havaintoja

Turvallisuuspolitiikka ja -ohjeistus

Noin 75 %:ssa vastaajayhtiöistä on turvallisuuspolitiikkoja määritelty, mutta vastanneista vain puolessa yhtiöistä on kattava turvallisuusohjeistus.

Käytössä olevia turvallisuusmenettelyjä on auditoitu ulkopuolisen asiantuntijan toimesta noin puolessa yhtiöitä ja osin satunnaisesti.

Turvallisuuden ja tietoturvan käytännön vastuu

Turvallisuusohjeistuksen laadinta- ja muu käytännön vastuu jakaantuu yhtiöissä hyvin kirjavasti. Vastuu tietoturvasta on keskitetty sangen tiukasti (22 vastausta), mutta vastuussa olevan henkilön toimenkuva vaihtelee suuresti yhtiöstä toiseen.

Tietoturvaohjeistuksen kattamat osa-alueet

Noin puolet kyselyssä esitetyistä tietoturva-alueista oli huomioitu kyselyyn vastanneiden yhtiöiden ohjeistuksessa. Neljässä yhtiössä tietoturvaohjeistusta ei ole laadittu.

Kriittisistä toiminnoista vastaavien henkilöiden taustaselvitykset

Taustaselvityksiä tehdään vähän ja lähinnä vain rekrytointien yhteydessä. Sähköverkkoyhtiöillä on pääsääntöisesti mahdollisuus käyttää suojelupoliisin henkilöturvallisuusselvityksiä esimerkiksi rekrytoidessaan uutta henkilöstöä.

Yritysverkkojen ja –tietojärjestelmien suojaaminen

Yhtiöissä on sangen laaja skaala erilaisia keinoja käytössään tavanomaisten yritysverkkojen ja tietojärjestelmien suojaamisessa. Suosituimpia ovat palomuurit, VPN-tunnelointi ja säännöllisesti päivitettävä virussuojaus.

Käytönvalvontajärjestelmän suojaaminen

Käytönvalvontajärjestelmän suojaaminen on toteutettu sijoittamalla järjestelmä erilliseen, palomuureilla turvattuun lähiverkkoalueeseen, joka on joissain yhtiöissä lisäsi segmentoitu aliverkkoihin. Vahvat suojausmenetelmät ovat vain muutamien yhtiöiden käytössä. Ulkoiset yhteydet on sitä vastoin sangen kattavasti suojattu, mutta suojauksen taso vaihtelee.

Tietoturvauhkien arviointi

Vastaajien tunnistamia tietoturvauhkia on käsitelty jo raportin luvussa 4.4.

Koettu verkostoautomaatiojärjestelmien tietoturvan taso

Yhtiöiden itse arvioima tietoturvan taso on koettu yleensä olevan hyvä. Kuusi vastaaja piti tasoa välttävänä ja vain yksi erinomaisena.

5.2.2 Yhteenveto ja havaintoja haastatteluista

Haastatteluja on kirjoitushetkellä tehty yli 25 kpl ja ne kohdistuivat laaja-alaisesti alan toimijoihin painopisteen ollessa sähköyhtiöiden esimies- ja johtotehtävissä työskentelevissä henkilöissä tai tietotekniikan asiantuntijoissa. Tietoturvariskeihin ja haavoittuvuuksiin liittyviä, haastatteluissa esitettyjä näkemyksiä on jo käsitelty myös luvussa 4.5.

Verkostoautomaatiojärjestelmien laite- ja ohjelmistoalustojen kehitystrendit

Käytössä olevien verkostoautomaatiojärjestelmien ikäkirjo on suuri. Verkostoautomaatiojärjestelmiä uusitaan huomattavasti harvemmalla syklillä kuin esimerkiksi toimistojärjestelmiä. Käytössä on vielä iäkkäitä valmistajakohtaisia ratkaisuja samaan aikaan kun uusien järjestelmien laite- ja ohjelmistoalustojen päätoteutustavaksi ovat muodostuneet teollisuusstandardien mukaiset työasema-, palvelin- ja käyttöjärjestelmätuotteet. Uusissa asennuksissa varusohjelmistot (käyttöjärjestelmät ja laiteajurit) ovat lähes poikkeuksetta markkinoilta yleisesti saatavissa olevia vakiotuotteita. Käyttöjärjestelminä käytetään lähinnä Microsoftin Windows-perheen tuotteita tai erilaisia Linux-versioita. Kehityksestä seuraa, että uusia verkostoautomaatioratkaisuja vaivaavat osin samat haavoittuvuudet kuin tavanomaisia toimistojärjestelmiäkin. Toisaalta järjestelmien ylläpidon koetaan samalla helpottuvan.

Suojauslaitteiden osalta tilanne on parempi, koska niissä käytetään yleisesti vähennetyn käskykannan suorittimia, esimerkiksi ARM-suorittimet ja sulautettuja ohjelmistoja. Ohjelmoitavia logiikkoja on lähinnä monimutkaisissa toimilaitteissa.

Yhtiöissä koetaan, että sähkönhuollon kasvavat luotettavuus- ja turvallisuus-vaatimukset lisäävät paineita myös verkostoautomaatiojärjestelmille sekä niiden tietoliikenteelle ja tietoturvalle. Verkostoautomaation ja tietoliikenteen ulkoistaminen on tuonut yhtiöille uusia haasteita, samoin myös Energiamarkkinaviraston tiukka ohjaus. Älykkään sähköverkon (Smart Grid) tulo koetaan isoksi muutokseksi myös verkostoautomaatiojärjestelmille.

Verkostoautomaatiojärjestelmien tietoliikenteen kehitystrendit

Verkostoautomaatiojärjestelmien tietoliikenteen kehitystrendeistä nousee selvästi esille ethernet- ja IP-tekniikoiden voimakas yleistyminen. Tekniikkoja käytetään uusien sähköasemien lähiverkoissa ja laajasti käyttökeskuksen ja sähköasemien välisessä käytönvalvontaliikenteessä. Sähköasemien uudet sovellukset, kuten video- ja kulunvalvonta, käyttävät IP-pohjaista tiedonsiirtoa. IP-liikennettä toteutetaan sähköasemille reititin- ja kytkinpohjaisin ratkaisuin tai piirikytkentäisen SDH-verkon yli ethernet-siirtona.

Uuden sukupoven SDH-järjestelmillä on etu, että niillä voidaan toteuttaa myös kulkuaikakriittisiä sovelluksia IP-siirtoa selvästi luotettavammin, esimerkkinä suojausyhteydet.

IP-pohjaisia tietoverkkoja on segmentoitu vaihtelevasti. Eräiden yhtiöiden valvomoverkko on segmentoitu pitkälle lähinnä VLAN-tekniikkaa hyödyntäen. Joissain tapauksissa segmentointiin on käytetty myös palomuureja. Trendi on selvä: segmentointi lisääntyy ja verkostoautomaation tietoliikenne kulkee jatkossakin joko omissa tietoverkoissa tai liikenne on eritetty IP-verkon erillisiin segmentteihin.

Siirtomediana valokuitujen käyttö lisääntyy eteenkin kaupunkien verkkoyhtiöissä niiden ylivoimaisten teknisten ja tietoturvaominaisuuksien takia. Valokuituihin perustuen rakennetaan enenevässä määrin sähköasemien välisiä etäsuojausyhteyksiä eli differentiaali- ja distanssisuojien yhteyksiä. Uusrakennuskohteissa sähköasemien sisäiset väyläratkaisut on usein valokuiduilla toteutettuja. Valokuiduilla on myös helppo toteuttaa monesti sähköasemilla tarvittava vaarajännitesuojaus. Tekniikan merkittävin haittapuoli on investointien kalleus eteenkin toteutettaessa pitkiä yhteyksiä haja-asutusalueiden verkoissa.

Radiolinkkejä ja radiomodeemeja on käytetty pitkään sähköasemien viestiyhteyksien toteuttamisessa ja ne ovat edelleen kätevä ja edullinen tapa toteuttaa pikiäkin siirtoyhteyksiä sähköasemille. Iäkkäiden, analogisten radiomodeemi- ja radiolinkkiyhteyksien heikkous on niiden olematon tietoturva. Uusien radiolinkkien ominaisuudet mahdollistavat myös pakettikytkentäisen IP-liikenteen siirtämisen.

Julkisten matkaviestinverkkojen käyttö on lisääntynyt verkostoautomaatiosovelluksissa. Erityisesti niitä käytetään edullisuutensa takia uusissa erotinohjausyhteyksissä tai sähköasemien käytönvalvonnan varayhteyksinä.

Asianmukaisesti toteutettuna, esimerkiksi VPN-tunnelointia käyttäen, matkaviestinyhteyksien tietoturva on hyvää tasoa. Kaikissa langattomissa ratkaisuissa saadaan kylkiäisenä vaarajännitesuojaus.

Verkostoautomaatiojärjestelmien tietoliikenneprotokollat olivat aikaisemmin valmistajakohtaisia. Nykyisin uusissa järjestelmissä käytetään poikkeuksetta standardien mukaisia avoimia protokollia.

Tietoturvan taso ja haasteet

Verkostoautomaatiojärjestelmien tietoturvan taso koetaan kirjavaksi. Joissain yhtiöissä se on hyvä ja osassa vain välttävä. Erityisesti pienillä verkkoyhtiöillä on haasteellista pysyä kehityksessä mukana ja taata riittävät osaavat resurssit järjestelmähankintoihin ja ylläpidon toteuttamiseen. Yleisesti ottaen alan yhtiöissä pidettiin verkostoautomaatio-järjestelmien tietoturvan tasoa selvästi parempana kuin järjestelmätoimittajien ja palvelutuottajien keskuudessa.

Voimakas tietojärjestelmien keskinäinen integroituminen koetaan suureksi haasteeksi tietoturvan kannalta. Esimerkiksi toimistoverkoissa sijaitsevien järjestelmien ja verkostoautomaatiojärjestelmien välille tarvitaan jatkuvasti uusia liityntöjä erilaisten uusien sovellusten vuoksi. Järjestelmiä uusittaessa ja uusien liityntöjen rakentamisessa halutaan edetä maltillisesti, hyviksi koettuihin ratkaisuihin perustuen, jotta järjestelmien tietoturva ja käytettävyys voitaisiin taata. Usein uusia ratkaisuja halutaan pilotoida ennen niiden varsinaista tuotantokäyttöä. Tähän on kuitenkin verkkoyhtiöillä nykyään yhä vähemmän resursseja käytettävissään.

Työlääksi koettiin myös IDS- ja whitelisting-sovellusten toteuttaminen ja ylläpito automaatioverkkoympäristössä. Jopa tavanomaisten virustorjuntaohjelmistojen käyttö on hankalaa tai jopa mahdotonta mm. yhteensopivuus- ja vasteaikavaatimusten takia.

Tietoturvaosaaminen ja yhteistyö

Tietoturvaosaamista Suomessa koetaan olevan runsaasti, mutta osaajien saaminen verkostoautomaatiohankkeisiin on haastavampi tehtävä. Osaamista pidetään osin siiloutuneena ja ongelmana on saada aikaan riittävä keskustelu eri toimenkuvan omaavien asiantuntijoiden kesken. Usein sähköverkon käytöstä vastaavien automaatioinsinöörien ja tietotekniikan asiantuntijoiden on vaikeaa löytää yhteistä kieltä ja ymmärtää toistensa käyttämää terminologiaa. Myös asenteissa on parantamisen varaa. Yritysjohdolle on usein vaikea perustella ”tuottamattomia” tietoturvainvestointeja.

Tietoturvaviranomaisten osaamisesta ei ollut selvää käsitystä, mutta erityisesti Viestintäviraston toimintaan ollaan tyytyväisiä.

Alan yhteistyötä kaivataan selvästi lisää erityisesti pienten ja keskisuurten yhtiöiden mukaan. Myös viranomaisten ja alan etujärjestöjen sekä yritysten toivotaan järjestävän enemmän verkostoautomaatiojärjestelmien tietoturvaan liittyviä seminaareja ja koulutustilaisuuksia sekä tiedottavan järjestettävistä tapahtumista paremmin. Kaivattiin lisäksi ”hyvien” verkostoitumista.

Ulkoistukset ovat vähentäneet sähköyhtiöiden osaamista, kompetenssi toimittajilla ja palveluyrityksissä.

Ulkoisia asiantuntija- ja auditointipalveluja käytetään hyvin vaihtelevasti. Ongelmana voi joissain tapauksissa olla oikeiden asiantuntijoiden löytäminen. Kiinnostuksen tietoturvaan kasvaessa osaajien ja tarjottavien palvelujen saatavuuskin lisääntyy.

Järjestelmien käyttäjät ja ylläpitäjät tarvitsevat räätälöityjä, tietoturvaan keskittyviä koulutustilaisuuksia.

Turvallisuusjohtaminen ja tietoturvan hallinta

Tietoturvan johtaminen ja selkeästi määritellyt tietoturvapolitiikat ja -ohjeistus koettiin tärkeiksi. Tietoturvaohjeistuksen tulee olla mahdollisimman selkeää ja käytännönläheistä myös asiaan vihkiytymättömälle. Kyberturvallisuus nähtiin sähköisenä osana laajempaa tietoturvaa.

Monessa energiayhtiössä tietoturvapolitiikka ja sitä tarkentava ohjeistus olivat puutteellisia tai niitä ei ollut sovitettu verkkoyhtiön tarpeisiin. Joissakin yhtiöissä tietoturvapolitiikka oli tarkoitettu lähinnä hallitukselle. Jotkut haastatelluista liiketoimintajohtajista kokivat yritysturvallisuuden selvästi hieman etäisenä viitekehyksenä

Nähtiin, että tietoturvapolitiikka ja -ohjeistus tulee olla kirjallisesti dokumentoitu ja henkilöstö on laajasti perehdytettävä niiden sisältöön.

Vastuu tietoturvan yksityiskohtaisesta määrittelystä ja valvonnasta tulee olla erikseen nimetyillä henkilöillä ja vastuun tulisi olla yhtiöittäin keskitetty. Tietoturvaa tekevät ja toteuttavat kuitenkin kaikki yrityksen työtekijät toimitusjohtajasta määräaikaisiin harjoittelijoihin.

Vastuu tietoturvan toteutuksesta voi toisinaan hämärtyä liiketoiminnallisen vastuu ollessa eri yhtiöissä tai liiketoimintayksiköissä.

Laatusertifioinnin koettiin tukevan turvallisuusajattelua.

Toivomukset viranomaisten ja alan järjestöjen suuntaan

<u>Viranomaiset</u>

Verkostoautomaatiojärjestelmien rakenteeseen ja tietoturvan tasoon toivottiin joissain haastatteluissa regulaatiota, jossa järjestelmien vähimmäistaso määritettäisiin ja toiminnallista ohjeistusta lisättäisiin. Viranomaiset esimerkiksi määräisivät vaatimukset ja yksityiset sertifioidut yritykset voisivat suorittaa arvioinnin (vertaa autojen katsastukset). Mahdollisen regulaation tulisi olla vähintään EU-tasoista. Vertailuksi otettiin mm. USA, jossa yhteiskunnan kriittisen infrastruktuurin täytyy täyttää tietyt pakolliset normit tai standardit, esimerkkinä sähköverkkojen tulee täyttää NERC CIP-vaatimukset. Virallisten vähimmäisvaatimusten vahvistamisen jälkeen uskotaan asian pallottelun loppuvan toimittajien ja verkkoyhtiöiden välillä. Todettiin, että nykylait eivät mahdollista viranomaisten taholta pakkokeinoja.

Ainoastaan voidaan antaa suosituksia ja jakaa tietoa verkkoyhtiöille. EU:n uusimistyön alla olevan tietosuojadirektiivin arvioitiin tuovan joitain muutoksia myös energiayhtiöiden tietoturvavaatimuksiin.

Erikseen nostettiin esiin, että Energiamarkkinaviraston ohjausmallia pitää tarkistaa, jotta siinä huomioitaisiin panostukset myös tietoturvan kehittämiseksi. Lisäksi viranomaisten toivottiin nostavan viestiverkoilta vaadittavia varakäyntiaikoja.

Esitettiin myös kantoja, että yksityiskohtaista sääntelyä ei tarvita, sillä se jäykistää liiaksi toimintaa. Annetaan toimialan hoitaa asia parhaimmalla mahdollisella tavalla.

Yhteiskunnan huoltovarmuuskriittisten verkkojen ja järjestelmien turvallisuuden ja tietoturvan tason auditointeja toivottiin myös joissain haastatteluissa.

Viranomaisten toivottiin järjestävän alalle räätälöityjä harjoitustilaisuuksia, jossa yhtiöiden valmiuksia koeponnistettaisiin. Viranomaisilta odotettiin myös tietoturvaan liittyvää tietoutta mm. hyvistä käytännöistä.

Viestintävirasto CERT FI:n HAVARO-palvelua pidettiin hyvänä, mutta kalliina pienille verkkoyhtiöille (HAVARO= Tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä).

Järjestöt

Haastateltavien keskuudessa toivottiin toimialalla yhteistyötä parannettaessa tietoisuutta verkostoautomaatiojärjestelmiin liittyvistä tietoturvauhista ja hyvistä käytännöistä ja ratkaisuista. Edelleen haluttiin yhteistyötä edistettäessä alan kansallista tutkimusta, vaikutettaessa mahdollisesti tulevaan sääntelyyn ja luotaessa ohjeistusta. Yhteistyötä johtavaksi organisaatioksi nousi esiin Energiateollisuus ja Huoltovarmuuskeskus. Toimialalla pitäisi olla taho, joka seuraa meneillään olevaa tietoturvan EU-tasoista lainsäädäntötyötä.

Selvityksen tekemistä pidettiin hyvänä asiana, se tuo tietoturva-asiat keskustelujen kohteeksi.

Tietoverkkojen tunnistettuja tietoturvan kehittämiskohteita

Käyttökeskuksen lähiverkkoympäristö

- Segmentointi, Active Directory-hakemistopalvelun tms. käyttöönotto, whitelisting, secure käyttöjärjestelmät (esimerkiksi LSP LINUX), roolipohjaiset käyttöoikeudet
- Eri työasemat operointia, ylläpitoa ja muuta työskentelyä varten
- USB-muistitikkujen käytön kontrollointi
- Segmentointi oltava pitkälle viety, porttien avaamista ei voi käytännössä valvoa
- Aluekontrolli ehdotettiin hoidettavaksi IP-osoitteilla (segmentointi)
- Fyysinen kulunvalvonta oltava kunnossa
- Kattava lokien käyttäminen ja lokien tietojen säännöllinen läpikäynti ja raportointi

Käyttökeskuksen ja sähköasemien välinen tietoliikenne

- Tietoliikenteen salaaminen, käyttötoiminnan tietoliikenne omaan segmenttiin tai verkkoon
- Erillisverkkojen käyttö

Käyttökeskuksen ja julkisen internet-verkon välinen liikennöinti

- Edistyksellisten palomuurien avulla rakennetut DMZ-alueet, vahva, monitasoinen autentikointi, VPN-tunneloinnin käyttäminen ja liikenteen salaaminen
- Välityspalvelimien (proxy) ja mediaattorilaitteiden käyttäminen, RAS-palvelimet

Käyttökeskuksen lähiverkon ja muun yritysverkon välinen liikennöinti

- Palomuurit, IDS/IPS-ominaisuudet, DMZ-alueet, välityspalvelimien käyttäminen
- Yhteyksien salliminen vain tiettyjen IP- osoitteiden välillä
- Vahva autentikointi

Sähköasemien lähiverkkoympäristö

- Palomuurit, IP-osoitteiden käytön rajaaminen
- Käyttämättömien porttien sulkeminen ja/tai mekaaninen lukitseminen
- USB-muistitikkujen käytön estäminen
- Käytetään ylläpidossa vain erikseen verifioituja työasemia

Vahva autentikointi ja käyttöoikeuksien hallinta

- Active Directory-hakemistopalvelu tai vastaava mahdollisuuksien mukaan käyttöön myös automaatioverkoissa
- Keskitetty pääsynhallinta ja vahva autentikointi
- Roolipohjainen käyttöoikeuksien hallinta

5.3 Arvio tietoturvan tasosta Suomessa

Verkostoautomaatiojärjestelmien tietoturvan taso vaihtelee Suomessa kovasti yhtiöstä toiseen. Tasoon vaikuttavat hyvin monet seikat, esimerkiksi tietoverkkoarkkitehtuuri, käytetyt suojausmenetelmät, verkostoautomaatiojärjestelmien sukupolvi, tietoliikenneverkoissa käytetty tekniikka, tietoturvallisuuden johtaminen ja organisointi jne. Yhtiön koosta ei voi suoraan vetää johtopäätöstä olettaen, että suurissa yhtiöissä asiat olisi hoidettu hyvin ja pienissä huonosti. Molemmista kasteista löytyy sekä hyviä että huonoja esimerkkejä. Myös järjestelmien toimittajien keskuudessa näyttää olevan jonkin verran eroja niiden suhtautumisessa verkostoautomaatiojärjestelmien tietoturvaan.

Järjestelmien voimakas integraatio ja IP-teknologian vahva yleistyminen myös sähköasemien tietoliikenteessä on luonut runsaasti uusia haasteita ratkaistavaksi.

Yleisarviona voidaan esittää, että verkostoautomaatiojärjestelmien tietoturva on tyypillisesti tasoa tyydyttävä-hyvä. Mutta myös välttäviä ja kiitettäviä esimerkkejä löytyy.

6 TURVALLINEN VERKOSTOAUTOMAATIOYMPÄRISTÖ

6.1 Periaatteet verkostoautomaation tietoturvan toteuttamisessa

Turvallisen verkostoautomaatioympäristön rakentaminen ja ylläpitäminen on kokonaisvaltainen, jatkuva prosessi, joka rakentuu osallistavasta ja asiantuntevasta johtamisesta, yhteisestä turvallisuuden viitekehyksestä sekä yhteisesti ymmärretystä kielestä ja käsitteistä. Turvallisuus ja erityisesti tietoturva pitää rakentaa jokapäiväiseksi osaksi kaikkia toimintaprosesseja.

Tietoturvan toteuttaminen pitää suunnitella ja sen toteutumista pitää valvoa, mitata ja raportoida säännöllisesti osana yrityksen normaalia johtamisjärjestelmää ja –prosesseja. Pelkkien vakavien poikkeamien raportointi ei ole riittävää. Hyvä tietoturva on kuin vakuutus - se ei ole välttämätön, mutta ilman sitä on ongelmatilanteissa vaikea tulla toimeen.

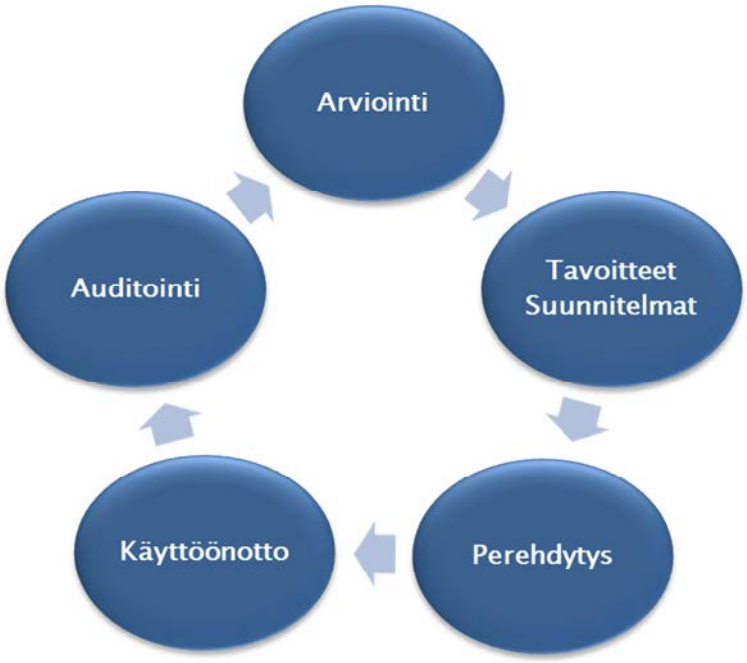
Tietoturva ja siihen liittyvä kyberturvallisuus on oleellinen osa jatkuvuussuunnittelua ja kattaa ainakin seuraavat osa-alueet:

1. Kriittisten tieto- ja tietoliikennejärjestelmien tunnistaminen, inventointi ja dokumentointi
2. Järjestelmiin liittyvien liiketoimintariskien arviointi (osana jatkuvuussuunnittelua)
3. Tietoturvallisen järjestelmäarkkitehtuurin rakentaminen ja ylläpitäminen
4. Havainnointi- ja torjuntakyvyn rakentaminen
5. Kolmansien osapuolien hallinnointi
6. Investointi- ja muutosprojektien hallinnointi ja ohjeistaminen
7. Hyvän hallintomenettelyn rakentaminen
8. Jatkuva seuranta, raportointi ja säännölliset auditoinnit

Kuvassa 6-1 on havainnollistettu automaatiojärjestelmien kyberturvallisuuden rakentamiseen ja ylläpitämiseen liittyvää hyvien käytäntöjen viitekehystä. Viitekehyksen asiasisältö perustuu brittiläiseen CPNI:n dokumentiin Good practice guide, Process control and SCADA security, /11/. Lähde on sarjan päädokumentti ja kultakin osa-alueelta löytyy omat alakuvaukset.

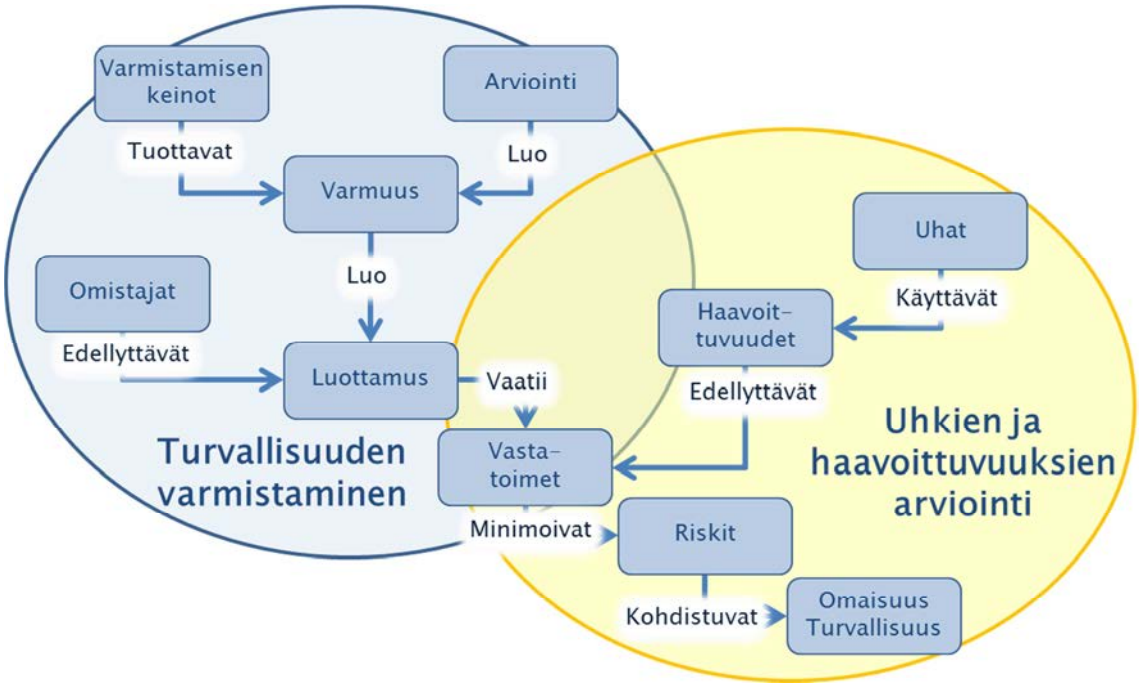
Kuva 6-1 Kyberturvallisuuden rakentamiseen ja ylläpitämiseen hyvät käytännöt

Tietoturvan ylläpitäminen on jatkuva prosessi. Kuvassa 6-2 on visualisoitu yleisen tietoturvaprosessin toimintoja.



Kuva 6-2 Tietoturvaprosessin toimintoja

IEC TC65 työskentelee automaatiojärjestelmien tietoturvastandardien parissa, muun muassa standardi IEC 62443 Industrial network and system security. Kuvassa 6-3 on työryhmän yksityiskohtaisempi näkemys automaatiojärjestelmän tietoturvan varmistamisesta, /9/.



Kuva 6-3 IEC TC65:n näkemys automaatiojärjestelmien tietoturvan varmistamisesta

6.2 Turvallisuusjohtaminen ja hallinnointi

Yrityksen johdon ohjaaman määrittelytyön tuloksena luodaan tarvittavat turvallisuuspolitiikat ja yksityiskohtainen turvallisuusohjeistus eri alueille. Tietoturvan määrittelytyö on yrityksen johtoa, esimiesporrasta, asiantuntijoita ja käyttäjiä laajasti osallistava prosessi.

Tietoturva johtaminen

Tietoturvallisuus ei synny itsestään eikä varsinkaan sellaiseksi kuin sen haluttaisiin olevan. Tietoturvallisuuden saavuttaminen edellyttää johtamista. Toisaalta tietoturvan johtaminen ei juuri poikkea muista vastaavien toimintojen johtamisesta. Se on tavoitteellista työtä, jota lähinnä haittaa tilanteen epämääräisyys ja epävarmuus puhumattakaan monikirjaimisten lyhenteiden määrästä ja käsitteiden sameudesta.

Tietoturva pitää ajatella liiketoiminnan varmistajana. Se on kuin vakuutus, josta on ikävä maksaa, mutta joka on kuitenkin välttämätön. Useimmat haastatelluista verkkoliiketoiminnan ja tietohallinnon johdon edustajista piti yrityksen liiketoiminnan jatkuvuuden varmistamista oleellisimpana tietoturvan johtamisen tavoitteena. Liiketoiminnan riskien hallinta liittyy tietoturvaan jatkuvuuden varmistamisen kautta. Vastuu yrityksen tietoturvasta on viime kädessä toimitusjohtajalla, eikä tätä vastuuta voi ulkoistaa.

Tavoitetilan määritteleminen

On oleellista tunnistaa yrityksen tietoturvan tilannekuva ja muodostaa sen perusteella tavoitetila verkkoliiketoiminnan tietoturvan kehittämiselle. Tietoturvallisuuden tilannekuva kattaa arvion tietojärjestelmien ja -verkkojen turvallisuuden nykytasosta, mahdollisimman kattavasti tunnistetut uhkat ja haavoittuvuudet sekä arvion uhkien ja haavoittuvuuksien liiketoiminnan jatkuvuudelle aiheuttamista riskeistä. Nykyisen muotoinen tietoturvapolitiikka ei kaikilta osin luo tarpeeksi selkeää ja konkreettista päämäärää tietoturvan kehittämiselle, minkä vuoksi tarvitaan erillinen tavoitetilan määrittely. Tietoturvapolitiikan sisällölle ei ole yhdenmukaista sisältöä, vaan se vaihtelee yrityksestä toiseen.

Tietoturvan tavoitetila määrittelee liiketoiminnan osa-alueittain tietoturvaratkaisujen tason käytettävissä järjestelmissä. Edelleen se määrittelee niin oman henkilöstön kuin sidosryhmienkin toimintatavat sekä esimerkiksi käytännöt käyttö- ja pääsyoikeuksien myöntämiseen ja hallintaan.

Haasteena tässä määrittelyssä on tunnistaa oleelliset ja todelliset asiat sekä kyky arvioida niiden kriittisyyksiä. Edelleen tavoitetilan määrittelyssä pitää pyrkiä hyvin konkreettiseen asioiden kuvaamiseen. Liioittelulla tavoitetilan määrittelyssä voi olla merkittäviä kustannusvaikutuksia, mutta niin voi olla vähättelylläkin.

Toisena haasteena on maailman muuttuminen hyvinkin nopeasti. Muutoksia tulee seurata ja tarvittaessa tietoturvallisuuden tilannekuva ja sitä vastaava tavoitetila tulee päivittää.

Toimeenpaneminen ja seuranta

Osana johtamista on huolehtia siitä, että tietoturvallisuuden tavoitetilan saavuttamisen edellyttämät toimenpiteet suunnitellaan ja käynnistetään. Toimenpiteet kattavat teknisten ratkaisujen päivittämisiä ja ylläpitämistä, toimintaohjeiden ja -prosessien päivittämistä ja henkilöiden perehdyttämistä. Käytännönläheiset ja helposti saatavilla olevat tietoturvaohjeet ovat onnistumisen edellytyksenä tietoturvan tavoitetilan saavuttamiseksi. Toimenpiteitä on yleensä paljon, jolloin ne pitää saada tärkeysjärjestykseen toteuttamisien ajoittamiseksi. Ajoituksissa pitää kuitenkin huomioida mahdolliset toimenpiteiden liitokset toisiin toimenpiteisiin tai ulkoisiin seikkoihin, kuten järjestelmäpäivityksiin ja organisaatiomuutoksiin.

Tietoturvan kehittäminen ja ylläpitäminen edellyttävät selkeää toiminnan organisoimista vastuumäärittelyineen. Haasteena on asioiden monet ulottuvuudet, esimerkiksi tekninen ratkaisu ei yksistään riitä vaan sen yhteydessä pitää huolehtia liiketoimintaprosessien toimivuuksista, liittyvien järjestelmien yhteensovittamisista, tarvittavien ohjeiden päivityksistä, käyttöoikeuksien hallinnoinnista ja henkilöiden perehdyttämisistä. Vastuiden jakamisen lisäksi pitää varmistaa eri osapuolten yhteistoiminta harmaiden alueiden välttämiseksi.

Tietoturvallisuuden johtamisen vastuu pitää useimpien haastateltujen liiketoimintojen ja tietohallinnon johtajien mukaan olla liiketoiminnan johdolla. Pääsyynä nähtiin olevan tietoturvan läheinen kytkös liiketoiminnan jatkuvuuden varmistamiseen ja riskien hallintaan. Edelleen nähtiin vastuu teknisestä tietoturvasta selkeästi olevan tietohallinnosta vastaavalla henkilöllä. Mikäli yrityksessä on erillinen tietoturvapäällikkö, hän kuuluu yleensä tietohallinnon organisaatioon.

Johtamiseen liittyvä toteutuksien etenemisten seuranta on jatkuvaa toimintaa. Tämä edellyttää toimivaa, konkreettisiin mittareihin perustuvaa säännöllistä seurantaa ja raportointia.

Tietoturvan kehittäminen on ikuista, koska uhkat muuttuvat, toiminta ja järjestelmät kehittyvät ja uusia haavoittuvuuksia havaitaan koko ajan. Tavoitetilaakin on täsmennettävä ja tarvittavia toimenpiteitä on tarkasteltava säännöllisesti, vähintään kerran vuodessa. Johdon osallistuminen tietoturvan kehittämiseen on oleellinen indikaattori asian tärkeydestä.

Tiedottaminen

Tietoturva ei toteudu, jos siihen liittyviä asioita ei tunneta eikä ohjeita ymmärretä. Tiedottaminen on elintärkeää onnistumisen kannalta. Tämän vuoksi liiketoiminnan johdon pitää vastata tietoturvaan liittyvästä yleisestä tiedottamisesta. Tietoturvan teknisen tiedottamisen vastuu on tietoturva-asiantuntijoilla.

Tiedottaminen pitää olla monikanavaista ja toistuvaa. Johdon esimerkillinen oma toiminta on erittäin vahva viesti.

Osaksi tiedottamista voidaan lukea myös ohjeiden ajan tasalla pitäminen, niiden saatavilla oleminen ja helppokäyttöisyys. Eräässä yrityksessä ohjeistus perustuu wiki-ratkaisuun, mikä mahdollistaa paremman ohjeistuksen hallinnan ja loogisuuden, helpot haut ja hypertekstin käytön. Edelleen ohjeiden päivittäminen on teknisesti helpompaa.

Tiedottamisella on kuitenkin rajansa ja turvallisuuskriittiset, yksityiskohtaiset tietoturvaohjeet eivät saa joutua asiattomien käsiin.

6.3 Järjestelmäarkkitehtuuri ja tietoverkon rakenne

6.3.1 Verkostoautomaatiojärjestelmän erityispiirteet

Uudet verkostoautomaatiojärjestelmät muistuttavat laitteistoiltaan ja varusohjelmistoltaan (käyttöjärjestelmä, ajurit yms.) tavanomaisia, yritystietoverkossa käytettäviä tietojärjestelmiä järjestelmätoimittajien ryhdyttyä käyttämään verkostoautomaatiojärjestelmissään teollisuusstandardien mukaisia tietokonelaitteita ja varusohjelmistoja. Tästä seuraa, että toimistojärjestelmissä hyviksi koetut ja tehokkaat rakennemallit, toimintaprosessit, työkalut sekä osaaminen ovat käytettävissä myös verkostoautomaatiojärjestelmien suojaamisessa.

Poikkeuksia tavanomaisten tietojärjestelmien ja verkostoautomaatiojärjestelmien välillä löytyy erityisesti vanhempien automaatiojärjestelmien osalta.

Tavanomaisten tietojärjestelmien ja verkostoautomaatiojärjestelmien välisiä eroja:

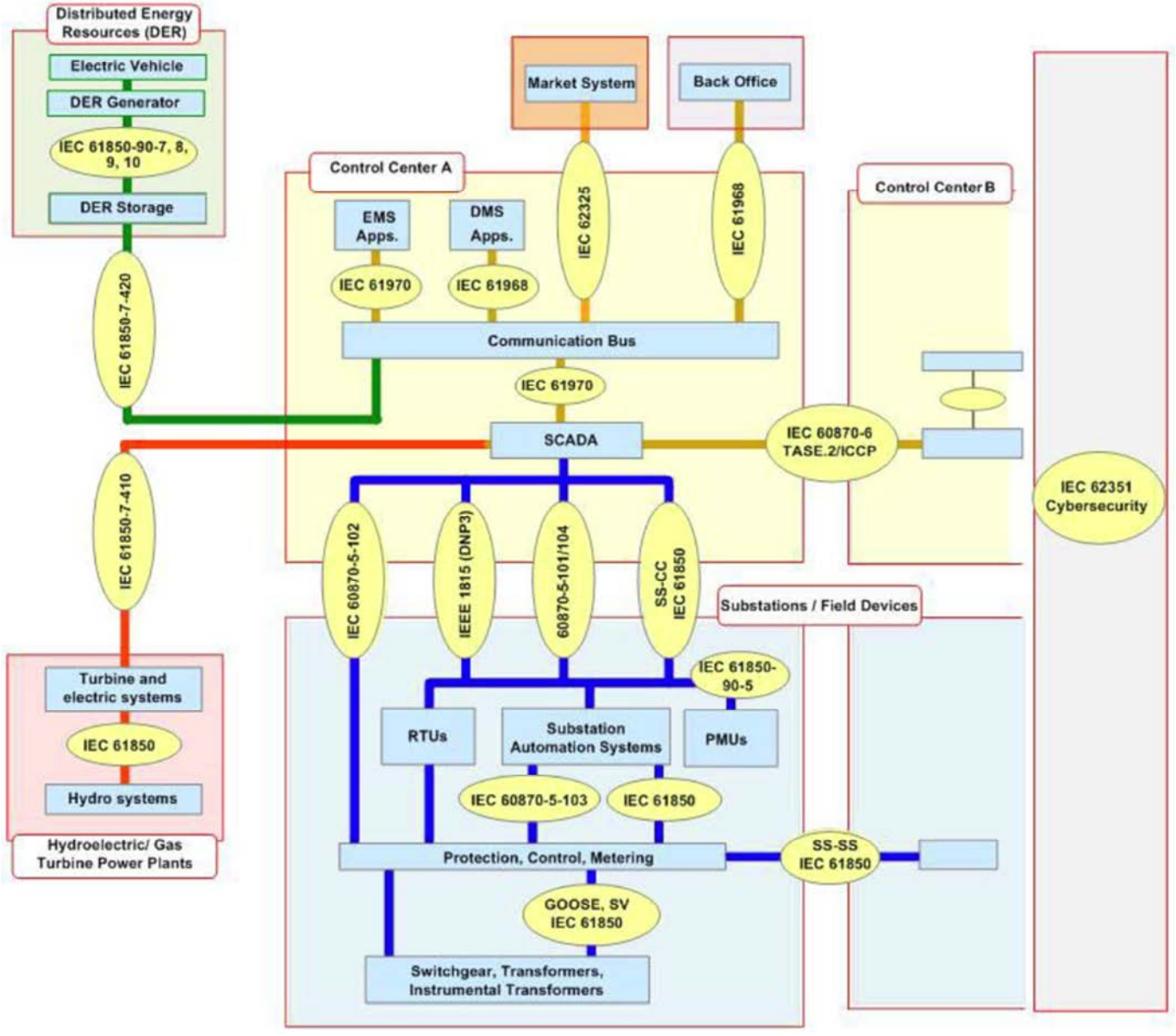
- Verkostoautomaatiojärjestelmä valvoo ja ohjaa jatkuvaa reaaliaikaista prosessia, jonka vasteaikavaatimukset ovat tiukat, tyypillisesti millisekunteja, suojaussovelluksissa jopa 0,1 millisekuntia
- Verkostoautomaatiojärjestelmä ohjaa yhteiskunnan toiminnan kannalta kriittistä infrastruktuuria, jolloin järjestelmien käytettävyysvaatimus on kertaluokkaa tiukempi, tyyppisesti vähintään 99,95 % ajasta

- Verkostoautomaatiojärjestelmän on toimittava jatkuvasti keskeytyksettä, jolloin sen kunnossa- ja ylläpito sekä valvonta on järjestettävä 24/7-periaatteella
- Verkostoautomaatiojärjestelmän turvallisuus ja luotettavuus on oltava huippuluokkaa, virhetoiminnoista voi olla seurauksena huomattavat taloudelliset ja ihmisten terveyttä vaarantavat vahingot
- Verkostoautomaatiojärjestelmä on yleensä huomattavasti pitkäikäisempi kuin tavanomainen tietojärjestelmä, käyttöikä on tyypillisesti yli 10 vuotta.
- Muutoksia ja päivityksiä tehdään huomattavasti harvemmin ja ne on poikkeuksetta testattava erillisissä testijärjestelmissä
- Vanhoista, jopa nykyisistä verkostoautomaatiojärjestelmistä ja niiden käyttämistä tiedonsiirtoprotokollista puuttuvat rakenteellisesti integroidut tietoturvaominaisuudet
- Valtaosa käytössä olevista tietoturvaohjelmista on laadittu yleisessä käytössä toimistoissa ja kotona oleviin järjestelmiin. Näitä ohjelmistoja ei usein voida käyttää verkostoautomaatiojärjestelmässä niiden aiheuttaman epäkäytettävyysriskin takia
- Verkostoautomaatiojärjestelmä voi tarvittaessa toimia kokonaan omassa, täysin eristetyssä tietoverkon vyöhykkeessään (saareke), verkostoautomaatiojärjestelmä on yleensä varsin riippumaton muiden tietojärjestelmien toiminnasta
- Tiedonsiirtotarve verkostoautomaatiojärjestelmän ja yrityksen muiden tietojärjestelmien välillä on pääasiassa yksisuuntaista (verkostoautomaatiojärjestelmä -> yritysverkko) ja on ajoittaista
- Osa verkostoautomaatiojärjestelmän laitteista, esimerkiksi ala-asemat ja suojareleet sijaitsevat sähköisesti häiriöllisessä ja vaativassa ympäristössä, joissa ei normaalisti työskentele ihmisiä, jotka tekisivät ongelmatilanteissa käyttötoimenpiteitä
- Verkostoautomaatiojärjestelmässä tehdään harvoin isoja muutoksia, jolloin järjestelmien muutosten ja testausten suunnittelu- ja asiantuntijatyökustannuksilla ei ole niin suurta merkitystä
- Verkostoautomaatiojärjestelmän tietosisältö muodostaa tarkasti tunnetun joukon, jossa poikkeavuuksien havaitseminen on suhteellisen helppoa
- Laitteet on fyysisesti suhteellisen helppo suojata ja kulku laitetiloihin voidaan sallia vain tietylle rajatulle, hyvin tunnistetulle joukolle
- Automaatiojärjestelmien laitteiden prosessointikyky on yleensä huomattavasti pienempi kuin tavanomaisissa tietojärjestelmissä. Tämä rajoittaa verkostoautomaatiojärjestelmän laitteiden kykyä suorittaa ylimääräisiä tietoturvaohjelmia (virussuojausohjelmat, salausprotokollat jne.). Tyypillinen mitoituskriteeri verkostoautomaatiojärjestelmille on ollut laajan häiriötilanteen edellyttämä tietojen käsittelykyky. Tällaisessa tilanteessa kaikki prosessointikapasiteetti on käytössä
- Käytönvalvontajärjestelmien sisäisessä tiedonsiirrossa käytetään perinteisesti hidasta, usein langatonta sarjamuotoista tiedonsiirtoa, joka rajoittaa esimerkiksi salausprotokollien käyttöä. Poikkeuksena eräät kaupunkiyhtiöt ja kantaverkko, joissa tiedonsiirtoon käytetään lähinnä suuren siirtokapasiteetin omaavia valokuituja
- Jatkuvasti toimivia yhteyksiä julkisten televerkkojen välityksellä ei välttämättä tarvita tai ne voidaan tarvittaessa suojata helposti erittäin vahvalla suojauksella
- Verkostoautomaatiojärjestelmiä suunnittelevalla, operoivalla ja ylläpitävällä henkilöstöllä ei usein ole riittävää tietoturvatuntemusta.

6.3.2 Modulaarinen, standardeihin rajapintoihin perustuva järjestelmäarkkitehtuuri

Järjestelmäarkkitehtuurilla on ratkaiseva vaikutus verkostoautomaatioympäristön tietoturvaan. Hyvä käytäntö on rakentaa yrityksen tietoverkkoarkkitehtuuri erikseen suojattuihin alueisiin, joissa suojaus perustuu tietoverkkoalueen käyttötarkoituksesta, tarpeesta liikennöidä julkisiin televerkkoihin tai niiden välityksellä sekä erityisesti tietoverkkoalueen järjestelmien ja niiden sisältämän tiedon luottamuksellisuudesta ja kriittisyydestä. Vyöhykepuolustusstrategiaa ja siihen liittyvää tietoverkon jakamista alueisiin on käsitelty tarkemmin luvussa 6.3.3.

Oheisessa, lähteestä /6/ peräisin olevassa kuvassa on IEC TC57-standardointityöryhmän visualisoima näkemys turvallisesta verkostoautomaation järjestelmäarkkitehtuurista ja siihen liittyvistä standardeista. Ymmärrettävistä syistä rakenne tukeutuu pääosin IEC-standardeihin.

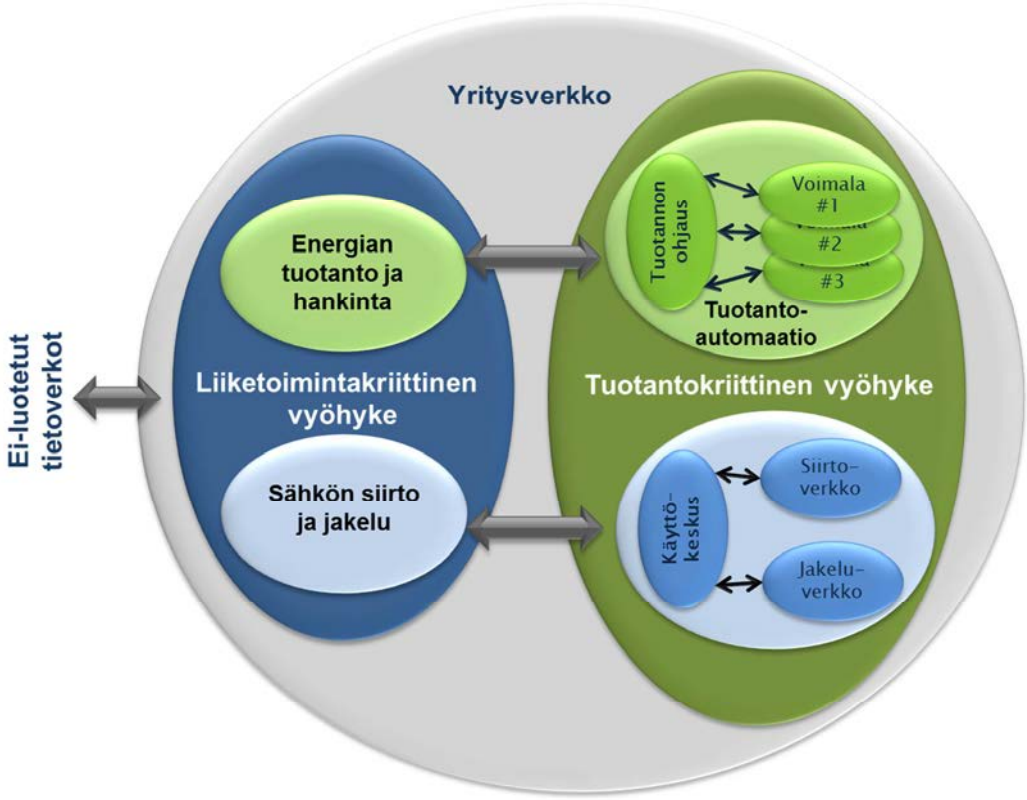


Kuva 6-4 IEC TC57:n näkemys järjestelmäarkkitehtuurista standardien näkökulmasta

Luvussa 6.4 on tarkemmin käsitelty turvallisen verkostoautomaatioympäristön rakentamiseen soveltuvia standardeja.

6.3.3 Tietoverkon rakenne ja vyöhykepuolustusstrategia

Sähköyhtiön tietojärjestelmät ja tietoverkot tulee suunnitella ja rakentaa erikseen suojatuiksi alueiksi. Liiketoiminnan jatkuvuuden kannalta kriittisten sähkön siirron ja jakelun verkostoautomaatiojärjestelmien tulee sijaita vihamielisten hyökkäysten kannalta mahdollisimman suojatussa ja turvallisessa tietoverkkoalueessa. Eri alueiden välinen tietoliikenne suojataan vähintään palomuurein. Kunkin alueen tietoturvalle määritetään omat vaatimukset ja menettelytavat tietoturvan suhteen. Kunkin alueen sisällä käytetään sinne parhaiten sopivia työkaluja haittaohjelmien muiden tietoturvauhkien tunnistamiseen ja eliminointiin. Tietoverkon luotettavuus perustuu sen tietoturvatasoon. Esimerkkinä vaarallisesta ympäristöstä ja ei-luotetusta verkosta on julkinen internet-verkko. Kuvassa 6-5 on visualisoitu vyöhykestrategian periaatetta.



Kuva 6-5 Esimerkki vyöhykepuolustusstrategian mukaisesta aluerakenteesta

Vyöhykepuolustusstrategialle on ominaista:

1. Tietoverkon topologia on rakennettu alueista (zone) ja suojatuista kerroksista, joissa kriittisimmät järjestelmät ja tiedot sijaitsevat kaikkein turvallisimmalla ja luotettavimmalla alueella. Vertaa ns. sipulimalli, jossa turvarakenne perustuu sisäkkäisiin, erikseen suojattuihin alueisiin
2. Tietoturvapolitiikassa on huomioitu toimintakriittiset verkostoautomaatiojärjestelmät. Prosessit ja koulutus on suunniteltu niitä silmällä pitäen

3. Tieto- ja tietoliikennejärjestelmien rakenteissa käytetään hyviksi koettuja malleja ja mahdollisimman standardeja rakenneosia
4. Viranomaisten laatimia suosituksia ja määräyksiä noudatetaan tunnollisesti
5. Suojattavat järjestelmät on tunnistettu ja dokumentoitu huolella. Erityisesti kaikki järjestelmien väliset integraatiot ulkoisiin verkkoihin ja muilla alueilla sijaitseviin sisäisiin järjestelmiin on dokumentoitu ja arvioitu
6. Liitynnät on toteutettu huolella ja testattu perusteellisesti. Kaikki ylimääräiset tai turhat liitynnät on poistettu ja tarpeettomat tietoliikenneportit on poistettu käytöstä
7. Tietoverkkoarkkitehtuuria kuvattaessa ja rakennettaessa yhteistyö eri henkilöstöryhmien ja luotettujen yhteistyökumppanien kanssa on erittäin hyödyllistä ja usein välttämätöntä. Esimerkiksi riskianalyyseihin on osallistuttava asiantuntijoita yrityksen eri yksiköistä, mm. johtoa, turvallisuusjohtoa ja tietoturva-asiantuntijoita, käytön edustajia sekä automaatio- ja tietoliikenneasiantuntijoita. Usein hyödynnetään myös ulkopuolista asiantuntemusta
8. Tietoturvallisen järjestelmäarkkitehtuurin rakentaminen ja ylläpitäminen on jatkuvaa toimintaa. Muutostarpeet pitää käsitellä samalla tavalla kuin suunnittelussa. Tietojärjestelmien osalta pitää tietoturva huomioida koko niiden elinkaaren ajalta sisältäen suunnittelun, rakentamisen, käyttöönoton ja testaamisen, käytön, ylläpidon sekä romuttamisen
9. Yrityksen yleinen yritysverkko ja toimintakriittisiä verkostoautomaatiojärjestelmiä palveleva tietoverkko sijoitetaan omille suojatuille alueilleen ja ovat loogisesti erotettu toisistaan
10. Erityistekniikkana käytetään mm. palomuureja ja DMZ-välityspalvelimia ja erillisiä IP-numeroavaruuksia. Katso periaatekuva 7-1
11. Turvalliset alueet jaetaan tarvittaessa edelleen erillisiksi segmenteiksi esimerkiksi VLAN-tekniikkaa hyödyntäen
12. Verkostoautomaatiojärjestelmien turvallisista alueista rakennetaan suoria liityntöjä julkiseen internet-verkkoon vain erittäin painavista syistä. Tällaisiin yhteyksiin käytetään vahvoja suojausmenetelmiä sekä liikenteen salausta. Yhteydet pidetään suljettuna aina, kun niitä ei tarvita
13. Kriittiset järjestelmät on rakennettu vikasietoisiksi, jolloin kaikki verkostoautomaatio-järjestelmän kriittiset komponentit on varmennettu. Riittävä varmennus yleensä saavutetaan, kun kaikki kriittiset järjestelmäkomponentit on toisistaan riippumattomasti kahdennettu. Joskus sopiva menetelmä voi olla ”n+1 varmennus”, minkä mukaisesti järjestelmä sietää minkä tahansa yhden yksikön menetyksen toiminnan häiriintymättä
14. Järjestelmät kovennetaan eli kaikki tarpeettomat liitynnät, ohjelmistot ja tietoliikenneportit on poistettu käytöstä
15. Fyysisenä suojauksena järjestelmän laitteet on sijoitettu lukittuihin kaappeihin ja laitetiloihin
16. Järjestelmien käyttöoikeuksia hallinnoidaan keskitetysti ja kunkin henkilön käyttöoikeudet on rajoitettu hänen roolinsa mukaiseksi (roolipohjaiset käyttöoikeudet)
17. Verkostoautomaation tietoverkoissa on käytetty omaa erillistä vahvaa autentikointia, joka on riippumaton muista energiayhtiön järjestelmistä
18. Edistyksellisiä menetelmiä käytetään henkilöiden tunnistamisessa. Sellaisia ovat esimerkiksi älykortit ja biometrinen tunnistaminen

19. Eri tietoverkkojen (alueiden) yhdysliikenneväyliin on rakennettu vahvat kontrollit käyttäen palomuureja ja tarvittaessa IDS/IPS-järjestelmiä sekä DMZ-alueelle sijoitettuja välityspalvelimia (proxy). Näiden laitteiden tulee tunnista myös epänormaali liikenne. Myös etäkäytön RAS-palvelimet on sijoitettu DMZ-alueelle
20. Palvelimissa ja työasemissa käytetään tunnettujen haittaohjelmien eliminoimiseksi virustarkistusta ja tiedostojen eheyden tarkistavia ohjelmia
21. Vahvaa salausta on käytettävä kriittisten tietokantojen ja tietoliikenteen suojaamiseen, mikäli se vasteajat ja käytetty tekniikka huomioon ottaen on mahdollista
22. Etätyöskentelyssä käytettävien, erityisesti kannettavien työasemien massamuistit salataan (kryptataan)
23. Kaikki uudet verkostoautomaatiojärjestelmien tietoturvaratkaisut testataan perusteellisesti testijärjestelmissä ennen niiden asentamista tuotantoympäristöön
24. Tietoturvalaitteista, -ohjelmista ja lokeista saatavaa tietoa kerätään ja analysoidaan systemaattisesti ja tietoturvaraportointi on liitetty osaksi normaalia prosessiraportointia.
25. Ulkopuolisia, luotettavia asiantuntijoita käytetään säännöllisesti auditoimaan järjestelmien tietoturvan taso

6.4 Standardit, normit ja ohjeistus

6.4.1 Tietoturvastandardit

Tietoturvallisuuteen sekä verkostoautomaatiojärjestelmien käytettävyyteen ja luotettavuuteen liittyviä standardeja, toimintaohjeistusta ja soveltuvia viranomaismääräyksiä on laaja kirjo. Ongelmana on tunnistaa niistä kuhunkin yksittäiseen tarpeeseen parhaiten soveltuvat osat ja osata laatia niistä parhaiten kunkin yrityksen tarpeita tyydyttävät määrittelyt ja toimintaohjeet. Jäljempänä käsitellään lähinnä verkostoautomaation kannalta hyödyllisimmät standardit ja ohjeet. Lisäksi esitetään viittauksia ja linkkejä saatavilla olevaan kansainväliseen ja kansalliseen alan materiaaliin.

Taulukossa 6-1 on listattu tärkeimpiä verkostoautomaatiojärjestelmien suunnittelussa, rakentamisessa ja ylläpitämisessä yleisesti käytettyjä tietoturvastandardeja ja standardin luontoisia normeja tai vapaamuotoisempia ohjeita. Taulukossa mainitut dokumentit ovat aihealueiltaan osin päällekkäisiä ja asioiden esitystapa vaihtelee suuresti.

Taulukko 6-1 Tietoturvastandardeja, normeja ja ohjeita

Standardi/ normi/ohje	Sovellusalue	Status	Käyttökohde
ISO/IEC 270xx, xx= 00…37	Kansainvälinen standardi, hyvin kattava	-01, -02 ja -05 laajasti käytössä	Yleinen IT-ohjeistus ja vaatimukset tietoturvan hallintaan yms.
IEC 62351	Kansainvälinen tekninen spesifikaatio	Julkistettu, soveltaminen käynnistynyt	Verkostoautomaatio-järjestelmien data- ja protokollasuojaus
IEEE 1711	IEEE standardi, globaalisti relevantti	Julkistettu, soveltaminen käynnistynyt	Erityisesti ala-asemien perinteisen sarjaliikenteen salaaminen
IEEE 1686	IEEE standardi, globaalisti relevantti	Julkistettu, soveltaminen käynnistynyt	Kenttälaitteiden vaatimusmäärittely, perustuu NERC CIP -vaatimuksiin
ANSI/ISA-99 IEC 62443	USA-lähtöinen, globaalisti relevantti	Osa julkistettu. Työ jatkuu	Teollisuusautomaatio-järjestelmien ja verkkojen tietoturvan toimintamallit yms.
NIST SP800-82	USA-lähtöinen, globaalisti relevantti	Julkistettu ja käytössä laajasti	Guide for Industrial Control System (ICS) Security, tietoverkkoinfrastruktuurin kybersuojaus
NERC CIP	USA ja Kanada, globaalisti relevantti	Julkistettu, pakollinen amerikkalaisille voimayhtiöille	Tietoverkkoinfrastruktuurin kybersuojauksen suunnittelusääntöjä ja toimintaohjeita
CPNI suositukset	Iso-Britania, globaalisti relevantti	Julkistettu, käytössä	Kybersuojauksen viitekehys ja hyvät käytännöt
COREQ-VE, COREQ-ACT	Suomi	Käytössä	Teollisuusautomaatio-järjestelmän tietoturvavaatimuksia

IEC = International Electrotechnical Commission IEC, http://www.iec.ch
IEEE = Institute of Electrical and Electronics Engineers, http://www.ieee.org
NIST = National Institute of Standards and Technology, http://www.nist.gov
NERC = North American Electric Reliability Corporation, http://www.nerc.com
CPNI = Centre for the Protection of National Infrastructure, http://www.cpni.gov.uk

Oheisessa taulukossa on esimerkin vuoksi esitetty standardin IEC 62351 rakenne. Standardi on osin keskeneräinen ja osia siitä ollaan joiltain osin päivittämässä, jotta standardia voitaisiin helpommin soveltaa käytännössä. Standardia tullaan käyttämään laajasti mm. ala-asema- ja suojausyhteyksien tietosuojauksen toteuttamisessa.

Taulukko 6-2 Tietoturvastandardin IEC 62351 rakenne

IEC 62351 rakenne

IEC 62351-1 — Communication networks and system security - Introduction to security issues

IEC 62351-2 — Glossary of terms

IEC 62351-3 — Security for profiles including TCP/IP

- TLS Encryption
- Node Authentication
- Message Authentication

IEC 62351-4 — Security for profiles including MMS, (i.e. IEC 60870-6, IEC 61850, etc.)

- Authentication for MMS
- TLS (RFC 2246)

IEC 62351-5 — Security for IEC 60870-5 and derivatives (i.e. DNP3)

- TLS for TCP/IP profiles and encryption for serial profiles

IEC 62351-6 — Security for IEC 61850

- VLAN use is made as mandatory for GOOSE
- RFC 2030 to be used for SNTP

IEC 62351-7 — Network and system management (NSM) data object models

- Defines Management Information Base (MIBs) that are specific for the power industry, to handle network and system management through SNMP based methods

IEC 62351-8 — Role-based access control.

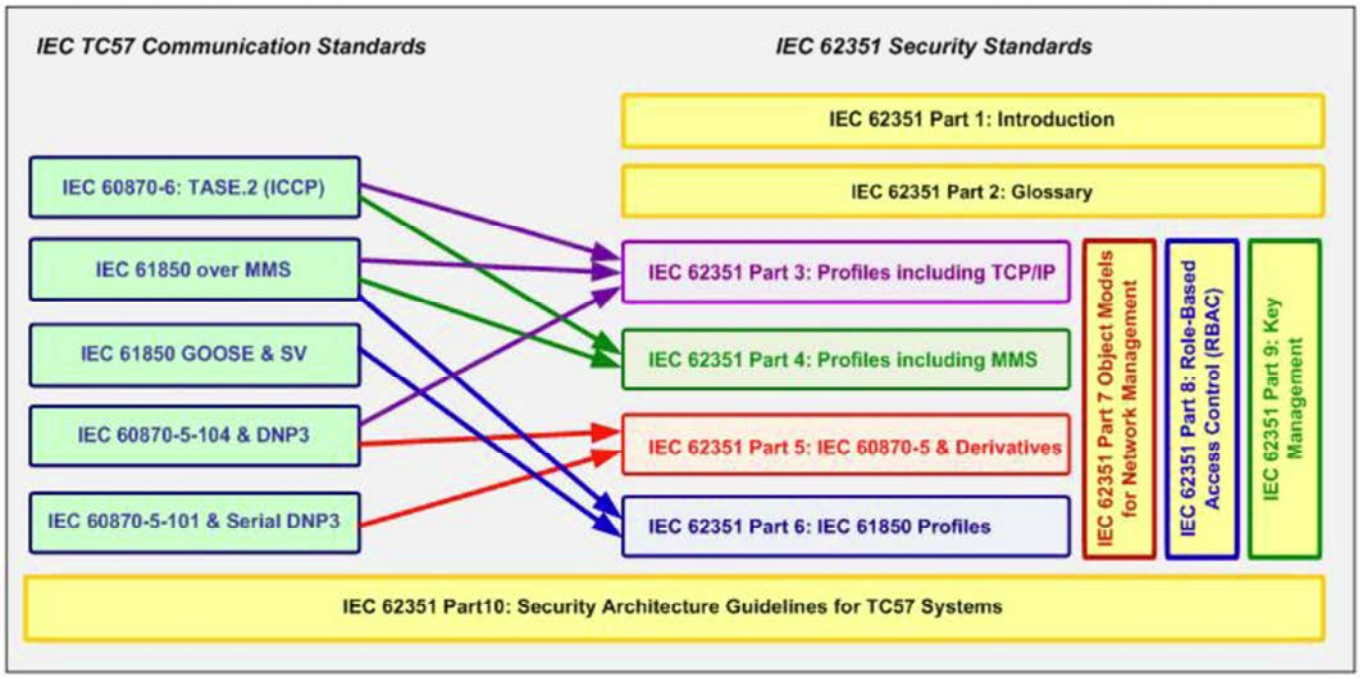
- Covers the access control of users and automated agents to data objects in power systems by means of role-based access control (RBAC)

IEC 62351-9 — Key Management

IEC 62351-10 — Security Architecture Guidelines

IEC 62351-11 — Security for XML Files

Kuvassa 6-6 on esitetty eri IEC:n tiedonsiirtostandardien ja tietoturvastandardin IEC 62351 osien soveltamisen riippuvuudet.



Kuva 6-6 IEC:n tiedonsiirtostandardien ja tietoturvastandardin IEC 62351 väliset riippuvuudet

Lisää tietoturvallisten automaatiojärjestelmien suunnitteluun, rakentamiseen ja ylläpitoon soveltuvia standardeja ja ohjeita on esitetty VTT:n TITAN-käsikirjassa, /8/. Dokumentti sisältää mm. taulukon Smart Grid-ympäristöön soveltuvista tietoturvastandardeista. Dokumentissa on myös ansiokkaasti arvioitu kunkin eri standardin tai suunnitteluohjeistojen vahvuuksia ja soveltuvuutta automaatiojärjestelmien tarpeisiin.

6.4.2 Tietoliikenneverkkojen rakenteiden, ominaisuuksien ja fyysisen suojaamisen standardeja

Ohessa on lueteltu hyödyllisiä tietoliikennestandardeja ja Viestintäviraston määräyksiä, joita noudattamalla saadaan tietoliikenneverkkojen käyttävyyttä, fyysistä suojausta ja tietoturvaa parannettua.

Ethernet-verkon virtualisointiominaisuuksien ja segmentoinnin tuki:

- IEEE 802.1Q VLAN

Ethernet-verkon tiedonsiirron varmennusominaisuuksien tuki:

- IEEE 802.1D-2004 Rapid Spanning Tree
- IEEE 802.1w Rapid Spanning Tree
- IEEE 802.1s Multiple Spanning Tree
- IEEE 802.1ad Provider Bridge
- IEEE 802.17 Resilient Packet Ring (RPR)
- IEEE 802.3ad Link Aggregation Control
- ITU-T G.8031/Y.1720 Ethernet Protection Switch
- ITU-T G.8032/Y.1344 Ethernet Rings Protection Switching

Ethernet-siirto piirikytkentäisen SDH-verkon yli:

- ITU-T G.7041, Generic Framing Procedure (GFP),
- ITU-T extension G.707, Virtual Concatenation (VCAT),
- ITU-T G.7042, Link Capacity Adjustment (LCAS)

Suojausyhteyksien optinen tiedonsiirto:

- IEEE C37.94

Viestintäverkkojen ja -laitteiden varmentaminen ja fyysinen suojaaminen:

- Viestintäviraston määräys 54 A/2010 M, /24/

Sähköasemien sähkömagneettisten häiriöiden sieto ja televerkkojen sähköinen suojaaminen:

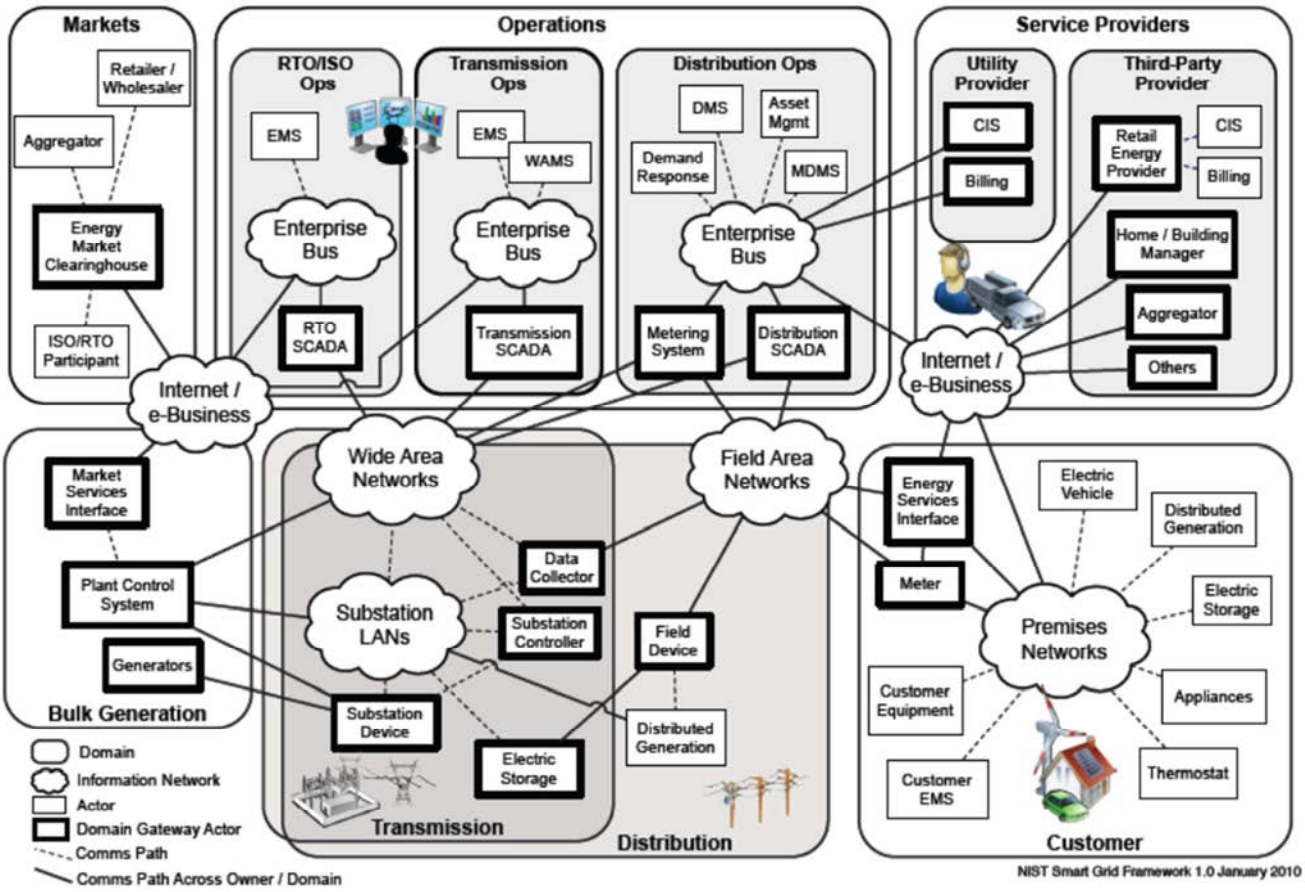
- IEEE 1613 EMC-vaatimukset (soveltuu erityisesti sähköasemaympäristöön)
- Soveltuvat CENELEC- ja ETSI-ympäristöstandardit
- Televerkkojen sähköinen suojaaminen, Viestintäviraston määräys 43 D/2010 M, /25/

6.4.3 Älykkäiden sähköverkkojen (Smart Grid) tuomat erityispiirteet

Älykkäille sähköverkoille on ominaista tehon ja tiedon siirtyminen verkoissa molempiin suuntiin. Suojattavia tietolähteitä on vähintään yhtä paljon kuin on sähköverkossa energian tuotanto- ja kulutuspisteitä. Nämä tietolähteet ovat hyvin hajallaan eri puolella sähköverkkoa ja edellyttävät siten myös yhteysmäärältään hyvin tiheää ja maantieteellisesti kattavaa tietoliikenneverkkoa. Usein kustannustehokkainta on toteuttaa tietoliikenne jakeluverkon alueella hajallaan sijaitseviin kulutus- ja hajatuotantokohteisiin julkisilla matkaviestinverkoilla, joiden kapasiteetti ja tietoturvaominaisuudet oikein konfiguroituna ovat tarkoitukseen yleensä riittävät, esimerkkinä etäluettavien mittareiden tietoliikenne. Kiinteitä yhteyksiä käytetään aina silloin, kun se on teknistaloudellisesti järkevää. Tiedonsiirtoon osallistuvien suuresta määrästä johtuen tarvitaan edistyksellisiä menetelmiä kohteiden identiteetin tunnistamisessa. Sellaisia ovat esimerkiksi älykortit tai mobiilitunnistaminen. Viimeksi mainittu voidaan toteuttaa SIM-korttiin perustuvana lisäpalveluna.

Älykkäitä sähköverkkoja tutkitaan aktiivisesti eri puolilla maailmaa ja niiden standardointia kehitetään kovaa vauhtia. Eräs standardeja ja tietoturvallisia käytäntöjä älykkäitä sähköverkkoja varten kehittävistä tahoista on yhdysvaltalainen National Institute of Standards and Technology (NIST), kuvassa 6-7 on NIST:n näkemys älykkään sähköverkon viitekehyksestä.

Kuva osoittaa sen, miten laajan verkottuneen kokonaisuuden energiayhtiön älyverkkoon liittyvät järjestelmät muodostavat. Tietoturvan rakentamiselle ja ylläpitämiselle tämä tuo aivan erityisiä haasteita.



Kuva 6-7 National Institute of Standards and Technologyn (NIST) Smart Grid-viitekehys

7 KÄYTÄNNÖN OHJEITA TIETOTURVALLISEN VERKOSTOAUTOMAATIO-YMPÄRISTÖN RAKENTAMISEKSI JA YLLÄPITÄMISEKSI

7.1 Toimenpidelista tietoturvallisuutta parantavista toimenpiteistä

Välittömät toimenpiteet (muutama päivä, enintään kuukausi)

1. Tunnista kaikki verkostoautomaatiojärjestelmän tai -laitteen ulkoiset tietoliikenneliitännät
2. Poista kaikki tarpeettomat ulkoiset liitännät, jätä vain ehdottoman välttämättömät
3. Arvio jäljelle jääneiden liityntöjen turvallisuuden taso ja paranna niitä kaikin käytettävissä olevin nopein keinoin
4. Kovenna verkostoautomaatiojärjestelmä poistamalla tai deaktivoimalla siitä kaikki tarpeettomat sovellukset, tietoliikenneportit ja USB-väylät. Tee tämä myös sähköasemilla ja verkostossa sijaitseville laitteille.
5. Huolehdi, että kaikista järjestelmän ohjelmista ja -datasta on ajantasaiset ja toimivat varmuuskopiot verkostoautomaatiojärjestelmien palauttamiseksi kriisitilanteissa
6. Poista kaikki tarpeettomat käyttöoikeudet järjestelmiin ja pääsyoikeudet toimitiloihin
7. Vaihda salasanat heti ja myöhemmin riittävän usein. Käytä vain vahvoja, mielellään vähintään 10-merkkisiä salasanoja
8. Tarkista, että pääsy ulkoisista, erityisesti julkisista verkoista verkostoautomaatio-järjestelmiin on toteutettu vahvaa autentikointia käyttäen. Tarkista myös, että liikenne julkisissa tietoverkoissa on salattu teknisesti luotettavalla tavalla. Tee tarvittaessa muutokset viivytyksettä

Lähiajan toimenpiteet (1 kuukausi - 1 vuosi)

1. Määritä tietoturvan johtamisen roolit ja vastuut, järjestelmien omistajien ja ylläpitäjien tehtäväkuvat sekä käyttäjien vastuut
2. Eristä julkiset tietoverkot, yrityksen sisäinen tietoverkko ja sen sisällä oleva turvallinen verkostoautomaation tietoverkko toisistaan sijoittamalla palomuurien ja välityspalvelimien avulla rakennetut DMZ-alueet verkkojen rajapintoihin (tietoliikenneväyliin). Lisää IDS/IPS-toiminnallisuus joko osana palomuureja tai erillisenä järjestelmänä vähintään kuhunkin julkisen televerkon ja turvallisen sisäverkon rajapintaan. Älä salli kiertoteitä palomuurien tai välityspalvelimien ohittamiseksi
3. Segmentoi käyttökeskuksen ja sähköasemien lähiverkot esimerkiksi VLAN-tekniikan avulla ja siirrä toimintakriittinen tietoliikenne ja muu tietoliikenne loogisesti erillisiin tietoverkkoihin. Käytännössä tulisi toteuttaa erilliset tietoliikennejärjestelmät, omat kanavat piirikytkentäisissä siirtojärjestelmissä (PDH/SDH) tai vähintään omat VLANit IP-verkossa. Älä kytke suojausyhteyksiä IP-pohjaiseen tietoliikenneverkkoon
4. Rakenna järjestelmien käyttöoikeuksien hallinta keskitetyksi, käyttäjien rooliin perustuvaksi. Älä käytä samaa Active Directory:ä tms. yrityksen sisäisen tietoverkon kanssa ja rakenna autentikointi vahvaan tunnistamiseen perustuvaksi esimerkiksi kertakäyttöisillä salasanoilla
5. Älä luota perinteisten ala-asema-protokollien kykyyn suojata verkostoautomaatio-järjestelmä vaan salaa tietoliikenne yhdessä järjestelmätoimittajan kanssa, mikäli se on teknisesti mahdollista

6. Rakenna muutkin verkostoautomaatiojärjestelmän tietoturvaominaisuudet yhdessä järjestelmätoimittajan kanssa
7. Tarkista ja suojaa kaikki mahdolliset takaportit tunkeutua järjestelmään
8. Analysoi ja varmista sähkö- ja viestiasemien ja muiden laitetilojen fyysisen turvallisuuden taso. Minimissään asemien on oltava aidattu, rakennusten sekä laitetilojen lukittu sekä varustettu sähköisellä kulunvalvonnalla ja tallentavalla videovalvonnalla
9. Kuvaa tietoverkkoarkkitehtuuri kattaen myös tietoliikennejärjestelmät, tunnista kriittisiä toimintoja palvelevat järjestelmät ja määritä järjestelmien luottamuksellinen ja toimintakriittinen tieto, joka tarvitsee vahvennettua suojausta
10. Määrittele järjestelmien tietoturvavaatimukset
11. Perusta 24/7-pohjainen valvontatoiminto verkkoliikenteen monitorointiin ja poikkeamien havaitsemiseen lähtien olettamuksesta, että kaikkiin suojattuihin tietoverkkoalueisiin voidaan tunkeutua. Valvontakyky voidaan rakentaa itse tai käyttää ulkopuolisia palvelutoimittajia. Esimerkiksi Viestintäviraston CERT-FI:llä on HAVARO-palvelu huoltovarmuuskriittisille yrityksille.
12. Perusta eri organisaatioyksiköiden asiantuntijoista koostuva ”palokuntaryhmä” tunnistamaan tietoturvauhkia, luomaan menettelyt tietoturvapoikkeamien hallintaan sekä tarvittaessa tunnistamaan ja eliminoimaan mahdolliset hyökkäykset
13. Huolehdi henkilöstön riittävästä perehdyttämisestä tietoturvaan ja järjestelmien käyttöön sekä huolehdi tietoturvaosaamisen ylläpidosta
14. Harjoittele järjestelmien palauttamista kriisitilanteissa
15. Teetä ulkopuolisilla asiantuntijoilla verkostoautomaatiojärjestelmän tietoturva-auditointi
16. Teetä tarvittaessa verkostoautomaatiojärjetelmän tai sen osan kattava tietoturvatestaus joko omassa testiympäristössä tai toimittajan järjestelmäympäristössä. Testausohjeistusta löytyy lähteestä /8/ ja työkaluja lähteestä /23/

Pitkän ajan kehitysohjelma (1-5 vuotta)

1. Rakenna tietoverkkoarkkitehtuuri vyöhykepuolustusstrategiaan perustuvaksi, jossa turvallisuuskriittisimmät tietoverkot ja järjestelmät ovat kukin omalla suojatulla alueellaan mahdollisimman kaukana julkisista avoimista televerkoista. Rakenna kyky tunnistaa ja eliminoida jo järjestelmän sisälle päässyt haittaohjelma tai tietoturvauhka
2. Määritä ja ylläpidä turvallinen ja tehokas menettely järjestelmien ja tietoliikenneverkon konfiguraation hallintaan
3. Osana jatkuvuussuunnittelua kuvaa, rakenna ja ylläpidä toiminnan kannalta kriittisten järjestelmien riskienhallintaprosessi sisältäen järjestelmien palauttamissuunnitelmat
4. Rakenna jatkuvasti toimiva prosessi järjestelmien ohjelmistojen päivittämiseksi. Testaa verkostoautomaatiojärjestelmien ohjelmapäivitykset ja uudet ohjelmat aina ennen tuotantoympäristöön vientiä joko omassa tai toimittajan testijärjestelmässä
5. Teetä säännöllisesti puolueeton arviointi yrityksen kriittisten järjestelmien ja tietoliikenneverkkojen tietoturvan tasosta ulkopuolisilla tietoturva-asiantuntijoilla

7.2 Yhtiön toimintaympäristön vaikutus järjestelmäratkaisuihin ja toimintamalleihin

Valtakunnalliset toimijat tai isot kaupunkiyhtiöt

Sähköyhtiön koko, toimialue ja harjoitettavien liiketoimintojen luonne ja laajuus vaikuttavat tietoverkkojen teknisiin ratkaisuihin ja siten myös tietoturvaan. Isoilla kaupunkiyhtiöillä on usein sähkökaupan ja sähkönjakelun lisäksi omia voimalaitoksia sekä lämmönjakelua. Monilla yhtiöillä on omia suurjänniteverkkoja, jotka on suojattava monipuolisesti. Yhtiöt toimivat yhteiskunnan elinkeinoelämän kannalta keskeisillä alueilla ja ne luokitellaan huoltovarmuuden kannalta erittäin tärkeiksi yhtiöiksi. Tämä korostaa tietoturvan tärkeyttä järjestelmäarkkitehtuuria suunniteltaessa ja järjestelmäratkaisuja toteutettaessa. Omassa luokassaan toimii maamme ainoa kantaverkkoyhtiö, Fingrid Oyj.

Kaupungissa on kustannustehokasta rakentaa korkean tietoturvan kuituverkkoa rakenteellisena osana voimasiirtojohtoihin tai kaukolämpöputkistojen yhteyteen. Isoilla yhtiöillä on usein omat tietojärjestelmä- ja tietoverkkoasiantuntijat, monesti myös tietoturvaan erikoistuneita asiantuntijoita. Nämä yhtiöt kykenevät suunnittelemaan ja toteuttamaan pitkälle omin resurssein tietoverkkoarkkitehtuurin, joka tukee parhaiten konsernin liiketoimintoja ja järjestelmäarkkitehtuuria. Yhtiöt käyttävät ulkopuolisia palveluja lähinnä sähkö- ja tietoverkkojen rakentamiseen ja kunnossapitoon. Jotkin ostavat verkostoautomaatiojärjestelmien tietoliikenneyhteyksiä palveluna ulkopuoliselta toimittajalta, joka lisää yhtiöiden välisen yhteistyön ja yhteisen toimintakulttuurin merkitystä. Nämä yhtiöt teettävät tietoturva-auditointeja ulkoisilla asiantuntijoilla säännöllisesti ja ostavat muitakin tietoturvapalveluja selvästi pieniä yhtiöitä enemmän.

Alueelliset verkkoyhtiöt

Alueellisissa verkkoyhtiöissä harjoitettavia liiketoimintoja on monesti isoja kaupunkiyhtiöitä vähemmän, mikä pienentää tietojärjestelmien määrää ja yksinkertaistaa tietoverkkoarkkitehtuuria. Keski- ja pienjänniteverkkoja on toisaalta johtomäärältään paljon verkkoasiakkaisiin nähden. Tämä lisää riskiä luonnonvoimien aiheuttamille suurhäiriöille sekä vaikuttaa toimintaprosesseihin, järjestelmärakenteisiin ja varautumiseen. Yhtiöillä ei välttämättä ole jokaiselle ICT-tekniikan osa-alueelle päätoimisia tai edes sivutoimisia asiantuntijoita, joten näiltä osin on usein turvauduttava ulkoisiin palveluihin. Omaa osaamista ja resursseja täydennetään verkottumalla. Järjestelmiä hankitaan usein kokonaistoimituksina avaimet käteen -periaatteella.

Suurilla alueellisilla verkkoyhtiöillä haasteena ovat pitkät yhteysetäisyydet sähköasemien välillä ja niistä käyttökeskukseen. Usein langattomat tiedonsiirtotekniikat katsotaan teknistaloudellisesti parhaaksi vaihtoehdoksi rakentaa verkostoautomaation tarvitsema tietoliikenneverkko. Tekniikkoina käytetään pääsääntöisesti radiolinkkejä, radiomodeemeja tai matkaviestinyhteyksiä. Uudet omat tietoliikenneverkot perustuvat nykyisin digitaalisiin päätelaitteisiin ja käyttävät usein pakettikytkentäistä siirtotekniikkaa. Näitä käyttäen on mahdollista rakentaa korkean tietoturvan ja käytettävyyden tieliikenne-yhteyksiä, kun tietoturvan asettamat lisävaatimukset tietoverkkoarkkitehtuurille otetaan huomioon.

Kuluttajien etäluettavien mittareiden tietoliikenteeseen käytetään kasvavassa määrin matkaviestinyhteyksiä, jotka ovat suosittuja myös sähköasemien varayhteyksinä. Maastoerotinasemien yhteydet ovat usein toteutettu joko oman analogisen radiopuhelin- tai radiomodeemiverkon avulla tai ostettu palveluna matkaviestinoperaattorilta. Vanhoihin analogisiin radioverkkoihin liittyy merkittävä tietoturvariski.

Paikalliset verkkoyhtiöt

Paikallisissa verkkoyhtiöissä oma osaaminen keskittyy pitkälti sähköverkko-liiketoiminnan ydintoimintoihin. Tietotekniikka- sekä tietoturvaosaaminen ovat pitkälti ostopalvelujen varassa. Nämä yhtiöt ovat muita sähköyhtiöitä enemmän riippuvaisia järjestelmätoimittajien palveluista ja toimintamalleista.

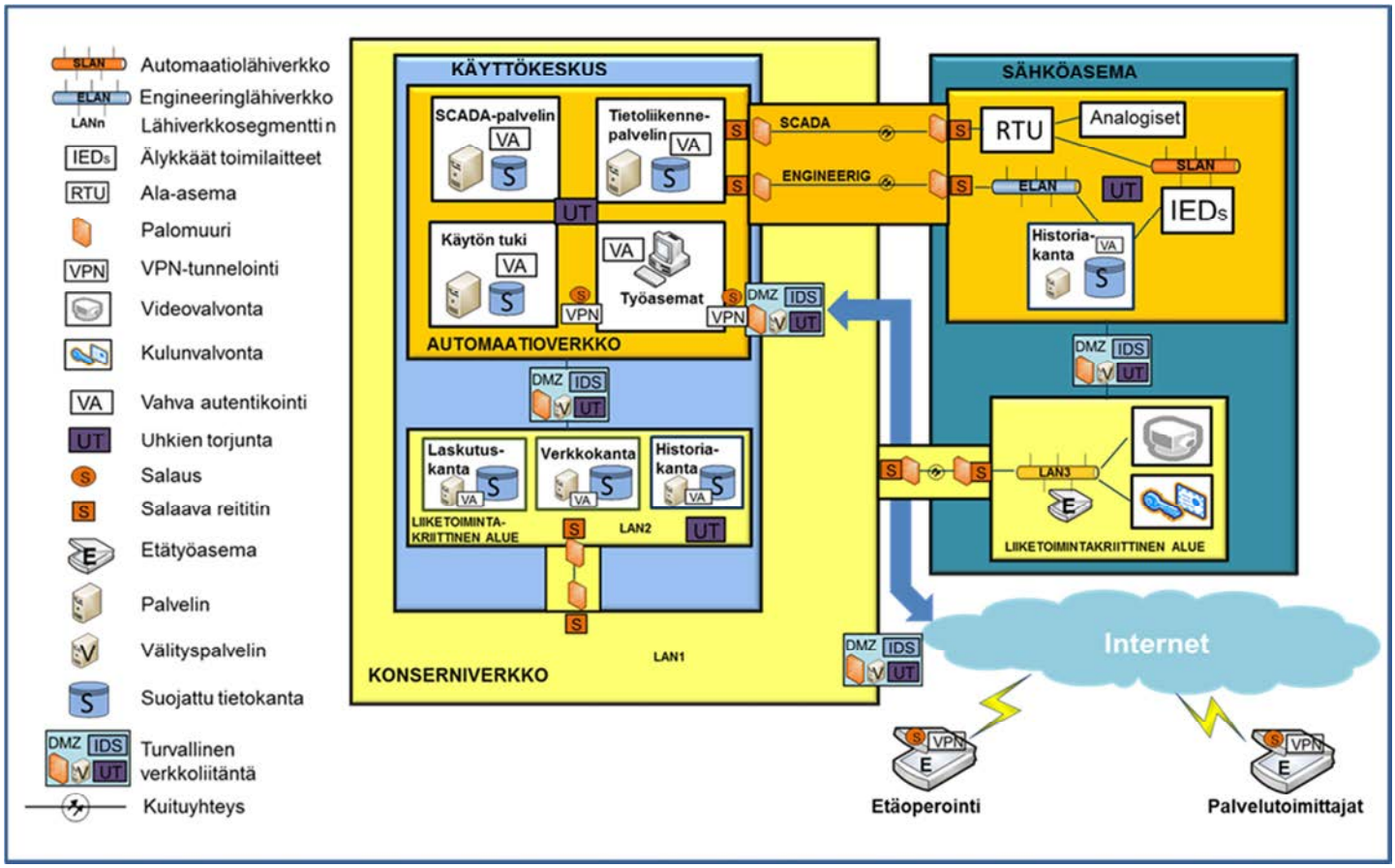
7.3 Hyviä käytäntöjä verkostoautomaatiojärjestelmiä suunniteltaessa

7.3.1 Käyttökeskuksen järjestelmäympäristö

Sähköverkkoyhtiön käyttökeskus laitetiloineen ja järjestelmineen muodostaa verkostoautomaatiojärjestelmän sydämen. Kriittisimmät järjestelmät tulee kahdentaa mielellään mahdollisimman kattavasti. Toisiaan kahdentavat järjestelmät sijoitetaan riittävän etäällä oleviin erillisiin laitetiloihin. Nämä laitetilat on hyvä sijaita eri rakennuksissa ja ne tulisi varustaa täysin erillisillä ja varmennetuilla sähkönsyöttöjärjestelmillä. Käyttökeskuksen tilojen suositellaan täyttävän viestintäviraston määräyksen 54 A/2012 M tärkeysluokka 1 tai 2 mukaiset vaatimukset, /24/. Laitetilan fyysisen suojaamisen osalta käyttökeskuksen tiloihin ja yhteyksiin sovelletaan taulukoiden 3 Laitetilan kulunvalvonta ja 4 Laitetilojen rakenne ainoastaan tärkeysluokan 1 vaatimuksia. Varavalvomon laitetilat voivat olla myös tärkeysluokan 2 vaatimusten mukaisia. Asiakaskasmäärältään ja liikevaihdoltaan pienet verkkoyhtiöt voivat erityisen painavista syistä poiketa näistä vaatimuksista, mutta poikkeamisen syy on oltava perusteltu ja heikennetty turvallisuus/vaatimustaso on oltava erityisen seurannan ja ylläpidon piirissä. Mahdollisten ongelmien ilmetessä tilojen ja yhteyksien vaatimustasoa on kiristettävä mahdollisimman nopeasti.

Käyttökeskuksen verkostoautomaatiojärjestelmien tietoverkko tulee eristää julkisista tietoverkoista ja yrityksen/konsernin yritysverkosta vahvan suojauksen omaavilla laitteilla ja tietoturvasovelluksilla, kuten kuvassa 7-1 on esitetty. Yritysverkon suojaus julkisten verkkojen suuntaan on aina syytä tehdä palomuurein ja välityspalvelimin varustetun DMZ-alueen kautta. Alueelle voidaan lisäksi sijoittaa monitorointia ja haittaohjelmien poistoa tekeviä palvelimia, esimerkiksi IDS/IPS-laitteita.

Keskinkertaisesti luotetun yritysverkon ja käyttökeskuksen turvallisen verkostoautomaatio-verkon väliseen suojaukseen soveltuu periaatteessa samat ratkaisut kuin yritysverkon suojaamiseen julkisten verkkojen suuntaan. Välityspalvelimien ja palomuurien parametrointi ja varustus on sovitettava suojattavien verkostoautomaatiojärjestelmien erityisvaatimusten mukaisesti. Palomuurien on oletusarvoisesti kiellettävä kaikki liikenne. Vain välttämättömät IP-osoitteet avataan. Paras suoja saadaan, mikäli välitys-, RAS- yms. palvelimet on sijoitettu DMZ-alueelle, joka on suojattu erillisin palomuurein kaikkiin mahdollisiin liikennöintisuuntiin.



Kuva 7-1 Sähköverkkoyhtiön tietoverkon periaaterakenne

Käyttökeskuksen automaatioverkossa suositellaan käytettävän yksityistä IP-osoiteavaruutta ja verkko on hyvä segmentoida aliverkkoihin esimerkiksi VLAN-tekniikkaa hyödyntäen. Omat aliverkot voivat olla esimerkiksi tietoliikennepalvelimilla, järjestelmäpalvelimilla, ylläpitojärjestelmillä sekä käytön työasemilla. Myös käyttökeskuksen yritysverkko (kuvassa 7-1 VLAN2) on eritetty muusta konsernin yritysverkosta omaan segmenttiinsä.

Verkostoautomaatiojärjestelmän palvelimet ja tietoliikennelaitteet on kovennettava. Toisin sanoen kaikki turhat ohjelmat on poistettava tai deaktivoitava luotettavasti ja kaikki turhat tietoliikenneportit on syytä sulkea. Verkostoautomaatiojärjestelmän palvelinten ja työasemien USB-porttien suositellaan olevan lukittavaa mallia ja niitä saa käyttää vain tietoturvasta tai järjestelmästä vastaavan henkilön suostumuksella ja valvonnan alaisena.

Palvelimet suositellaan suojattavaksi virusturva- ja whitelisting-ohjelmistoilla, mikäli järjestelmän toimittaja antaa siihen luvan.

Käyttöoikeuksien hallinnointi verkostoautomaation tietoverkoissa on suositeltavaa tehdä keskitetysti roolipohjaisena ja erillään muusta yritysverkon käyttöoikeuksien hallinnoinnista. Vahvaa, moniportaista autentikointia suositellaan käytettäväksi joko kertakäyttöisillä tai riittävän monimutkaisilla salasanoilla (suositus vähintään 10 merkkiä). Yhteisistä salasanoista on luovuttava mahdollisimman nopeasti. Missään olosuhteissa ei saa käyttää järjestelmätoimittajan oletussalasanoja.

7.3.2 Sähköaseman järjestelmäympäristö

Sähköasema on fyysisenä laiteympäristönä haasteellinen satunnaisesti esiintyvien suurten sähkömagneettisten häiriöiden takia. Sähköasemien laitetilojen ja tietoliikenneyhteyksien fyysisessä suojaamisessa suositellaan käytettäväksi soveltuvin osin Viestintäviraston määräystä 54 A/2012 M, /24/ sekä muita soveltuvia alan standardeja.

Uusissa automaatioverkkoratkaisuissa suositellaan sähköverkon toimilaitteiden (katkasijat, suojareleet, mittamuuntajat, muuntajat tms.) paikallisautomaation lähiverkko rakennettavaksi metallittomiin optisiin kuituihin perustuvaksi. Uudiskohteissa verkkoprotokollana sähköaseman verkostoautomaation lähiverkossa käytetään jatkossa lähes yksinomaan IEC 61850-prokollaa. Engineering- ja etätyöskentelyn ethernet-lähiverkot voivat perustua suojattuihin metallikaapeleihin ja ruggeroituihin tiedonsiirtolaitteisiin (ruggeroitu = rakennettu vaikeita ympäristöolosuhteita kestäväksi). Engineeringlähiverkkoa (huoltoverkko) käytetään sähköaseman järjestelmien ylläpitoon, katso kuva 7-1 ELAN-lähiverkko. Engineeringlähiverkkoon voidaan liittää myös aseman video- ja kulunvalvontajärjestelmiä ellei niille haluta rakentaa omaa loogista verkkosegmenttiä. Etätyöskentelyverkkoa käytetään nimensä mukaisesti etätyöskentelyyn sähköasemilla ja se on yritysverkon aliverkko. Etätyöskentelyverkon kautta on mahdollista liikennöidä myös julkiseen internet-verkkoon. Kuvassa 7-1 etätyöskentelyverkkoa edustaa LAN3-lähiverkko.

Sähköasemien verkostoautomaatiolähiverkko suositellaan suojattavaksi palomuurein. Verkostoautomaatioliikenteen VPN-tunnelointi on välttämätöntä, mikäli yhteyksissä käytetään julkisia verkkoja. Julkisten verkkojen kautta välitettävä verkostoautomaatioliikenne on salattava ja salaus on suositeltavaa myös käytettäessä verkkoyhtiön omia tietoliikenneverkkoja.

Sähköasemien verkostoautomaation toimilaitteet, mahdolliset palvelimet ja työasemat on suojattava käyttöoikeuksien roolipohjaisella hallinnalla ja mahdollisimman vahvalla autentikoinnilla. Koventamista suositellaan käytettäväksi myös sähköasemilla olevien palvelimien, työasemien ja tietoliikenneverkkojen laitteiden suojaamiseksi.

7.3.3 Tietoliikenneyhteydet

Verkostoautomaatiojärjestelmien tietoliikenteen osalta on oleellista hallita kaikkia tietoliikenteen osa-alueita yhteysväleittäin, jotta kokonaisuudesta saadaan eheä, kattava ja kaikilta osin turvallinen ja luotettava. Tietoturvallisuuden lisäksi verkostoautomaatio-yhteyksiltä vaaditaan korkeaa käytettävyyttä ja joissain tapauksissa erittäin nopeaa vasteaikaa. Kriittisissä kohteissa, kuten esimerkiksi kantaverkossa, verkostoautomaatio-yhteyksien käytettävyyden on oltava huippuluokkaa, tyypillisesti 99,95-99,99% ajasta. Helpointa on toteuttaa vaatimukset omassa määräysvallassa olevan tietoliikenneverkon avulla. Myös alan erikoisyhtiöt ovat valmiita räätälöimään sähköverkkoyhtiöiden tarvitsemia verkostoautomaatioyhteyksiä mittatilaustyönä. Tällöin yhteyksien käytettävyys/luotettavuus saadaan halutulle tasolle, mikä ei usein onnistu suurten teleoperaattoreiden palveluja käytettäessä.

Tarvittaessa myös julkisten verkkojen ja yhteyksien käyttö saadaan useimmiten riittävän tietoturvalliseksi, kun käytetään oikeita teknisiä ratkaisuja, esimerkkinä mainittakoon VPN-tunnelointi ja vahva salaus. Kanta- ja alueverkkoissa verkostoautomaatioyhteyksien käytettävyysvaatimusten saavuttaminen voi kuitenkin olla haasteellista julkisia yhteyksiä käytettäessä. Matkaviestinyhteydet soveltuvat lähinnä jakeluverkon automaation tarvitsemiin yhteyksiin, kun otetaan huomioon mahdolliset käyttökatkot suurhäiriöiden aikana.

Perinteinen piirikytkentäinen tietoliikenne, esimerkiksi PDH- ja SDH-järjestelmät, ovat pakettikytkentäisiä IP-järjestelmiä tietoturvallisempia, koska yhteydet on rakennettu kanavoimalla ja piste-piste-periaatteella eristettyyn ”putkeen”. Piirikytkentäinen tietoliikenne ei käytännössä pääse missään olosuhteissa ei toivottuun paikkaan tai sekoittumaan haitallisen liikenteen kanssa. Tällainen vaara on periaatteessa olemassa pakettikytkentäisen liikenteen osalta.

Pakettikytkentäiset tietoliikenneverkot ovat edullisempia rakentaa ja niiden käyttö on piirikytkentäisiä ratkaisuja joustavampaa. Erityisesti julkinen internet-verkko ja yritysverkot, lähiverkot (LAN) ja laajaverkot (WAN), ovat oivia esimerkkejä pakettikytkentäisen IP-tekniikan voittokulusta. Näistä syistä johtuen pakettikytkentäiset verkot ovat voimakkaasti yleistynyt myös käytönvalvontayhteyksissä. IP-tekniikan tuloa sähköasemien sisäisiin ja ulkoisiin yhteyksiin ovat vauhdittaneet myös alan uudet IP-pohjaiset yhteysmenettelyt ja protokollat. Suojayhteyksissä IP-siirtotekniikkaa ei kuitenkaan suositella käytettäväksi. Tämä pätee erityisesti differentiaalisuojauksessa sen erittäin tiukkojen kulkuaikavaatimusten (jopa 0,1 ms) vuoksi. Uuden ”hybridivaihtoehdon” mahdollistavat niin sanottua Next Generation SDH-tekniikkaa (NG-SDH) käyttävät laitteet. Niissä SDH-siirtokerroksen päällä voidaan siirtää sekä piirikytkentäisiä että pakettikytkentäisiä yhteyksiä. IP-siirto toteutetaan teknisesti L2-tason ethernet-siirtona lomitettuna SDH-kehyksiin. Myös SDH-ethernet-yhteyksien virtualisointi segmentteihin on mahdollista.

Siirtotekniikkana tietoturvallisimpia ovat valokuituihin perustuvat ratkaisut niin piirikytkentäisten kuin IP-järjestelmienkin osalta. Kuitumäärän ollessä pieni voidaan niiden kapasiteetin käyttöä tehostaa aallonpituusjakomultipleksoinnilla (WDM-tekniikka). Tekniikalla voidaan yhdessä kuidussa tai kuituparissa siirtää turvallisesti sekä tavallisia yritysverkko-yhteyksiä että kriittisiä verkostoautomaation yhteyksiä. Kuitujen lisäetu muihin siirtotekniikoihin verrattuna on niiden ylivoimainen siirtokapasiteetti. Siirtotarpeiden kasvaessa muun muassa kuvasiirron myötä siirtokapasiteettia on helppo kasvattaa suhteellisen edullisia päätelaitteita päivittämällä tai vaihtamalla.

Digitaalinen siirto perinteisissä kuparikaapeleissa voi olla kaupunkiyhtiöille kustannustehokas vaihtoehto täydentämään optisia valokaapeliyhteyksiä. Kupariyhteyksissä käytetään nykyisin yleensä adaptiivisia xDSL-tekniikoita perinteisten piirikytkentäisten PCM-johtolaitteiden jäätyä pois käytöstä.

Tarvittaessa pitkiä yhteysetäisyyksiä ja riittävää taattua kapasiteettia kohtuulliseen hintaan on tarjolla vaihtoehtona digitaaliset radiolinkit. Näitä on saatavana sekä piiri- että pakettikytkentäisinä siirtokapasiteetin ollessa parhaimmillaan satoja megabittejä sekunnissa. Käytössä on vielä runsaasti analogisia radiolinkkejä ja radiopuhelinjärjestelmiä, eikä niitä voida suositella tietoturvallisten verkostoautomaatioyhteyksien rakentamiseen.

Nämä laitteet/järjestelmät suositellaan uusittavaksi nopeutetulla aikataululla, mikäli niitä käytetään verkostoautomaatioyhteyksien alustoina. Puhekäytössä ne ovat vielä käyttökelpoisia.

Satelliittiyhteyksiä on käytetty myös jonkin verran käytönvalvontayhteyksiin. Niiden haittapuolina voidaan mainita korkeahko hinta, suuri kulkuaikaviive sekä riski käytettävyydestä teknisen vian sattuessa tai kansainvälisen kriisin yhteydessä.

Julkisten teleoperaattoreiden datansiirtoon rakennettuja erikoisverkkoja (esimerkiksi WIMAX-verkot) käytetään pienissä määrin sähkö- ja erotinasemien yhteyksien toteuttamisessa. Tukiasemien kapasiteetti näissä verkoissa on yleensä jaettu kaikkien käyttäjien kesken ja taattu siirtonopeus vaatii erityisjärjestelyjä. Lisäksi niiden kaupallinen saatavuus näyttää uhatulta.

Erikoisverkkoihin on luettavissa myös viranomaisten VIRVE-radiopuhelinverkko. Käyttötoiminnan puheyhteyksiin verkko soveltuu hyvin, mutta erittäin rajallisen datasiirtokapasiteetin takia verkkoa ei voi suositella uusien/suurien sähköasemien tiedonsiirtoratkaisuksi.

WLAN-tekniikat mahdollistavat langattoman, potentiaalivapaan siirron sähköasemien sisäisissä lähiverkoissa. Näiden ratkaisujen tietoturva on rakennettava vahvaksi ja hyvin huolellisesti, jotta ulkoiset tahot eivät pääse suoraan tunkeutumaan verkostoautomaatio-järjestelmän ytimeen.

Etäkäyttöyhteydet muodostetaan yleensä julkisten verkkojen välityksellä luotettuun verkostoautomaatioverkkoon. Tällöin on välttämätöntä käyttää vahvaa, moniportaista autentikointia, yhteyksien suojausta (VPN-tunnelointi) ja riittävää salausta. Liikenteen salaamiseen on lukusia vaihtoehtoja alkaen HTTPS-protokollasta päätyen erittäin kehittyneisiin salausalgoritmeihin. Lisäturvaa tuovat alustariippumattomien virtualisoitujen käyttöliittymien käyttäminen etätyöskentelyssä (esimerkiksi CITRIX).

Uudet kannettavat älypuhelimet ja kämmenpäätelaitteet mahdollistavat jo etätyöskentelyn ja etäoperoinnin julkisten matkaviestinverkkojen välityksellä. Laitteiden tietoturva on vasta kehittymässä ja niiden käyttöön tietoturvakriittisiin yhteyksiin pitää suhtautua toistaiseksi suurella varauksella.

Käytönvalvonta- ja suojausyhteyksien salaaminen kannattaa toteuttaa standardeja menetelmiä käyttäen hyödyntäen esimerkiksi tuoretta IEC 62351-standardia.

Kuvassa 7-1 käytönvalvontaliikenteen lisäksi sähköasemien engineering- ja liiketoimintakriittiset yritysverkkoyhteydet on salattu. Kahden viimeksi mainitun yhteystyypin osalta salauksesta voidaan luopua, mikäli käytetään muutoin riittävän vahvaa suojausta, esimerkiksi vahvaa autentikointia ja VPN-tunnelointi. Kuvassa 7-1 ei ole otettu kantaa sähköasemayhteyksien siirtotekniikkaan. Yhteydet voivat olla joko piirikytkettyjä tai käyttää IP-tekniikkaa. Kuituyhteydet voidaan tarvittaessa korvata luotettavilla langattomilla yhteyksillä, esimerkiksi radiolinkeillä.

Omia tietoliikenneverkkoja täytyy operoida ja ylläpitää jatkuvasti. Vahvasti varmennetussa tietoliikenneverkossa esiintyvät viat voivat jäädä huomaamatta ilman hallintajärjestelmää. Parhaiten maantieteellisesti hajanaisen ja laajan tietoliikenneverkon operointi ja hallinta onnistuu sopivaa verkonhallintajärjestelmää (NMS) käyttäen tehtiinpä operointi verkkoyhtiön oman henkilökunnan tai palvelutoimittajan toimesta. Tietoliikenneverkon hallintajärjestelmä on tarpeellinen sekä piirikytketyissä että IP-pohjaisissa tietoliikenneverkoissa.

8 JOHTOPÄÄTÖKSET

Tieto- ja kyberturvallisuus ovat nousseet viimeisen parin vuoden aikana julkisuuteen erityisesti muutaman näyttävän kansainvälistä huomioita saaneen tietomurto- ja tiedusteluoperaation myötä (Stuxnet-mato ja NSA:n tiedusteluoperaatio). Suomen valtion viranomaiset ovat olleet huolissaan uusista uhkakuvista, jotka voivat vaarantaa elinkeinoelämän ja julkisen sektorin tietoturvan ja samalla toiminnan jatkuvuuden. Tietoturvaa uhkaavat perinteisten hakkereiden, ääriliikkeiden ja tietorikollisten lisäksi nyt myös valtiolliset sähköiseen tiedusteluun ja kybersodankäyntiin erikoistuneet yksiköt. Lisääntyvien uhkakuvien takia maahan on laadittu ja vahvistettu kyberturvallisuusstrategia ja perusteilla on kyberturvallisuuskeskus Viestintäviraston CERT-FI-yksikön yhteyteen.

Tietoturvallisuusuhkia ja haavoittuvuuksia lisää tietotekniikan siirtyminen yleiskäyttöisiin käyttöjärjestelmiin myös automaatiojärjestelmien ohjelmistoalustoina. Erilaisten järjestelmien määrä on kasvanut viimeisen kymmenen vuoden aikana huimasti. Tämä on johtanut voimakkaasti lisääntyneeseen järjestelmien väliseen integraatioon ja tiedonsiirtoon. Samaan aikaan on tapahtunut voimakas muutos kohden IP-pohjaista ja julkista internet-verkkoa hyödyntävää globaalia tietoverkkoa. Tämä on tuonut valtaisan määrän tietoa jokaisen saataville. Valitettavasti kaikilla verkon käyttäjillä ei ole vilpittömät ajatukset ja yhteiskunnan toiminnan kannalta kriittinen infrastruktuuri on tullut vihamielisten tahojen ulottuville. Taistelu vihamielisiä tahoja vastaan jatkuu herkeämättä. Tällä hetkellä rosvot näyttävät valitettavasti olevan kisassa selvässä johdossa ja huoli tietoturvasta ja toiminnan jatkuvuudesta on erittäin aiheellinen.

Työssä tehtyjen selvitysten perusteella verkostoautomaatiojärjestelmien tietoturvan taso vaihteli välttävän ja hyvän välillä. Tietoturvan kirjo arvioitiin laajaksi ja lähes koko perinteinen kouluarvosana-asteikko on käytössä. Toisaalta eri yritykset ovat asettaneet itselleen erilaisia tietoturvan tavoitetasoja. Ongelmia on sekä vanhoissa järjestelmissä että uusissa IP-pohjaisissa ratkaisuissa. Verkostoautomaatiojärjestelmien tietoturvan kehittämisestä tekee haastavan järjestelmien hidas uusiutumisväli, tyypillisesti yli kymmenen vuotta. Oma haasteensa verkostoautomaatiojärjestelmien tietoturvalle luo lisääntyvä älykkäiden laitteiden määrä jakeluverkossa ja sovellusten monimutkaistuminen samoin kuin yleistynyt etätyöskentely ja järjestelmien ylläpito etäyhteyksin julkisen internet-verkon yli.

Raporttiin on koottu luettelo verkostoautomaatiojärjestelmien tietoturvaa parantavista toimenpiteistä. Nämä on ryhmitelty välittömiin, lähiajan ja pitkän ajan toimenpiteisiin. Verkkoyhtiöiden suositellaan tekevän esitetyt välittömät toimenpiteet viivytyksettä. Muille toimenpiteille on syytä samalla laatia toteutusaikataulu.

Verkostoautomaation tietoturva on tiukasta rajauksestaan huolimatta laaja ja osin poikkiteknologinen kokonaisuus. Tietotekniikkaa, tietoliikennettä sekä niiden tieto- ja kyberturvallisuutta käsitteleviä standardeja, suosituksia, raportteja, ohjeistusta ja parhaita käytäntöjä on julkaistu valtava määrä. Verkostoautomaatiojärjestelmien kannalta merkittävää standardointityötä on meneillään useilla tahoilla, muun muassa IEC:n toimesta. Euroopan unionin lainsäädäntötyö tietosuojasääntelyn uudistamiseksi tullee osaltaan vaikuttamaan myös sähköyhtiöiden toimintaan. Verkkoyhtiöiden koko, liiketoimintojen laajuus ja luonne, omistuspohja ja kumppaniverkostot vaihtelevat merkittävästi ja yhtä, kaikille sopivaa malliratkaisua on vaikeaa kiteyttää. Hopealuotia ei ole vielä löydetty.

Verkkoyhtiöt joutuvatkin tietoturvaa kehittäessään tekemään yhtiökohtaisia valintoja myös raporttiin sisällytettyjen ja lähdeaineistoissa määriteltyjen hyvien käytäntöjen osalta.

Tietoturvan teknisiä yksityiskohtia ja laitetason ratkaisuja ei raportin puitteissa ole mahdollista esittää niiden laajuuden ja osin luottamuksellisuuden takia. Käytettävä tietoverkko-arkkitehtuuri ja toimintamallit ovat tietoturvan rakentamisen kannalta keskeisessä asemassa, joten niihin on syytä ensin keskittyä.

Energia- ja sähköverkkoyhtiöille ehdotetaan kattavaa turvallisuuspolitiikan määrittelyä yhtenä erityisenä tarkastelualueena tieto- ja kyberturvallisuus. Työ on luontevaa tehdä osana muuta jatkuvuussuunnittelua ja riskien hallintaa. Tietoturva tulee samalla integroiduksi osaksi johtamista, toimintaprosesseja ja toiminnan seurantaa. Jatkuvuussuunnittelussa keskeisessä osassa on järjestelmien käytettävyys ja palauttaminen kriisi- ja häiriötilanteista. Osassa verkkoyhtiöitä työtä on pitkälle tehty ja asiat hyvässä kunnossa, mutta kaikille riittää vielä tekemistä.

Henkilöstön turvallisuusselvityksiä teetetään sähköverkkoyhtiöissä vähänlaisesti ja niiden käyttöä voisi lisätä rekrytoitaessa avainhenkilöitä kriittisten järjestelmien suunnittelu-, operointi- ja ylläpitotehtäviin.

Sähköyhtiöissä käytetään sangen vähän ulkopuolisia asiantuntijoita arvioimaan ja auditoimaan järjestelmiä ja niiden tietoturvan tasoa. Ammattimaisesti tehty nykytilan tunnistaminen on edellytys haluttuun ja selkeästi määriteltyyn tavoitetilaan pääsemiseksi. Myös järjestelmien testaukseen ja valvontaan on tarjolla toimittajien, kaupallisten palvelutuottajien sekä viranomaisten palveluja. Hyvänä esimerkkinä ulkoisesta havainnointipalvelusta on Viestintäviraston HAVARO-palvelu, joka on tarjolla huoltovarmuuskriittisille yrityksille.

Tietoturva liittyy tietojärjestelmään kaikkiin sen elinkaaren vaiheisiin. Esisuunnittelussa määritellään liiketoimintalähtöisesti järjestelmän kriittisyys ja sen edellyttämä tietoturvan taso. Hankintavaiheessa verkkoyhtiö määrittelee tarjouspyynnössään vaatimukset tietoturvalle, toimittaja kuvaa tarjouksessaan vaatimukset täyttävän ratkaisun ja sopimukseen kirjataan järjestelmän mukana toimitettava tietoturvaratkaisu. Toimitusprojektin aikana toimittaja varmistaa tietoturvaratkaisun vaatimusten mukaisuuden osana omaa laadunvarmistustaan ja tilaaja tarkastaa tietoturvan vastaanottotarkastuksessa. Järjestelmän käytön aikana tietoturvaa pitää päivittää uusien uhkien ja muuttuvan järjestelmäarkkitehtuurin myötä. Päivitykset pitää tehdä rivakasti, jottei olemassa olevia haavoittuvuuksia ehditä käyttää hyväksi. On myös oleellista, ettei saavutettua tietoturvaa heikennetä minkään uuden ohjelmistoversion tai laitteiden päivityksen yhteydessä. Käytön aikaiset ylläpidon menettelytavat pitää huomioida ylläpitosopimuksissa. Järjestelmässä olevat tiedot pitää käsitellä asianmukaisesti luottamuksellisuuden varmistamiseksi, kun siitä sammutetaan valot elinkaaren lopussa.

Maamme sähköverkkoyhtiöiden määrä on suuri yleistä televerkkoa omistavien teleyhtiöiden määrään verrattuna. Kooltaan suuremmilla yhtiöillä tai yhteenliittymillä on selkeästi laajempi osaaminen ja resurssit panostaa toiminnan kehittämiseen, muun muassa tietotekniikan ja sen tietoturvan kehittämiseen. Sähköverkkoyhtiöiden tulisikin yhdistää voimiaan vaativissa verkostoautomaatiohankkeissa nykyistä enemmän.

9 LÄHDELUETTELO

/1/ IEC 60870-5 & -6 Communication Protocol Standards

/2/ IEC 61850. Series of detailed standard for the design of electrical substation automation

/3/ IEC 62351. Security Standard for Power System Information Infrastructure

/4/ IEEE 1711-2010 Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links

/5/ IEEE 1686, IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities, IEEE 2007

/6/ IEC TC57 WG15 White Paper IEC62351-2012

/7/ NIST (National Institute of Standards and Technology), Special Publication 800-82 Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security, Revision 1, NIST Toukokuu 2013, http://csrc.nist.gov/publications/PubsSPs.html

/8/ VTT:n tiedote 2545, 2010, TITAN-käsikirja, http://www.vtt.fi/inf/pdf/tiedotteet/2010/T2545.pdf

/9/ IEC TC65, Tom Phinneyn esitys ,IEC 62443: Industrial Network and System Security

/10/ North American Electric Reliability Corporation, NERC-CIP standardit CIP-001… CIP-011

/11/ CPNI (Centre for the Protection of National Infrastructure), Good practice guide Process control and SCADA security, Verkkojulkaisu, http://www.cpni.gov.uk/

/12/ ISO/IEC 27002:2005, Information Technology -- Security techniques -- Code of practice for Information Security Management

/13/ ISO/IEC 27005:2011, Information technology -- Security techniques -- Information security risk management

/14/ IEC 61968. Series of detailed standards to define information exchanges between electrical distribution systems, IEC 2003

/15/ CIGRE, WG D2.22, 2010, TB 419 Treatment of Information Security for EPU (Electrical Power Utility)

/16/ CIGRE, WGD2.23, 2011, The use of Ethernet Technology in the Power Utility Environment

/17/ CIGRE, D2/B3/C2.01, 2007, 317 Security for Information Systems and Intranets in Electric Power Systems

/18/ CIGRE, Colloquium Reports:

1. D2-02 B08 Information Security applied to the network access, Argentina 2011;
2. B5-105 IT Security for Utility Automation Systems, Paris 2004;
3. D2-02 B04 Communication Architecture for IP-based Substation Applications, Argentina 2011
4. D2-02 B08 Information Security applied to the network access: a methodological approach, Argentina 2011

5. D2-02 B09 Graded approach to cyber security for EPUs: Clarifying the security levels and zones concepts, Argentina 2011
6. D2-02 B10 Modelling of cyber attacks for assessing smart grid security, Argentina 2011
7. D2-02 B11 Cyber Security requirements and related standards for Substation Automation Systems, Argentina 2011
8. D2-02 B12 Privileged User Management System Development, Argentina 2011

/19/ Information security in smart grid demonstration environment; Kim Paananen, Diplomityö Tampereen teknillinen yliopisto, 2011

/20/ Sovellutusten sallimislistaus teollisuusautomaatiojärjestelmissä; Pia Olli, Diplomityö Oulun yliopisto, 2013

/21/ Viestintäviraston CERT FI-palvelu, www.cert.fi

/22/ Yhdysvaltalainen automaatiojärjestelmien CERT-palvelu, http://ics-cert.us-cert.gov

/23/ Erilaisia testaus- yms. työkaluja http://sectools.org

/24/ Viestintäviraston määräys 54 A/2012, https://www.viestintavirasto.fi/ohjausjavalvonta/lainsaadanto/maaraykset/maarays54viestintaverkkojenja-palvelujenvarmistamisesta.html

/25/ Viestintäviraston määräys 43 D/2010 M, Televerkkojen sähköinen suojaaminen https://www.viestintavirasto.fi/ohjausjavalvonta/lainsaadanto/maaraykset/maarays43viestintaverkonsahkoisestasuojaamisesta.html

10 LYHENTEITÄ JA TERMEJÄ

Lyhenne/Termi		Selitys
AES	Advanced Encryption Standard	Salausalgoritmistandardi
AMR	Automated Meter Reading	Automaattinen energiamittareiden etäluenta
ANSI	American National Standards Institute	Yhdysvaltalainen standadointijärjestö
Bottiverkko		Verkkorikollisten haltuunsa ottamia tietokoneita, jotka voidaan etäkäskyllä aktivoida tekemään rikollisten määräämiä toimenpiteitä
CERT	Computer Emergency Readiness Team	Tietoturvapalvelu(keskus), Suomessa CERT-FI Viestintäviraston yhteydessä
CIGRE	International Council on Large Electric Systems	Kansainvälinen sähköyhtiöalan järjestö
CIP	Critical Infrastructure Protection	Kriittisen infrastruktuurin suojaaminen
CIRED	International Conference on Electrical Distribution	Kansainvälinen järjestö sähkönjakelun toiminnan ja tekniikan kehittämiseksi
CIS	Customer Information System	Asiakastietojärjestelmä
CoS	Class of Service	Palvelutasoluokka
CWDM	Coarse Wavelength Division Multiplexing	Karkea optinen aallonpituuskanavointi
DMZ	De-militarized Zone	Demilitarisoitu vyöhyke
DNP3	Distributed Network Protocol	Käytönvalvontajärjestelmissä käytetty tiedonsiirtomenettely
DNS	Domain Name Server	Nimipalvelin, joka muuttaa verkkotunnuksia IP-osoitteiksi
DoS	Denial-of-Service	Palvelunestohyökkäys
ELAN		Ylläpitotyön lähiverkko
EMS	Energy Management System	Energian hallintajärjestelmä
EoS	Ethernet over SDH	Siirtotekniikka, jolla L2-tason Ethernet-yhteys siiretään SDH-siirtoverkon yli
Ethernet		IEEE 802-standardiperheen määrittelemä lähiverkoissa (LAN) käytettävä tiedonsiirtomenettely
FTP	File Transfer Protocol	Tiedonsiirtomenettely
FW	Firewall	Palomuuri
GCHQ	Government Communications HeadQuarters	Brittiläinen signaalitiedusteluorganisaatio
GE	Gigabit Ethernet	“gigaethernet”
GOOSE	Generic Object-Oriented Substation Event	Sähköasematapahtuma
GUI	Graphic User Interface	Graafinen käyttöliittymä
HDLC	High-level Data Link Control	Synkroninen siirtokerroksen tiedonsiirtomenettely

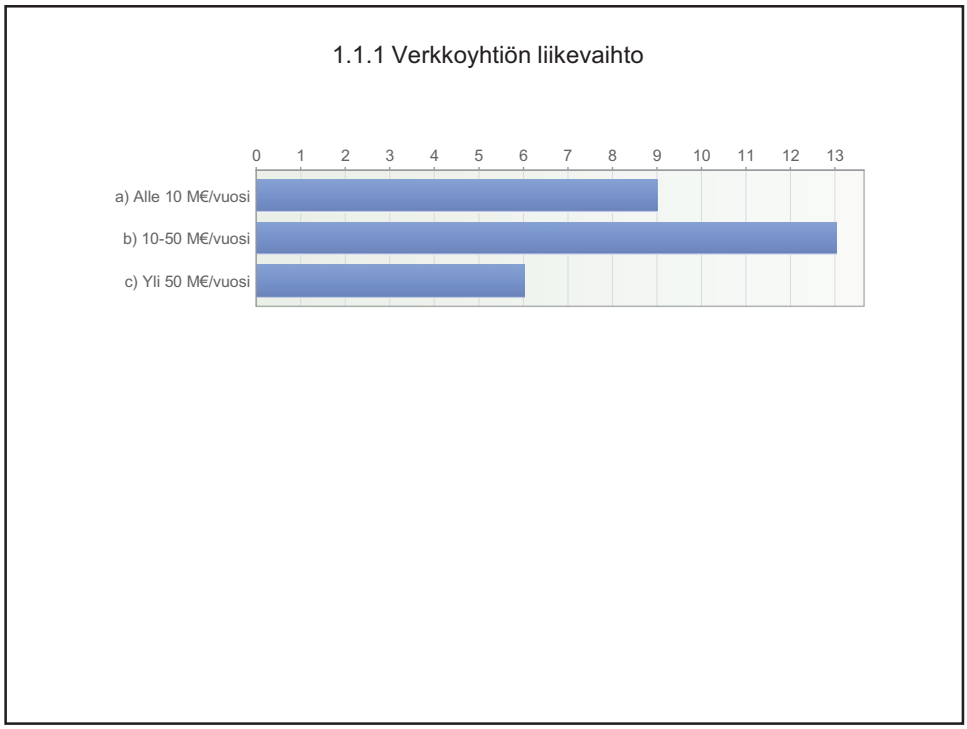
Lyhenne/Termi		Selitys
Help Desk/Service Desk		Palvelukeskus, joka vastaanottaa vikailmoituksia ja palvelupyyntöjä ja käynnistää toimenpiteitä
HMI	Human-Machine Interface	Henkilöiden käyttämä järjestelmän käyttöliittymä
HTML	HyperText Markup Language	Kuvauskieli esimerkiksi internetsivuille
HTTPS	Hyper Text Transfer Protocol Secure	Suojattu tiedonsiirtomenettely
ICCP	Inter-Control Center Communications Protocol	Standardin IEC 60870-6 mukainen tiedonsiirtoprotokolla tietojärjestelmien välillä.
ICS	Industrial Control Systems	Teollisuusautomaatiojärjestelmä
ICT	Information and Communication Technology	Informaatio- ja tietoliikennetekniikka
IDS	Intrusion Detection System	Hyökkäyksen ja tunkeutumisen tunnistusjärjestelmä
IEC	International Electrotechnical Commission	Sähköalan standartointijärjestö
IEC 61850 protokolla		IEC:n määrittelemä Ethernet-pohjainen lähiverkkoprotokolla, joka on suunniteltu käytettäväksi erityisesti sähköasemaympäristössä
IED	Intelligent Electronic Device	Ohjelmoitava elektroninen laite
IEEE	Institute of Electrical and Electronic Engineers	Sähköalan standardointijärjestö
IETF	Internet Engineering Task Force	Internet-standardointijärjestö
IP	Internet Protocol	Pakettikytkentäinen tiedonsiirtoprotokolla
IP-päätelaite		IP-yhteyksien tuottamisessa käytettävä IP-pohjainen, normaalisti asiakkaan tiloissa sijaitsevat telepäätelaite (esim. hubi, kytkin, reititin)
IPS	Intrusion Protection System	Hyökkäyksen ja tunkeutumisen suojausjärjestelmä
IPSec	IP Security Architecture	Tiedonsiirron suojausmenettely
IP-verkko		IP-tiedonsiirtomenettelyä käyttävä verkko
ISA	International Society of Automation	Automaatioalan järjestö
ISO	International Organization for Standardization	Kansainvälinen standardointijärjestö
ISO OSI	Open Systems Interconnection Reference Model,	Kansainvälisen ISO-standardin mukainen tiedonsiirron referenssiviitekehys
IT	Information Technology	Informaatiotekniikka
ITU	International Telecommunication Union	Tietoliikennealan standartointijärjestö
LAN	Local Area Network (LAN)	Lähiverkko
LCAS	Link Capacity Adjustment	Tiedonsiirtomenettely SDH-verkoissa
MAC-osoite	Media Access Control-osoite	Verkkolaitteen ethernet-verkossa yksilöivä osoite

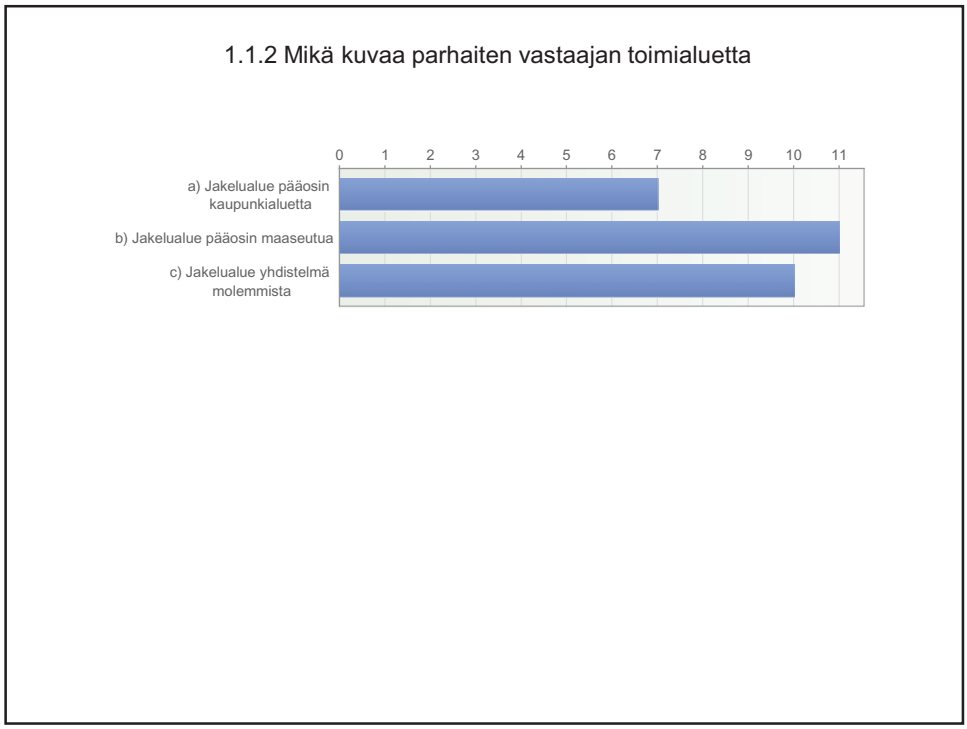
Lyhenne/Termi		Selitys
MDMS	Meter Data Management System	Mittaustietojen hallintajärjestelmä
MPLS	Multi Protocol Label Switching	Tiedonsiirtomenettely IP-verkoissa
MPLS-TP	MPLS Transport Profile	Siirtokerroksen tiedonsiirtomenettely
NASL	Nessus Attack Scripting Language	Ohjelmointikieli
NERC	North American Electric Reliability Corporation	Sähköalan järjestö (USA)
NG-SDH	Next Generation Synchronous Digital Hierarchy	Piirikytkentäinen synkroninen tiedonsiirtomenettely, voi siirtää myös pakettikytkentäistä liikennettä
NIST	National Institute of Standards and Technology	Standardointijärjestö
NMS	Network Management System	Tietoliikenneverkon hallintajärjestelmä
NSA	National Security Agency	Kansallinen turvallisuusvirasto (USA)
NTP	Network Time Protocol	Synkronointitiedonsiirtomenettely
ODF	Optical Distribution Frame	Optinen ristikytkentä
OS	Operating System	Käyttöjärjestelmä
OSI	Open Systems Interconnection	Tiedonsiirtostandardiperhe
PDH	Plesiochronous Digital Hierarchy	Plesiokroninen digitaalinen piirikytkentäinen tiedonsiirtomenettely
PDH-telelaitteet		PDH-tekniikkaan perustuvia piirikytkentäisiä tiedonsiirtolaitteita, tyypillisesti optisia siirtolaitteita, radiolinkkejä, Cu-johtolaitteita, kanavointi- ja ristikytkentälaitteita sekä tietoliikennesovittimia
PKI	Public Key Infrastructure	Salausmenetelmä
PLC	Programmable Logic Controller	Ohjelmoitava logiikka
QoS	Quality of Service	Palvelutaso
RAS	Remote Access Server	Etäkäyttöpalvelin
RBAC	Role Based Access Control	Roolipohjainen käyttöoikeuksien hallinta
RSA	Rivest, Shamir, Adelman; (RSA Server)	Julkisen avaimen salausalgoritmi, EMC Corporationin kaupallinen tuote
RTU	Remote Terminal Unit	Käytönvalvontajärjestelmän ala-asema
SCADA	Supervisory Control and Data Acquisition	Käytönvalvontajärjestelmä
SDH	Synchronous Digital Hierarchy	Synkroninen ITU:n määrittelemä digitaalinen piirikytkentäinen tiedonsiirtomenettely
SDH-telepäätelaitteet		SDH-tekniikkaan perustuvia optisia siirtolaitteita tai radiolinkkejä sekä kanavointi- ja ristikytkentälaitteita, joita käytetään laajasti erilaisissa tietoliikenneverkoissa
SFP	Small Form-factor Pluggable,	Kuituoptinen liitäntäyksikkö
SFTP	Secure File Transfer Protocol	Suojattu tiedonsiirtomenettely

Lyhenne/Termi		Selitys
Siirtoyhteys		SDH-, PDH- tai IP-pohjaisilla telelaitteilla toteutettu ISO-OSI tason 2 mukainen tietoliikenneyhteys
SLA	Service Level Agreement	Palvelutasosopimus
SLAN	Substation Local Area Network	Sähköaseman lähiverkko, jota käytetään sähköverkon suojaukseen, ohjaukseen ja valvontaan
SNMP	Simple Network Management Protocol	Verkonhallinnan tiedonsiirtomenettely
SNTP	Simple Network Time Protocol	Tiedonsiirtomenettely
SOA	Service-Oriented Architecture	Palvelukeskeinen tietoverkkoarkkitehtuuri
SQL	Structured Query Language	Standardoitu kyselykieli, jolla voidaan tehdä hakuja tietokantoihin
SSH	Secure Shell	Suojattu tiedonsiirtomenettely
SSO	Single Sign-On	Kertakirjautuminen on menetelmä, jossa pääsy useisiin palveluihin toteutetaan yhdellä käyttäjän autentikoinnilla.
TC57		IEC:n työryhmä, joka laatii käytönvalvonnan ja sen tietoliikenteen standardeja
TC65		IEC:n työryhmä, joka laatii standardeja teollisuusprosessien mittauksiin ja ohjauksiin
TCP	Transport Control Protocol	Tiedonsiirtomenettely
UDP	User Datagram Protocol	Tiedonsiirtomenettely, joka ei varmista paketin perillemenoa
URL	Uniform Resource Locator	Internetosoite
USB	Universal Serial Bus	Sarjaliikenneväylämäärittely
WAN	Wide Area Network	Laajaverkko
Varusohjelmisto		Tietokoneen tai tietoliikennelaitteen käyttöjärjestelmä ajureineen
WDM	Wavelength Division Multiplexing	Optinen aallonpituuskanavointi
Whitelisting		Toiminto, jolla hallitaan sallittuja IP-osoitteita, sovelluksia tai sähköpostiosoitteita
VLAN	Virtual Local Area Network	Loogisesti erotettu lähiverkon osa
WIMAX		Langaton pakettikytkentäinen tiedonsiirtotekniikka
WLAN	Wireless Local Area Network	Langaton lähiverkko
VPN	Virtual Private Network	Loogisesti erotettu suojattu verkko-osa
xDSL	Digital Subscriber Line	Digitaalinen siirtoyhteysmenettelyjen perhe normaalissa tilaajapuhelinjohdossa
XML	eXtensible Markup Language	Standardoitu merkintäkieli

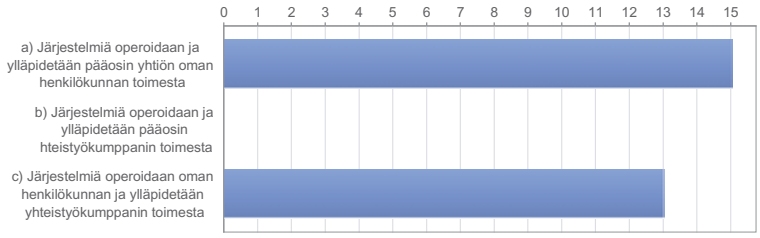
LIITE 1 Nettikyselyn tulokset

Vaaka-asteikko: Kysymykseen vastanneiden määrä/kpl

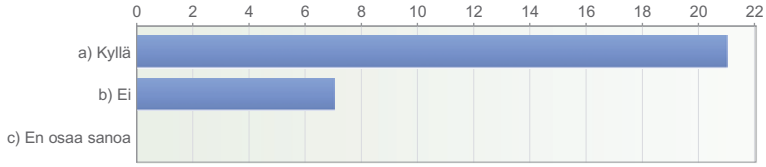




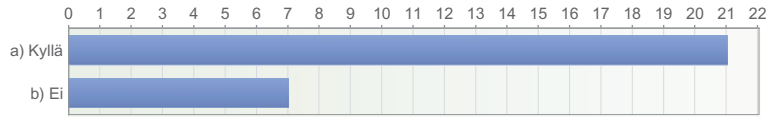
1.1.3 Sähköverkon verkostoautomaatio- ja käytönvalvontajärjestelmien operoinnin ja ylläpidon järjestelyt



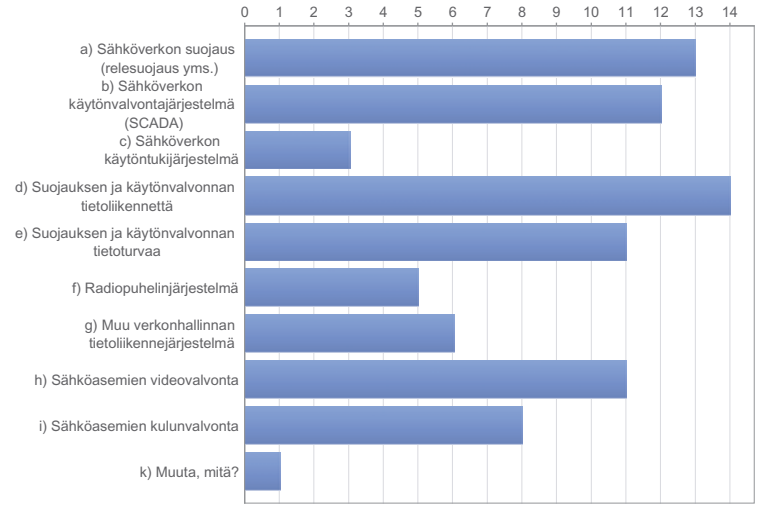
1.1.4 Onko yhtiön tai konsernin palveluksessa sähköverkon käytönvalvonta- ja suojausjärjestelmien sekä niiden tietoliikenteen ja tietoturvan määrittelyyn ja ylläpitoon perehtynyt asiantuntija/asiantuntijoita?



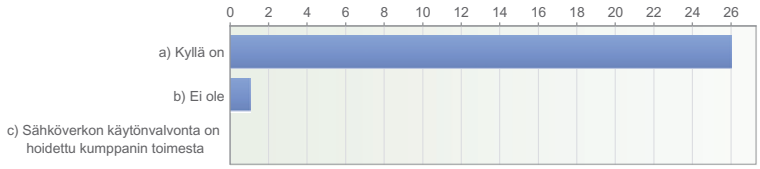
1.1.5 Oletteko uusimassa tai merkittävästi kehittämässä yhtiönne verkostoautomaatio- ja käytönvalvontajärjestelmiä tai niitä palvelevia tietoliikennejärjestelmiä/-palveluita tai tietoturvaa 1-3 vuoden sisällä?



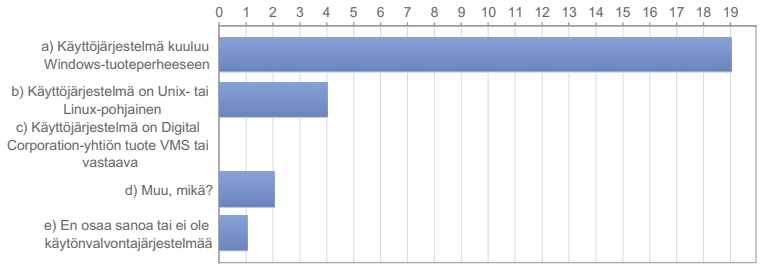
1.1.6 Mikäli vastauksenne edelliseen kysymykseen oli kyllä, niin mitä seuraavista järjestelmistä/palveluista tulette uusimaan tai merkittävästi kehittämään? Merkitse kaikki, joita aiotte kehittää.



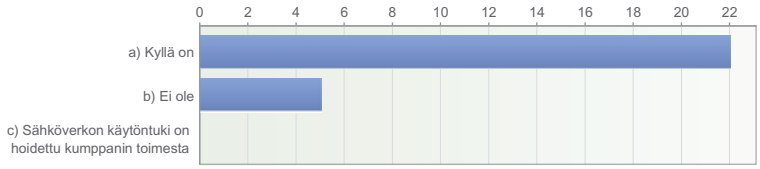
2.1.1 Onko yhtiössänne käytönvalvontajärjestelmä (SCADA)?



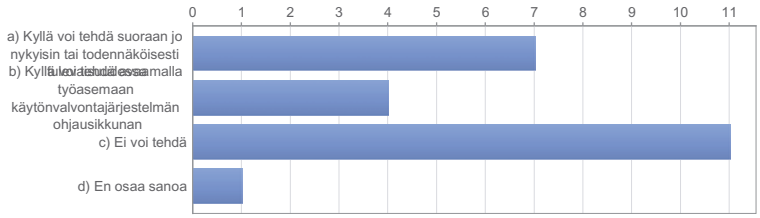
2.1.2 Käytönvalvontajärjestelmän käyttöjärjestelmän (operating system) tyyppi?



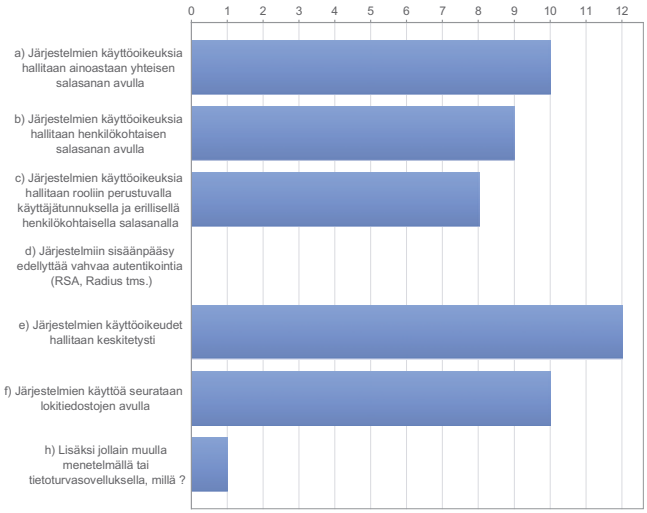
2.1.3 Onko yhtiössänne käytöntukijärjestelmä?



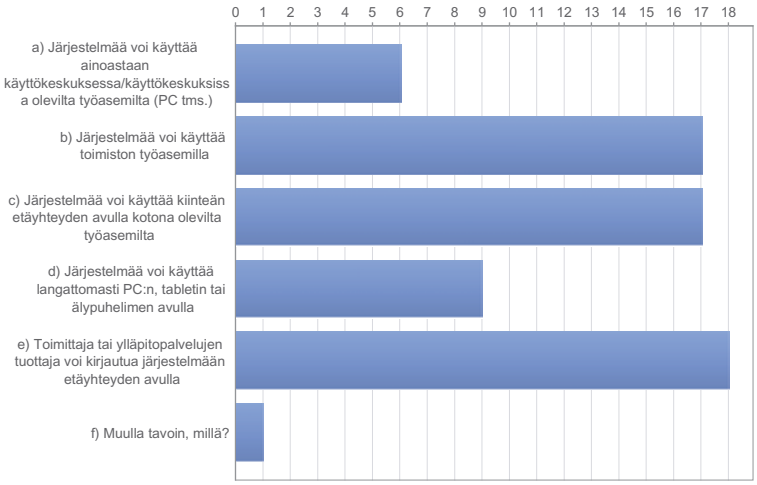
2.1.4 Mikäli käytössänne on käytöntukijärjestelmä, niin voiko sillä tehdä sähköverkon ohjauksia?



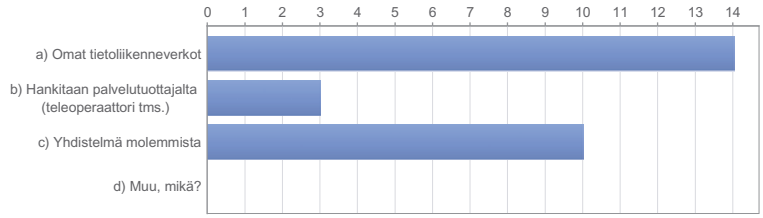
2.1.5 Mikä seuraavista vaihtoehdoista kuvaavat sähköverkon käytönvalvonta järjestelmien käyttöoikeuksien hallintaa ja käytön seurantaa (voi merkitä useita kohtia)?



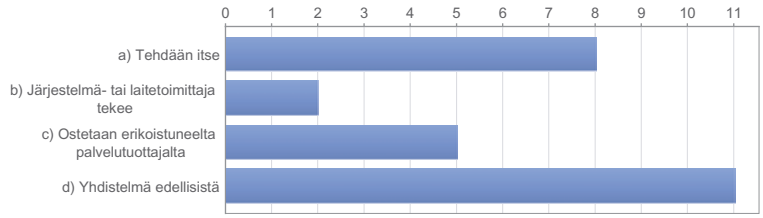
2.1.6 Mitkä seuraavista kuvaavat yrityksenne sähköverkon käytönvalvontajärjestelmän käyttöä ja kytkeytymistapoja? Rastita kaikki kohdat, jotka kuvaavat toimintaa.



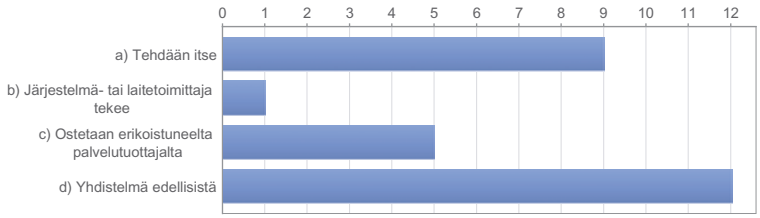
3.1.1 Sähköverkon käytönvalvonnan ja suojauksen tietoliikennepalvelujen toteutustapa?



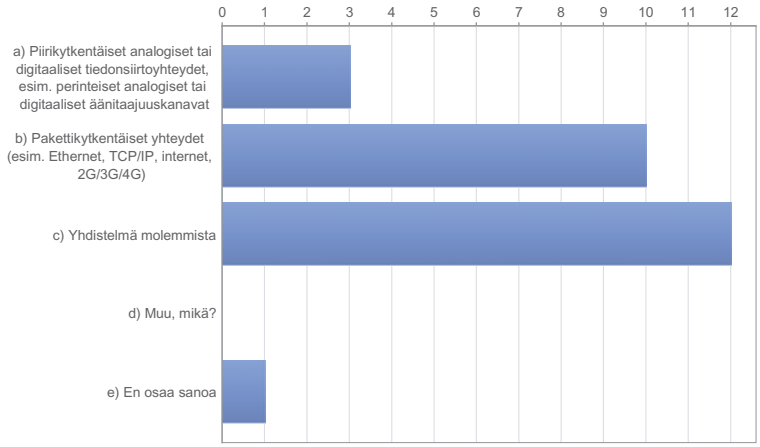
3.1.2 Tietoliikenneverkon tai -palvelujen suunnittelu ja rakentaminen pääsääntöisesti



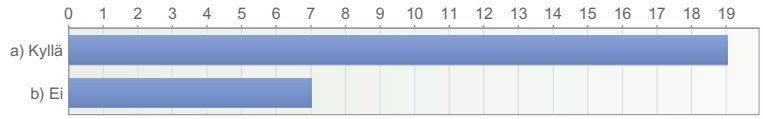
3.1.3 Tietoliikenneverkon operointi, vikavalvonta ja kunnossapito pääsääntöisesti



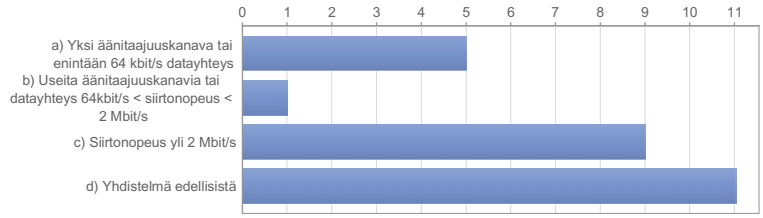
3.2.1 Verkostoautomaatiojärjestelmien tietoliikenneyhteyksien pääsääntöinen tyyppi



3.2.2 Ovatko verkostoautomaatiojärjestelmien tietoliikenneyhteydet pääsääntöisesti varmennettuja (kahdennettuja)?

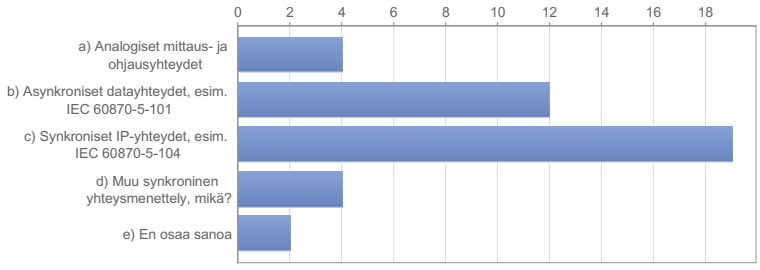


3.2.3 Tyypillinen yhteyden tiedonsiirtonopeus asemaa kohden

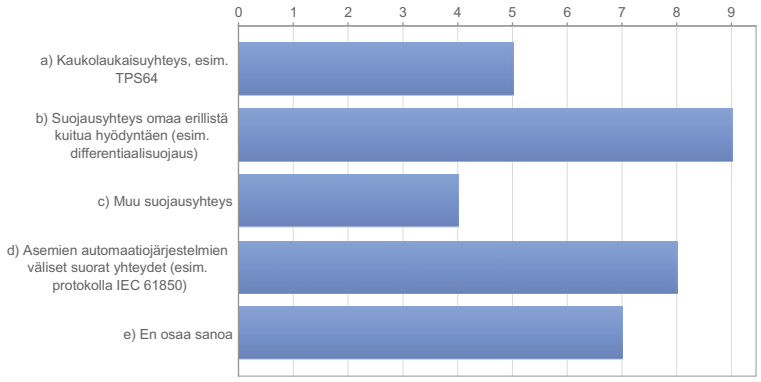


3.2.4 Tärkeysluokittele asemayhteyksien toteutustavat eri siirtomedioita käyttäen arvioimalla esim. kunkin siirtomedian määrällistä osuutta ja merkitystä kaikista asemayhteyksistä, tärkeysluokat asteikolla 1 -10: 10= tärkein, 1= vähiten tärkeä. Siirtomediakohdat, jotka eivät ole käytössä tai joiden tärkeys marginaalinen jätetään tyhjiksi.

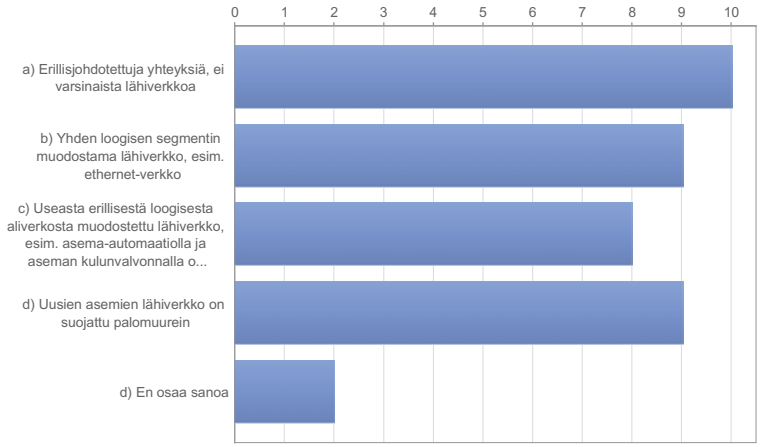
3.2.6 Käytönvalvonnan keskusaseman ja ala-asemien välisten yhteyksien tiedonsiirtomenettely (protokolla). Merkitse käytössä olevat tiedonsiirtomenettelyt



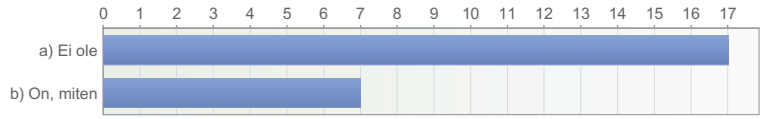
3.2.7 Asemien väliset suorat yhteydet. Merkitse käyttötarkoituksen mukaan ne yhteystyypit, jotka ovat yhtiössänne käytössä asemien välisessä liikennöinnissä.



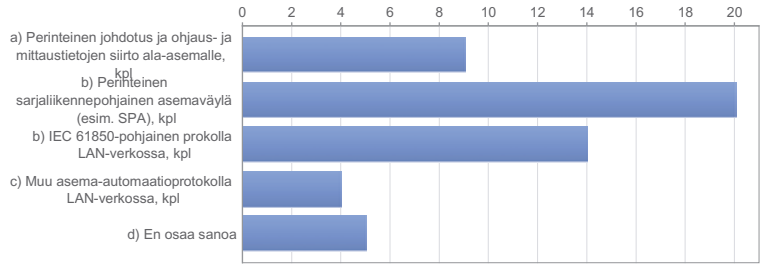
3.2.9 Asemien lähiverkon tyypillinen rakenne ja ominaisuudet. Merkitse soveltuvat



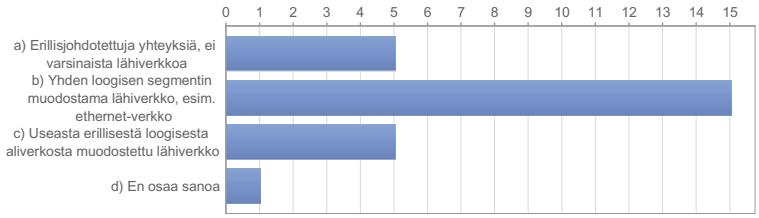
3.2.10 Onko käytönvalvonnan keskusaseman ja ala-asemien (RTU) väliset tietoliikenneyhteydet tai asemien väliset suojausyhteydet salattu?



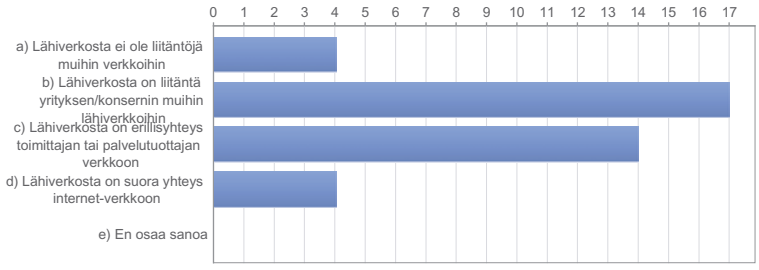
3.2.11 Asemien verkostoautomaatioväylän tiedonsiirtomenettely (protokolla). Arvio osuudet asemien määrän perusteella.



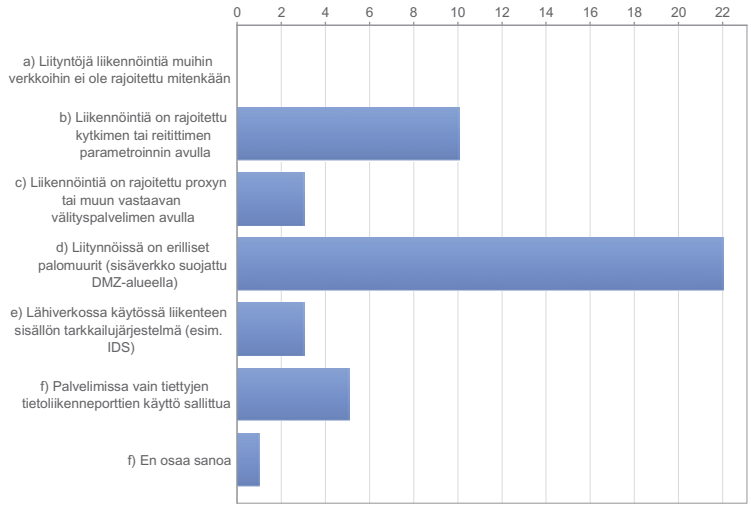
3.3.1 Käyttökeskuksen/käyttökeskusten (verkkovalvomo) lähiverkon rakenne ja ominaisuudet



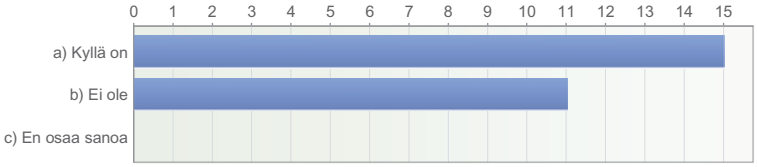
3.3.2 Käyttökeskuksen lähiverkon liitännät. Merkitse käytössä olevat liitännät



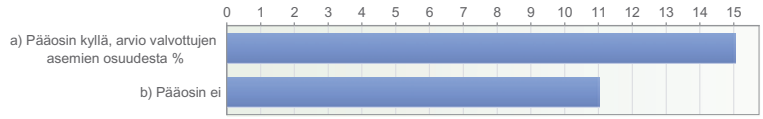
3.3.3 Käyttökeskuksen lähiverkon suojaaminen. Merkitse käytössä olevat tavat



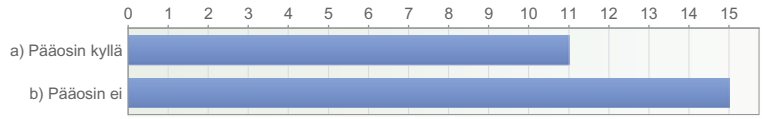
3.3.4 Onko käyttökeskuksen käytönvalvontajärjestelmästä suoria yhteyksiä internet-verkkoon tai toimittajan tai palveluntuottajan verkkoon?



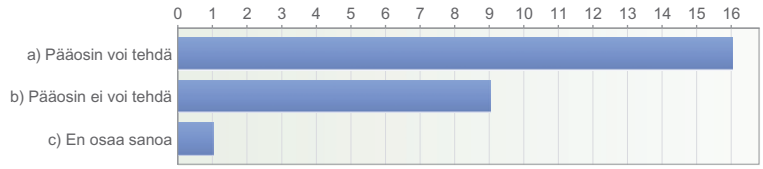
3.4.1 Onko sähkö-, muunto- kytkin- tai voimala-asemarakennusten kulun- ja/tai videovalvonta järjestetty etäyhteyksin?



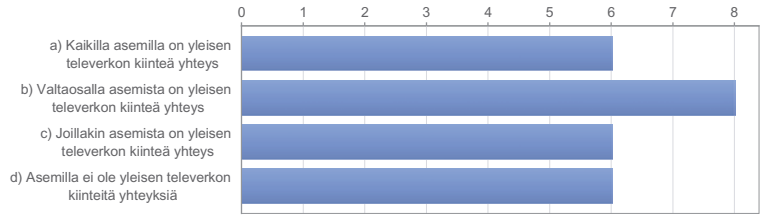
3.4.2 Onko asemille rakennettu työasemia varten kiinteitä etätyöskentely-yhteyksiä?



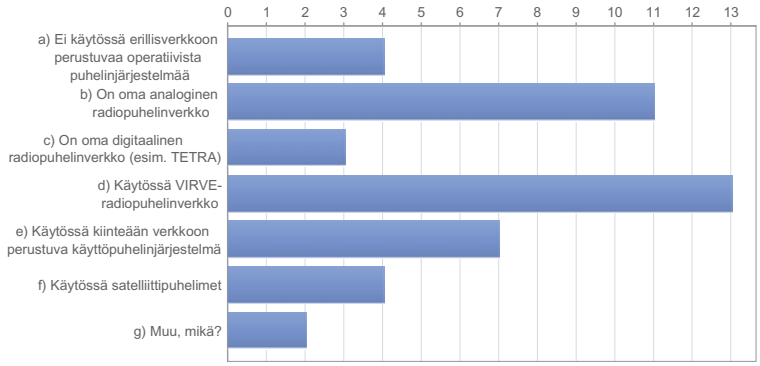
3.4.3 Voiko asemien suojareleiden tapahtumalokien lukemista tai suojausparametrien asettelua tehdä etäyhteyksien avulla?



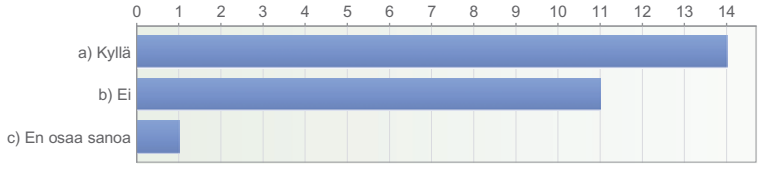
3.4.4 Arvio asemilla olevien yleisen televerkon kiinteiden yhteyksien (esim. puhelinliittymä tai laajakaistayhteys) yleisyydestä



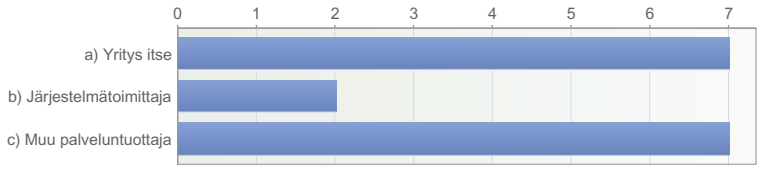
3.4.5 Onko verkkoyhtiöllä käytössä erillinen, käyttötoimintaa tukeva puhelinjärjestelmä? Merkitse kaikki käytössä olevat järjestelmät/verkot.



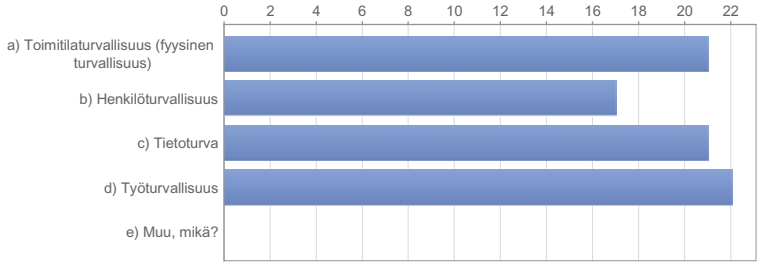
3.5.1 Hallitaanko omaa tietoliikenneverkkoa erillisellä hallintajärjestelmällä?



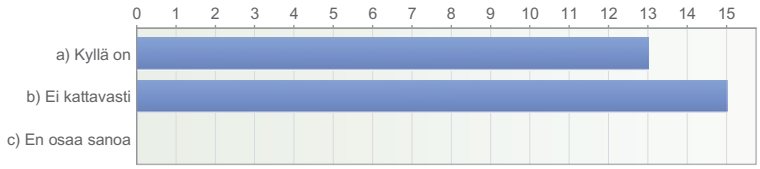
3.5.2 Jos vastaus edelliseen kysymykseen kyllä, niin kuka omistaa ja hallinnoi tietoliikenneverkon hallintajärjestelmän?



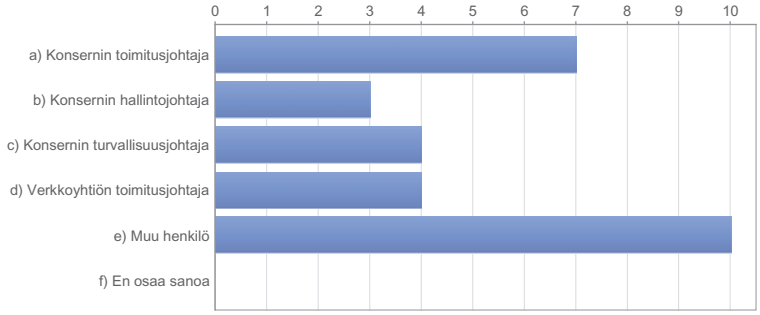
4.1.1 Onko verkkoyhtiössänne tai konsernissa määritelty turvallisuuspolitiikka? Myönteisessä tapauksessa merkitse turvallisuuspolitiikan kattamat osa-alueet:



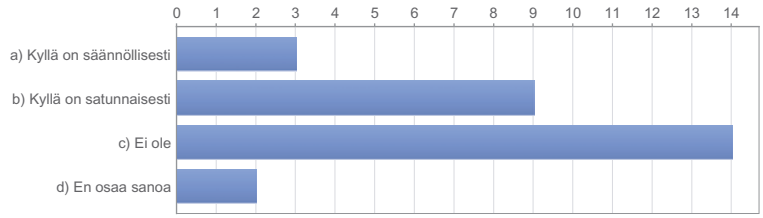
4.1.2 Onko yrityksessä/konsernissa laadittu kattavasti turvallisuusohjeistus em. osa-alueet käsittäen?



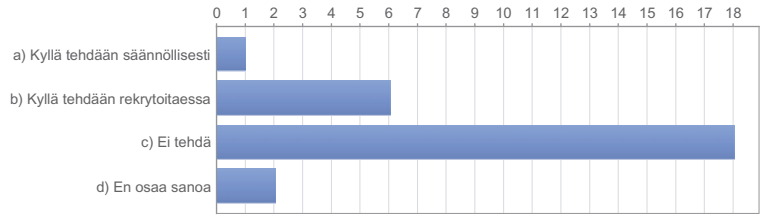
4.1.3 Kuka vastaa yrityksessänne/konsernissanne turvallisuuspolitiikan ohjeistuksen laadinnasta, toteutuksesta ja valvonnasta?



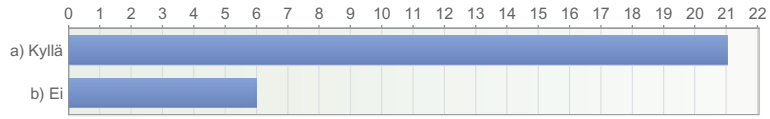
4.1.4 Onko yrityksenne/konserninne turvallisuusjärjestelmä auditoitu ulkopuolisen turvallisuusasiantuntijan toimesta?



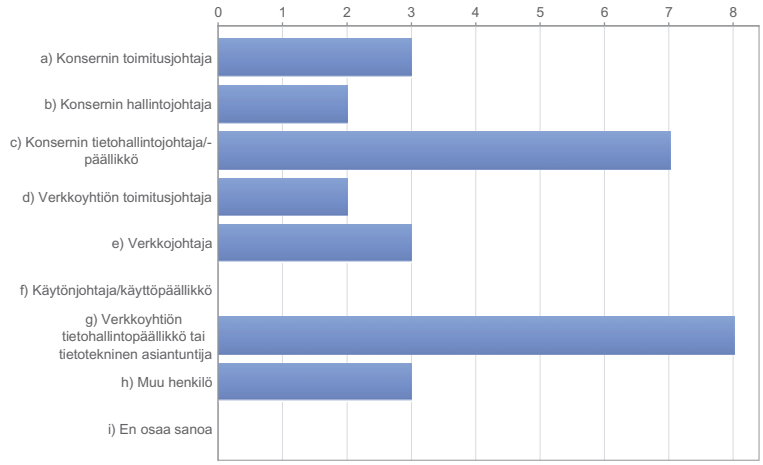
4.1.5 Tehdäänkö yrityksenne sähköverkon käytöstä, tietoliikenteestä ja tietotuvasta vastaaville henkilöille turvallisuus- ja taustaselvityksiä ?



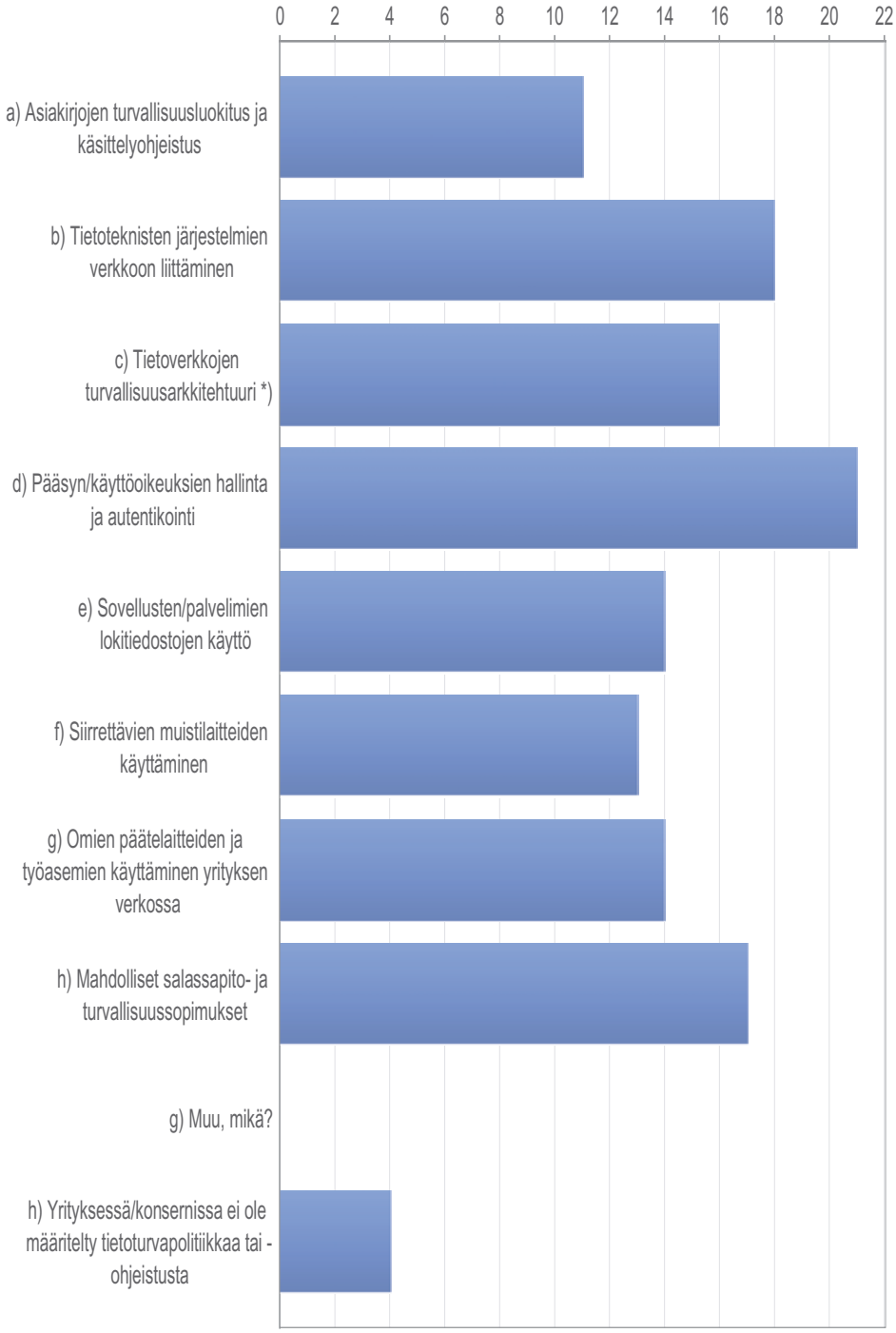
4.2.1 Onko konsernissanne keskitetty vastuu tietoturvasta?



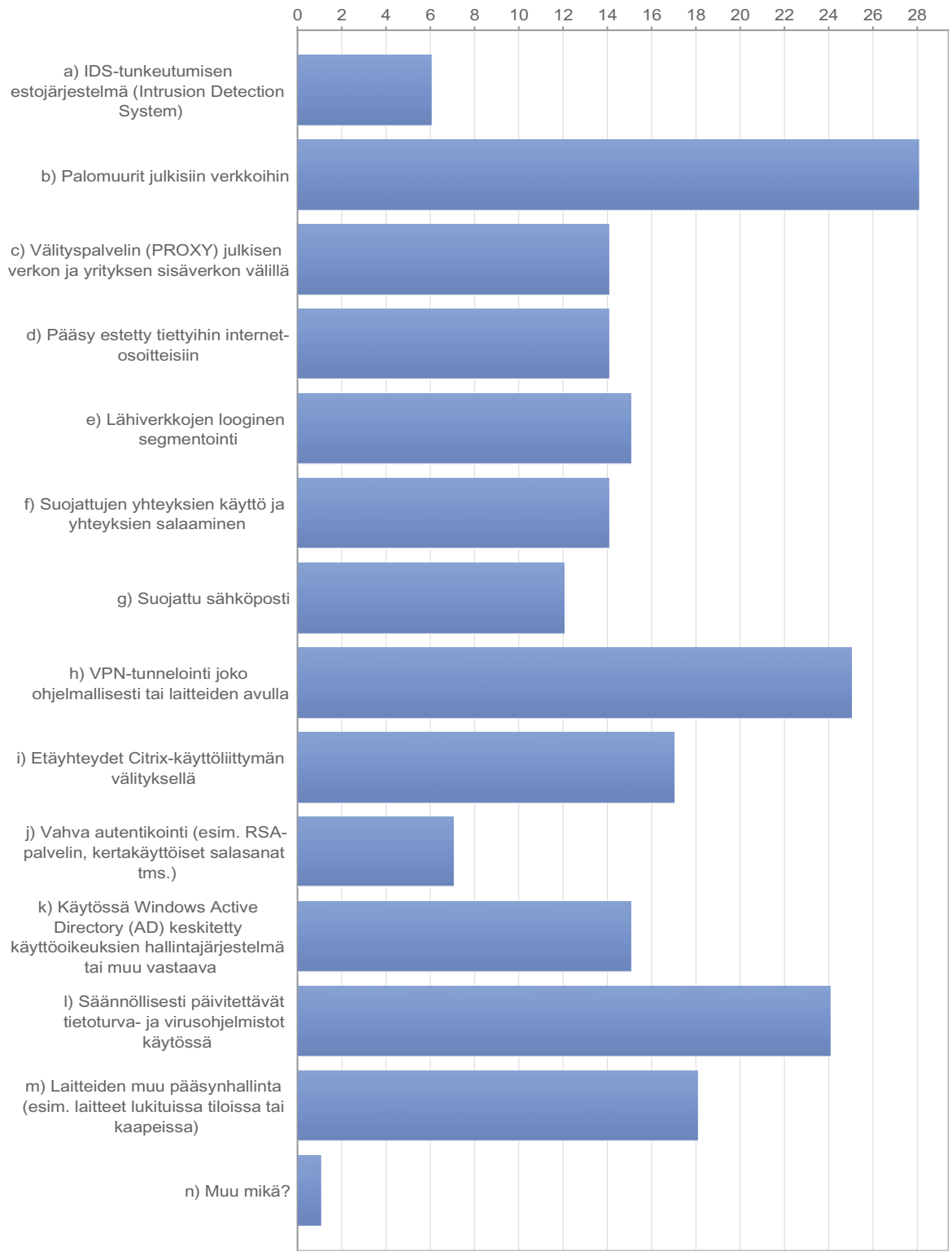
4.2.2 Kuka vastaa verkkoyhtiön tietoturvasta käytännössä?



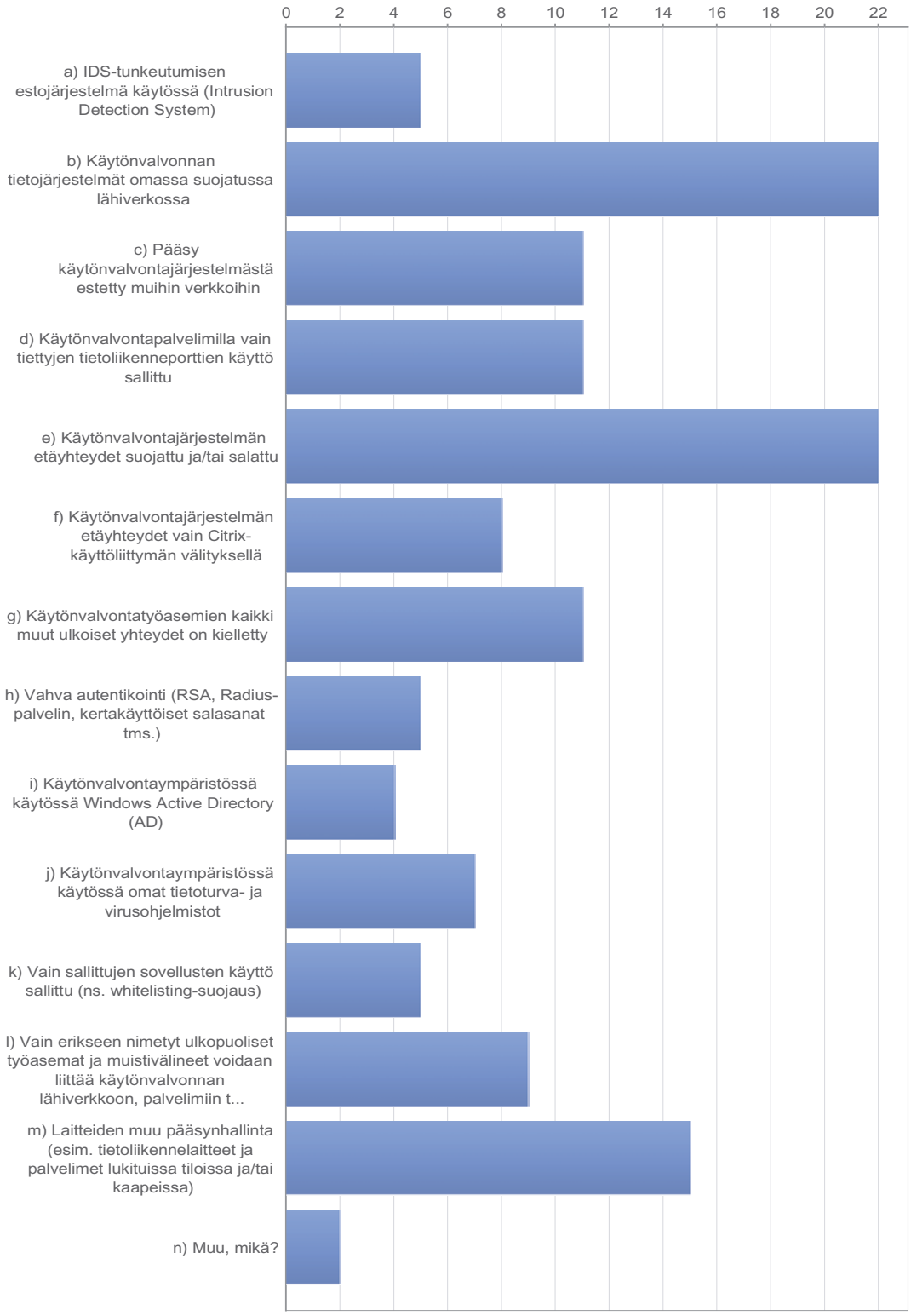
4.2.3 Merkitse konsernissanne/yrityksessänne käytössä olevan tietoturvapolitiikan ja tietoturvaohjeistuksen kattamat osa-alueet



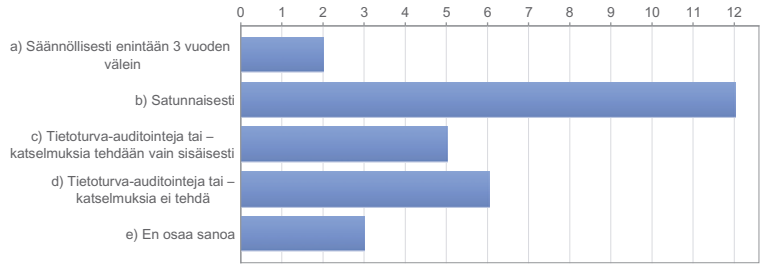
4.2.5 Millaisilla tekniikoilla konserninne/yrityksenne yritysverkot ja yritystietojärjestelmät ja tavanomainen yritystietoliikenne on suojattu? Merkitse kaikki käytössä olevat



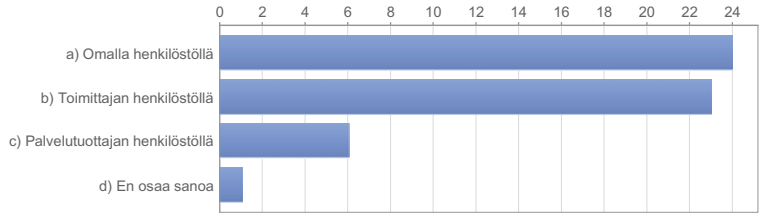
4.2.6 Millaisilla tekniikoilla verkkoyhtiönne käytönvalvonnan tietojärjestelmät (tietokannat ja sovellukset) on suojattu ulkopuolelta tulevilta uhilta? Merkitse kaikki soveltuvat kohdat



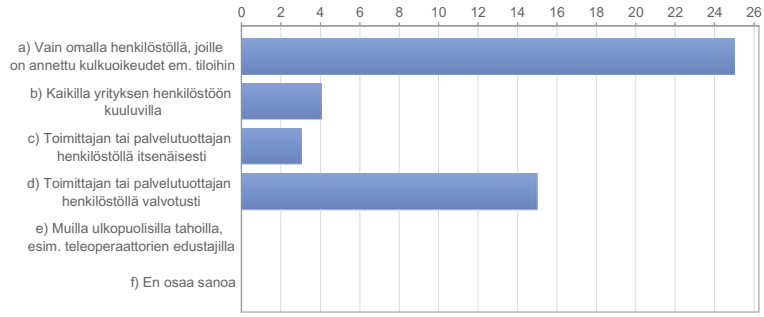
4.2.7 Miten usein yrityksessänne tehdään ulkopuolisen asiantuntijan toimesta tietoturva-auditointeja tai -katselmuksia?



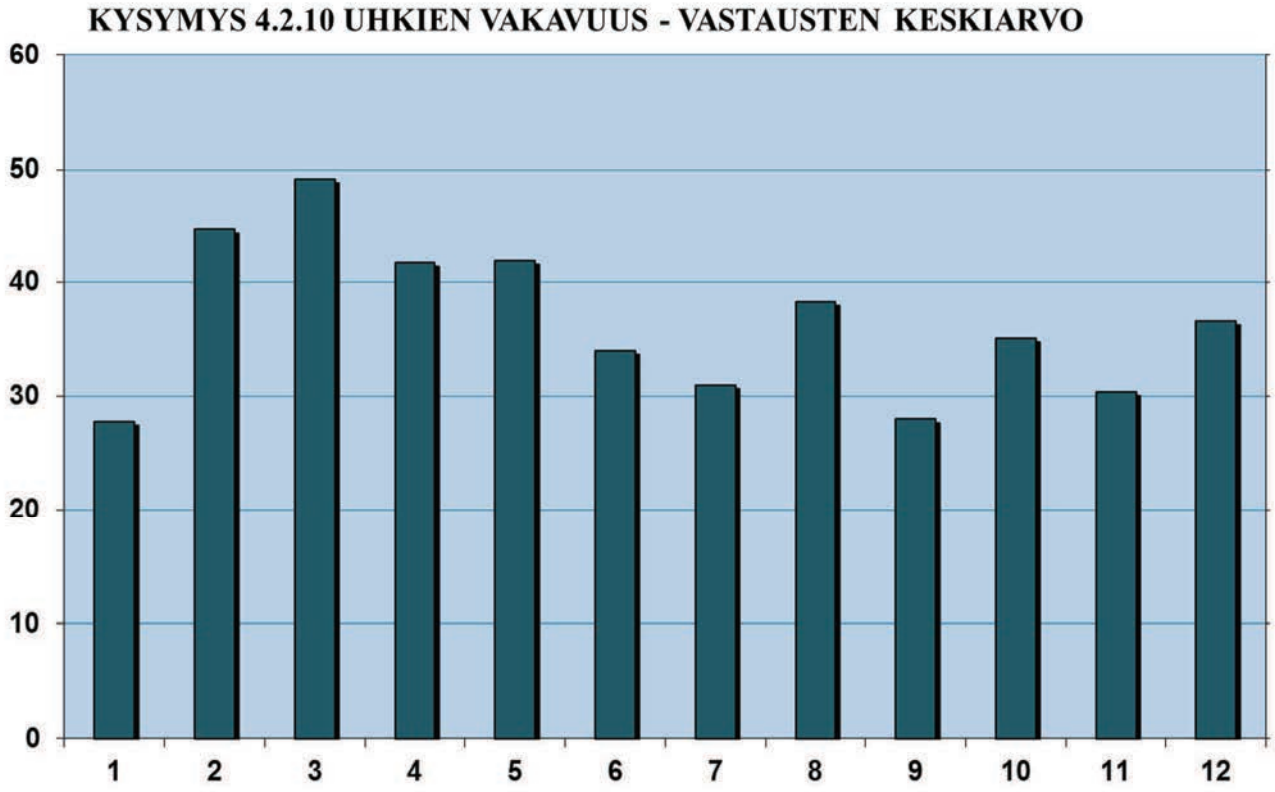
4.2.8 Kenellä on hallintayhteyksien/etäyhteyksien kautta pääsy verkostoautomaatiojärjestelmiin tai –laitteisiin tai verkostoautomaatiojärjestelmien tietoliikenneverkkoihin tai tietoliikennelaitteisiin? Merkitse soveltuvat kohdat



4.2.9 Kenellä on pääsy IT-, verkostoautomaatio- sekä tietoliikennelaitteita sisältäviin laitetiloihin? Merkitse soveltuvat kohdat



4.2.10 Arvioikaa verkkoyhtiönne toiminnan kannalta jäljempänä lueteltuja (tieto)turvallisuusuhkia vakavuusasteikolla 0-100 ottamalla huomioon uhan todennäköisyys ja uhan vaikuttavuus. Uhan vakavuus arvioidaan vaikuttavuuden (asteikolla 0-10) ja todennäköisyyden (asteikolla 0-10) tulona, suurempi luku on vaikuttavampi ja todennäköisempi. Hyvin vakavat uhat saavat arvon 100. Uhan vakavuus on 0, jos sen todennäköisyys on mitättömän pieni tai vaikuttavuus marginaalinen. Esimerkiksi sähköaseman tulipalon todennäköisyydeksi arvioidaan 1 ja vaikuttavuudeksi 8 (toiminnan kannalta). Tällöin sähköaseman tulipalouhan vakavuus on 8 (1 x 8 = 8).



KUVITELTU UHKA TAI HAAVOITTUVUUS

1 Palvelunestohyökkäys internet- tai extranet-sivuille
2 Tietomurto verkkoyhtiön tietojärjestelmiin (ei SCADA)
3 Tietomurto käytönvalvontajärjestelmään
4 Tietomurto sähköverkon suojauslaitteisiin (esim. suojarele)
5 Haittaohjelman tai haitakkeen pääsy verkkoyhtiön käyttökeskuksen sisäverkkoon riittämättömän tietoturvan takia
6 Oman henkilökunnan huolimaton tietovälineiden käyttö
7 Toimittajan tai palvelutuottajan huolimaton tietovälineiden käyttö
8 Asiakirjojen, salasanojen, avaimien tai muun luottamuksellisen materiaalin joutuminen asiattomien tahojen haltuun
9 Sähköpostin tai muun luottamuksellisen viestinnän päätyminen asiattomien haltuun
10 Sähkö- tai viestiasemien fyysisen suojaus ja valvonta puutteellista
11 Oman, toimittajan tai palvelutuottajan henkilökunnan palveluksessa olevan tai joskus olleen henkilön tahallisesti aiheuttama tietojärjestelmävaurio tai vikaohjaus
12 Kaikkien kysymyksien vastausten keskiarvo

4.2.11 Oma arvionne yhtiönne sähköverkon käytönhallinnan, sähköverkon suojauksen sekä niitä palvelevien tietoliikennejärjestelmien tietoturvan nykytilasta?