Säteilyturvakeskus

101/0002/2016
12.2.2021

Ohje YVL A.12, Ydinlaitoksen tietoturvallisuuden hallinta

1 Johdanto

Tietoturvallisuudella tarkoitetaan kokonaisuutta, jolla pyritään varmistamaan organisaation toiminta ja kehittämään organisaation toiminnan laatua. Tietoturvallisuutta ohjataan tietoturvallisuuden hallintajärjestelmän (ISMS) kautta, ja toimiakseen hallintajärjestelmän on syytä olla osa organisaation riskienhallintaa ja toimintajärjestelmää.

Tietoturvallisuuden hallintaa ja hallintajärjestelmää käsitellään ISO/IEC 27000 -standardisarjassa, joka on pyrittyhuomioimaan myös tämän ohjeen päivityksessä, erityisesti sanaston osalta. Ydinlaitosten erityisvaatimuksia on käsitelty ohjeen luvussa 4, jonka vaatimukset kohdistuvat turvallisuuden kannalta tärkeisiin järjestelmiin ja laitteisiin.

Tietoturvaa käsittelevää aineistoa ja sen toimittamista ei luokitella turvallisuusluokittelun mukaisesti, koska turvallisuusluokittelua ei tehdä tietoturvallisuuden kannalta. Esimerkiksiturvallisuusluokkaan EYT kuuluva laite voi olla tietoturvallisuuden kannalta merkityksellinen.

2 Soveltamisala

Ohjeessa YVL A.12 esitetään ydinlaitosten tietoturvallisuutta koskevat määräykset ja niiden soveltamista koskevat vaatimukset. Ohjetta sovelletaan ydinlaitoksiin niiden elinkaaren kaikissa vaiheissa. Ohje on tarkoitettu ydinlaitosten luvanhakijoille ja luvanhaltijoille, ja sitä sovelletaan organisaatioihin, joilla on vaikutusta ydinlaitosten tietoturvallisuuteen sekä muuhun ydinenergian käyttöön. Muita ydinenergian käyttäjiä ovat uraanin tuottajat, pienten ydinmateriaalimäärien ja luvanvaraisten tietoaineistojen haltijat sekä ydinmateriaalivalvontaan kuuluvat ydinpolttoainekierron tutkimustoimintaa toteuttavat tutkimuslaitokset. Yleisiä vaatimuksia ja STUKin suorittamaa valvontaa kuvataan myös A-sarjan YVL-ohjeissa sekä YVL-ohjeissa:

- B.1 Ydinvoimalaitoksen turvallisuussuunnittelu
- B.2 Ydinvoimalaitoksen järjestelmien, rakenteiden ja laitteiden luokittelu
- B.7 Varautuminen sisäisiin ja ulkoisiin uhkiin ydinlaitoksessa
- C.5 Ydinvoimalaitoksen valmiusjärjestelyt
- E.7 Ydinlaitoksen sähkö- ja automaatiolaitteet.

Ydinlaitosten turvajärjestelyjä valvovana viranomaisena toimii ydinenergialain (990/1987) 55 §:n mukaisesti Säteilyturvakeskus (STUK). Turvajärjestelyistä vastaa ydinenergialain (990/1987) 9 §:n mukaisesti luvanhaltija siltä osin kuin nämä tehtävät eivät kuulu viranomaisille.

3 Vaatimusten perustelut

Turvajärjestelyjä koskevat yleiset velvoitteet esitetään ydinenergialaissa (990/1987) ja Säteilyturvakeskuksen määräyksissä ydinenergian käytön turvajärjestelyistä

(STUK Y/3/2020) ja ydinvoimalaitoksen turvallisuudesta (STUK Y/1/2018). Velvoitteita sisältyy myös Suomen tekemiin kansainvälisiin ydinenergia-alan sopimuksiin, hallitusten välisiin muihin sopimusjärjestelyihin sekä Suomen antamiin sitoumuksiin.

Ohjeessa YVL A.12 annetaan vaatimuksia ydinlaitoksen tietoturvallisuuden hallinnalle ja täsmennetään STUKin määräyksessä STUK Y/3/2020 esitettyjä vaatimuksia. Valtioneuvoston asetuksen ydinenergian käytön turvajärjestelyistä (734/2008) korvanneen STUKin määräyksen STUK Y/3/2016 päivitetyn version STUK Y/3/2020 4 §:n 5 kohdan mukaan *järjestelmien ja laitteiden suunnittelussa ja ylläpidossa on käytettävä tarkoituksenmukaisia tietoturvallisuusperiaatteita*. Turvajärjestelyjä, mukaan lukien tietoturvallisuus, koskevien asiakirjojen julkisuudesta on voimassa se, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään. Turvajärjestelyjä koskevia suunnitelmia koskee vaitiolovelvollisuus, josta säädetään ydinenergialain 78 §:ssä.

Ohjeessa käytetään termejä *luvanhaltija* ja *luvanhakija* johtuen mm. ydinlaitoksen elinkaaren eri vaiheista. Vaikka kyseessä olisi luvanhaltijaa koskeva vaatimus, se velvoittaa yhtä lailla myös luvanhakijaa (esim. vaatimus 312).

3.1 Luku 3 Tietoturvallisuuden hallinta

Tietoturvallisuuden hallinnan avulla saadaan kuvattua organisaation toimenpiteet sekä menetelmät, joilla osoitetaan organisaation sitoutuminen tietoturvallisuuden ylläpitoon ja kehittämiseen. Ohjeessa YVL A.12 annetaan vaatimuksia tietoturvallisuuden hallintajärjestelmälle, jossa on tietoturvaorganisaation kuvauksen lisäksi myös huomioitava ulkoiset toimijat vastuineen. Organisaation on määriteltävä tietoturvallisuuden hallintajärjestelmän kannalta olennaiset sidosryhmät (esimerkiksi alihankkijat, konsultit sekä urakoitsijat) sekä niiden asettamat vaatimukset. Ohjeen YVL A.12 vaatimukset ovat linjassa ISO/IEC 27001 -standardin kanssa.

Luvanhaltijan on ymmärrettävä toimintaympäristönsä ja päätettävä tietoturvallisuuden hallintajärjestelmän soveltamisesta sekä rajauksista, jotta järjestelmän toiminnallisuudet vastaavat todellisuutta. Sekä luvanhaltijan että muiden organisaatioiden suorittamien toimintojen rajapinnat ja riippuvuudet on kuvattava dokumentaatiossa.

3.1.1 Luku 3.1 Tietoturvallisuuden hallintajärjestelmä

Luvanhaltijan on määriteltävä tietoturvallisuuden hallintapolitiikka, joka voi olla itsenäinen asiakirja tai osa laajempaa kokonaisuutta. Politiikan pohjalta luvanhaltijan on luotava tietoturvallisuuden hallintajärjestelmä osana johtamisjärjestelmää. Hallintajärjestelmässä määritellään mm. tietoturvallisuusperiaatteet.

Tietoturvallisuuden hallintajärjestelmän on katettava tietoturvallisuuteen liittyvät toimenpiteet ja menettelyt. Ohjeen edellisessä versiossa (2013) käytettiin termejä *hallinnollinen* ja *tekninen tietoturva*, uudessa ohjeessa käytetään vain termiä *hallintakeino* ISO/IEC 27000 -standardin mukaisesti. Tietoturvallisuuden hallintajärjestelmää tehtäessä on huomioitava alan kansainväliset ja kansalliset standardit. Standardeja on listattu ohjeen YVL A.12 viiteluettelossa.

Tietoturvallisuuden hallintajärjestelmän tarkoitus on ylläpitää ja kehittää turvallisia prosesseja, joiden avulla voidaan huomioida organisaation prosesseille tavoitteeksi asetettu kypsyysaste ja sen asettamat reunaehdot. Hallintajärjestelmän tulee kattaa kaikki tietoturvallisuuden kannalta olennaiset laitteet ja järjestelmät. Tietoturvallisuuden hallintajärjestelmään kuuluvat tieto-, tietoliikenne-, sähkö- sekä automaatiojärjestelmät. Järjestelmässä olevat laitteet voivat olla verkottuneita tai erillislaitteita. Vaikka toimistoverkon ja laitosautomaatioverkon hallinta itsessään olisi eriytetty, hallintajärjestelmän tulee kattaa koko laitosympäristö yhteyspisteineen.

Tietoturvallisuuden hallintajärjestelmän tulee sisältää ulkoisten resurssien ohjaaminen ja valvonta tietoturvallisuuden osalta. Henkilöiden taustaselvitykset on tehtävä ja järjestelmien käyttöoikeudet ja kulkuoikeudet rajattava tehtävän mukaan. Työsuhteen päättyessä oikeudet on poistettava oikea-aikaisesti, toimenpiteellä hallitaan myös insider-uhkaa.

Tietoturvallisuuden tavoitteet on esitettävä osana tietoturvallisuuden hallintajärjestelmää. Tavoitteilla tarkoitetaan jatkuvan parantamisen periaatteen noudattamista. Jatkuvaan seurantaan ja tavoitteiden ylläpitämiseen tulee kiinnittää huomiota, koska tietoturvallisuuden uhkat muuttuvat jatkuvasti. Toimijoiden vastuut, velvollisuudet, resurssitarpeet, toteutus- ja ylläpitoaikataulut sekä toimenpiteet ja niiden arviointi ja kehittäminen on esitettävä toteutussuunnitelmissa.

Ohjeen YVL A.12 mukaisesti tietoa on suojattava luokituksen mukaisesti luvattomalta käytöltä, muuttamiselta ja tuhoamiselta. Tietoturvallisuuden auditointityökalu (KATAKRI) ja VAHTI-ohjeet tarjoavat viranomaisen luovuttaman salassa pidettävän tiedon suojaukseen käytettävät keinot ja menettelyt. Viranomaisen luovuttaman salassa pidettävän tiedon suojaukseen on käytettävä myös neuvoston päätöksen 2013/488/EU (muutettu päätöksillä 2014/233/EU ja (EU) 2019/2247) mukaisia menettelyjä. Salassa pidettävien asiakirjojen käsittely ja säilytys tulee olla luokituksensa mukaista.

Ennen viranomaisen turvallisuusluokittelemaa, salassa pidettävää tai näistä johdettua tietoa sisältävän aineiston luovuttamista kolmannelle osapuolelle, luvanhaltijan tai luvanhakijan on haettava aineiston laatineen viranomaisen hyväksyntä tiedon luovuttamiselle.

Päivityksen yhteydessä ohjeen YVL A.12 vaatimukset kohteiden suojaamisesta on kirjoitettu uusiksi, mutta vaatimustaso ei käytännössä ole muuttunut. Luvanhaltijan on tehtävä ja ylläpidettävä hallintajärjestelmän mukaista riski- ja uhka-arviota. Arvion perusteella on tunnistettava suojattavat kohteet, ja niille on määriteltävä riittävät suojaustoimenpiteet. Vaatimuksissa 314 ja 315 mainitaan uhka- ja riskiarviointi, analysointi, suojaavat toimenpiteet ja menetelmät. Suojaavat toimenpiteet ja menetelmät voidaan valita vasta, kun on analysoitu, mitä uhkaa tai riskiä sillä halutaan torjua. Uhka- ja riskiarviointia tehdessä voi käyttää tietoturvallisuusloukkausten vaikutusten arvioinnin pohjana ohjeen YVL B.1 edellyttämiä vikaantumisanalyysejä. Nämä vikaantumisanalyysit eivät kuitenkaan välttämättä kata tahallisen toiminnan kaikkia vaikutuksia. Automaatio- ja sähköjärjestelmien vaikutusten arviointiin tulisi osallistua tietoturvaosaajien lisäksi laitosprosessien sekä automaatio- ja sähköjärjestelmien asiantuntijoita.

Ohje YVL A.12 ei edellytä riskiarviolle eikä suojattaville kohteille luokittelua, vyöhykejakoa tai muutakaan ennalta määrittelyä mallia, vaan luvanhaltijan on määriteltävä omaan laitokseensa ja toimintaansa sopiva tapa. Esimerkiksi IAEA:n ohjeessa NSS 17 on annettu esimerkkejä kohteiden jaosta vyöhykkeisiin. Vaikkei varsinaista vyöhykejakoa vaaditakaan, ohjeen YVL A.12 vaatimuksissa 405a–h edellytetään suojausjärjestelmän ja muun automaatioarkkitehtuurin sekä automaatioarkkitehtuurin ja ulkoisen verkon välisen yhteyden fyysistä yksisuuntaistamista. Suojattavia kohteita arvioitaessa on huomioitava varsinaisten automaatiojärjestelmien lisäksi mahdolliset järjestelmien ja laitteiden ylläpitoon ja määräaikaistestaukseen tarvittavat tietokoneet sekä erilaiset suunnittelutyökalut. Vaatimuksessa 404 vaaditaan eksplisiittisesti, että myös sähkö- ja turvavalvontajärjestelmät sekä valmiustoiminnan viestijärjestelmät on suojattava. Edellä mainittujen järjestelmien ja laitteiden lisäksi niihin liittyvä tieto, kuten järjestelmien dokumentaatio ja niiden parametrit, on suojattava asianmukaisesti vaatimuksen 404a mukaisesti.

3.1.2 Resurssien hallinta

Työn suunnitelmallisuus, riittävät resurssit sekä työntekijöiden koulutus osaaminen on tunnistettu tärkeiksi myös tietoturvallisuuden näkökulmasta. Ydinalan henkilöstön koulutukseen kohdistuvia vaatimuksia esitetään ohjeessa YVL A.3 (esim. vaatimukset 311a ja 605). Ohjeen YVL A.12 vaatimus 322 tarkentaa tietoturvallisuudesta vastaavien henkilöiden koulutuksen ja osaamisen. Vaatimuksen 321 mukaan tietoturvallisuuden hallintaan liittyvät keskeiset henkilöt ja resurssit tulee olla luvanhaltijan palveluksessa tai omistuksessa. Vaatimuksen 323 mukaan sekä luvanhaltijan että ulkoisten resurssien tietoturvallisuuden tason ja vastuujärjestelyiden on oltava vähintään samalla tasolla kuin luvanhaltijalla on vastaavissa toimissa.

Ohje YVL A.12 tarkentaa ohjeessa YVL A.3 annettuja vaatimuksia resursseista ja osaamisesta kahden asian suhteen. Vaatimuksen 321 mukaisesti keskeisten tietoturvaan liittyvien henkilöiden tai resurssien on oltava suoraan luvanhaltijan palveluksessa tai omistuksessa. Mikäli tietojärjestelmien käyttö- tai ylläpitotoimintaa ulkoistetaan, ulkoistuksen riskit on arvioitava. Lisäksi vaatimuksessa 323 edellytetään, että ulkoistettavan toiminnan osalta toimittajalla on oltava vähintään sama tietoturvallisuustaso kuin luvanhaltijalla. Tässä on syytä huomata, että eri toiminnoille voi olla eritasoisia vaatimuksia tietoturvalle, esimerkkinä suunnittelutyökalujen ylläpito tai laitoksella tehtävä turvavalvontajärjestelmien parametrointi.

3.1.3 Luku 3.4 Tietoturvallisuuden hallintajärjestelmän arvioinnit, tarkastukset ja katselmoinnit

Tietoturvallisuuden hallintajärjestelmän riittävyyden todentamiseksi luvanhaltijan on järjestettävä itsearviointi vuosittain. Itsearvioinnin voi tehdä osa-alueittain, mutta kuitenkin niin, että kaikki hallintajärjestelmän osa-alueet on katettu kolmen vuoden ajanjaksolla.

Itsearviointien lisäksi luvanhaltijan tulee järjestää riippumaton laaja-alainen tietoturvallisuuden arviointi neljän vuoden ajanjaksolla. Tätä varten luvanhaltijan kutsuu kokoon toiminnastaan riippumattoman asiantuntijaryhmän. Koska

asiantuntijaryhmä on riippumaton, sen perehdyttämiseen sekä tarkastuksen laajuuteen ja syvyyteen on kiinnitettävä erityistä huomiota.

Luvanhaltijan tulee ilmoittaa itsearvioinneista sekä riippumattomista arvioinneista, tarkastuksista ja katselmoinneista riittävän ajoissa STUKille, jotta STUK voi harkintansa mukaan seurata näiden toteuttamista. Tarkastukset ja katselmoinnit sekä niiden tulokset on dokumentoitava. Dokumenttien on oltava STUKin tarkastettavissa esimerkiksi luvanhaltijan tiloissa

3.1.4 Luku 3.5 Tietoturvallisuuden hallintajärjestelmän parantaminen

Tietoturvallisuuden hallintajärjestelmän osalta tulee noudattaa jatkuvan parantamisen periaatetta. Jatkuvassa parantamisessa tulee hyödyntää ja huomioida oman sekä muiden toimialojen tietoturvallisuuden hallinnasta saatuja käyttökokemuksia. Luvanhaltijan tietoturvallisuuden tietämyksen tulee olla ajantasaista. Uusien uhkien turvallisuusvaikutusta pitää arvioida ennakoivasti.

Johdon on edistettävä turvallisuuskulttuuria kehittäviä ja ylläpitäviä tapoja, joilla koko henkilökunta osallistuu tietoturvallisuuden hallintajärjestelmän toteuttamiseen ja jatkuvaan parantamiseen. Tätä voidaan pitää myös osana turvallisuuskulttuuria. Ohjeen vanhassa versiossa puhuttiin luvanhaltijan johdosta, mutta nykyinen versio korostaa, mutta myös muiden toimijoiden johdon on huolehdittava omissa organisaatioissaan tietoturvallisuuden hallintajärjestelmän noudattamisesta ja parantamisesta. Luvanhaltijan johdon on varmistettava, että hallintajärjestelmään kohdistuvat parannukset ovat asetettujen tavoitteiden mukaisia.

3.2 Luku 4 Turvallisuuden kannalta tärkeiden järjestelmien suojaaminen

Ydinlaitoksen turvallisuuteen vaikuttavien laitteiden ja järjestelmien, kuten tieto-, tietoliikenne-, sähkö- ja automaatiojärjestelmien, tietoturvallisuus ja arkkitehtuuri on suunniteltava ja toteutettava siten, että luvaton pääsy on estetty riittävien fyysisten, teknisten ja hallinnollisten turvajärjestelyjen avulla niin hyvin kuin käytännöllisin toimenpitein on mahdollista.

Ydinlaitoksen tietoturvallisuuteen suoraan tai välillisesti vaikuttavat järjestelmät ja laitteet tulee olla tunnistettu ja niiden tietoturvallisuusmerkitys arvioitu. Järjestelmien merkitystä arvioitaessa tulee siis huomioida myös järjestelmät, jotka eivät suoraan vaikuta ydinturvallisuuteen, mutta joiden kautta välillinen vaikuttaminen on mahdollista. Tällaisia järjestelmiä voivat olla mm. toimistoverkko, suunnittelutyökalut ja -tietokannat sekä turvavalvontajärjestelmät. Järjestelmien ylläpitoon tai parametrointiin tarvittavien tietokoneiden merkitykseen tietoturvalle on kiinnitettävä erityistä huomiota.

Tietoturvallisuuden merkitys on lisääntynyt ydinturvallisuudessa. Elektroniset automaatiolaitteistot korvautuvat valmistajien ratkaisuilla, joissa on mukana enemmän tietotekniikkaa. Tietoturvallisuudesta on huolehdittava tietotekniikkaa sisältävien laitteiden osalta laitoksen elinkaaren kaikissa vaiheissa, suunnittelusta rakentamiseen ja edelleen käyttöönotosta aina käytöstä poistoon. Käytön aikana yksittäisiä muutostöitä tai isompia parannuksia tehtäessä on huomioitava laitteiden tietoturvamerkitys, ja toisaalta on ymmärrettävä niiden mahdollinen merkitys

alkuperäisiin suunnitteluperusteisiin nähden. Tarvittavat tietoturvallisuuden hallintakeinot ovat eri elinkaaren vaiheissa erilaisia, ja uuteen vaiheeseen siirryttäessä on ajoissa etukäteen huomioitava, mitä muutoksia hallintakeinoihin mahdollisesti tarvitaan.

Sähkö- ja automaatiotiloihin pääsyä tulee valvoa siten, että pääsy näihin tiloihin on ainoastaan asianomaisilla henkilöillä ja että käynnit ovat jäljitettävissä. Vaatimuksen 403b mukaan muutokset järjestelmien ja laitteiden ohjelmistoihin, parametreihin ja tietokantoihin on voitava jäljittää. Jäljittäminen ei välttämättä tarkoita teknistä ratkaisua, joka ei varsinkaan vanhempien laitteiden kohdalla olisi välttämättä mahdollistakaan.

Luvattomien laitteiden ja ohjelmien asentaminen on estettävä vaatimusten 403 ja 403a mukaisesti. Järjestelmän tai laitteen ylläpitoon, testaamiseen tai kalibrointiin liittyvien laitteiden ja mahdollisten ohjelmistojen asennus on lähtökohtaisesti luvallista sovittuna ajankohtana.

Ydinlaitoksen laitteet ja järjestelmät sekä turvavalvonnan järjestelmät ja valmiustoiminnan viestintäjärjestelmät on suojattava tietoturvallisuuteen liittyvien vyöhykkeiden ja ohjeen YVL A.11 vaatimien turvajärjestelyvyöhykkeiden tason mukaisesti. Vyöhykkeissä tulee huomioida niiden turvallisuusmerkitys laitoksen turvallisuudelle sekä hallittu vyöhykkeiden välinen liikennöinti.

Verkottuneet laitteet kattavat kaikki ne laitteet, jotka on liitetty toiseen laitteeseen tietoliikenteen mahdollistavalla verkolla/kaapelilla. Näihin liittyvät kaapeloinnit ja tietoliikenne on suojattava luvattomalta toiminnalta.

Tarvittavat hallintakeinot eri järjestelmien sekä tietojärjestelmän sisältämän tiedon suojaamiseksi on arvioitava vaatimusten 314–316a mukaisesti. Riskiarviosta riippumatta vaatimuksessa 404 vaaditaan tiettyjen järjestelmien suojaamista, mutta ei erikseen määritellä suojauksen tasoa.

Näiden lisäksi vaatimuksissa 405–406b vaaditaan eksplisiittisesti tiettyjä suojauksia muiden hallintakeinojen lisäksi. IAEA:n ohje NSS-17 edellyttää järjestelmien jakamista tietoturvavyöhykkeisiin. Useissa malleissa, kuten myös edellä mainitussa, vyöhykkeitä on viisi. Ohje YVL A.12 ei anna vaatimuksia järjestelmien jakamisesta eri vyöhykkeisiin eikä siten myöskään vyöhykkeiden määrästä. Kahden järjestelmän osalta kuitenkin rajoitetaan tiedonsiirtoa samaan tapaan kuin IAEA:n vyöhykemallissa. Suojausjärjestelmä on erotettava muista automaatiojärjestelmistä, samoin myös automaatioarkkitehtuuri hallinnollisista tietojärjestelmistä. Erottaminen tapahtuu yhdensuuntaistamalla tiedonsiirto siten, että tiedonsiirto on estetty käyttäen fyysisesti yhdensuuntaistavaa erotinta, kuten datadiodia. Ohjelmistopohjainen tiedonsiirron yksisuuntaisuuden järjestäminen ei ole riittävä. Muiden vyöhykkeiden osalta vaatimus 405a edellyttää niin hyvää erottelua kuin käytännössä on mahdollista toteuttaa. Vaikkei ohje YVL A.12 vyöhykejakoa edellytäkään, on se kuitenkin käytännössä yksi hyvä tapa toteuttaa järjestelmien jako pienempiin ja helpommin hallittaviin osakokonaisuuksiin. Tietoturvan vyöhykejakoa ei kuitenkaan pidä sekoittaa edellä mainittuun STUKin määräyksen STUK Y/3/2020 4 §:n vaatimiin turvajärjestelyvyöhykkeisiin.

Verkkojen fyysinen ja looginen erottelu sekä verkkojen tietoliikenteen valvonta on toteutettava niin hyvin kuin käytännöllisin toimenpitein on mahdollista, kun otetaan huomioon verkkojen turvallisuusmerkitys ja automaatiojärjestelmien tekniset rajoitukset. Automaatiojärjestelmien osalta verkon erottelun säännöt ja liikenteen valvonnan rajoitukset tulevat yleensä automaatiojärjestelmäalustan toimittajalta, jolloin verkot on suunniteltava näiden sääntöjen ja rajoitusten mukaisesti.

Ydinlaitoksen turvallisuuden kannalta keskeisiin ohjelmistopohjaisiin järjestelmiin ei saa olla fyysistä mahdollisuutta muodostaa tiedonsiirtoyhteyttä järjestelmän ulkopuolelta sisäänpäin. Ohjeen YVL B.1 vaatimus 5206 kieltää langattomat yhteydet turvallisuustoiminnoissa.

Vaatimuksen 406 mukaan on rajoitettava yksittäisen henkilön mahdollisuutta asentaa haitallinen toiminnallisuus useisiin rinnakkaisiin laitteisiin tai järjestelmiin. Vaatimus on huomioitava sekä järjestelmän suunnittelussa ja teknisessä toteutuksessa että käytön aikaisissa hallinnollisissa ohjeissa. On hyvä huomata, että kyse on nimenomaan mahdollisuuden rajoittamisesta, ei kieltämisestä. Myös tässä valitut automaatiojärjestelmäalustat saattavat tarjota valmiita sisäänrakennettuja toimintoja, tai vastaavasti hankaloittaa vaatimuksen täyttymistä.

Vaatimuksessa 406b edellytetään suojaustoiminnon lamauttamisen tai haitallisen toiminnon asentamisen havaitsemista. Korkeampiin turvallisuusluokkiin käytettävät automaatiojärjestelmäalustat tyypillisesti sisältävät tähän soveltuvaa itsediagnostiikkaa. Lisäksi määräaikaiskokeilla voinee, niiden kattavuudesta riippuen, havaita suojaustoimintojen epänormaalin toiminnan.

Tietoturvallisuudesta tulee huolehtia kaikissa järjestelmän elinkaaren vaiheissa. Luvanhaltijan on kiinnitettävä huomiota myös ennakoivaan tietoturvallisuuteen sekä käyttökokemusten keräämiseen ja hyödyntämiseen. Järjestelmät ja niiden väliset yhteydet on suunniteltava ja toteutettava siten, että vain toiminnan tarkoituksen kannalta tarpeelliset toiminnot ovat käytettävissä. Vaatimuksessa 404b edellytetään, että laitosmuutosten yhteydessä laitos- ja järjestelmätason tietoturvavaatimukset on arvioitava uudelleen. Vaikka pieni muutos ei välttämättä edellytä uutta periaatesuunnitelmaa, tietoturvavaatimusten uudelleenarvio on tehtävä joka tapauksessa.

3.2.1 Luku 4.4. Tietoturvallisuustapahtumien hallinta

Tietoturvallisuustapahtumia kuten kirjautumisia, tietoliikennettä ja tiedonsiirtoa pitää pystyä tarkkailemaan sekä tallentamaan tietoa niistä. Lisäksi tietoturvallisuuden hallintajärjestelmässä tulee kuvata menettelyt tietoturvallisuuspoikkeamien tunnistamiseen, selvittämiseen ja käsittelyyn.

Tietoturvallisuuspoikkeamien ilmoittamiseen on luotava menettelyt. Vaatimuksen 417 mukaisesti STUKille on ilmoitettava kaikki turvallisuuden kannalta viipymättä merkittävät tietoturvallisuuspoikkeamat. Vaatimus 327 määrittelee, että poikkeamia arvioitaessa on kiinnitettävä huomiota toistuviin havaintoihin ja poikkeamiin. Sellaisten perussyyt on arvioitava ja korjaavat sekä ennaltaehkäisevät toimet on toteutettava siten, että toistuvat poikkeamat saadaan hallintaan.

Tietoturvallisuuspoikkeamista ilmoittamiseen on luotava menettelyt. STUKille on ilmoitettava tapahtuneista tietoturvallisuuspoikkeamista, samoin kuin mahdollisista uhista, tapahtumista ja ilmiöistä. Turvallisuuden kannalta merkittävistä poikkeamista on ilmoitettava viipymättä.

3.2.2 Luku 4.5 Käyttöoikeuksien hallinta

Käyttöoikeuksien hallinnalle on oltava hallintaperiaatteet. Käyttöoikeuksien säännöllisellä katselmoinnilla on tarkoitus pitää käyttöoikeudet ajantasaisina, dokumentoituina ja tehtävien kannalta oikeanlaisina. Tämä korostuu erityisesti työtehtävien muutosten yhteydessä tai henkilön lähtiessä organisaatiosta. Eri järjestelmien pääkäyttäjäoikeuksien tulee olla rajoitettu mahdollisimman pienelle joukolle soveltaen turvajärjestelyissä yleisesti käytössä olevaa ”need to know” -periaatetta. Käyttöoikeudet on myönnettävä vain työtehtävien mukaisesti. Käyttöoikeuksiin salasanapolitiikka tulee olla määritelty, ja siinä tulee huomioida erilaisten järjestelmien ja laitteiden teknologiset rajoitteet mm. salasanan pituuden osalta. Lisäohjeita voi katsoa esimerkiksi Vahti-ohjeesta.

Ulkoisten resurssien osalta turvallisella tietojenkäsittelyllä tarkoitetaan laitteiden turvallisuutta, käyttöoikeuksien valvontaa ja ohjeistusta toimintatavoista sekä niiden noudattamisen valvontaa.

3.2.3 Luku 4.6 Järjestelmien tietoturvallisuustestaaminen

YVL-ohjeen luvussa 4.6 vaaditaan, että tietoturvallisuuden kannalta tärkeiden verkottuneiden järjestelmien testaamisessa on käytettävä kehittyneitä testaamismenettelyjä. Esimerkkejä kehittyneistä testausjärjestelmistä löytyy IAEA:n ohjeesta NSS 17. Tietoturvatestaamista suunniteltaessa on kiinnitettävä huomioita kattavaan tehdastestaukseen, koska laitospaikalla tehtävä testaaminen voi olla hyvin rajattua tai se voi aiheuttaa merkittävää vaaraa henkilöille tai laitokselle.

Turvajärjestelyjen valvontaan liittyvien järjestelmien tietoturvallisuutta tulee testata. Tietoturvan testaamista voidaan suorittaa myös ohjeen YVL A.11 edellyttämien turvajärjestelyjen vaikuttavuuden osoittamiseksi järjestettävien harjoituksien yhteydessä.

Automaatiojärjestelmäalustojen, sähkö- ja automaatiolaitteiden ja -järjestelmien kelpoistuksessa ja testaamisessa on huomioitava myös tietoturvallisuuden testaaminen. Tietoturvallisuuden kannalta tärkeiden verkottuneiden järjestelmien testaamisessa on käytettävä kehittyneitä testaamismenettelyjä.

Jos uusia ja vanhoja järjestelmiä yhdistetään, on tärkeä arvioida yhdistelmän tietoturvallisuutta.

3.3 Luku 5 Säteilyturvakeskuksen valvontaa varten toimitettavat asiakirjat

Säteilyturvakeskuksen valvontamenettelyt, jotka kohdistuvat luvanhaltijan tietoturvallisuuden hallintajärjestelmään, esitetään luvussa 5. Luvussa on esitetty ydinlaitoksen elinkaaren eri vaiheissa STUKille toimitettavat asiakirjat, STUKin antamat lausunnot sekä tarkastukset ja muu valvonta.

Rakentamislupavaiheessa toimitetaan mm. tietoturvallisuusvaatimukset, järjestelmätasoiset tietoturvallisuussuunnitelmat ja järjestelmien suunnitteluvaatimukset mukaan lukien kuvaus järjestelmien välisistä yhteyksistä. YVL B.1 vaatimuksen 608 mukaisesti järjestelmien vaatimusmäärittelyt pitäisi olla mahdollista tehdä rakentamislupavaiheen aineiston perusteella. Kaikki järjestelmäkohtaiset vaatimukset eivät ole välttämättä selvillä, mutta ylätasolta järjestelmään johtuvat vaatimukset pitäisi olla. Rakentamislupahakemuksessa voi tarkemmin selvittää, miltä osin vaatimukset saattavat olla puutteelliset.

4 Ohjeen alaa koskeva kansainvälinen säännöstö

"IAEA NSS 17 Computer Security at Nuclear Facilities (TechDoc)" on merkittävin referenssi. Ohjeessa YVL A.12 on otettu huomioon siinä esitetyt menettelyt.

Ohjeen teossa on huomioitu ISO/IEC 27000 -sarjan standardit sekä IEC 62443 -sarjan standardit.

Muita huomionarvoisia standardeja:

- IEC 62645:2014 Nuclear power plants - Instrumentation and control systems - Requirements for security programmes for computer-based systems
- IEC 62859:2016 Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity.

5 Tepco Fukushima Dai-ichi onnettomuuden vaikutukset

Ohje YVL A.12 on julkaistu ensimmäisen kerran vuonna 2013 Fukushiman onnettomuuden jälkeen, joten vaatimukset on huomioitu alusta pitäen.

6 Päivityksessä huomioidut muutostarpeet

Ohjeen YVL A.12 vaatimustasoon ei ole tehty merkittäviä muutoksia. Muutokset liittyvät ohjeen selkeyttämiseen. Hallinnollista taakkaa on kevennetty siten, että tietoturvallisuuteen liittyviä vaatimuksia on siirretty ohjeeseen YVL A.12 ohjeista YVL B.1 ja YVL E.7. Tietoturvallisuuteen liittyviä vaatimuksia on siis keskitetty ohjeeseen A.12. Selkeytystä on tehty sekä kielellisesti että jakamalla useita vaatimuksia sisältäneitä kohtia omiksi vaatimuksikseen.

Uusia tai merkittävästi muuttuneita ovat vaatimus 415a, jossa vaaditaan harjoituksia ohjeen YVL A.11 tapaan, sekä vaatimus 417a, joka määrittelee, milloin STUKille on ilmoitettava tapahtumista.

Luku 5, STUKin valvontaa varten toimitettavat asiakirjat, on kirjoitettu käytännössä uusiksi. Hallinnollista taakkaa on merkittävästi kevennetty vähentämällä STUKille toimitettavien asiakirjojen määrää. Lisäksi rakentamislupa- ja käyttölupavaiheen dokumenteissa on huomioitu ohjeeseen YVL B.1 tehdyt muutokset.

Aikaisemmassa ohjeen versiossa (2013) ollut erillinen luku "Tietoturvallisuuteen liittyvien järjestelmien hankinta, kehitys ja ylläpito" on poistettu, koska vastaavia vaatimuksia on kirjoitettu muihin lukuihin. Myös luku "Tietoliikenteen ja ICT – palveluiden hallinta ja kontrollointi" on poistettu päivitetystä ohjeesta.

Selkeytetty ja yksiselitteisempi ohje YVL A.12 poistaa tulkinnanvaraisuuksia, ja näin helpottaa osaltaan luvanhaltijoiden toimintaa sekä viranomaisen tarkastustoimintaa.