STUK

OHJE **YVL A.12** / 22.11.2013

YDINLAITOKSEN TIETOTURVALLISUUDEN HALLINTA

jatkuu

Uusien ydinlaitosten osalta tämä ohje on voimassa 1.12.2013 alkaen toistaiseksi. Rakenteilla olevilla ja käyvillä ydinlaitoksilla tämä ohje saatetaan voimaan erillisellä STUKin päätöksellä.

Ensimmäinen painos
Helsinki 2013

ISBN 978-952-478-958-5 (nid.) Kopijyvä Oy 2013
ISBN 978-952-478-959-2 (pdf)
ISBN 978-952-478-960-8 (html)

STUK • SÄTEILYTURVAKESKUS
STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

Osoite/Address • Laippatie 4, 00880 Helsinki
Postiosoite / Postal address • PL / P.O.Box 14, FIN-00881 Helsinki, FINLAND
Puh./Tel. (09) 759 881, +358 9 759 881 • Fax (09) 759 88 500, +358 9 759 88 500 • www.stuk.fi

Valtuutusperusteet

Ydinenergialain (990/1987) 7 r §:n mukaan Säteilyturvakeskuksen tehtävänä on asettaa ydinenergialain mukaisen turvallisuustason toteuttamista koskevat yksityiskohtaiset turvallisuusvaatimukset.

Soveltamissäännöt

YVL-ohjeen julkaiseminen ei sinänsä muuta Säteilyturvakeskuksen ennen ohjeen julkaisemista tekemiä päätöksiä. Vasta kuultuaan asianosaisia Säteilyturvakeskus antaa erillisen päätöksen siitä, miten uutta tai uusittua YVL-ohjetta sovelletaan käytössä tai rakenteilla oleviin ydinlaitoksiin ja luvanhaltijoiden toimintoihin. Uusiin ydinlaitoksiin ohjeita sovelletaan sellaisenaan.

Kun Säteilyturvakeskus harkitsee YVL-ohjeissa esitettyjen, uusien turvallisuusvaatimuksien soveltamista käytössä tai rakenteilla oleviin ydinlaitoksiin, se ottaa huomioon ydinenergialain (990/1987) 7 a §:ssä säädetyt periaatteet: *Ydinenergian käytön turvallisuus on pidettävä niin korkealla tasolla kuin käytännöllisin toimenpitein on mahdollista. Turvallisuuden edelleen kehittämiseksi on toteutettava toimenpiteet, joita käyttökokemukset ja turvallisuustutkimukset sekä tieteen ja tekniikan kehittyminen huomioon ottaen voidaan pitää perusteltuina.*

Ydinenergialain 7 r §:n kolmannen momentin mukaan *Säteilyturvakeskuksen turvallisuusvaatimukset velvoittavat luvanhaltijaa, kuitenkin niin, että luvanhaltijalla on oikeus esittää muunkinlainen kuin vaatimuksissa edellytetty menettelytapa tai ratkaisu. Jos luvanhaltija vakuuttavasti osoittaa, että esitetty menettelytapa tai ratkaisu toteuttaa tämän lain mukaisen turvallisuustason, Säteilyturvakeskus voi sen hyväksyä.*

1 Johdanto

101. Tässä ohjeessa annetaan vaatimuksia ydinlaitoksen tietoturvallisuuden hallinnalle ja täsmennetään valtioneuvoston asetuksessa ydinenergian käytön turvajärjestelyistä (734/2008) [2] säädettyjä suunnitteluvaatimuksia. Asetuksen 4 §:n mukaan ydinlaitoksen ja sen tieto-, tietoliikenne- ja automaatiojärjestelmien suunnittelussa on käytettävä kehittyneitä tietoturvallisuusperiaatteita. Luvaton pääsy ydinlaitoksen suojaus-, ohjaus- ja säätöjärjestelmiin on estettävä.

102. Turvajärjestelyjä, mukaan lukien tietoturvallisuus, koskevien asiakirjojen julkisuudesta on voimassa se, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) [4] säädetään. Vaitiolovelvollisuudesta säädetään ydinenergialain (990/1987) 78 §:ssä [1]. Vaitiolovelvollisuus koskee turvajärjestelyjä koskevia suunnitelmia.

103. Turvajärjestelyjä koskevat yleiset velvoitteet esitetään ydinenergialaissa (990/1987) [1] ja sen nojalla annetuissa valtioneuvoston asetuksissa ydinenergian käytön turvajärjestelyistä (734/2008) [2] ja ydinvoimalaitoksen turvallisuudesta (717/2013) [3]. Velvoitteita sisältyy myös Suomen tekemiin kansainvälisiin ydinenergia-alan sopimuksiin, hallitusten välisiin muihin sopimusjärjestelyihin sekä Suomen antamiin sitoumuksiin. Suunnitteluperusteuhka (DBT) on esitetty erillisessä asiakirjassa ”Ydinenergian ja säteilyn käytön suunnitteluperusteuhka”, joka toimitetaan ohjeessa YVL A.11 määriteltyjen laitosluokkien luvanhaltijoille käytettäväksi turvajärjestelyjen ja tietoturvallisuuden hallinnan suunnittelun perusteena. STUKin ohjeet YVL A.11 ja YVL A.12 yhdessä edellä mainittujen asiakirjojen kanssa muodostavat perustan ydinlaitosten turvajärjestelyille. Ydinlaitosten turvajärjestelyjä valvovana viranomaisena toimii ydinenergialain 55 §:n mukaisesti Säteilyturvakeskus (STUK). Turvajärjestelyistä vastaa ydinenergialain 9 §:n mukaisesti luvanhaltija siltä osin, kuin nämä tehtävät eivät kuulu viranomaisille [1].

104. Tietoturvallisuudella tarkoitetaan tietojen, tietoturvallisuuteen liittyvien järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen eheyttä, kiistämättömyyttä, käytettävyyttä ja luottamuksellisuutta turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta. Tietoturvallisuus on osa luvanhaltijan johtamisjärjestelmää ja turvajärjestelyjä.

105. Tietoturvallisuus kattaa tiedon eheyden, kiistämättömyyden, käytettävyyden ja luottamuksellisuuden turvaamisen sen kaikissa olomuodoissaan aina tiedon luomisesta sen tuhoamiseen asti. Tiedolla tarkoitetaan eri muodossa talletettavaa, käsiteltävää tai siirrettävää tietoa. Tieto voi olla esimerkiksi yksittäisenä paperiasiakirjana, tiedostona, tietokantana tai suoritettavana ohjelmana, filmillä tai ääni- tai kuvatallenteena.

2 Soveltamisala

201. Tässä ohjeessa 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. Yleisiä vaatimuksia ja STUKin suorittamaa valvontaa kuvataan myös YVL A-sarjan ohjeissa sekä ohjeissa YVL B.1, B.2, B.7, C.5, D.1, D.2, D.3, D.5 ja E.7.

3 Tietoturvallisuuden hallinta

3.1 Yleiset vaatimukset

301. Ydinlaitoksen johdon on osoitettava sitoutumisensa tietoturvallisuuden hallintaan.

302. Tietoturvallisuuden hallintajärjestelmä on osa luvanhakijan/haltijan johtamisjärjestelmää, jonka on täytettävä ohjeen YVL A.3 vaatimukset.

303. Tietoturvallisuuden hallintajärjestelmän on katettava sekä hallinnolliseen että tekniseen

tietoturvallisuuteen liittyvät toimenpiteet ja menettelyt, ja sen tulee sisältää myös ulkoisten resurssien ohjaaminen ja valvonta tietoturvallisuuden osalta.

304. Kansainväliset tietoturvallisuuden standardit ja ohjeistukset [5–8, 12, 14, 18] ja kansalliset ohjeistukset [9–11, 13] on otettava huomioon tietoturvallisuuden hallintajärjestelmän kehittämisessä soveltuvin osin.

305. Ohje YVL A.11 esittää vaatimuksen tilannekuvan välittämisestä. Tilannekuvan välittämisessä on huomioitava tietoturvallisuus, kuitenkin siten ettei tietoturvallisuudesta huolehtiminen saa vaarantaa ajantasaisen tilannekuvan välittämistä.

306. Valtioneuvoston asetusten (717/2013) [3] 28 §:n ja (736/2008) [17] 19 §:n mukaisesti ydinlaitoksen on ylläpidettävä hyvää turvallisuuskulttuuria. Tietoturvallisuudesta huolehtiminen on osa hyvää turvallisuuskulttuuria.

307. Suunnitteluperusteuhka (DBT) määrittelee uhkan, jota käytetään turvajärjestelyjen vaatimusten, suunnittelun ja arvioinnin perusteena. Luvanhaltijan on suunniteltava tietoturvallisuuden hallintajärjestelmänsä siten, että tietoturvallisuuteen liittyvä suunnitteluperusteuhka voidaan torjua suunnitteluperusteuhka-asiakirjassa asetettujen suojaustavoitteiden mukaisesti niin hyvin kuin käytännöllisin toimenpitein on mahdollista.

3.2 Tietoturvallisuuden hallintajärjestelmä

308. Luvanhaltijan on määriteltävä tietoturvallisuuden hallintajärjestelmän kattavuus ja rajat sekä tietoturvallisuuden hallintapolitiikka. Tietoturvallisuuden hallintapolitiikka voi olla itsenäinen asiakirja tai osa laajempaa kokonaisuutta. Kattavuutta ja tietoturvallisuuden hallintapolitiikkaa on arvioitava sekä määräajoin että merkittävien turvallisuutta tai tietoturvallisuutta koskevien tapahtumien, muutosten tai uusien uhkien ilmentyessä.

309. Tietoturvallisuuden tavoitteet on esitettävä osana tietoturvallisuuden hallintajärjestelmää. Tietoturvallisuustavoitteiden saavuttamisen mittaamiseen on kiinnitettävä huomiota, niiden saavuttamista on seurattava ja tavoitteita on arvioitava jatkuvan parantamisen periaatetta noudattaen. Toimijoiden vastuut ja velvollisuudet, toimenpiteet, resurssitarpeet, toteutus- ja ylläpitoaikataulut sekä se, kuinka toimenpiteiden vaikuttavuutta arvioidaan ja kehitetään, on esitettävä toteutussuunnitelmissa.

310. Tietoturvallisuus on huomioitava kaikilla organisaation toiminnan tasoilla. Tietoturvallisuusorganisaatio on kuvattava tietoturvallisuuden hallintajärjestelmässä. Kuvauksessa on otettava huomioon myös ulkoiset toimijat ja näiden vastuut, mikäli näillä tai näiden toiminnalla on vaikutusta ydinlaitoksen tietoturvallisuuteen. Tehtävät ja vastuualueet on tarpeen mukaan eriytettävä, jotta vähennetään organisaation suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä.

311. Luvanhaltijan on dokumentoitava, mitä kriteereitä ja standardeja hyödyntäen tietoturvallisuuden hallintajärjestelmä on toteutettu. Viranomaisen luovuttaman salassa pidettävän tiedon suojaukseen on käytettävä viranomaisen noudattamia menettelyjä [10] ja suojauksen tietoturvallisuuden arviointiin on käytettävä KATAKRI-kriteeristöä [13].

312. Tietoturvallisuusriskien arviointi ja hallinta on osa tietoturvallisuuden hallintajärjestelmää. Riskejä on arvioitava kuhunkin aihealueeseen ja järjestelmään parhaiten soveltuvilla menetelmillä. Luvanhaltijan on varmistettava, että tietoturvallisuusriskien arviointiin käytetyt menettelyt ovat riittävät ydinlaitoksen turvallisuuden kannalta ja että merkittävät riskit on tunnistettu.

313. Riskienhallinnan kokonaisuus on dokumentoitava.

314. Luvanhaltijan on tehtävä tietoturvallisuuden uhka- ja riskienarviointi, ja se on päivitettävä vuosittain ja merkittävien tietoturvallisuutta koskevien tapahtumien, muutosten tai uusien uhkien ilmentyessä.

315. Tietoturvallisuuteen liittyvät uhkat ja riskit on systemaattisesti analysoitava, ja suojaavat toimenpiteet ja menetelmät valittava analyysin perusteella. Analyysiä on ylläpidettävä ja kehitettävä.

316. Suojattavat kohteet on tunnistettava ja määriteltävä riittävällä yksityiskohtaisuuden tasolla. Kohteisiin liittyvät uhkat ja haavoittuvuudet sekä tietoturvallisuusloukkausten aiheuttamat vaikutukset on analysoitava ja määriteltävä tarpeelliset suojaustoimenpiteet. Suojaustoimenpiteet on dokumentoitava.

317. Pääsyä suojattaviin kohteisiin on valvottava lokimenettelyin. Lokimerkintöjen täytyy sisältää riittävät tiedot tapahtuman ja käyttäjän jäljittämiseen. Lokitiedostot on suojattava asiattomilta muutoksilta.

3.3 Asiakirjoja koskevat vaatimukset

318. Luvanhaltijan asiakirjoja koskevat yleiset vaatimukset on esitetty ohjeissa YVL A.1, YVL A.3 ja YVL A.11, ja näitä on noudatettava tietoturvallisuutta koskevissa asiakirjoissa.

319. Asiakirjoja on suojattava luvattomalta käytöltä, muuttamiselta ja tuhoamiselta ja niiden saatavuus luvalliselle käyttäjälle on turvattava. Asiakirjat on luokiteltava niiden tietoturvallisuus- ja turvallisuusmerkityksen mukaan. Asiakirjoja on suojattava niiden luokituksen mukaisesti.

3.4 Resurssien hallinta

320. Luvanhaltijan on huolehdittava siitä, että sillä on käytettävissään riittävät resurssit ja osaaminen tietoturvallisuuden hallinnan suunnitteluun, toteuttamiseen, arviointiin ja jatkuvaan parantamiseen. Ohjeet YVL A.4 ja A.11 osoittavat yleiset vaatimukset resurssien hallinnan osalta. Resurssien on katettava henkilöstöresurssit, tarvittava osaaminen sekä teknologiset resurssit.

321. Keskeisten tietoturvallisuuden hallintaan liittyvien henkilöiden ja muiden resurssien on oltava luvanhakijan/luvanhaltijan palveluksessa tai omistuksessa. Ennen kuin tietojärjestelmien ylläpito-, huolto- ja käyttötoimintaa voidaan ulkoistaa, on tehtävä sitä koskeva riskien arviointi ja osoitettava, että jäännösriski on hyväksyttävällä tasolla.

322. Tietoturvallisuuden kouluttamiseen, kehittämiseen ja ylläpitoon osallistuvien henkilöiden koulutus ja osaamisen ylläpito on oltava riittävää heidän tietoturvallisuuteen liittyvien tehtäviensä toteuttamiseksi. Ydinlaitoksen koko henkilökunnan sekä ulkoisten resurssien on oltava tietoisia tietoturvallisuuden hallintaan liittyvistä asioista tehtäviensä asianmukaisen hoitamisen kannalta riittävässä määrin. Tietoturvallisuuteen liittyvät koulutustapahtumat on dokumentoitava.

323. Ulkoisten resurssien käytön osalta luvanhaltijan on sopimuksin ja tarkastusmenettelyiden avulla huolehdittava, että niiden tietoturvallisuuden taso ja vastuujärjestelyt ovat vähintään samalla tasolla kuin luvanhaltijalla vastaavissa toimissa. Luvanhaltijan on esitettävä ne toimenpiteet, joilla se valvoo toimittajaosapuolen tai muun vastaavan ulkoisen resurssin tietoturvallisuutta. Varmistuksissa on huomioitava mahdolliset alihankintaketjut.

3.5 Tietoturvallisuuden hallintajärjestelmän tarkastukset ja katselmoinnit

324. Tietoturvallisuuden riittävyyden todentamiseksi luvanhaltijan on järjestettävä tietoturvallisuuden itsearviointi vuosittain siten, että tietoturvallisuuden hallintajärjestelmän kaikki osa-alueet arvioidaan vähintään kolmen vuoden välein. Arvioinnin yhteydessä on selvitettävä myös mahdolliset riskienarviointiin ja uhkakuvaan tulleet muutokset sekä ajanjaksolla ilmenneiden tietoturvallisuustapahtumien merkitys hallintajärjestelmälle.

325. Luvanhaltijan on erikseen kokoon kutsutun, luvanhaltijan toiminnasta riippumattoman asiantuntija-ryhmän avulla toteutettava laaja-alainen tietoturvallisuuden arviointi määräajoin, kuitenkin vähintään neljän vuoden välein.

326. Itsearvioinneista, riippumattoman asiantuntijaryhmän ja mahdollisten ulkoisten resurssien toteuttamista arvioinneista, tarkastuksista ja katselmoinneista on ilmoitettava riittävän ajoissa etukäteen STUKille, jotta STUK voi harkintansa mukaan seurata näiden toteuttamista.

327. 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.

328. Luvanhaltijan on tarkastettava ulkoisten resurssien tietoturvallisuus. Ulkoisten resurssien tarkastusten on katettava riittävässä määrin vastaavat toiminnot kuin luvanhaltijalla on. Ohjeissa YVL A.3 ja A.5 on esitetty vaatimuksia toimittajien valvonnalle.

329. Tarkastukset ja katselmoinnit on dokumentoitava.

3.6 Tietoturvallisuuden hallintajärjestelmän parantaminen

330. Jatkuvassa parantamisessa on hyödynnettävä sekä oman että muiden toimialojen tietoturvallisuuden hallinnasta saatuja käyttökokemuksia.

331. Luvanhaltijan johdon on edistettävä tapoja, joilla koko henkilökunta osallistuu tietoturvallisuuden hallintajärjestelmän toteuttamiseen ja jatkuvaan parantamiseen.

332. Luvanhaltijan johdon on varmistettava, että hallintajärjestelmään kohdistuvat parannukset ovat asetettujen tavoitteiden mukaisia.

4 Turvallisuuden kannalta tärkeiden järjestelmien suojaaminen

401. Valtioneuvoston asetuksen (734/2008) [2] 4 §:n mukaisesti *ydinlaitoksen ja sen tieto-, tietoliikenne- ja automaatiojärjestelmien suunnittelussa on käytettävä kehittyneitä tietoturvallisuusperiaatteita. Luvaton pääsy ydinlaitoksen suojaus-, ohjaus- ja säätöjärjestelmiin on estettävä.*

4.1 Yleiset vaatimukset

402. Ydinlaitoksen ydinturvallisuuteen suoraan tai välillisesti vaikuttavien järjestelmien, kuten tieto-, tietoliikenne-, sähkö- ja automaatiojärjestelmien tietoturvallisuus ja tietoturvallisuusarkkitehtuuri on suunniteltava ja toteutettava siten, että luvaton pääsy niihin on estetty riittävien fyysisten, teknisten ja hallinnollisten turvajärjestelyjen avulla niin hyvin kuin käytännöllisin toimenpitein on mahdollista.

403. Tietoturvallisuutta uhkaavien laitteiden ja ohjelmien asentaminen on estettävä luotettavasti. Ohjelmistoihin tehdyt muutokset on voitava havaita ja jäljittää.

404. Ydinlaitoksen turvajärjestelyjen on perustuttava vyöhykkeisiin ohjeen YVL A.11 mukaisesti. Ydinlaitoksen tieto-, tietoliikenne-, sähkö- ja automaatiojärjestelmät, verkottuneet laitteet ja erillisjärjestelmät sekä turvavalvonnan järjestelmät ja valmiustoiminnan viestintäjärjestelmät on suojattava asianmukaisesti.

405. Verkottuneet laitteet kattavat kaikki ne laitteet, jotka on liitetty toiseen laitteeseen tietoliikenteen mahdollistavalla verkolla/kaapelilla. Näihin liittyvät kaapeloinnit ja tietoliikenne on suojattava lainvastaiselta toiminnalta. Verkkojen fyysinen ja looginen erottelu sekä verkkojen tietoliikenteen valvonta on toteutettava niin hyvin kuin käytännöllisin toimenpitein on mahdollista verkkojen turvallisuusmerkitys huomioon ottaen.

406. Luvanhaltijan on käytettävissä olevin keinoin estettävä yksittäisen henkilön mahdollisuus asentaa haitallinen toiminnallisuus useisiin rinnakkaisiin laitteisiin tai ohjelmistoihin. Yksittäisen ohjelmiston haitallinen vaikutus ydinlaitoksen turvallisuuteen on tehtävä niin pieneksi kuin käytännöllisin keinoin on mahdollista. Haitallisen toiminnallisuuden asentaminen tai suojaustoiminnon lamauttaminen on voitava havaita luotettavasti.

407. Ydinlaitoksen ja sen tieto-, tietoliikenne-, automaatio-, sähkö-, turvavalvonta- ja viestintäjärjestelmiä koskevat asiakirjat ja tiedot on niiden turvallisuusmerkityksen mukaisesti suojattava siten, että vain henkilöt, joilla on oikeus niiden käsittelyyn voivat saada ne haltuunsa.

4.2 Tietoliikenteen ja käyttötoimintojen hallinta ja kontrollointi

408. Luvanhaltijalla on oltava kirjalliset menettelyohjeet turvallisille tietojenkäsittelypalveluille. Ohjeita on ylläpidettävä ja niiden on oltava kaikkien niitä tarvitsevien käyttäjien saatavilla.

409. Tietoturvallisuusmuutosten hallinnassa on noudatettava ohjeessa YVL B.1:ssä esitettyjä konfiguraatiohallinnan menettelyjä.

4.3 Tietoturvallisuuteen liittyvien järjestelmien hankinta, kehitys ja ylläpito

410. Tietoturvallisuuteen liittyvien järjestelmien hankinta, kehitys ja ylläpito on toteutettava siten, että tietoturvallisuus huomioidaan kaikissa järjestelmän elinkaaren vaiheissa. Luvanhaltijan on kiinnitettävä erityistä huomiota ennakoivaan tietoturvallisuuteen sekä oman ja toisten organisaatioiden käyttökokemusten keräämiseen ja hyödyntämiseen.

411. Järjestelmien hankintaan, kehitykseen ja ylläpitoon liittyvän tietoturvallisuusdokumentaation on oltava kattavaa ja ajantasaista. Dokumentaation on selkeästi liityttävä muuhun järjestelmädokumentaatioon.

412. Järjestelmien ja niiden osakomponenttien väliset toiminnalliset riippuvuudet on tunnistettava ja niiden vaikutus tietoturvallisuuteen on analysoitava ja arvioitava sekä poistettava haitalliset riippuvuudet.

413. Verkottuneiden järjestelmien osalta on kuvattava kattavasti ja yksiselitteisesti eri järjestelmien rajapinnat, yhteydet, käytetyt protokollat sekä kommunikoivat osapuolet.

414. Järjestelmät ja niiden väliset yhteydet on suunniteltava ja toteutettava siten, että vain toiminnan tarkoituksen kannalta tarpeelliset toiminnot ovat käytettävissä.

4.4 Tietoturvallisuuspoikkeamien hallinta

415. Luvanhaltijan on luotava menettelyt sille, että tietojärjestelmien tai -palvelujen kehittämisessä ja käytössä havaituista epätavallisista tapahtumista tai epäillyistä suojauksen heikkouksista raportoidaan luvanhaltijalle, toimittajalle ja tarvittaessa STUKille mahdollisimman ajantasaisesti.

416. Luvanhaltijan on luotava menettelyt järjestelmälliseen reagointiin tietoturvallisuuspoikkeamien varalta.

417. Tietoturvallisuuspoikkeamien ilmoittamiseen on luotava menettelyt. STUKille on ilmoitettava kaikki ydinturvallisuuden kannalta merkittävät tietoturvallisuuspoikkeamat viipymättä. Poikkeamien hallintaan liittyy YVL A.3 ohje, joka on huomioitava käsiteltäessä tietoturvallisuuspoikkeamia.

4.5 Käyttöoikeuksien hallinta

418. Käyttöoikeuksien valvontaperiaatteet on laadittava, dokumentoitava ja katselmoitava.

419. Eri järjestelmien pääkäyttäjäoikeudet on rajoitettava. Käyttöoikeudet on myönnettävä vain työtehtävien mukaisesti.

420. Käyttäjien käyttöoikeudet on katselmoitava säännöllisesti ja työtehtävien muutosten yhteydessä.

421. Salasanapolitiikka on määriteltävä ja otettava käytäntöön. Toteutumista on valvottava.

422. Etätyöhön ja ulkoisten resurssien tekemään työhön on luotava turvallisen tietojenkäsittelyn ja järjestelmien käytön menettelyt ja näiden noudattamista on valvottava.

4. 6 Turvallisuuteen liittyvien järjestelmien tietoturvallisuustestaaminen

423. Turvajärjestelyjen valvontaan liittyvät järjestelmät on testattava tietoturvallisuuteen kohdistuvia hyökkäyksiä vastaan. Testaaminen voidaan suorittaa ohjeen YVL A.11 edellyttämien turvajärjestelyjen vaikuttavuuden osoittamiseksi järjestettävien harjoituksien yhteydessä.

424. Ohjeen YVL E.7 edellyttämien ydinlaitoksen sähkö- ja automaatiolaitteiden ja järjestelmien kelpoistuksessa ja testaamisessa on huomioitava myös tietoturvallisuuden testaaminen.

425. Turvallisuuden kannalta tärkeiden verkottuneiden järjestelmien testaamisessa on käytettävä kehittyneitä testaamismenettelyjä riittävän kattavasti toiminnallisen testaamisen lisäksi. Erillisjärjestelmien osalta testaamista on toteutettava perustuen näiden järjestelmien riskiarvioon. Testaustulokset on dokumentoitava.

426. Erityistä huomiota on kiinnitettävä uusien ja mahdollisten vanhojen järjestelmien muodostaman kokonaisjärjestelmän tietoturvallisuuden arviointiin.

5 Säteilyturvakeskuksen valvontaa varten toimitettavat asiakirjat

5.1 Periaatepäätösvaihe

501. Ydinenergia-asetuksen (161/1988) [15] 24 §:n mukaisesti ydinlaitoksen periaatepäätöstä koskevaan hakemukseen on liitettävä selvitys suunnitellun sijaintipaikan sopivuudesta tarkoitukseensa ottaen huomioon paikallisten olosuhteiden vaikutus turvajärjestelyihin [16].

5.2 Rakentamislupavaihe

502. Rakentamislupahakemuksen yhteydessä luvanhakijan on toimitettava seuraavat asiakirjat STUKille hyväksyttäväksi:

1. Luvanhakijan tietoturvallisuuden hallintajärjestelmän kuvaus ja siihen liittyvät asiakirjat, mukaan lukien tietoturvallisuuden hallintapolitiikka.
2. Tietoturvallisuusriskien arviointisuunnitelma ja riskienarviointien tulokset.
3. Tietoturvallisuusvaatimukset ja tietoturvallisuuden testausvaatimukset.
4. Järjestelmätasoiset tietoturvallisuussuunnitelmat sisältäen suojattavat kohteet, ja niihin liittyvät suojausmenettelyt, tietoturvallisuuteen liittyvät vyöhykkeet sekä kokonaisarkkitehtuurisuunnitelma.
5. Kuvaus luvanhakijan tietoturvallisuusorganisaatiosta rakentamisvaihetta varten
6. Suunnitelma ydinlaitoksen rakentamisen aikaisista toimittajiin kohdistuvista tietoturvallisuuden valvontatoimista.

503. Seuraavat asiakirjat on toimitettava STUKille tiedoksi:

1. Asiakirjojen ja tietojen luokitteluun ja käsittelyyn liittävät kuvaukset sekä suojaus- ja menettelyohjeet rakentamisen aikana.
2. Järjestelmien hankintaan liittyvät tietoturvallisuusmenettelyohjeet.
3. Järjestelmien suunnitteluvaatimukset mukaan lukien kuvaus järjestelmien välisistä yhteyksistä.

504. Perustelluista syistä kohdassa 503 esitetyt asiakirjat voidaan STUKille toimittamisen sijasta todentaa myös rakentamisluvan hakijan osoittamassa paikassa.

505. Vaatimuksissa 502 ja 503 esitetyt asiakirjat on pidettävä ajan tasalla. Edellä mainittujen asiakirjojen muutoksille on hankittava STUKin hyväksyntä tai ne on toimitettava tiedoksi, kuten edellä on mainittu.

5. 3 Rakentamisvaihe

506. Ydinlaitoksen rakentamisen aikana STUKin hyväksyttäväksi on toimitettava seuraavat asiakirjat ja näiden päivitykset:

1. Tietoturvallisuuden hallintajärjestelmän mahdolliset merkittävät muutokset.
2. Yksityiskohtaiset tietoturvallisuuden testaussuunnitelmat.
3. Rakentamisen aikainen tietoturvallisuusriskien arviointisuunnitelma ja riskienarviointien tulokset.

507. Seuraavat asiakirjat ja näiden päivitykset on toimitettava STUKille tiedoksi:

1. tietoturvallisuuden hallintajärjestelmän vähäiset muutokset
2. päivitetyt tietoturvallisuussuunnitelmat
3. tietoturvallisuuden tarkastusten ja katselmointien raportit ja tietoturvallisuustestausraportit.

508. Perustelluista syistä vaatimuksessa 507 esitetyt asiakirjat voidaan STUKille toimittamisen sijasta todentaa myös rakentamisluvan hakijan osoittamassa paikassa.

509. Vaatimuksissa 506 ja 507 esitetyt asiakirjat on pidettävä ajan tasalla. Edellä mainittujen asiakirjojen muutoksille on hankittava STUKin hyväksyntä tai ne on toimitettava tiedoksi, kuten edellä on mainittu.

5.4 Käyttölupavaihe

510. Käyttölupahakemuksen käsittelyn yhteydessä STUK antaa hakemusta koskevan lausunnon työ- ja elinkeinoministeriölle ja liittää lausuntoon laatimansa turvallisuusarvion ja ydinenergia-asetuksen (161/1988) 36 §:n mukaisia asiakirjoja koskevan arvion, jossa käsitellään muun muassa suunniteltuja tietoturvallisuusjärjestelyjä. Turvallisuusarviota valmistellessaan STUK pyytää sisäasiainministeriöltä lausunnon YEA 36 §:n kohdassa 7 tarkoitetuista selvityksistä, jotka koskevat turva- ja valmiusjärjestelyjä [15].

511. Käyttölupahakemuksen käsittelyä varten on STUKille toimitettava rakentamislupa- ja rakentamisvaiheen asiakirjat lopullisessa muodossaan sekä muut STUKin vaatimat asiakirjat ja selvitykset, joilla voidaan todentaa tietoturvallisuuden riittävä taso.

5.5 Käyttövaihe

512. Käyttövaiheessa luvanhakijan on toimitettava seuraavat asiakirjat ja näiden päivitykset STUKille hyväksyttäväksi:

1. Tietoturvallisuuden hallintajärjestelmän kuvaus.
2. Tietoturvallisuusriskien arviointisuunnitelma ja käytön aikaisten riskien arviointia koskevat tulokset.
3. Järjestelmätasoiset tietoturvallisuuskuvaukset, tietoturvallisuuteen liittyvien vyöhykkeiden kuvaus ja kokonaisarkkitehtuurikuvaus.
4. Tietoturvallisuusvaatimukset ja kuvaus tietoturvallisuuden testaamismenettelyistä.

513. Seuraavat asiakirjat ja näiden päivitykset on toimitettava STUKille tiedoksi:

1. Asiakirjojen ja tietojen luokitteluun ja käsittelyyn liittävät kuvaukset sekä tietosuojaus- ja menettelyohjeet.
2. Järjestelmien hankintaan ja ylläpitoon liittyvät tietoturvallisuusmenettelyohjeet.
3. Tietoturvallisuuden tavoitteet ja mittarit.
4. Tietoturvallisuuskoulutusohjelma.
5. Tietoturvallisuushäiriöihin liittyvät menettelyohjeet ja raportoinnit.
6. Tarkastusten ja katselmointien raportit.
7. Järjestelmien tietoturvallisuusdokumentaation ohjeistus (voi olla osana muuta dokumentaatiota) mukaan lukien tietoturvallisuustestaaminen ja näiden toteutuminen.
8. Järjestelmien suunnitteluohjeet mukaan lukien järjestelmien väliset yhteydet.
9. Kuvaus tunnistetuista suojattavista kohteista ja niihin liittyvistä suojausmenettelyistä.
10. Kuvaus tietoturvallisuusorganisaatiosta.
11. Ulkoisiin toimijoihin kohdistuvat tietoturvallisuuden valvontatoimet.

514. Perustelluista syistä tiedoksi toimitettavat asiakirjat tai vastaavat tiedot voidaan todentaa myös luvanhaltijan osoittamassa paikassa.

5.6 Käytöstäpoistovaihe

515. Luvanhaltijan on toimitettava STUKille hyväksyttäväksi selvitys menettelyistä, joilla tietoturvallisuus toteutetaan käytöstäpoistovaiheen aikana ennen käytöstäpoistotoimien aloittamista.

6 Säteilyturvakeskuksen valvontamenettelyt

6.1 Periaatepäätösvaihe

601. Ydinenergia-asetuksen (161/1988) [15] 25 §:n mukaisesti *Säteilyturvakeskuksen on liitettävä periaatepäätöshakemuksesta antamaansa alustavaan turvallisuusarvioon YEL 56 § 2 momentissa tarkoitetun neuvottelukunnan lausunto.*

6.2 Rakentamislupavaihe

602. Rakentamislupaa haettaessa STUK antaa hakemusta koskevan lausunnon työ- ja elinkeinoministeriölle ja liittää lausuntoon laatimansa turvallisuusarvion ja YEA 35 §:n mukaisia asiakirjoja koskevan arvion. Turvallisuusarviota valmistellessaan STUK pyytää sisäasiainministeriöltä lausunnon YEA 35 §:n kohdassa 6 tarkoitetuista selvityksistä, jotka koskevat turva- ja valmiusjärjestelyjä [15].

603. STUK todentaa luvussa 5.2 mainittujen asiakirjojen ja niihin liittyvien tai niissä esiteltyjen menetelmien ja ratkaisujen kattavuuden asiakirjatarkastuksin ja tarkastusten avulla. Tarkastukset voivat olla ennalta ilmoitettuja tai ilmoittamattomia. Edellä mainituille suunnitelmille ja asiakirjoille sekä niitä koskeville muutoksille on hankittava STUKin hyväksyntä tai ne on toimitettava tiedoksi, kuten luvussa 5.2 on mainittu.

604. Rakentamislupahakemuksen käsittelyn aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset voivat integroitua osaksi muuta STUKin suorittamaa tarkastustoimintaa.

605. Rakentamislupahakemuksen käsittelyn aikana STUK voi osallistua harkintansa mukaan luvanhakijan tekemiin tietoturvallisuuteen liittyviin tarkastuksiin ja katselmointeihin. Tarkastuksista ja katselmoinneista on ilmoitettava riittävän ajoissa.

6.3 Rakentamisvaihe

606. Luvussa 5.3 mainituille suunnitelmille ja asiakirjoille sekä niitä koskeville muutoksille on hankittava STUKin hyväksyntä tai ne on toimitettava tiedoksi, kuten luvussa 5.3 on mainittu. STUK todentaa edellä mainittujen asiakirjojen ja niihin liittyvien tai niissä esiteltyjen menetelmien ja ratkaisujen kattavuuden asiakirjatarkastuksin ja tarkastusten avulla. Tarkastukset voivat olla ennalta ilmoitettuja tai ilmoittamattomia.

607. Rakentamisen aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset voivat integroitua osaksi muuta STUKin suorittamaa tarkastustoimintaa.

608. STUK voi osallistua harkintansa mukaan rakentamisen aikaisiin luvanhakijan tekemiin tietoturvallisuuteen liittyviin tarkastuksiin ja katselmointeihin. Tarkastuksista ja katselmoinneista on ilmoitettava STUKille riittävän ajoissa.

6.4 Käyttölupavaihe

609. Käyttölupaa haettaessa STUK antaa hakemusta koskevan lausunnon työ- ja elinkeinoministeriölle ja liittää lausuntoon laatimansa turvallisuusarvion ja YEA 36 §:n mukaisia asiakirjoja koskevan arvion. Turvallisuuden kokonaisarviota valmistellessaan STUK käsittelee myös tietoturvallisuuden hallintaa ja pyytää sisäasiainministeriöltä lausunnon YEA 36 §:n kohdassa 7 tarkoitetuista selvityksistä, jotka koskevat turva- ja valmiusjärjestelyjä [15].

610. STUK todentaa luvussa 5.4 mainittujen asiakirjojen ja niihin liittyvien tai niissä esiteltyjen menetelmien ja ratkaisujen kattavuuden asiakirjatarkastuksin ja tarkastusten avulla. Tarkastukset voivat olla ennalta ilmoitettuja tai ilmoittamattomia.

611. Käyttölupavaiheen aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset voivat integroitua osaksi muuta STUKin suorittamaa tarkastustoimintaa.

6.5 Käyttövaihe

612. Suunnitelmille ja asiakirjoille sekä niitä koskeville muutoksille on hankittava STUKin hyväksyntä tai ne on toimitettava tiedoksi, kuten luvussa 5.5 on mainittu. STUK todentaa luvussa 5.5 mainittujen asiakirjojen ja niihin liittyvien tai niissä esiteltyjen menetelmien ja ratkaisujen kattavuuden asiakirjatarkastuksin ja tarkastusten avulla. Tarkastukset voivat olla ennalta ilmoitettuja tai ilmoittamattomia.

613. Käytön aikaiset tietoturvallisuuteen ja turvallisuuskulttuuriin liittyvät tarkastukset voivat nivoutua osaksi muuta STUKin suorittamaa tarkastustoimintaa.

614. Käytön aikaisiin luvanhakijan tekemiin tietoturvallisuuteen liittyviin tarkastuksiin ja katselmointeihin STUK voi osallistua harkintansa mukaan. Tarkastuksista ja katselmoinneista on ilmoitettava riittävän ajoissa.

615. STUK valvoo tietoturvallisuuden hallintajärjestelmän toimintoja osana käytön valvonnan tarkastusohjelmaa. Lisäksi STUK tekee tarkastuksia luvanhaltijan pyynnöstä ja harkintansa mukaan. Tarkastukset voivat kohdistua luvanhaltijaan tai luvanhaltijan käyttämään toimittajaan. Tarkastukset voivat olla ennalta ilmoitettuja tai ilmoittamattomia.

6.6 Käytöstäpoistovaihe

616. STUK valvoo käytöstäpoistovaiheessa luvanhaltijan tietoturvallisuuteen liittyvien tietojen tallettamista sekä tietojen ja järjestelmien turvallista tuhoamista.

617. STUK valvoo, että tietoturvallisuustoiminnot ovat riittävät lainvastaisen uhkan torjumiseen ja ydinturvallisuuden varmistamiseen myös käytöstäpoistovaiheessa.

618. STUK todentaa käytöstäpoistovaiheeseen liittyvien asiakirjojen ja niihin liittyvien tai niissä esiteltyjen menetelmien ja ratkaisujen kattavuuden asiakirjatarkastuksin ja tarkastusten avulla. Tarkastukset voivat olla ennalta ilmoitettuja tai ilmoittamattomia.

Määritelmät

Riskianalyysi

Riskianalyysillä tarkoitetaan järjestelmällisin menetelmin tehtäviä selvityksiä uhkien, ongelmien ja haavoittuvuuksien tunnistamiseksi, niiden syiden ja seurauksien kartoittamiseksi sekä niihin liittyvien riskien arvioimiseksi (VNA 734/2008).

Turvajärjestelyt

Turvajärjestelyillä tarkoitetaan ydinenergian käytön turvaamiseksi lainvastaiselta toiminnalta tarvittavia toimenpiteitä ydinlaitoksessa, sen alueella taikka muussa paikassa tai kulkuvälineessä, jossa ydinenergian käyttöä harjoitetaan.

Järjestelmä (tietoturvallisuuteen liittyvä)

Tietoturvallisuuteen liittyvällä järjestelmällä tarkoitetaan Ihmisistä, tietojenkäsittelylaitteista, datansiirtolaitteista ja ohjelmista koostuvaa järjestelmää, jonka tarkoitus on tietoja käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi. Järjestelmä voi olla esimerkiksi tieto-, tietoliikenne-, sähkö- tai automaatiojärjestelmä tai turvavalvonnan ja valmiustoiminnan viestintäjärjestelmä.

Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmällä tarkoitetaan sitä osaa ydinlaitoksen yleisestä johtamisjärjestelmästää, joka luodaan ja toteutetaan ja jota käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan jatkuvasti. Tietoturvallisuuden hallintajärjestelmä sisältää organisaatiorakenteen, tietoturvallisuuden hallintapolitiikan, suunnittelutoimenpiteet, vastuut, menettelytavat, menetelmät, prosessit ja resurssit.

Viitteet

1. Ydinenergialaki (990/1987).
2. Valtioneuvoston asetus ydinenergian käytön turvajärjestelyistä (734/2008).
3. Valtioneuvoston asetus ydinvoimalaitoksen turvallisuudesta (717/2013).
4. Laki viranomaisten toiminnan julkisuudesta (621/1999).
5. ISO/IEC 27002. Information technology — Security techniques — Code of practice for information security management.
6. ISO/IEC 27001:fi. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden Hallintajrjestelmät. Vaatimukset.
7. ISO/IEC 27005. Information technology – Security techniques – Information security risk management.
8. IEC 62443 -sarja.
9. Vahti 6/2006. Tietoturvatavoitteiden asettaminen ja mittaaminen.
10. Vahti 2/2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta.
11. Vahti 1/2013. Sovelluskehityksen tietoturvaohje.
12. COBIT. Control Objectives for Information and Related Technology.
13. KATAKRI II kansallinen turvallisuusauditointikriteeristö, kuitenkin uusin EK:n vahvistama versio.
14. NIST 800 -sarja.
15. Ydinenergia-asetus (161/1988).
16. Valtioneuvoston asetus ydinenergia-asetuksen muuttamisesta (755/2013).
17. Valtioneuvoston asetus ydinjätteiden loppusijoituksen turvallisuudesta (736/2008).
18. ISO/IEC 31000. Riskienhallinta. Periaatteet ja ohjeet.