Regulaation vaikutus ydinvoimalaitoksen turvajärjestelyjen uhkienhallintaan

16. Turvallisuusjohdon koulutusohjelma

Kehitysprojektin raportti

Timo Summa

Sigma Consulting Oy

Helsinki 4.5.2020

Aalto University Professional Development – Aalto PRO

Tiivistelmä

Uhkien hallinta on keskeinen osa yritysten johtamista. Se tavoitteena on tukea yrityksen strategian toteutumista ja liiketoiminnallisten tavoitteiden saavuttamista sekä ehkäistä kielteisten vaikutusten syntymistä yrityksessä ja sen toimintaympäristössä.

Ydinvoimatoimialaan liittyvällä regulaatiolla ja valvovan viranomaisen asettamilla vaatimuksilla tulisi olla vaikutus yrityksen arvoihin ja sitä kautta myös keskeisiin liiketoiminnan vaatimuksiin ja yrityksen johtamisjärjestelmään. Viranomaisvaatimukset ovat kuitenkin hyvin korkean tason vaatimuksia, joiden tulkinnassa yrityskohtaisessa toteutustavassa on paljon tulkinnanvaraan.

Tässä tutkielmassa pyritään tulkitsemaan sitä, miten viranomainen pyrkii ohjaamaan regulaatiolla ydinvoimatoimialan yrityksiä, ja miten yrityksen on huomioitava regulaation asettamat vaatimukset osana uhkaperusteista toiminnan suunnittelua. Uhkaperusteinen toiminnan suunnittelu auttaa yritystä ennakoimaan liiketoimintaan kohdistuvia uhkatilanteita, ja hallitsemaan liiketoiminnan haavoittuvuuksia. Hyvä johtamiskulttuuri ja turvallisuuskulttuuri luovat pohjan jatkuvalle turvallisuuden kehittämiselle.

Toimialan regulaatio antaa toiminnalle reunaehtoja, mutta yritys on itse vastuussa liiketoimintansa kannattavuudesta ja siihen tehtävistä investoinneista. Uhkaperusteisessa ajattelussa lähtökohtana on tunnistaa yrityksen suojattava omaisuus ja muodostaa omaisuudelle riittävä suoja uhkia vastaan.

Uhkien vaikutuksen pienentämiseksi uhat on tunnistettava ja analysoitava niiden perusteella liiketoimintaan kohdistuvat riskit sekä haavoittuvuudet.

Yrityksen toimintaa tulee arvioida jatkuvasti. Uuden uhan ilmetessä tulee tarkastella uhan vaikutusta turvallisuuskulttuuriin, johtamisjärjestelmään, organisointiin, prosesseihin, toimintoihin ja ohjeistukseen.

Alkusanat

Tämä tutkielma on tehty Aalto PROn Turvallisuusjohdon koulutusohjelman TJK16 lopputyönä. Koulutuksen ja tutkielman rahoittajana on toiminut Sigma Consulting Oy.

Haluan kiittää tutkielmani ohjaajana ja tarkastajana toiminutta Jani Kalliota, joka on antanut hyödyllisiä neuvoja ja lähdeaineistoja tutkielmaani varten.

Lisäksi haluan kiittää seuraavia henkilöitä tutkielmani kommentoinnista ja tutkielmaan annetuista kehittämisehdotuksista:

Kari Eronen, Satu Summa.

Sisältö

1 Johdanto

Yrityksen liiketoimintaa kohdistuu jatkuvasti uhkia. Uhkien hallinnan tavoitteena on tukea yrityksen liiketoimintaa sekä yrityksen tavoitteiden toteuttamista, ja siten varmistaa osaltaan liiketoiminnan jatkuvuutta. Uhkien hallinnan tulee olla osana yrityksen perusprosesseja, ja siten vaikuttaa kiinteästi yrityksen tapaan implementoida turvallisuusajattelu yrityksen strategiseen suunnitteluun ja toiminnan kehittämissuunnitteluun.

Liiketoiminnan uhkien arviointi ja liiketoiminnan haavoittuvuuksien arviointi ovat merkittäviä yrityksen ennaltaehkäiseviä toimia, joilla voidaan vaikuttaa yrityksen riskitason pienentämiseen.

Turvallisuus- ja huoltovarmuuskriittisissä yrityksissä, kuten ydinvoimayrityksissä, on lisäksi vahva valvovan viranomaisen määrittelemä lainsäädäntö ja regulaatiopohjainen vaatimus ottaa huomioon merkittävät yhteiskunnalliset ja toimialasidonnaiset uhkakuvat.

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] [4:101]. Velvoitteita sisältyy myös Suomen tekemiin kansainvälisiin ydinenergia-alan sopimuksiin, hallitusten välisiin muihin sopimusjärjestelyihin sekä Suomen antamiin sitoumuksiin [17] [18].

Ydinlaitosten turvajärjestelyjä valvovana viranomaisena toimii ydinenergialain 55 §:n mukaisesti Säteilyturvakeskus (STUK). Turva-järjestelyistä vastaa ydinenergialain 9 §:n mukaisesti luvanhaltija siltä osin, kuin nämä tehtävät eivät kuulu viranomaisille [4:102].

STUK on valtioneuvoston asetuksen (734/2008) [2] perusteella asettanut vaatimukset ydinlaitosten turvallisuudelle. STUK noudattelee ohjeistuksessaan

ja vaatimusten asettelussaan IAEAn (International Atomic Energy Agency) antamia suorituksia ydinturvallisuuteen liittyen.

Suomessa on useita voimakkaasti reguloituja toimialoja, joista merkityksellisimpiä ovat lääketeollisuus, vakuutus-, finanssiala, ilmailuala sekä ydinvoima-ala. Näistä toimialoista tässä tutkielmassa keskitytään ydinvoima-alan turvajärjestelyihin kohdistuvaan regulaatioon ja siinä lähinnä STUKin turvajärjestelyjä koskevaan määräyksiin ja ohjeistukseen.

1.1 Tutkimustavoitteet

Tutkielman päätavoitteena on arvioida turvajärjestelyihin liittyvän regulaation ja ohjeistuksen soveltuvuutta ja vaikutusta ydinvoima-alan yrityksen tapaan johtaa, suunnitella ja implementoida uhka- ja riskiperusteinen ajattelu yrityksen toimintaan.

Tutkimuksessa arvioidaan, miten regulaation asettamat vaatimukset tukevat uhkaperusteista lähestymistapaa, sekä arvioidaan regulaation kyvykkyyttä ohjata yrityksen toimintaa uhka- ja riskiperusteiseen toimintamalliin.

Erityistä huomiota kiinnitetään STUKin turvajärjestelyihin liittyvän ohjeen YVL A.11 [4] merkitykseen turvajärjestelyjä ohjaavana ohjeistuksena.

Vaikka tässä tutkielmassa asiaa tarkastellaan ydinvoimayhtiön turvajärjestelyjen näkökulmasta, on huomiot pyritty yleistämään sellaiselle tasolle, että niitä pystytään soveltamaan myös muille toimialoille.

1.2 Tutkimusmenetelmät

Tutkimus on tehty julkisen kirjallisuus- ja asiakirjalähteiden pohjalta. Tutkijan oman tarkasteluun ja vertailuun perustuen tutkielmassa arvioidaan parhaita menettelyjä regulaation asettamien vaatimuksien toteuttamiseksi.

Tutkimuksessa nostetaan esille regulaation turvajärjestelyille asettamia vaatimuksia ja analysoidaan niiden merkitystä yrityksen toimintaan tai toimintaprosesseihin.

Tutkielman sisällön arviointiin ja tutkielman tarkastamiseen on osallistunut Fennovoiman turvajärjestelyjen suunnitteluun osallistuvia henkilöitä.

1.3 Rajaukset

Tutkimuskohdetta käsitellään ydinenergiayrityksen kohdistuvan regulaation rajaamana. Ydinenergia-alalla perusarvona on ydinvoiman käytön turvallisuus, joka ilmenee toiminnan kolmena peruspilarina Safety, Safe Guard ja Security. Näistä Safety keskittyy ydinvoiman käytön turvallisuuteen, Safe Guard ydinmateriaalin valvontaan ja Security lainvastaisen toiminnan estämiseen. Tässä tutkielmassa ei käsitellä Safety ja Safe Guard -vaatimuksia, vaan tutkielmassa keskitytään ainoastaan tarkastelemaan asioita Security-näkökulmasta (turvajärjestelyt).

Tässä tutkielmassa ei kuvata uhkien määrittelyprosessia eikä riskienhallintaprosessia, vaan näitä prosesseja käsitellään yleisluonteisesti.

2 Tutkielman rakenne

2.1 Luvut

Luvussa 1 kuvataan johdanto, tutkimusmenetelmä ja tutkimuksen rajaus.

Luvussa 2 kuvataan tutkielman rakenne.

Luvussa 3 kuvataan keskeiset tässä tutkielmassa käytetyt käsitteet ja lyhenteet. Termeinä ja käsitteinä on pyritty käyttämään suomenkielisiä termejä ja käsitteitä. Mikäli termi tai käsite voi aiheuttaa tulkintaongelman, niin termistä tai käsitteestä on voitu käyttää myös englanninkielistä vastinetta. Englanninkielinen vastine voidaan ilmaista myös suluissa termin tai lyhenteen yhteydessä.

Luvussa 4 kuvataan keskeiset asiat liittyen yrityksen arvomaailmaan, johtamis- ja turvallisuuskulttuurin sekä politiikkojen ja strategian merkitys turvajärjestelyille.

Luvussa 5 kuvataan ydinenergiayrityksiin kohdistuvaa regulaatiota ja lainsäädäntöä yleisellä tasolla, niiltä osin kuin se kohdistuu turvajärjestelyihin.

Luvussa 6 kuvattaan suojattavaan pääomaan kohdistuvat vaatimukset ja suojauskeinot kriittisen pääoman suojaamiseksi uhka- ja riskienhallinnan menettelyin.

Luvussa 7 paneudutaan yrityksen johtamisjärjestelmään ja yrityksen tapaan järjestää jatkuva ja määräajoin tapahtuva toiminnan suunnittelu ja arviointitehtävät.

Luvussa 8 pureudutaan vaatimuksenmukaisuuteen ja sen todentamiseen.

Luvussa 9 arvioidaan toimina jatkuvuudenhallinnan merkitystä turvajärjestelyn tehokkuuden ja ajanmukaisuuden näkökulmasta.

Luvussa 10 arvioidaan uhkien ja riskinhallinnan merkitystä, ja niitä keinoja joilla ne sidotaan yrityksen päivittäistoimintaan. Luvussa paneudutaan uhkien luokitteluun sekä uhka-analyysien ja riskianalyysien merkitykseen. Luvussa arvioidaan myös uhkaperusteisen toimintamallin vaikutusta turvajärjestelyjen kehittämiseen ja suunnitteluun.

Luvussa 11 arvioidaan, miten jatkuvan kehittämisen vaatimus huomioidaan yrityksen toiminnassa uhkien ja riskien hallinnan näkökulmasta.

Luvussa 12 on tutkielman yhteenveto, ja tutkielman tekijän näkemys regulaation ohjaavuudesta ydinvoimalaitoksen turvajärjestelyjen toimintaan ja turvajärjestelyjen suunnitteluun.

Luvussa 13 on viiteluettelo käytettyihin lähdeaineistoihin.

2.2 Lukujen rakenne

Mikäli luvun aihealue on regulaation tai viranomaisohjeistuksen alaista, kappaleen ***regulaatio-osassa*** kuvataan, miten regulaattori pyrkii ohjaamaan yrityksen toimintaa esittämillään vaatimuksilla ja ohjeilla.

Jokaisessa Luvussa on ***hyvät käytännöt*** **-osassa**, jossa kuvataan ydinvoimayrityksen hyviä käytäntöjä, jotka osittain voidaan johtaa ydinenergia-alan regulaatiosta ja ohjeistuksesta.

Mikäli kappaleen aihealue on säännöstelyn tai viranomaisohjeistuksen alaista, kappaleen ***arviointiosassa*** arvioidaan, miten regulaatio on onnistunut ohjauksessaan, ja mitkä ovat ohjauksen keskeiset haasteet.

3 Keskeiset käsitteet ja lyhenteet

Business Impact -analyysi (BIA) - on menetelmä, jolla erityisesti keskeytysriskin vaikutuksia voidaan arvioida organisaation toimintaan liittyen. Sen avulla voidaan tunnistaa organisaation kriittiset prosessit, toiminnot ja niihin liittyvät resurssit sekä näiden väliset riippuvuudet. Lisäksi BIA:n avulla voidaan tunnistaa keskeytysriskin vaikutukset organisaation tavoitteiden saavuttamiseen sekä keskeytysriskien hallitsemisen ja keskeytymisestä toipumisen edellyttämät kyvykkyydet ja resurssit. BIA:n arviointimenetelmässä kuvataan myös koko toimitusketju (Supply Chain), jotta kaikki operatiiviset riskit niin omassa kuin kumppaninkin verkossa voitaisiin tunnistaa ja arvioida. BIA soveltuukin hyvin operatiivisiin riskeihin kuuluvan liiketoiminnan jatkuvuus -osa-alueen riskiarviointimenetelmäksi (47 ISO/IEC 31010:2009, s. 43).

Haavoittuvuus - voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Esimerkiksi ohjelmistossa voi olla haavoittuvuus, joka mahdollistaa järjestelmän väärinkäytön (Sanastokeskus TSK ry).

Heikkous järjestelmässä tai ryhmässä järjestelmiä, joka voidaan hyödyntää yhteen tai useampaan uhkaan (International Organization for Standardization, 2005).

Haavoittuvuudella tarkoitetaan riskien hallintaan liittyvää epävarmuutta, joka uhkaa organisaation toimintaa (Vahti-ohje).

Huoltovarmuuskriittinen organisaatio – Organisaatio, joka on erityisen merkittävä yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta. Huoltovarmuuskriittinen organisaatio voi olla yritys tai muu organisaatio (Huoltovarmuuskeskus – sanasto).

International Atom Energy Agency (IAEA) - The IAEA is the world's centre for cooperation in the nuclear field and seeks to promote the safe, secure and peaceful use of nuclear technologies (IAEA).

Konfiguraationhallinta – On prosessi, jonka vastuulla on varmistaa, että palvelujen tuottamiseen tarvittavaa palveluomaisuutta hallitaan oikealla tavalla, ja että omaisuudesta on saatavilla tarkkaa ja luotettavaa tietoa milloin ja missä sitä tarvitaankin. Tämä tieto sisältää yksityiskohtia siitä, miten omaisuuserät ovat konfiguroitu, ja mitkä ovat omaisuuserien väliset suhteet (ITIL-sanasto).

Lainvastainen toiminta (unlawful action) - Lainvastaisella toiminnalla tarkoitetaan toimintaa tai toimenpidettä, jonka tarkoituksena on välitön tai välillinen ydinlaitoksen, ydinmateriaalin tai ydinjätteen ydin- tai säteilyturvallisuuden vaarantaminen. Tällaisena toimintana tai toimenpiteenä pidetään ydinlaitokseen, ydinmateriaaliin tai ydinjätteeseen tai ydinlaitoksella oleviin henkilöihin kohdistuvaa tahallista tai tuottamuksellista toimintaa, joka lainsäädännössä on säädetty rangaistavaksi (STUK Y/3/2016).

Luokitteleva lähestymistapa (graded approach) - Luokittelevalla lähestymistavalla tarkoitetaan periaatetta, jonka mukaisesti turvajärjestelyjen vaatimusten asettamisessa ja turvajärjestelyjen suunnittelussa ja toteutuksessa otetaan huomioon kulloinenkin uhka-arvio, ydinaineiden ominaisuudet sekä ydinaineisiin kohdistuvan lainvastaisen toiminnan mahdolliset seuraukset.

Luvanhaltija/lisenssinhaltija - Luvanhaltijalla tarkoitetaan ydinenergian käyttöön oikeuttavan luvan haltijaa (YEL 990/1987).

Regulaatio – Regulaatiolla, tässä tutkielmassa tarkoitetaan sitä lainsäädäntöä, säädöspohjaa ja muuta viranomaisen antamaan ohjeistoa, joka säätelee ydinvoima-alan turvajärjestelyjen (Security) toimialaa.

Riski – todennäköisyys, että uhka toteutuu aiheuttaen tietyn menetyksen tai vahingon (VAHTI 8/2008).

Riskianalyysi (risk analysis) - Riskianalyysillä tarkoitetaan järjestelmällisin menetelmin tehtäviä selvityksiä uhkien, ongelmien ja haavoittuvuuksien tunnistamiseksi, niiden syiden ja seurauksien kartoittamiseksi sekä niihin liittyvien riskien arvioimiseksi (STUK Y/3/2016). Katso myös luku 3.1 Käsitteistä ja terminologiasta.

Riskienhallinta - järjestelmällinen toiminta riskien rajoittamiseksi niin, että ne ovat optimisuhteessa riskien rajoittamisen kustannuksiin samalla kun organisaation toiminnalle asetetut tavoitteet voidaan saavuttaa.

Riskienhallinnan vaiheita ovat riskianalyysi, riskienhallintamenetelmän

valinta, päätös riskien poistamisesta, alentamisesta tai pitämisestä omalla vastuulla, sekä riskienhallinnan organisointi (VAHTI 8/2008).

Sisäinen uhka - organisaation oman henkilöstön toiminnasta aiheutuva uhka (VAHTI 8/2008).

Säteilyturvakeskus (**STUK**) - on sosiaali- ja terveysministeriön hallinnonalan viranomainen, joka valvoo säteily- ja ydinturvallisuutta Suomessa. Tavoitteenamme on ihmisten, yhteiskunnan, ympäristön ja tulevien sukupolvien suojelu säteilyn haitallisilta vaikutuksilta (STUK).

Suunnitteluperusteuhka Design Based Threat (DBT) -

Suunnitteluperusteuhalla tarkoitetaan lainvastaisen toiminnan uhkaa, jota käytetään luvanhaltijan vastuulla olevien turvajärjestelyjen suunnittelun ja arvioinnin perusteena (734/2008).

Turvallisuus (Safety) – Turvallisuudella tarkoitetaan tässä dokumentissa ydinturvallisuutta, jolla on yleisestä käytännöstä poikkeava merkitys ydinvoima-alalla. Säteilyturvallisuus on ydinvoima-alalla osa turvallisuutta.

Turvajärjestelyt (Security arrangements) - Turvajärjestelyillä tarkoitetaan ydinenergian käytön turvaamiseksi lainvastaiselta toiminnalta tarvittavia toimenpiteitä ydinlaitoksessa, sen alueella taikka muussa paikassa tai kulkuvälineessä, jossa ydinenergian käyttöä harjoitetaan (990/1987).

Turvaorganisaatio (security organisation) - Turvaorganisaatiolla tarkoitetaan ydinlaitoksen turvajärjestelyjä suunnittelevan, toteuttavan tai valvovan henkilöstön muodostamaa työyhteisöä ja toiminnanharjoittajan omalla turvaorganisaatiolla vastaavasti suoraan toiminnanharjoittajan palveluksessa olevaa vastaavan henkilöstön muodostamaa työyhteisöä.

Uhka (Threat) - On haitallinen tapahtuma, joka voi mahdollisesti toteutua, tai useampi mahdollinen häiriö, joka tapahtuessaan voi aiheuttaa sen että tiedoille, muulle omaisuudelle tai toiminnalle tapahtuu ei-toivottua (VAHTI 8/2008).

Uhkienhallinta - organisaation prosessi, jolla tunnistetaan toiminnan uhkat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa.

Uhkatilanne - Uhkatilanteella tarkoitetaan tilannetta, jossa todetaan tai on syytä epäillä ydinlaitokseen taikka ydinmateriaaliin tai ydinjätteeseen kohdistuvaa lainvastaista toimintaa (734/2008).

Valmiusjärjestelyt - Valmiusjärjestelyillä tarkoitetaan varautumista ennakkoon onnettomuuksiin tai turvallisuutta heikentäviin tapahtumiin ydinlaitoksessa tai sen alueella taikka muussa paikassa tai kulkuvälineessä, jossa ydinenergian käyttöä harjoitetaan(990/1987).

Viranomainen – viranomainen, joka säätelee ydintoimialalla tapahtuvaa toimintaa. Keskeisestä sääntelystä vastaa STUK.

Ydinlaitos - Ydinlaitoksella tarkoitetaan ydinenergian aikaansaamiseen käytettäviä laitoksia, tutkimusreaktorit mukaan luettuina, ydinjätteiden laajamittaista loppusijoitusta toteuttavia laitoksia sekä ydinaineen ja ydinjätteen laajamittaiseen valmistamiseen, tuottamiseen, käyttämiseen, käsittelyyn tai varastointiin käytettäviä laitoksia (YVL A.11)

Ydinvoimalaitos - Ydinvoimalaitoksella tarkoitetaan sähkön tai lämmön tuotantoon tarkoitettua ydinreaktorilla varustettua ydinlaitosta tai samalle laitospaikalle sijoitettujen ydinvoimalaitosyksiköiden ja niiden yhteydessä toimivien muiden ydinlaitosten muodostamaa laitoskokonaisuutta (990/1987).

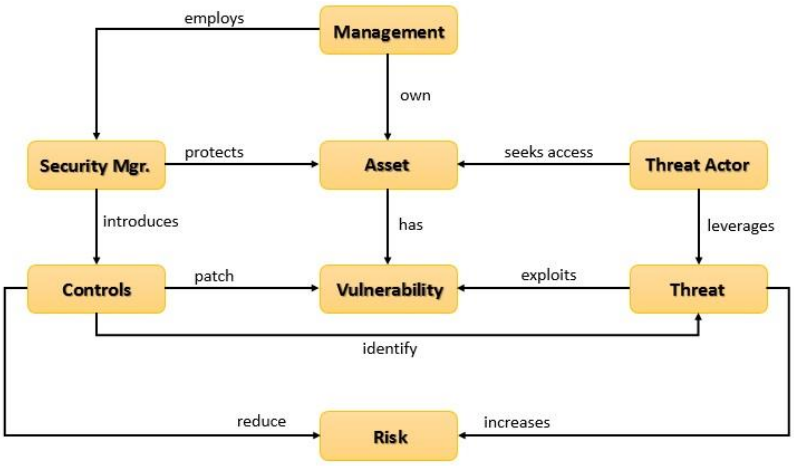
3.1 Käsitteistä ja terminologiasta

Lukijaa pyydetään kiinnittämään huomiota, että ydinvoima-alalla suomen kielisissä teksteissä käsitteellä *turvallisuus* käsitetään ydinturvallisuutta. Englannin kielisessä ydinvoima-alan kirjallisuudessa termille turvallisuus on oma käsite *Safety*.

Tässä tutkielmassa tekstissä käsitteellä *turvajärjestelyt* käsitetään turvajärjestelyjen johtamista, tietoturvallisuutta ja fyysistä turvallisuutta. Tämä käsite ei siis kata kaikkia EK-mallissa kuvattuja turvallisuuden osa-alueita. Englannin kielisessä ydinvoima-alan kirjallisuudessa termille turvajärjestelyt on käsite *Security arrangements*.

STUKin käyttämä määritelmä riskianalyysistä, ”Riskianalyysillä tarkoitetaan järjestelmällisin menetelmin tehtäviä selvityksiä uhkien, ongelmien ja haavoittuvuuksien tunnistamiseksi, niiden syiden ja seurauksien kartoittamiseksi sekä niihin liittyvien riskien arvioimiseksi”, voi aiheuttaa tulkintaongelmia. Tämä johtuen siitä, että välillä STUKin ohjeissa käytetään uhka-analyysiä ja välillä riskianalyysiä samassa merkityksessä. Tutkielman muissa teksteissä kuin regulaation vaatimuksissa on pyritty tekemään selkeä ero uhka-analyysille ja riskianalyysille.

Kuvan 1. kaaviossa on pyritty kuvaamaan keskeiset englanninkieliset käsitteet ja niiden riippuvuussuhteet toisiinsa. (https://nigesecurityguy.files.wordpress.com/2013/06/risk-analysis.jpg)



Kuva 1 Käsitteiden riippuvuussuhteet

4 Yrityksen arvomaailma

Yrityksen tulee sisäistää ne yhteiskunnalliset vaatimukset ja velvoitteet, jotka koskettavat yrityksen toimialaa ja yritystä itseään. Voimakkaasti reguloiduilla toimialoilla valvovien viranomaisten asettamat vaatimukset toiminnalle on otettava huomioon yrityksen toimintaperiaatteissa.

Yrityksen arvot ja turvallisuuskulttuurin tulee luonnollisesti perustua toimialalta edellytettyihin vaatimuksiin. Yrityksen arvomaailma ei kuitenkaan voi perustua ainoastaan regulaation asettamien vaatimusten täyttämiseen, vaan yrityksellä on velvoite tuottaa voittoa omistajilleen [5: 5 §]. Omistajien vaatimukset yritykselle tarkoittavat luonnollisesti liiketoiminnan kannattavuutta, hyvää johtamista ja toimivia prosesseja. Tämä voi aiheuttaa ristiriitaa tulkinnassa siitä, miten lain, asetuksen ja viranomaisen määräyksiä on tulkittava ja missä laajuudessa sekä millä kustannustasolla ne voidaan toimeenpanna.

Ydinenergiatoimialalla erityisesti hyvän turvallisuuskulttuurin edellytetään olevan yksi keskeisistä yrityksen arvoista [20: s.15]. Ydinvoimalan regulaatio korostaakin hyvän turvallisuuskulttuurin välttämättömyyttä ennaltaehkäisemään vakavien onnettomuuksien mahdollisuutta.

Missio

Huoltovarmuuskriittisissä yrityksissä, joihin ydinvoimayritykset kuuluvat, yrityksen tulee kiinnittää huomiota yrityksen yhteiskunnalliseen merkitykseen ja yrityksen merkitykseen osana Suomen huoltovarmuutta. Vaikka yritys pyrkii toteuttamaan omia liiketoiminnallisia päämääriään, on yrityksen arvioitava oma roolinsa yhteiskunnassa ja osana yhteiskunnan toiminnallista rakennetta [24].

Yrityksen missio ei yleensä sisällä lausumia turvajärjestelyjen merkityksestä, vaan missio lausumat keskittyvät osoittamaan yrityksen olemassaolon merki-

tystä. Turvallisuuskriittisessä yrityksessä olisi kuitenkin hyvä luoda turvajärjestelyistä vastaavalle toiminnolle oma missio, joka osaltaan tukee yrityksen missiota, mutta täsmentää turvaorganisaation ja turvajärjestelyjen merkityksen liiketoiminnan tukifunktiona ja siten myös turvajärjestelyjen merkitystä huoltovarmuuskriittisessä yrityksessä jatkuvuudenhallinnan merkittävänä osatekijänä.

VNA 717/2013 28 §:n mukaisesti ydinvoimalaitosta suunniteltaessa, rakennettaessa, käytettäessä ja käytöstä poistettaessa on ylläpidettävä hyvää turvallisuuskulttuuria [4: 302].

4.1 Arvot

Ydinvoimalaitoksen turvajärjestelyjen keskeisenä arvona on toiminnan jatkuvuuden turvaaminen. Turvajärjestelyjen tulee mahdollistaa joustava liikkuminen ydinvoimalaitoksen alueella ja samalla valvoa alueella tapahtuvaa toimintaa sekä reagoida mahdollisiin turvapoikkeamiin.

Uhka- ja häiriötilanteissa tulee pystyä palautumaan normaalitilanteeseen mahdollisimman nopeasti ja mahdollisimman pienin haittavaikutuksin.

Regulaatio

Keskeisenä ydinvoima-alaa turvajärjestelyjä koskevassa regulaatiossa on, että ydinvoimayritys perustaa toimintansa suunnittelun vakavien onnettomuustilanteiden ennaltaehkäisyyn. Turvajärjestelyjen osalta tämä tarkoittaa varautumista lainvastaiseen toimintaan ydinvoimalaitoksella. Regulaation lähtökohta on hyvin ydinturvallisuuskeskeinen ja keskittyy siihen, että ydinvoimalaitokseen kohdistuvasta uhasta ei aiheudu säteilyvaaraa.

Hyvät käytänteet

Määriteltäessä turvajärjestelyihin liittyviä arvoja, tulee edellytyksenä olla, että turvajärjestelyjä johdetaan hallitusti, ja toiminta tulee olla suunniteltujen prosessien ja ohjeistuksen mukaista, sekä dokumentoitua.

Arviointi

Turvajärjestelyihin liittyvän regulaation perusteella voisi olettaa, että keskeisenä ydinvoimayrityksen arvona tulisi olla turvallinen toimintaympäristö. Regulaatio painottaa hyvää turvallisuuskulttuuria ja sen osana ydinturvallisuutta.

4.2 Turvallisuuskulttuuri

Yrityskulttuurilla ja turvallisuuskulttuurilla on suuri merkitys siihen, miten yritys selviytyy sitä uhkaavista tilanteista. Turvallisuustietoinen yritys kykenee ennalta ehkäisemään uhkatilanteita sekä reagoimaan että toipumaan uhkatilanteista nopeammin.

Regulaatio

Regulaatio painottaa yrityksen turvallisuuskulttuurin merkitystä ja sen jatkuvaa kasvattamista.

Valtioneuvoston asetuksen (717/2013) [3] 28§:n mukaisesti Ydinvoimalaitosta suunniteltaessa, rakennettaessa, käytettäessä ja käytöstä poistettaessa on ylläpidettävä hyvää turvallisuuskulttuuria. Ydin- ja säteilyturvallisuus on asetettava etusijalle kaikessa toiminnassa. Kaikkien edellä mainittuun toimintaan osallistuvien organisaatioiden johdon on osoitettava päätöksillään ja toiminnallaan sitoutumisensa turvallisuutta edistäviin toimintatapoihin ja ratkaisuihin. Henkilöstöä on kannustettava vastuuntuntoiseen työskentelyyn ja turvallisuutta vaarantavien tekijöiden tunnistamiseen, raportointiin ja poistamiseen. Henkilöstöllä on oltava mahdollisuus osallistua turvallisuuden jatkuvaan kehittämiseen [6] [7] [8: 1].

Hyvät käytänteet

Yrityskulttuuri lähtee yrityksen ja sen johdon sitoutumisesta jatkuvaan yrityksen turvallisuuskulttuurin kehittämiseen.

Turvallisuuskulttuuriin suhtautuminen tulee olla holistinen, eli annettuja ohjeita ja määräyksiä tulee noudattaa. Holistinen lähestymistapa eri kuitenkaan tarkoita sitä, että rikkomuksista aina rangaistaisiin, vaan että tapahtuneista rikkeistä ja laiminlyönneistä keskustellaan avoimesti ja ohjataan toimintaa

ohjeistusta, opastusta ja koulutusta hyväksikäyttäen formaalimpaan toimintamalliin.

Turvallisuustietoisuuden lisääminen on tärkeää. Henkilöstölle, toimittajille ja urakoitsijoille suunnataan turvallisuuden ohjelma, jonka toteuttaminen edistää organisaation ja sen sidosryhmien turvallisuuskulttuuria. Vahva turvallisuustietoisuusohjelma edellyttää selkeitä turvallisuuspolitiikkoja, turvallisuuskäytäntöjen noudattamista ja jatkuvaa koulutusta (https://nigesecurityguy.wordpress.com/2013/06/20/threat-and-vulnerability-management/).

Ydinvoimayrityksen tulee sisällyttää jatkuva turvallisuuskulttuurin kehittäminen omaan toimintamalliinsa. Turvallisuuskulttuurin kehittäminen edellyttää, että turvallisuutta vaarantavat tekijät tunnistetaan. Tunnistamisessa on oleellista tunnistaa sekä ulkoiset että sisäiset uhat. Henkilöstölle ja urakoitsijoille suunnatun vahvan tietoturvaohjelman toteuttaminen edistää organisaation jatkuvaa turvallisuuskulttuurin kehittämistä. Vahva turvallisuustietoisuusohjelma edellyttää selkeitä turvallisuuspolitiikkoja, turvallisuuskäytäntöjen noudattamista ja jatkuvaa koulutusta.

Arviointi

Regulaation ohjaus on selkeä ja tavoitteellinen. Mikäli turvallisuuskulttuuria ei aloiteta rakentamaan heti yrityksen yhtenä perusajatuksena, on turvallisuuskulttuurin luominen jälkikäteen erittäin haastavaa tai osittain jopa mahdotonta.

Kulttuurin rakentaminen ei ole ainoastaan yritystason tehtävä vaan kaikkien toimintaan osallistuvien tahojen, sisäisten ja ulkoisten sidosryhmien, on omaksuttava ja hyväksyttävä yrityksen turvallisuuskulttuuri ja sen säännöt.

Toimintaa uhkaavat tekijät on pyrittämä arvioimaan mahdollisimman varhaisessa vaiheessa, ja ne on otettava huomioon suunniteltaessa yrityksen johtamismenettelyjä, yrityksen fyysistä toiminta ympäristöä sekä yrityksessä hyödynnettävää teknologiaa.

Yrityksen henkilöstön osalta tämä tarkoittaa jatkuvaa turvallisuustilanteen seuraamista, henkilöstön kouluttamista ja henkilöstön aktivoimista poikkeavien asioiden esilletuomiseen ja niiden parantamiseen. Turvallisuustietoisuutta on edistettävä suunnitelmallisesti.

4.3 Politiikat

Kuten edellisessä Luvussa todettiin, yrityksen laatimat turvallisuuteen liittyvät politiikat ovat tärkeä väline määriteltäessä niitä periaatteita, joita turvallisuuden suhteen yrityksessä halutaan noudatettavan.

Regulaatio

STUKin ohje YVL A.3 [8] täsmentää turvallisuuteen liittyvien politiikkojen merkitystä seuraavasti. ”Politiikassa on määriteltävä turvallisuuden ensisijaisuus toiminnassa ja päätöksenteossa. Politiikassa on lisäksi esitettävä turvallisuuteen ja laatuun liittyvät yleiset tavoitteet sekä sitoutuminen ydin- ja säteilyturvallisuuden kehittämiseen, hyvään turvallisuuskulttuuriin, korkeaan laatuun ja jatkuvaan parantamiseen.” [8: 323].

Hyvät käytänteet

Vaikuttavan turvallisuuskulttuurin aikaansaamiseksi on yrityksen määriteltävä tarvittavat politiikat, jotka tukevat turvallisuuskulttuurin rakentamista.

Keskeistä on löytää sellaiset yrityspolitiikan osa-alueet, joilla pystytään parhaiten vaikuttamaan turvallisuuskulttuurin syntyyn ja sen kehittämiseen. Turvajärjestelyjen kannalta merkityksellisiä politiikan osa-alueita ovat johtaminen, uhkien hallinta ja toiminnan kehittäminen. Politiikoista tulee tunnistaa regulaation keskeiset vaatimukset ja yrityksen arvot.

Politiikkojen tulee olla selkeitä ja niistä on pystyttävä johtamaan selkeät strategiat ja toiminnalliset vaatimukset politiikkojen toteuttamiseksi.

Yrityksellä tulee olla uhkien- ja riskienhallintapolitiikka. Politiikan on sisällettävä ne keskeiset tavoitteet, joilla varmistetaan regulaation täyttyminen ja yrityksen sisäiset periaatteet uhkien havaitsemiseksi ja torjumiseksi. Politiikoista johdetut toimintastrategiat, joilla toimintaa ohjataan ja kehitetään, ovat oleellinen osa yrityksen johtamista. Ilman selkeää strategiaa ja toimintaohjelmaa ei systemaattinen toiminnan kehittäminen ole mahdollista.

Arviointi

Regulaatio ottaa kantaa yrityksen politiikkoihin hyvin yleisellä tasolla, se ei täsmällisesti kerro millä toiminnan osa-alueilla pitää politiikkoja luoda. Regulaatio määrittelee politiikkojen keskeisiksi aihealueiksi turvallisuuden, laatuajattelun ja jatkuvaan toiminnan kehittämiseen.

Regulaatio jättää yritykselle paljon liikkumatilaa politiikkojen muodostamisessa.

4.4 Strategia

Hyvä toimintastrategia tunnistaa yrityksen nykytilan sekä toimintaympäristössä että toiminnassa tapahtuvat muutokset, ja on yhdenmukainen yrityksen arvomaailman ja politiikkojen kanssa. Strategia pyrkii kuvaamaan tavoitellun tilanteen strategiajakson päättyessä ja määrittelemään keinot tavoitteen saavuttamiseksi. Normaalisti strategiajakso on yksi vuosi tai muutamia vuosia.

Regulaatio

Ydinvoima-alan regulaatio tunnistaa strategisen suunnittelun merkityksen. Regulaatio edellyttää suunnitelmallisuutta ydinvoimalaitoksen rakentamisessa ja sen käytössä.

Johdon on laadittava strategiat ja toimintatavat sekä asetettava tavoitteet organisaatiolle. Näiden on tuettava turvallisuus- ja laatupolitiikan toteuttamista. Strategioiden, toimintatapojen ja tavoitteiden on oltava selkeitä ja johdonmukaisia ja niistä on tiedotettava henkilöstölle. Tavoitteiden toteuttamiseksi on oltava selkeät toimintasuunnitelmat ja menettelyt sekä riittävät resurssit [8: 411].

Hyvät käytänteet

Perinteisesti strategiat laaditaan kaupallisilla toimialoilla kilpailuedun saamiseksi, mutta ydintoimialalla regulaatio määrittelee strategiat ydinturvallisuuden tavoitteiden saavuttamiseksi.

Ydinvoimalaitoksia suunnitellaan, rakennetaan ja käytetään hyvin pitkäkestoisesti ja sen vuoksi tavoitteet on hyvä kuvata strategioiden välityksellä määräajoin tarkasteltaviksi ja tarkastettaviksi kokonaisuuksiksi.

Uhkien ja riskien hallinnan näkökulmasta kaksi merkittävää strategian osa-aluetta ovat turvallisuusstrategia ja varautumisstrategia. Näissä strategioissa tulisi määritellä kunkin edellä mainitun osa-kokonaisuuden aikaan sidotut vaihekohtaiset tavoitteet. Turvallisuusstrategian osana tai erillisenä strategiana tulisi käsitellä turvajärjestelyt -strategia.

Arviointi

Regulaatiossa olisi hyvä edellyttää muodostettavaksi strategisen suunnittelun eri tasot.

Strategisen suunnittelun tarve korostuu ydinvoimalaitoksen rakentamishankkeissa, joissa laitoksen elinkaari muodostuu suunnitteluvaiheesta, rakentamisvaiheesta, käyttöönottovaiheesta ja lopulta käyttövaiheesta. Jokaiselle näistä vaiheista pitäisi edellyttää myös vaihekohtaiset strategiat ja toimialakohtaiset/funktionaaliset strategiat. Toimialakohtaisilla strategioilla tarkoitetaan tässä yhteydessä vähintään niitä aihekokonaisuuksia, jotka yrityksen politiikoissa on määritelty tavoitteiksi.

Regulaatiossa ei ole riittävän hyvin eritelty missä ydinvoimalaitoksen rakentamisen ja käytön vaiheessa regulaation edellyttämät vaatimustenmukaisuus on oltava todennettavissa. Aihekohtaisissa strategioissa voitaisiin selventää missä vaiheessa vaaditut kyvykkyydet on tarkoitus saavuttaa, joka samalla helpottaisi myös dialogia lisenssinhaltijan ja viranomaisen välillä. Vaihtoehtona olisi tarkemmin kuvata regulaatiossa vaatimuskohtaisesti missä elinkaaren vaiheessa kyseisen vaatimuksen täyttyminen on oltava todennettavissa. Tämä helpottaisi ja selkiyttäisi myös strategioiden laadintaa.

5 Ydinvoima-alan sääntely turvajärjestelyjen näkökulmasta

Yrityksen on otettava toiminnassaan huomioon vallitseva lainsäädäntö. Tämä lisäksi toimialalla voi olla lukuisia määrääviä ohjeita tai käytäntöjä, jotka yrityksen tulee ottaa huomioon toimintaansa suunnitellessa. Ydinvoima-alan ohjeistus on laaja, kattaen keskeiset osat ydinvoimalaitoksen toiminnoista koko ydinvoimalaitoksen elinkaaren ajan.

Ydinvoiman käyttöä ohjaa Ydinenergialaki (990/1987) [1], jossa esitetään ydinenergian käyttöä koskevat perusvaatimukset ja lupamenettelyt, joka asettaa myös vaatimuksen turvajärjestelyjen uhka- ja riskiperusteiselle turvallisuuden suunnittelulle.

STUK on laatinut määräyksen [6], joka ohjaa ydinvoimaa käyttävien yritysten turvallisuussuunnittelua. Ydinenergialainsäädäntöön kirjattujen valtuuksien nojalla Säteilyturvakeskus julkaisee YVL-ohjeita, joissa esitetään sekä ydinenergian käyttöä koskevat yksityiskohtaiset turvallisuusvaatimukset että Säteilyturvakeskuksen työssään käyttämät valvontamenettelyt.

Kansallisen lainsäädännön lisäksi Suomea sitoo kansainvälinen sopimus ydinaseiden leviämisen estämisestä (11/1970) [9] ja ydinteknologian käytön valvonnasta.

Suomen lainsäädäntö, asetukset ja ohjeistus noudattelevat kansainvälisten sopimusten henkeä, joskin Suomessa käytössä oleva YVL-ohjeistus pyrkii laajentamaan ja tarkentamaan kansainvälisten suositusten asettamia vaatimuksia.

Turvajärjestelyjen suunnittelu

Ydinvoimalaitokselle suunniteltavat turvajärjestelyt on suunniteltava siten, että ne perustuvat uhka- ja riskiarvioon. Sekä kansainväliset yleissopimukset

että IAEAn ydinturvallisuuden ohjeet korostavat uhkien arvioinnin ja riskitietoisen lähestymistavan käyttöä ydinturvallisuudessa [10: 2,1].

IAEA:n lähestymistavan mukaisesti valtion ja sen viranomaisten tulisi perustaa valtion kriittisten toimintojen suojaaminen valtion nykyiseen uhan arviointiin. Ydinturvallisuuden hallinnassa tulee käyttää riskitietoisia lähestymistapoja, joissa otetaan huomioon valtion nykyinen arvio sekä sisäisistä että ulkoisista ydinturvallisuusuhista [10: 2.2].

Valtion tulee suunnitella ydinvoima-alaan kohdistuvat kansalliset uhkansa (suunnitteluperusteuhka) ja tarkastella määräajoin kansallista uhkaa ja arvioida uhan muutosten vaikutuksia ydinturvajärjestelmän suunnitteluun tai kehittämiseen [10: 2.3].

Viranomaisille on toimitettava alustavat suunnitelmat turva- ja valmiusjärjestelyiksi, jotka perustuvat suunnitteluperusteuhkaan. Yrityksen periaatesuunnitelmassa on selvitettävä kuinka suunnitteluperusteuhkaa on käytetty turvajärjestelyjen suunnittelun perusteena ja kuinka suunniteltujen turvajärjestelyjen avulla suunnitteluperusteuhka voidaan torjua siinä asetettujen suojaustavoitteiden mukaisesti niin hyvin kuin käytännöllisin toimenpitein on mahdollista [4: 704] [18: 307]. Valvovalle viranomaiselle on toimitettava selvitys siitä, kuinka suunnitteluperusteuhkaa tullaan käytön aikana käyttämään turvajärjestelyjen suunnittelun ja arvioinnin perusteena [4: 720]. Alustavien suunnitelmien on sisällettävä ydinlaitoksen käyttöä koskeva alustava turvasuunnitelma ja luonnos käytön aikaisesta turvaohjesäännöstä.

Julkinen sektorin yhteistoiminta

Ydinturvallisuudesta koskevat lait eivät koske ainoastaan ydinvoima tuottajia, vaan ne ulotettu koskemaan ydinturvallisuuden valvonnasta vastaavaa STUKia ja muita viranomaisia. Kansainväliset sopimukset asettavat valvovalle viranomaiselle vaatimuksen valvoa ydinteknologiaa käyttäviä yrityksiä, ja kansallisessa lainsäädännössä näistä tehtävistä osa on siirretty Suomessa poliisin tehtäviksi.

Kehitettäessä yrityksen uhkiin liittyvää toimintamallia on erityisen tärkeää huomioida viranomaissektori keskeisenä kumppanina uhkien ennaltaehkäisyssä, uhkatilanteiden hoidossa ja niiden jälkiselvittelyssä. Koska ydinvoi-

mayrityksen keinot ja valtuudet eivät yksinään ole välttämättä riittäviä uhkatilanteiden hallintaan, on myös poliisilla ja sille tarvittaessa virka-apua antavilla muilla viranomaisilla lainsäädännöllisiä velvoitteita turvallisuuden varmistamisessa [4: 315].

Ydinvoimayrityksen on pidettävä yllä omaa turvajärjestelyihinsä liittyvää tilannekuvaa ja tehtävä tarpeelliset uhkatilanteisiin ja toimintoihin liittyvät uhka-arviot. Luvanhaltijan vastuulla on selviytyä uhkatilanteesta, kunnes viranomaiset ottavat johtovastuun. Ydinvoimayrityksen on sovittava poliisiviranomaisen kanssa tilannekuvan välittämisestä poliisille [4: 315].

STUK ylläpitää suunnitteluperusteuhkaa ydinenergian ja säteilyn käyttöön mahdollisesti kohdistuvan lainvastaisen toiminnan uhkakuvan perusteella yhteistyössä muiden viranomaisten kanssa. Suunnitteluperusteuhka määrittelee uhkan, jota tulee käyttää turvajärjestelyjen vaatimusten, suunnittelun ja arvioinnin perusteena. Suunnitteluperusteuhka sisältää vakavuudeltaan eritasoisia uhkia [4: 314].

6 Yrityksen pääoma ja sen suojaaminen

Yrityksen on tärkeää tunnistaa sekä aineeton että aineellinen pääomansa. Pääoman kriittisin osa muodostaa yrityksen suojattavat kohteet. Suojattaville kohteille tyypillistä on, että niihin kohdistuvat uhat ovat myös merkityksellisimpiä huomioitavia uhkia yrityksen toiminnassa.

Yrityksen suojattava pääoma muodostuu tyypillisesti sen toiminta- ja tuotantoprosesseista, tuoteinnovaatioista, laitteista ja kalustosta, tietojärjestelmistä ja niiden tiedosta sekä henkilöstöstä. Useissa yrityksissä myös alihankintaketjut ja niiden palvelut sekä tuotteet ovat yrityksen suojattavaan pääomaan luettavia. Ydinvoima-alalla tuotannon turvallisuus eli ydinturvallisuus on keskeisessä roolissa suojattavana kohteena.

Regulaatio

Regulaatio tunnistaa ne tuotantoprosessin kriittiset osa, joita on suojattava ydinturvallisuusnäkökulmasta. Regulaatiossa huomio on kiinnitetty asioihin tai tapahtumiin, jotka voisivat suoranaisesti tai välillisesti aiheuttaa säteilypäästön.

Riskianalyysin perusteella on määriteltävä suojaustarpeet laitoksessa ja kuljetuksissa luokittelevan lähestymistavan mukaisesti suunnitteluperusteuhka huomioon ottaen [4: 307].

Suojaustarpeiden määrittämiseksi on määriteltävä mihin suojausluokkiin suojattavat kohteet luokitellaan.

Hyvät käytänteet

Jotta kokonaisvaltainen liiketoiminnan suojaaminen olisi mahdollista, tulisi koko liiketoimintaan liittyvät uhat kartoittaa, ja laatia suojaustoimenpiteet

myös niille liiketoiminnan osa-alueille, joihin viranomaisen suunnitteluperusteet eivät anna perusteita tai ohjeistusta.

Liiketoiminnan osa-alueiden uhkien arvioiti tulee olla jatkuvaa toimintaa. Uhkien arvioinnissa tule ottaa huomioon yrityksen ulkoisessa toimintaympäristössä ja sisäisessä toiminnassa tapahtuvat muutokset.

Suojaustoimenpiteet yrityksen pääomalle tulee mitoittaa siten, että pääomaan kohdistuva uhka ei aiheuta kohtuutonta menetystä liiketoiminnalle. Suojattavasta pääomasta on pidettävä kirjaa ja sekä aineellinen että aineeton pääoma on luokiteltava. Luokittelu voidaan tehdä esimerkiksi pääoman tuotantokriittisyyden tai sen jälleen hankinta-arvon perusteella.

Pääoma tulee myös arvostaa eli pääomalle olisi hyvä saada tuotantoarvo, joka kuvastaa esimerkiksi pääoman jälleenhankintakustannusta, sen aiheuttamaa tuotannollista tappiota tai imago-menetystä.

Arviointi

Regulaatiossa olisi hyvä painottaa koko liiketoiminnan kriittisten toimintojen ja järjestelmien kartoittamista ja sen määräajoin tehtävää suojattavan omaisuuden inventointia ja uhkatarkastelua. Hyvä malli liiketoiminnan arvioimiseksi on esimerkiksi Business Impact Analysis (BIA).

7 Yrityksen johtamisjärjestelmä

Yrityksen toiminta tulee perustua johtamisjärjestelmään. Jotta organisaatio toimii tehokkaasti, sen toiminta on systemaattista ja jatkuvasti kehittyvää, tarvitsee yritys tehokkaasti toimiakseen hyvät johtamiskäytännöt ja niitä tukevat järjestelmät.

Johtamisjärjestelmän neljä keskeistä osa-aluetta ovat:

- organisaation johtamisjärjestelmä (ohjeistus)
- organisaation johtaminen
- toiminnan jatkuva kehittäminen
- liiketoiminnan tukeminen.

Regulaatio

Ydinlaitoksella on oltava johtamisjärjestelmä. Luvanhaltijalla on vastuu ydinlaitoksen turvallisuudesta sekä johtamisjärjestelmän suunnittelusta, käyttöönotosta, ylläpidosta, toimivuudesta ja vaikuttavuudesta sekä järjestelmän jatkuvasta parantamisesta [1], [8: 101].

Ydinlaitoksen suunnitteluun, rakentamiseen, käyttöön ja käytöstä poistamiseen osallistuvilla organisaatioilla on oltava johtamisjärjestelmä, jolla huolehditaan turvallisuuden ja laadun hallinnasta. Johtamisjärjestelmän tavoitteena on varmistaa, että turvallisuus asetetaan aina etusijalle ja että laadun hallintaa koskevat vaatimukset vastaavat toiminnon turvallisuusmerkitystä. Johtamisjärjestelmää on suunnitelmallisesti arvioitava ja kehitettävä [8: 101].

Johtamisjärjestelmän on katettava kaikki ydinlaitoksen turvallisuuteen vaikuttavat organisaation toiminnot. Kunkin toiminnon osalta on tunnistettava turvallisuuden kannalta merkittävät vaatimukset ja kuvattava suunnitellut toimenpiteet sen varmistamiseksi, että vaatimukset täytetään. Organisaation toimintatapojen on oltava järjestelmällisiä ja ohjeistettuja [8:101].

Viranomaisen ohjeet edellyttävät, että ydinvoimalaitoksen johtamisjärjestelmä on suunniteltava ja toteutettava organisaation toiminnot kattavaksi, ja sitä on ylläpidettävä ja parannettava jatkuvasti. Johtamisjärjestelmän on oltava kokonaisuus, joka tukee organisaation tavoitteiden saavuttamista sekä varmistaa ydin- ja säteilyturvallisuuden vaatimusten täyttymisen. Yrityksen johdon on edistettävä tapoja, joilla koko henkilökunta osallistuu johtamisjärjestelmän toteuttamiseen ja sen jatkuvaan kehittämiseen [4: 301, 303, 304].

Hyvät käytänteet

Johtamisjärjestelmässä on määriteltävä organisaation rakenne ja henkilöstön vastuut, valtuudet ja päätöksentekoon liittyvät menettelyt niin, että otetaan huomioon kaikkien näiden turvallisuusvaikutukset.

Johtamisjärjestelmässä on oltava menettelyt ydinlaitokseen ja sen toimintaan liittyvien tietoturvallisuus- ja turvallisuusriskien tunnistamiseksi, arvioimiseksi ja hallitsemiseksi.

Yrityksen johtamisjärjestelmän tulee määritellä, miten uhka- ja riskienhallintaa johdetaan yrityksessä. Keskeistä on määritellä missä uhkiin ja riskeihin liittyvä päätöksenteko toteutuu. Yleisen käytännön mukaisesti riskienhallinnasta vastaava taho vastaa myös prosessin määrittelystä ja prosessissa tapahtuvista päätöksentekopisteistä. Myös uhkien ja riskien vuosikellon suunnittelu ja valvonta kuuluvat riskinhallinnasta vastaavalle taholle.

Johtamisjärjestelmän laadinnassa on suositeltavaa käyttää apuna eurooppalaista standardia ISO/IEC 27001:2006 [25].

Arviointi

Uhkien- ja riskienhallinnan kannalta regulaatio ohjaa yritystä suunnittelemaan toimintaprosessinsa siten, että riskienhallinta on osa yrityksen perustoimintoja. Regulaatiossa voisi vielä paremmin täsmentää, että uhkien- ja riskien hallinta ei ole erillinen toiminto, vaan uhkien- ja riskien tunnistaminen, arviointi ja niihin reagointi kuuluvat kaikkien yrityksen toimintojen tehtäviin.

7.1 Vuosikello

Toimivan johtamisjärjestelmän yhtenä edellytyksenä on, että toiminta on suunnitelmallista, ja rytmitettyä yrityksen vuosirytmiin. Yrityksen toiminta ja

toiminnot sidotaan toiminnalliseen rytmiin, jossa määräajoin suoritettavat tehtävät on pyritty sijoittamaan kronologiseen järjestykseen. Toiminnallinen rytmi on usein kuvattu vuosikellona, joka pyrkii kuvaamaan yritykseltä ja sen toiminnoilta velvoitettujen toimenpiteiden ja aikataulujen luetteloa.

Regulaatio

Regulaatio ei edellytä vuosikellon muodostamista ja sen noudattamista.

Regulaatio antaa yksittäisille asioille määreitä, joilla asiaa pitää tarkastella määräajoin tai säännöllisesti.

Hyvät käytänteet

Tyypillisiä yrityksen vuosikelloon sidottuja asioita ovat esimerkiksi tilinpäätös ja budjetointitehtävät. Regulaation alaisissa yrityksissä on myös tyypillistä, että regulaattori edellyttää määräaikaisraportointia yritykseltä, ja haluttujen yrityksen toimintojen sitomista johtamisjärjestelmään ja johtamisjärjestelmän määräämiksi määräajoin tehtäviksi suoritteiksi.

Mikäli yrityksen toiminnalta edellytetään uhka- ja riskiarvioita, tulee uhkienhallinnan ja riskienhallinnan tehtävät liittää yrityksen vuosikelloon, ja niiden toimintojen vuosikelloihin, joilta edellytetään määrämuotoista uhkien ja riskien hallintaa. Vuosikello toimii siten johtamisjärjestelmän valvontamenetelmänä, joka sitoo uhka- ja riskinhallintaprosessin yrityksen päivittäistoimintaan.

Arviointi

Regulaation olisi hyvä selkeästi määritellä ne asiat, jotka lisenssinhaltijan määrätään tarkasteltavan määräajoin, ja jotka tulee toimittaa viranomaisille arvioitaviksi.

8 Vaatimuksenmukaisuus

Liiketoimintaan liittyvät sääntelyviranomaiset ja niiden liiketoiminnalle asettamat vaatimukset on tunnistettava. Sääntelyviranomaiset suorittavat toimintaan liittyviä tarkastuksia ja edellyttävät omaehtoisia tarkastuksia, joiden avulla voidaan tarkistaa toiminnan vaatimustenmukaisuus.

Regulaatio

Prosessien ja tuotteiden vaatimuksenmukaisuutta on seurattava. Jos poikkeamia havaitaan, niiden merkitys on arvioitava. Poikkeamien syyt on selvitettävä kattavasti ja on päätettävä tarvittavat korjaavat sekä ehkäisevät toimenpiteet. Laitoksen rakennetta, käytettäviä menettelytapoja tai johtamisjärjestelmää on tarvittaessa parannettava. Vaatimusperusteisten korjaavien toimenpiteiden ja toiminnan parantamiseksi käynnistettyjen kehityshankkeiden vaikuttavuutta on seurattava ja arvioitava järjestelmällisesti [4:718, 811].

Toimivaltaisten viranomaisten on tarkistettava ja tarvittaessa muutettava ydinturvallisuusuhkien arvioinnin asiakirjoja ja suunnitteluun perustuvia uhkia. Päätös siitä, onko näiden asiakirjojen tarkistaminen tarkoituksenmukaista, voitaisiin tehdä määriteltyjen tarkistusjaksojen mukaisesti, mikäli uhkaympäristö muuttuu, ja/tai ydinturvallisuustapahtuman jälkeen opittujen kokemusten perusteella. Jos kyse on uusista tai nousevista ydinturvallisuusuhista, jotka vaativat välitöntä tarkastelua, toimivaltaisten viranomaisten on yhdessä toimijoiden kanssa toteutettava tarvittavat toimenpiteet näiden ydinturvallisuusuhkien hallitsemiseksi [10].

Hyvät käytänteet

Toimintaan liittyvät menettelyt olisi hyvä perustua asetettuun vaatimuspohjaan. Riippumatta siitä, kuka vaatimukset on asettanut, tulee vaatimusten täyttymistä seurata suunnitelmallisesti. Vaatimusten mukaisen toiminnan tarkas-

telu voi olla yrityksen omaa itsearviointia, viranomaisen suorittamaa arviointia toi kolmannen osapuolen toteuttamaa katselmointia tai auditointia [18: 324].

Arviointi

Regulaation asettamat vaatimukset ja yrityksen liiketoiminnan asettamat vaatimukset ovat lähtökohta yrityksen toiminnalle. Regulaattori pyrkii vaatimuksillaan asettamaan kaikille regulaation alaisille yrityksille saman vaatimuksellisen vähimmäistason. Tämä helpottaa sekä viranomaisen valvontatehtävää, että myös toimialan regulaation kehittymistä. Toimialan regulaatio kehittyy niiden kokemusten myötä mitä regulaation alaisten yritysten toiminnasta on saatu kokemuksia.

Kehittynyt regulaatio auttaa myös yritystä huomioimaan tarvittavat uhkiin liittyvät suojautumistarpeet, joita liiketoiminnan suunnittelussa ei muutoin toteutettaisi kustannus- tai muista käytännön syistä.

Vaatimuksenmukaisuuden todentaminen ja arvioiti edellyttää yritykseltä vaatimustenhallinnan käyttöjä ja vaatimusten täyttymisen osittavaa dokumentaatiota. Käytännössä regulaation asettamat vaatimukset eivät voi täyttyä, jollei niiden täyttymistä voida osoittaa dokumentaatioon ja seurantatietoon perustuen.

Yrityksen tuleekin luodessaan dokumentaatiota huomioida dokumentaatioon liittyvä vaatimusten jäljitysvelvoite. Mikäli regulaation tai yrityksen vaatimukset muuttuvat, on dokumentaatioon perustuen pystyttävä selvittämään muutoksen vaikutukset yrityksen toimintaan.

Uhka- ja riskianalyysien tuloksena tulisi syntyä toimenpide-ehdotuksia, jotka tulisi esittää vaatimuksina yrityksen toiminnoille. Uhka- ja riskienhallinnan vaatimukset eivät saa olla ristiriidassa regulaation tai yrityksen liiketoimintatavoitteiden kanssa.

9 Jatkuvuudenhallinta

Jatkuvuudenhallinta on huoltovarmuutta parantava, ja ydinvoima-alalla erityisesti käytettävyyttä varmentava organisaation prosessi, jolla organisaatio:

- tunnistaa liiketoimintansa uhkat, riskit, häiriötilanteet ja riippuvuudet
- arvioi uhkien vaikutukset organisaatiossa ja sen toimijaverkostossa
- organisoi ja toteuttaa menettelytavat häiriötilanteiden varalle
- varmistaa kriittisten kumppaneidensa kyvyn toimia häiriötilanteissa
- suojaa liiketoimintansa intressit ja arvontuotantokykynsä (HVO extranet).

Regulaatio

Turvajärjestelyihin liittyvät tapahtumat on kirjattava, ja ne on voitava todentaa jälkikäteen. Toiminnan jatkuvaksi parantamiseksi tapahtumia on arvioitava, määriteltävä mahdolliset kehityskohteet ja laitettava ne toimeen oikeaaikaisesti [4: 398, 402, 406].

Vikatilanteiden varalle on suunniteltava etukäteen toimenpiteet, joilla turvajärjestelyjen riittävä toimivuus varmistetaan [4:398]. Turvajärjestelyjen tehokkuus ei saa merkittävästi laskea yksittäisen turvajärjestelmän, -rakenteen tai laitteen vikaantumisen takia. Turvajärjestelyt on toteutettava siten, että niiden taso ei merkittävästi laske laitoksen mahdollisten yhteisvikojen tai vaaratilanteiden, kuten sähkönmenetyksen tai tulipalon sattuessa [4: 402].

Hyvät käytänteet

Jatkuvuudenhallinta on prosessi, jonka tarkoituksena on liiketoiminnan ja sen keskeisten prosessien jatkuvuuden turvaaminen keskeytystilanteissa. Jatku-

vuudenhallinnan prosesseissa on otettava huomioon varautuminen, valmiussuunnittelu, jatkuvuussuunnittelu ja toipumissuunnittelu [19: 3]. Myös kriisienhallinnan menettelyt on sidottava osaksi jatkuvuudenhallintaa.

Jatkuvuussuunnittelun tarkoituksena on varautua ennalta mahdollisiin ongelmatilanteisiin. Liiketoiminnan häiriötön jatkuvuus on yhä tärkeämpi menestyksen edellytys, ja tutkimusten mukaan kaikki ennakkosuunnittelu parantaa organisaation kykyä toipua odottamattomasta tapahtumasta (PwC Suomi web-sivut 20.1.2019).

Arviointi

Jatkuva uhkien ja riskien tunnistaminen ja niihin reagoiminen on perusedellytys jatkuvuudenhallinnalle. Uhka- ja riskianalyysejä voidaan käyttää toiminnan jatkuvuuden varmistamiseen arvioimalla säännöllisesti toimintaan ja järjestelmiin kohdistuvia uhkia ja riskejä, ja laatimalla suunnitelmat uhkien ja riskien poistamiseksi tai niiden vaikutusten vähentämiseksi. Regulaatio käsittelee hyvin niukasti jatkuvuuden hallintaa, mutta painottaa sen merkitystä ydinvoimalaitoksen elinkaaren hallinnassa.

Regulaatio ei korosta jatkuvuudenhallintaa prosessina vaan antaa kuvan siitä, että jatkuvuudenhallinta on yksittäisten huomioonotettavien tapahtumien arviointeja ja niiden perusteella tehtävien korjaavien toimenpiteiden toimeenpanoa.

Regulaatiossa olisi hyvä viitata johonkin lähteeseen, jonka suoritusten mukaisesti yrityksen jatkuvuuden hallintaa voisi kehittää. Esimerkiksi VAHTI 2/2016 Toiminnan jatkuvuuden hallinta -ohje [19] antaisi hyvät perusteen jatkuvuudenhallinnan suunnittelulle.

Jatkuva uhkien ja riskien tunnistaminen ja niihin reagoiminen on perusedellytys jatkuvuudenhallinnalle.

9.1 Toiminnan kyvykkyyden arviointi

Jotta johtamisjärjestelmä on tehokas, on johtamisjärjestelmän mukainen toiminta oltava arvioitavissa. Arviointi tulisi olla jatkuvaa määräajoin tehtävää tarkastelua eri johtamisjärjestelmän osa-alueille.

Regulaatio

Luvanhaltijan on osoitettava turvajärjestelyjen vaikuttavuus ja tehokkuus lainvastaista toimintaa vastaan ja järjestelyjen vastaavuus tähän ohjeeseen ydinlaitoksen elinkaaren eri vaiheissa: arvioitava järjestelyt säännöllisesti, dokumentoitava arvio ja toteutettava tarvittavat muutokset. Merkittävät muutokset on hyväksytettävä STUKissa ennen niiden täytäntöönpanoa. Luvanhaltijan on esitettävä mitä kriteerejä vastaan turvajärjestelyt arvioidaan. Turvajärjestelyjen arviointiin liittyvissä asioissa on käytettävä esim. Kansallista turvallisuusauditointikriteeristöä [11] [4: 602, 603, 604].

Luvanhaltijan on osoitettava, että laitoksella on varauduttu erilaisten uhkaavien tilanteiden varalle ja että turvajärjestelyihin liittyvät järjestelmät, rakenteet, laitteet ja toimenpiteet ovat riittäviä estämään tai viivyttämään riittävän kauan vahingontekijää aiheuttamasta laitoksen, sen henkilökunnan tai ympäristön turvallisuutta vaarantavaa tilannetta [4: 605].

Hyvät käytänteet

Johtamisjärjestelmään tehdyt arvioinnit tulee analysoida ja niiden perusteella tulee määritellä johtamisjärjestelmän kehittämiskohteet ja kehittämisaikataulut [18: 314].

Mikäli toiminnan luonne on sen kaltaista, että viranomaisen tulee tarkistaa toiminnan lain- ja asetuksenmukaisuus, on viranomaiselle esitettävä perustellut ratkaisut, mikäli aiotaan poiketa määräysistä.

Arviointi

On perusteltua, että arviointeja suoritetaan ja niiden perusteella tehdyt analyysit toimitetaan viranomaiselle tiedoksi. Päätöstä turvajärjestelyjen toteutustavasta ei tule antaa viranmaiselle. Viranomaisen tulee turvajärjestelyjä hyväksyessään arvioida vain turvajärjestelyjen vaatimustenmukaisuus, eikä viranomaisella pidä olla mahdollisuutta asettaa lisävaatimuksia, ellei erityisesti ole haettu poikkeamaan annetuista vaatimuksista. Turvajärjestelyjen ja yrityksen johtamismallin tulee perustua yrityksen omiin liiketoiminnan tavoitteisiin, eikä viranomainen voi olla päättämässä millaisella taloudellisella panostuksella ja toteutustavalla edellytetyt kyvykkyydet saavutetaan.

10 Uhkien hallinta

10.1 Suunnitteluperusteuhka suunnittelun perustana

IAEAn suosituksen mukaisesti valtiollisen viranomaisen on laadittava kansalliset ohjeet uhkien torjumiseksi. Suunnitelmissa tulee ottaa huomion IAEAn yleiset suoritukset ja kansalliset erityistarpeet. IAEAn määritelmä Design Basis Threat eli suunnitteluperusteuhka on Suomen turvallisuusviranomaisten laatima ohjeistus uhkien torjumiseksi ydinvoimalaitoksissa.

Ydinvoima-alla uhkien hallinta perustuu viranomaisen laatimaan suunnitteluperusteuhkaan. Viranomaisen laatima suunnitteluperusteuhka perustuu IAEA:n julkaisuun Objective and Essential Elements of a State's Nuclear Security Regime [12].

Suunnitteluperusteuhka määrittelee uhkan, jota käytetään turvajärjestelyjen vaatimusten, suunnittelun ja arvioinnin perusteena. Suunnitteluperusteuhka sisältää turvajärjestelyjen suunnitteluperusteena käytettävät määrittelyt lainvastaiseen toimintaan mahdollisesti ryhtyvien ryhmien/henkilöiden toimintakyvystä. Suunnitteluperusteuhka sisältää vakavuudeltaan eritasoisia uhkia.

STUK ylläpitää suunnitteluperusteuhkaa ydinenergian ja säteilyn käyttöön mahdollisesti kohdistuvan lainvastaisen toiminnan uhkakuvan perusteella yhteistyössä muiden viranomaisten kanssa. STUK arvioi suunnitteluperusteuhkaa säännöllisesti ja päivittää sitä tarpeen mukaan.

Regulaatio

Turvajärjestelyjen suunnittelun perusteena tulee käyttää suunnitteluperusteuhkaa, turvattavaa toimintaa koskevia riskianalyysejä ja niiden perusteella arvioituja suojaustarpeita [4: 302].

Luvanhaltijan on suunniteltava turvajärjestelyt siten, että suunnitteluperusteuhka voidaan torjua suunnitteluperusteuhka-asiakirjassa asetettujen suojaustavoitteiden mukaisesti niin hyvin kuin käytännöllisin toimenpitein on mahdollista. Turvajärjestelyjen suunnittelussa on varmistuttava siitä, että turvajärjestelyt eivät vaikeuta onnettomuuden hallintatoimenpiteitä laitoksella pitkäaikaisen sähkönmenetyksen yhteydessä [4, 304].

305. VNA 736/2008 8 §:n mukaisesti *ydinjätelaitoksen suunnittelussa on otettava huomioon mahdollisina pidettävistä luonnonilmiöistä ja muista laitoksen ulkopuolisista tapahtumista aiheutuvat vaikutukset. Ulkopuolisina tapahtumina on otettava huomioon myös lainvastaiset toimet laitoksen vahingoittamiseksi* [4: 305].

Hyvät käytänteet

Yrityksen on omaksuttava uhkien hallinnassa riskitietoinen lähestymistapa. Tärkeää on tunnistaa uhat ja tunnistaa sekä arvioida uhkien potentiaaliset seuraukset.

Yrityksen on laaja-alaisesti arvioitava sen toimintaan liittyvät uhkatekijät. Uhkatekijöitä voidaan tunnistaa esimerkiksi yleisesti saatavilla olevien uhkakatalogien perusteella [26] [22]. Uhkien tunnistaminen ja niiden arviointi ovat ennaltaehkäisevää riskienhallintaa. Oikein suunniteltu ja toteutettu uhkien ja haavoittuvuuksien hallintasuunnitelmat ovat avaintekijä organisaation turvajärjestelyissä tarjoamalla ennakoivan ja liiketoiminnan kannalta yhdenmukaisen lähestymistavan riskien ja uhkien vähentämiseen, eikä ainoastaan reagoivaan ja teknologiakeskeiseen lähestymistapaan.

YVL A.11 [4] vaatimus 304 antaa luvanhaltijalle mahdollisuuden suunnitella turvajärjestelyt kohteen erityisvaatimusten mukaisesti. Suunnitteluperusteuhka ei määrittele tapaa millä suojaaminen uhkia vastaan on toteutettava, mutta asettaa selkeät rajat vakavien uhkatilanteiden seurauksena syntyville säteilypäästöille.

Suunnitteluperusteuhkassa määriteltyjä uhkaskenaarioita arvioitaessa on huomioitava, että skenaarion mukainen uhka voi kohdistua useisiin kohteisiin ydinvoimalaitoksella, ja skenaarion mukainen uhkaava toiminta voidaan toteuttaa usealla eri toteutustavalla.

Arviointi

Regulaatio olettaa, että suunnitteluperusteuhan mukaisiin uhkaskenaarioihin varautuminen on riittävä suojaamaan ydinvoimalaitosta sitä uhkaavilta lainvastaisilta toimilta.

Suunnitteluperusteuhka sinällään antaa ydinvoimalaitoksen turvajärjestelyjen ja turvallisuusjärjestelyjen suunnittelu keskeiset kriteerit. Suunnitteluperusteuhka ei kuitenkaan ole täydellinen uhkamaailman kuvaus. Suunnitteluperusteuhka ei määrittele ratkaisuja miten operatiivisella toiminnalla, ohjeistuksella, fyysisillä rakenteilla ja turvatekniikalla voidaan uhka torjua. Tarkastelemalla uhkamaailmaa vain suunnitteluperusteuhan antamin perustein ei riittäviä suunnitteluperusteita uhkien ennaltaehkäisyyn ja niiden toteutuksen valmistelun estämiseen voida saavuttaa.

Suunnitteluperusteuhkan skenaarioiden lisäksi tulee uhkakartoituksissa huomioida sellaisia uhkaskenaariota, joilla voidaan valmistella ja edesauttaa suunnitteluperusteuhkassa esitettyjen skenaarioiden toteutumista.

10.2 Liiketoiminnan kytkeytyminen uhkien hallintaan

Yrityksen liiketoiminnan näkökulmasta on erityisen tärkeää suojautua uhkia vastaan. Oleellista on pystyä riittävissä määrin tunnistamaan keskeiset uhat ja niiden mahdollisen vaikutuksen liiketoimintaan.

Luonnollisesti kaikkia uhkia ei pystytä ennakolta tunnistamaan eikä niiden käyttäytymistä mallintamaan, mutta riittävän laaja uhkien käsittely ja niihin valmistautuminen antava lisäsuojaa myös tunnistamattomien uhkien torjuntaan.

Uhka voi olla tahallista tai tahattomasti aiheutettu. Tuottamuksellisesti aiheutettuihin uhkiin valmistautuminen on usein haastavaa sillä uhan aiheuttaja, aiheuttajan motiivit ja aiheuttajan toteutustapa eivät ole useinkaan ennakoitavissa.

Tahattomasti aiheutetut uhat ovat sitä vastoin helpommin tunnistettavissa, ja niille voidaankin pääsääntöisesti muodostaa ennakoivat- tai vastatoimet.

Yritykseen kohdistuvat uhat voidaan pääsääntöisesti jakaa kahteen kategoriaan: ulkoisiin uhkiin ja sisäisiin uhkiin.

Yrityksen turvallisuuskulttuurilla on erittäin suuri merkitys sekä ulkoisten että sisäisten uhkien muodostamiseen. Hyvä turvallisuuskulttuuri estää esimerkiksi vaarallisten työyhdistelmien muodostumisen ja kannustaa normaalista poikkeavien asioiden ja tapahtumien esilletuontia.

10.3 Sisäiset ja ulkoiset uhat

Ulkoiset uhat ovat yrityksen liiketoiminnasta riippumattomia ulkoisen tekijän aiheuttamia. Ulkoinen uhka muodostuu yleensä yrityksen toiminnasta riippumattomasti. Yrityksen tulee erikseen arvioida ne suojattavat kohteensa, jotka ovat erityisesti alttiita ulkoisille uhkille.

Regulaatio

Ulkoisilla uhkilla tarkoitetaan tässä yhteydessä etupäässä ydinlaitokseen sen ulkopuolelta kohdistuvaa tahallista tai tuottamuksellista toimintaa, joka ilman varautumista voisi vaarantaa ydinlaitoksen turvallisuuden. Uhkien määrittelyssä on pyrittävä ottamaan huomioon turvajärjestelyihin liittyvät ajankohtaiset tapahtumat, suunnitteilla, rakenteilla tai käytössä olevan laitosyksikön käyttöikä ja tulevaisuuden ennustamiseen liittyvät vaikeudet mm. yhteiskunnan erilaisten häiriötilanteiden ja kriisien osalta. Sotatoimet on kuitenkin jätetty luvanhakijaa ja luvanhaltijaa koskevien suunnitteluperusteiden ulkopuolelle [13: 314].

Uhkien hallinnassa olisi pyrittävä tunnistamaan muun muassa seuraavat toimintaan liittyvät uhat:

- globaalit, kotimaiset ja paikalliset uhat
- fyysisten, tietoverkkohyökkäysten ja hybridihyökkäysten mahdollisuus
- sisäpiiriin kohdistuvat uhat, ulkoiset vastustajat ja sisäpiiriin kohdistuvien uhkien ja ulkoisista vastustajista johtuvat uhat [10: 5.13].

Suojattavat kohteet on tunnistettava ja määriteltävä riittävällä yksityiskohtaisuuden tasolla. Kohteisiin liittyvät uhkat ja haavoittuvuudet sekä tietoturvallisuusloukkausten aiheuttamat vaikutukset on analysoitava ja määriteltävä tarpeelliset suojaustoimenpiteet. Suojaus-toimen-piteet on dokumentoitava [18: 316].

Hyvät käytänteet

Proaktiivisessa mallissa yrityksen suojattaviin kohteisiin liittyvät uhat on tunnistettu, uhkiin liittyvät haavoittuvuudet rajoitettu ja toimenpiteet uhkien vaikutuksen vähentämiseksi on suunniteltuja.

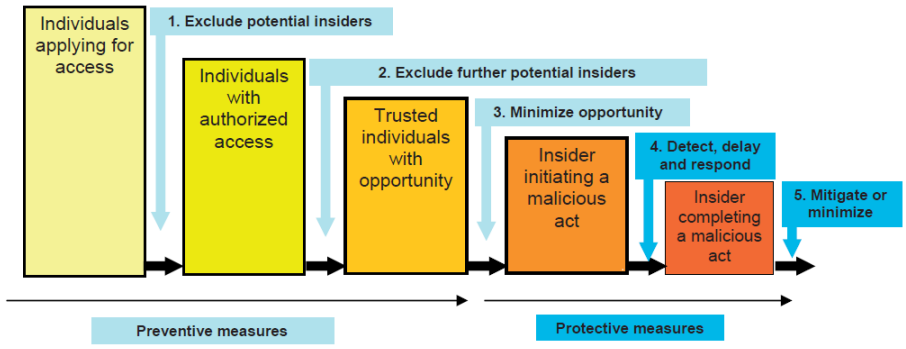
Arviointi

Usein yrityksessä havaitaan uhka vasta siinä vaiheessa, kun uhka on jo realisoitunut. Reaktiivisessa toimintamallissa ei useinkaan ole ennalta määriteltyjä toimintatapoja estää tai pienentää uhkan toteutumisen mahdollisuutta, vaan uhan aiheuttajan toimintaan päästään puuttumaan, kun uhka on jo realisoitunut tai merkittävä vahinko liiketoiminnalle on jo aiheutunut.

10.3.1 Sisäiset uhat

Uhka käsitetään usein ulkoisena uhkana, joka yrityksen ulkopuolelta vaikuttaa negatiivisesti yrityksen toimintaan. Sisältäpäin tapahtuvaa tahallista tai tuottamuksellista uhkaa kutsutaan Insider-uhaksi.

Regulaatio



Kuva 2 Sisäisen uhkan torjunta (IAEA).

Kuva 2. esittää IAEA:n lähestymistavan sisäisten uhkien torjuntaan. Keskeisenä tavoitteena on rajoittaa henkilöiden pääsyä suojattaviin kohteisiin, riippumatta siitä onko kyseessä aineellinen tai aineeton suojattava kohde.

IAEA:n lähestymistapa noudattelee syvyyssuuntaisen puolustuksen (Defence in Depth) periaatteita [20: s.15]. Syvyyssuuntaisen puolustuksen ajatuksena

on turvata suojattavat kohteet usealla sisäkkäisellä tasolla siten, että ainoastaan he tahot, joilla on oikeus käyttää, ylläpitää tai kunnossapitää suojattavaa kohdetta voivat operoida kohteen kanssa omien määriteltyjen valtuuksien puitteissa.

Hyvät käytänteet

Yrityksen on tärkeää myös huomioida yrityksen sisältäpäin muodostuvat henkilöuhkat, jotka muodostuvat joko tahallisesta tai tahattomasta toiminnasta. Uhan torjunnassa on haastavaa tunnistaa uhka, koska periaatteessa kaikki yrityksen työntekijät oletetaan olevan luotettavia. Kuitenkin Insidereillä on omat motiivinsa ja perusteensa uhan aiheuttamiseen, ja siten uhka on todellinen, ja se on otettava huomioon yrityksen toimintaa suunniteltaessa [21].

Arviointi

Ydinvoima-alalla painotetaan Insider-uhan ennaltaehkäisyä, sen havainnointia ja siihen reagointia. Merkittävässä roolissa on myös uhan aiheuttamasta vahingosta palautuminen.

Insider-uhkaan varautuminen ei kuitenkaan näy riittävän merkittävässä roolissa STUKin julkisissa YVL-ohjeissa. Asian voimakkaammin esille nostaminen regulaation ohjeistuksessa voisi vaikuttaa yrityskulttuurin luomiseen, ja sen asian hyväksymiseen, että myös oma henkilöstö voi olla uhan aiheuttaja.

10.4 Ennaltaehkäisevä toiminta

Luvussa 9. Jatkuvuudenhallinta on kuvattu jatkuvuussuunnittelun kannalta ennaltaehkäisevänä toimintana. Tässä luvussa pyritään hahmottamaan ohjeistuksen ja toiminnan harjoittelun merkitystä ennaltaehkäisevinä toimintoina.

Regulaatio

Turvajärjestelyjen on perustuttava usean sisäkkäisen turvallisuusvyöhykkeen käyttöön siten, että turvallisuuden kannalta tärkeät järjestelmät ja laitteet sekä ydinmateriaali ja -jäte ovat erityisen suojattuja ja että kulun- ja tavaraliikenteen valvonta voidaan järjestää. Edellä mainittujen kohteiden suojaamiseksi on käytettävä teknisiä, hallinnollisia ja operatiivisia menettelyjä [4: 321].

Tarkemmat laitoskohtaiset toimenpiteet uhkatilanteita vastaan on kuvattava turvaohjesäännössä ja/tai muissa asiaankuuluvissa ohjeissa [4: 508].

VNA 734/2008 6 §:n [2] mukaisesti turvasuunnitelman ja turvaohjesäännön mukaista toimintaa uhkatilanteissa on harjoiteltava vuosittain. Harjoituksia on järjestettävä myös asianomaisten viranomaisten kanssa säännöllisesti [2: 6§]. Poliisiviranomaisten kanssa on sovittava yhteisharjoituksista ja niiden lukumääristä harjoitusohjelmaa laadittaessa ottaen huomioon myös poliisin eri erityisryhmät [4: 607].

Hyvät käytänteet

Uhkien hallinta on ennaltaehkäisevää toimintaa, jonka tulee perustua tarpeeseen liiketoiminnan jatkuvuuden varmistamiseksi. Keskeiset turvallisuuteen liittyvät strategiset päätökset tulee näkyä myös uhkien hallinnassa ja toimissa, joilla pyritään varmistamaan uhkien muodostuminen.

Ennaltaehkäisevänä toimena tulisi säännöllisesti käydä läpi vallitseva uhkatilanne, johon tulisi yhdistää myös globaalit uhkakuvat, toimialaa valvovien organisaatioiden uhkakuvat ja kansalliset uhkakuvat.

Näistä uhkakuvista tulisi muodostaa yrityksen uhkaprofiili, jonka tarkastelu on jatkuvaa toimintaa. Varsinkin tietoturvallisuuden uhkakuvat muuttuvat erittäin nopealla syklillä, joka edellyttää jatkuvaa seurantaa ja haavoittuvuuksien arviointia.

Reagointi uhkaan edellyttää uhkan ilmenemismuodon ymmärtämistä ja erilaisten uhan hyökkäysvektoreiden mallintamista. Selkeät toimintaohjeet toimintaan uhan ilmettyä nopeuttavat vastatoimia ja täten todennäköisesti vähentävät uhan aiheuttamaa vahinkoa.

Arviointi

Toimintaohjeet uhan hallintaa eivät välttämättä ole riittäviä, vaan lisäksi tarvitaan organisaation systemaattista harjoittelua uhkatilanteiden hallitsemiseksi. Varsinkin ulkoisten uhkatilanteiden harjoittelussa on viranomaisyhteistyöllä ja viranomaisten kanssa tehdyllä yhteisellä harjoitustoiminnalla suuri merkitys uhkatilanteen haltuun saattamiseksi.

Mikäli yrityksellä on kriisinhallintaryhmä, turvallisuusvalvomo tai CIRT-toiminto kuuluvat ennaltaehkäisevät toiminnot heidän päivittäistehtäviensä piiriin.

10.5 Reaktiivinen toiminta

Uhka voi muodostua todelliseksi riippumatta kaikista uhkien torjuntaan tehdyistä toimenpiteistä. Turvaorganisaatiolla on oltava valmius reagoida myös yllättäviin ja ennalta tuntemattomiin uhkatilanteisiin.

Regulaatio

Uhkatilanteessa on arvioitava ilmenneen uhan todenperäisyys, laajuus ja merkitys. Tämä arviointi tehdään mahdollisuuksien mukaan yhteistyössä ydinlaitoksen ja poliisin edustajien kesken. Tällaisia tilanteita varten poliisi laatii ja ylläpitää toimintasuunnitelmia sekä niihin liittyviä valmiuksia. Tarvittavan koulutuksen ja harjoitustoiminnan järjestämisestä on huolehdittava yhteistyössä poliisin kanssa. Laitoksen edustajien on ylläpidettävä valmiutta em. arvion tekoon kiireellisessä tilanteessa itsenäisesti [4: 506].

Uhkatilanteessa on käynnistettävä seuraavat toimenpiteet:

- laitoksen turvallisuustoimintojen ja työntekijöiden turvallisuuden varmistaminen
- mahdollisten seurausten rajoittaminen
- uhkan torjuminen
- uhkan poistaminen [4: 507].

Hyvät käytänteet

Kaikkiin uhkiin ei voida kuitenkaan ennalta varautua. Osa uhkista on täysin ennalta arvaamattomia ja mahdollisesti niin laaja-alaisia, että yrityksessä tarvitaan ennalta määritelty kriisinhallintaryhmä reagoimaan muodostuneeseen uhkaan.

Yllättävän uhan ilmaantuminen ei kuitenkaan poista sitä tosiasiaa että, uhkan aiheuttaja, sen ilmenemismuoto ja uhan vaikutuspiirissä olevat suojattavat kohteet on tunnistettava. Tämä edellyttää toimivaa uhkan hallintaprosessia, joka on mahdollista käynnistää välittömästi uhkahavainnon perusteella.

Uhan arviointia ja vastatoimen käynnistä helpottaa turvaorganisaation muodostama tilannekuva, joka muodostetaan käytössä olevien valvontajärjestelmien ja turvaorganisaation havaintojen perusteella. Tilannekuvaa jaetaan uhkatilanteissa kriisinhallintaryhmälle, ydinvoimalaitoksen valvomoille ja turvallisuusviranomaisille.

Arviointi

Regulaatiossa painotetaan yhteistoimintaa polisin kanssa. On kuitenkin oleellisen tärkeää, että ydinvoimalaitoksen henkilökunta pystyy käynnistämään uhkaan liittyvät torjuntatoimet mahdollisimman varhaisessa vaiheessa. Poliisille uhkatilanteen johtovastuu siirtyy vasta kun poliisi ilmoittaa ottavansa johtovastuun. Johtovastuun siirtymiseen voi kulua jopa tunteja, ja sinä aikana kriisinhallintaryhmän ja turvaorganisaation on pystyttävä organisoitumaan ja aloittamaan uhkanhallinta toimet.

10.6 Yrityksen uhka- ja riskiprosessit

Yrityksellä on joukko ydinprosesseja, jotka ovat yrityksen toimintastrategian mukaisia. Yrityksen ydinprosesseissa tulisi olla menettelyt, joilla ilmaistaan välittömästi prosesseissa havaitut uhkatekijät ja prosesseissa ilmenneet haavoittuvuudet. Tieto prosessia uhkaavasta tekijästä tulee kyetä välittämään uhkien torjuntaan määritellylle taholle.

Uhkien hallintaprosessi usein liitetään turvallisuussektorin toimenkuvaan ja käsitetään usein riskienhallinta- ja turvallisuussektorin tehtäviksi. Uhka voi kuitenkin olla niin toiminto-, tuotanto tai järjestelmäspesifinen, että riskienhallinta- ja turvallisuussektorin asiantuntijat eivät pysty käsittelemään uhkaa ja sen vaikutuksia riittävän laajasti. Tämän vuoksi uhkien kuvaamisessa, ja niiden toimintatapojen selvittämisessä tulee olla riittävä osaaminen siitä substanssialueesta, jonka suojattavista arvoista on kysymys.

Regulaatio

Uhkien hallinta on riskitietoinen iteratiivinen prosessi, jossa tunnistetaan ja arvioidaan uhat ja riskit, kehitetään, arvioidaan ja toteutetaan riskienhallinnan

vaihtoehtoja sekä seurataan ja johdetaan tuloksena olevien toimien tarkoituksenmukaisuutta ja tehokkuutta [14].

Ydinturvallisuuden varmistamisen olennainen osa on riskitietoisten lähestymistapojen käyttö, mukaan lukien resurssien jakaminen ydinturvajärjestelmille ja ydinturvallisuustoimenpiteille ja ydinturvallisuuteen liittyvien toimien suorittaminen, jotka perustuvat asteittainen lähestymistapa ja syvyyssuuntaiseen puolustukseen [10: 2.5].

Arvio olemassa olevista ydinturvallisuuteen liittyvistä uhista, potentiaalisten vastustajien ominaisuuksista ja uhan ominaisuuksien määrittämisestä on tehtävä. Ydinturvallisuusuhkien arviointiprosessissa tulee hyödyntää maailmanlaajuisia, alueellisia ja kotimaisia tietolähteitä [10: 2.7].

Uhkien arviointiprosessin aikana kerätään ja analysoidaan tietoja olemassa olevista tai uskottavista mahdollisista uhista, ja tiedot uhan ominaisuuksista kootaan ja yhdistetään. Ydinturvallisuusuhkien arvioinnin tulos on yksityiskohtainen kuvaus ydinturvallisuuteen liittyvästä uhasta, jota kutsutaan ydinturvallisuusuhkien arviointidokumentaatioksi [10: 5.3].

Hyvät käytänteet

Uhkien tunnistaminen edellyttää riittävää toiminnan tuntemusta, siihen liittyvien toimintaprosessien tuntemusta ja toiminta ympäröivän toimintaympäristön tuntemista. Keskeisessä roolissa uhkien tunnistamisessa ovat ne henkilöt, jotka tuntevat toiminnan parhaiten, koska heillä on yleensä myös paras käsitys siitä, miten toimintaa voidaan vahingoittaa ja mitkä ovat toiminnan haavoittuvuudet.

Eri toimialoissa edellytetään myös uhkien ennalta tunnistamista, ja suunnitelmia uhkien ennalta ehkäisemiseksi.

Arviointi

Regulaatio edellyttää, että turvajärjestelyt suunnitellaan ja rakennetaan riskiperusteisesti. Regulaation tarkka noudattaminen edellyttäisi, että jokainen turvajärjestelyihin liittyvä ratkaisu tulisi pystyä tunnistamaan tehdyistä riskiarvioista. Käytännössä kuitenkin useat turvajärjestelyratkaisut toteutetaan parhaat käytännöt – periaatteiden mukaisesti ilman erillistä riskiarviointia.

10.7 Uhkakategoriat

Kaikki uhat eivät ole samanarvoisia, ja ne kohdistuvat liiketoiminnan eri osa-alueille. Tärkeää olisi luoda yritykselle uhkakategoriat, joko liiketoiminnan prosesseihin tai toimintojakoon perustuen.

Uhkakategorioiden luominen auttaa yritystä käsittelemään tiettyjen osa-alueiden uhkia yhtenä kokonaisuutena, ja auttaa myös hahmottamaan sitä henkilöresurssitarvetta, jota tarvitaan välttämättä uhkakategorian mukaisten uhkien käsittelyssä. Kategoriointi auttaa myös samankaltaisten uhkien käsittelyssä, jolloin esimerkiksi voidaan käyttää yhtä uhkaskenaariota perustana useamman uhan käsittelyssä.

Uhkaskenaarioihin liittyy myös tarve uhan metadataistamiseksi. Metadataistamisella tässä yhteydessä tarkoitetaan sitä, että uhkaskenaarioihin liitetään luokittelevaa tietoa, esimerkiksi siitä suojattavasta arvosta, johon uhkaskenaarion oletetaan kohdistuva.

Mikäli uhkien hallinta perustuu regulaation asettamiin määräyksiin tai vaatimuksiin, on metadatan hyvä sisältää tieto niistä vaatimuksista, joiden täyttymistä kyseisellä kategorialla tai uhkaskenaariolla voidaan arvioida. Kysymys on siis myös jäljitettävyyden hallinnasta, joka auttaa sekä yritystä itseään hallitsemaan vaatimusten hallintaansa ja regulaattoria arvioimaan toiminnan vaatimuksenmukaisuutta.

Yrityksen kehittämisvarojen saaminen ennaltaehkäiseviin toimiin on usein haastavaa niiden kustannus/hyöty suhteen todistamisen vaikeudesta johtuen. Standardoitu uhkien hallintamenettely ja mahdollistaa analyyttisemman lähestymisen myös toiminnan rahoitusta koskevissa esityksissä.

Regulaation asettamien vaatimusten todentaminen uhkamallinnuksen kautta auttaa myös yritysjohtoa havainnoimaan paremmin koko liiketoimintaan kohdistuvia uhkia.

10.8 Uhka-analyysit

Liiketoiminnassa on aina haavoittuvuuksia ja niiden kanssa täytyy tulla toimeen. Uhkaskenaarioilla ja niihin kohdistuvilla uhka-analyyseillä pyritään löytämään toimintaan liittyviä haavoittuvuuksia. Joihinkin haavoittuvuuksiin

voidaan vaikuttaa, osaan ei ole tarkoituksenmukaista vaikutta ja osaan ei pystytä vaikuttamaan. On kuitenkin oleellista tunnistaa liiketoiminnan haavoittuvuudet ja ottaa ne huomioon suunniteltaessa yrityksen jatkuvuudenhallintaan liittyviä menettelyjä.

Uhka-analyysit tulee laatia yhdessä liiketoiminnan asiantuntijoiden kanssa, jotta voidaan varmistaa, että uhan vaikutukset liiketoimintaan on riittävissä määrin huomioitu.

Regulaatio

Turvallisuusuhkien arviointiprosessin tulos on turvallisuusuhkien arviointidokumentaatio, joka kuvaa turvallisuuden yleistä uhkaympäristöä ja kaikkia tunnettuja uskottavia uhkia, jotka tulisi ottaa huomioon [10: 5.19].

Hyvät käytännöt

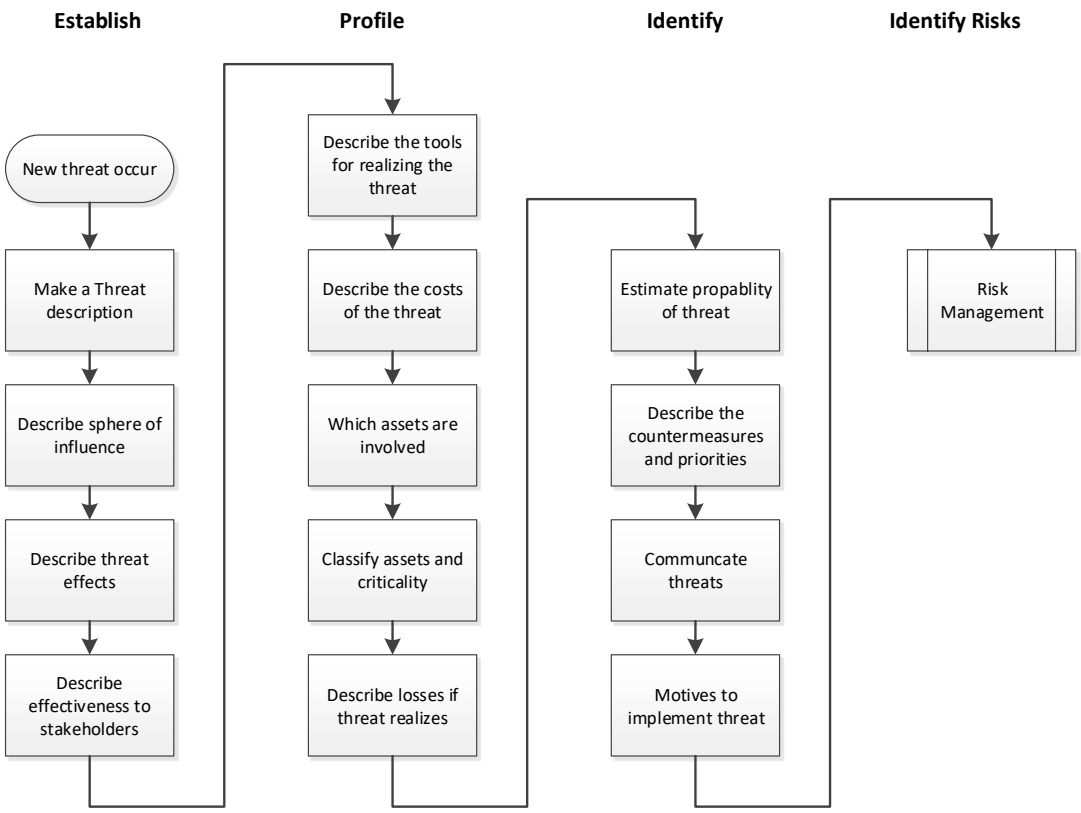
Uhka-analyysissä selvitetään, miten laadittu uhkaskenaario käyttäytyy yrityksen toimintaympäristössä. Laadukkaan uhka-analyysin edellytyksenä ovat riittävät toiminnan kuvaukset, kuten toimintaohjeet, prosessikuvaukset, järjestelmäkuvaukset ja toiminnasta kerätty seurantatieto.

Uhka-analyysi sekoitetaan usein riskianalyysiin, mutta uhka-analyysi on riskianalyysia edeltävä vaihe, joka tarkoituksena on tuottaa riskiehdokkaita riskianalyysiä varten. Uhka-analyysin tuloksissa liiketoiminnan haavoittuvuudet kirjoitetaan riskienhallinnan määrittelemään esitysmuotoon.

Näiden kahden analyysin toteuttamisessa on huomioitavaa, että uhka-analyysin laadinnassa on yleensä mukana uhkaan liittyvän toiminnon asiantuntijoita, ja riskianalyysissä on yleensä laajempi näkökulma johtuen riskien priorisoinnin, vaikuttavuuden ja valitusta riskin pienentämistavasta.

Kuvassa 3. on esitelty yksi uhkien arviointimalli, mutta Uhka-analyysimenetelmänä voidaan käyttää esimerkiksi seuraavia yleisesti tunnettuja malleja:

- Syy-seuraus-analyysi (CCA)
- Vika- ja vaikutusanalyysi (FMEA) (Failure Mode and Effect Analysis)
- Vikapuuanalyysi
- OWASP.



Kuva 3 Esimerkki uhkien hallintaprosessista.

Arviointi

Regulaatio ei ota kantaa miten uhka-analyysit pitää suorittaa. Uhka-analyyseille ei ole myöskään mitään kansainvälisesti standardoitua tapaa uhkaskenaarion mallintamiseksi. Kirjallisuudessa on esitetty erilaisia malleja uhkien arvioimiseksi, ja kaupalliset yritykset ovat myös tuotteistaneet uhkien arviointimenettelyjä.

Toiminnan tarkastettavuuden (uhat otettu huomioon) kannalta, olisi hyvä määritellä vähintään ne vaiheet, ja tuotokset joita uhkien arviointimenettelyssä tulisi toteuttaa. Olisi myös hyvä tarkentaa, mitkä ovat uhka-analyysin lopputulokset, ja miten niitä tulisi jatko hyödyntää.

10.9 Riskienhallinta

Riskien hallintaa suhtaudutaan vakavasti ydinvoima-alalla. toimialan regulaatio ja ohjeistus painottavat riskiperusteista lähestymistä ydinvoimalaitoksen suunnittelussa ja ydinvoiman käytössä.

Edellä kuvatut uhkienhallinnan menettelyt eivät yksin riitä kuvaamaan sitä, miten mahdolliseen uhkaan tulisi suhtautua. Uhka-analyysin perusteella tulee pystyä arvioimaan mitä riskejä uhkaskenaariot voivat aiheuttaa liiketoiminnalle.

Regulaatio

VNA 734/2008 [2] 2 §:ssä tarkoitettuja riskianalyysejä on käytettävä hyväksi suunniteltaessa laitosta ja sen rakenteellisia yksityiskohtia, käytännön valvontatoimenpiteitä sekä turvajärjestelyjen toteutuksesta vastaavaa organisaatiota. Riskianalyysin perusteella on määriteltävä suojaustarpeet laitoksessa ja kuljetuksissa luokittelevan lähestymistavan mukaisesti suunnitteluperusteuhka huomioon ottaen. Riskianalyysin käyttö on kuvattava suunnittelu- ja rakentamisvaiheiden johtamisjärjestelmässä. Turvajärjestelyjä koskevassa riskianalyysissä on käytettävä hyväksi VNA 717/2013:n [3] mukaisesti tehtyjä todennäköisyysperusteisia riskianalyyseja. Turvajärjestelyjä koskevassa riskien hallinnassa on soveltuvin osin otettava huomioon ohjeessa YVL A.7 Ydinvoimalaitoksen riskien hallinta [15] esitetyt vaatimukset [4: 307].

Hyvät käytännöt

Kaikki yritykseen kohdistuvat riskit eivät tule esille uhkamallinnuksessa, vaan osa riskeistä nousee esille yrityksen toimintaprosesseista. Tämä ei kuitenkaan tarkoita sitä etteikö, riskin esilletulo voisi aiheuttaa tarvetta uhkamallinnukseen ja sitä kautta laajempaa riskin tarkasteluun toimintaympäristössä.

On siis tärkeää, että myös riskien hallinnasta on kytkentä takaisin liiketoiminnan tavoitteisiin, liiketoiminta strategiaan ja sitä kautta myös yrityksen uhkatason pienentämiseen.

Riskienhallinnan tarkoituksena on käsitellä toiminnassa esiintyneet riskiehdokkaat, ja laatia ehdotukset riskien vaikutuksen pienentämiseksi. Ehdotukset riskien pienentämiseksi tulisi kohdentaa aiemmin esiteltyihin uhkakategorioihin, ja siten varmistaa riskin kohdistuminen halutulle vastuutaholle.

Riskinhallintaprosessin tulee varmistaa että, riskin pienentämistoimenpiteet on määritelty kyseisten toimenpiteiden suunnittelusta ja kehittämisestä vastuulliselle taholle.

Laadunhallinnan standardi ISO 9001:2005 [16] esittää, että:

- organisaatiolta vaaditaan sellaisten riskien määrittämistä, jotka voivat vaikuttaa sen kykyyn täyttää systeemille asetetut tavoitteet. Riskiperusteinen ajattelu tarkoittaa riskin määrällisten kuin laadullisten seikkojen huomioimista siinä ympäristössä, jossa yritys tai yhteisö toimivat
- organisaation johdon on osoitettava johtajuutta ja sitoutumista edistämällä prosessimaisen toimintamallin ja riskiperusteisen ajattelun käyttöä
- organisaatiota edellytetään tekemään toimenpiteitä tunnistaakseen riskit ja mahdollisuudet ja suunnittelemaan, kuinka käsitellä riskit ja mahdollisuudet, ja näihin liittyvät toimenpiteet
- organisaation on analysoitava ja arvioitava seurannasta ja mittauksista saatavaa tietoa riskien ja mahdollisten käsittelytoimenpiteiden vaikuttavuutta
- organisaation on määritettävä ja valittava parannusmahdollisuudet ja toteutettava tarvittavat toimenpiteet ei-toivottujen vaikutusten korjaamiseksi, estämiseksi ja vähentämiseksi. (http://www.sixsigma.fi/fi/artikkelit/rbt/).

Arviointi

Regulaatiossa tulisi painottaa voimakkaammin riskianalyysin riskinhallintatoimenpiteiden takaisinkytkentään liiketoimintaan. Takaisinkytkennällä tässä yhteydessä tarkoitetaan riskeistä johdettavien toiminnan vaatimusten ja muutosten kytkemistä yrityksen kehittämistehtäviin ja kehittämisvastuisiin.

10.10 Riskien pienentämistoimenpiteet

Ydinvoiman turvallisuus perustuu riskien minimointiin sellaisissa toiminnoissa ja järjestelmissä, joissa ilmenevät toiminnalliset tai laadulliset ongelmat voivat aiheuttaa säteilypäästöjä. Säteilypäästöjen minimoimiseksi riskinhallinnan toimenpiteillä tunnistetaan asiat, joilla voi olla merkitystä päästöjen aiheutumiseen.

Riskejä ei ole hallittu, jollei niille ole määritelty pienentämistoimenpiteitä. Riskien pienentäminen ei aina tarkoita riskin poistamista vaan sen saattamista hallittavalle ja hyväksyttävälle tasolle.

Regulaatio

Luvanhaltijan on pyrittävä hallitsemaan riskejä seuraavin menettelyin:

- havaitun riskin poistaminen tai pienentäminen ennalta ehkäisevin toimin, joka voi tapahtua esim.
    - parantamalla turvajärjestelyjen tehokkuutta, esim. lisäämällä fyysisiä esteitä tai hidasteita sekä parantamalla havaitsemista nykyaikaisten valvontajärjestelmien avulla
    - lisäämällä vastetta
    - vähentämällä lainvastaisella toiminnalla aiheutettujen seurausten vaikutuksia [4: 601].

Hyvät käytännöt

Riskienhallinta on yrityksessä jokaisen työntekijän vastuulla. Kaikkia riskejä on pyrittävä hallitsemaan nousevat ne sitten esille uhkienhallinnan menettelyjen kautta tai operatiivisessa toiminnassa tehtyjen havaintojen kautta. Hyvä turvallisuuskulttuuri luo tähän hyvät puitteet.

Riskien hallinnan tulee olla organisoitua ja hallinnoitua siten, että osapuolet, joihin toimintaan riski kohdistuu, on tietoinen riskin olemassaolosta ja sen vaikutuksista toimintaan. Riskihallinta ja riskin pienentämiseen liittyvät tehtävät siirtyvät johtamisjärjestelmässä kuvattujen vastuiden mukaisesti riskin vaikutusalueen toiminnasta vastaavalle taholle. Toiminnasta vastaavan tahon on varmistuttava, että riskienhallinnan edellyttämät toimenpiteet ovat linjassa yrityksen, liiketoiminnan ja strategian kanssa.

Toiminnasta vastaavan tahon on varmistuttava myös, että ratkaisut ovat linjassa regulaation vaatimusten kanssa, sekä toimintaan tehtävät muutokset ovat dokumentoituja. Riskiperusteisesti tehdyt toiminnan muutokset tulee olla jäljitettävissä. Jäljitettävyys tarkoittaa myös käsittelyprosessin jäljitettävyyttä uhka- ja riskianalyyseihin.

Arviointi

Regulaatiossa painotetaan säteilypäästöjen estämistä ja lainvastaisella toiminnalla aiheutettujen päästöjen minimoimista. Regulaatio myös tunnistaa, että kaikkien riskien toteutumista ei voida estää, vaan on luotava menettelyt, joilla riskin toteutumisen todennäköisyyttä voidaan merkittävästi pienentää.

10.11 Viestintä uhkatilanteissa

Viestintä normaalitilanteissa ja erilaisissa uhkatilanteissa on erittäin merkityksellinen turvajärjestelyjen kannalta.

Regulaatio

Kaikista laitoksen todetuista turvajärjestelyjä koskevista ja niihin liittyvistä uhista, tapahtumista, ilmiöistä ja henkilöistä, joilla saattaa olla merkitystä ydinturvallisuuden kannalta tai jotka voivat ylittää kansallisen tai kansainvälisen uutiskynnyksen on ilmoitettava mahdollisimman pian STUKille [4: 511].

Hyvät käytännöt

Uhkatilanteiden johtaminen on ensisijaisesti viestintää. Kaikkien uhkatilanteen hallintaan liittyvien sidosryhmien on oltava tilannetietoisia uhan kehittymisestä ja niistä toimenpiteistä, joita sidosryhmiltä kulloinkin edellytetään. Ydinvoimalaitoksella erityisesti ydinvoimalaitoksen valvomon, valmiusorganisaation ja turvajärjestelyjen hälytyskeskuksen välinen viestintä on korostunut.

Yrityksen viestintäosaaminen korostuu uhkatilanteissa, joissa pitää pystyä nopeasti ratkaisemaan etenemismallit uhkatilanteen estämiseksi tai sen vaikutusten pienentämiseksi.

Erityisen tärkeää uhkatilanteiden hallinnassa on viestintä viranomaisen kanssa. Koska viranomaisella on pääsääntöisesti vastuu uhkatilanteen hallinnasta, tulee tilannekuvan välittäminen uhkatilanteesta ja sen etenemisestä viranomaiselle varmistaa.

Normaalitilanteen ja uhkatilanteen viestintä ei saa merkittävästi poiketa toisistaan. Viestintävälineinä tulee käyttää normaalioloissa käytettäviä viestintävälineitä ja viestintä menetelmiä. Uhkatilanteissa voidaan joutua käyttä-

mään vaihtoehtoisia viestintätapoja esimerkiksi viestiliikenteen ruuhkautumisen tai sähkökatkojen johdosta. Koulutusta ja harjoituksia on järjestettävä viestintäkyvykkyyden varmistamiseksi uhkatilanteessa.

Viestintään tulee laatia menettelyt, viestintäryhmät ja viestintävälineet. Viestintävälineiden tulee soveltua uhkatilanteiden hoitoon, ja viestinnälle tulee luoda myös korvaavat viestintämenettelyt mikäli pääviestintävälineet eivät ole käytettävissä.

Arviointi

Regulaatio painottaa vaatimuksessaan viranomaisille tehtävää ilmoitusta poikkeavista tapahtumista. Viestinnän onnistuminen perustuu kuitenkin jatkuvaan viestintään ja viestinnän harjoitteluun yrityksessä ja sen sidosryhmissä. Viranomaiselle viestiminen on vain osa tätä kokonaisuutta.

Yrityksen tulisi laatia turvajärjestelyjen viestintäsuunnitelmat ja selvittää niihin liittyvät yrityksen sisäiset ja ulkoiset sidosryhmät.

Regulaatiossa tulisikin painottaa viranomaisviestinnän lisäksi yrityksen sisäisen viestinnän tärkeyttä ja sen harjoittelua normaali- ja uhkatilanteissa.

11 Toiminnan jatkuva parantaminen

Uhkien- ja riskienhallinnan lopputuloksena tulisi syntyä ehdotukset riskien pienentämiseksi ja haavoittuvuuksien vähentämiseksi. Tämä tarkoittaa käytännössä muutoksia toimintaan, jotka voivat edellyttää muutoksia tai tulkintaa voimassaoleviin määräyksiin, ohjeistuksen ja konfiguraatioon. Konfiguraatiolla tässä yhteydessä tarkoitetaan sitä kokonaisuutta, joka muodostuu johtamisjärjestelmästä sekä fyysisestä toimintaympäristöstä laitteineen ja rakennuksineen.

Uhkan ja siihen liittyvien haavoittuvuuksien ja toiminnallisten riskien pienentämiseksi annetaan toimintokohtaisia toimeksiantoja, joihin kootaan kyseiseen aihealueeseen liittyvät muutos ja kehittämistarpeet. Suuremmat kokonaisuudet tulisi toteuttaa projekteina ja pienemmät tarpeet voidaan hoitaa tehtävinä.

Regulaatio

Toimintojen turvallisuusmerkitys on otettava huomioon johtamisjärjestelmää ja sitä koskevia muutoksia suunniteltaessa ja toteutettaessa. Merkittävien muutosten soveltuvuus on arvioitava ennen muutoksen täytäntöönpanoa, ja tällaisten muutosten vaikutuksia on arvioitava ja seurattava [8: 305].

Johtamisjärjestelmän vaikuttavuuteen, toiminnan laatuun ja turvallisuuden hallintaan kohdistuneiden arviointien tulokset on käsiteltävä ja tarvittavat parantamistoimenpiteet on toteutettava suunnitellusti ja priorisoidusti ilman aiheetonta viivettä. Toimenpidesuunnitelmien on sisällettävä tarvittavien resurssien varaaminen [8: 722].

Parantamistoimenpiteiden etenemistä on seurattava. Lisäksi niiden loppuun saattamisesta ja vaikuttavuudesta on varmistuttava [8: 723].

Uhkien ja riskienhallintaan tulisi sisältyä haitallisten tekojen ja niiden mahdollisten seurausten säännöllisen uudelleenarvioinnin. On varmistettava, että käyttöön otetaan asianmukaiset turvajärjestelmät ja toimenpiteet tahallisen teon estämiseksi tai vähentämiseksi [10: 2.6].

Hyvät käytännöt

Johtamisjärjestelmän tulee tuottaa menettelyt, joilla uhat, riskit ja haavoittuvuudet voidaan tunnistaa. Johtamisjärjestelmän on myös huomioitava toimintaan kohdistettavat auditoinnit, katselmoinnit ja erilaiset palautejärjestelmät, joilla toimintaan liittyviä havaintoja voidaan ilmaista.

Organisaation tulisi toteuttaa prosessia, jossa priorisoidaan haavoittuvuuksien arvioinnin ja turvajärjestelmän auditoinnin avulla havaittujen haavoittuvuuksien lieventämistarpeet. Priorisoinnin tulisi perustua liiketoimintaan kohdistuvien riskien arviointiin. Neljää muuttujaa olisi arvioitava priorisoitaessa haavoittuvuuteen liittyviä kehittämis- ja lieventämistoimenpiteitä:

- haavoittuvuuden luonne ja haavoittuvuudella saavutettu haitan taso
- haavoittuvuuden todennäköisyys, että haavoittuvuutta hyväksikäytetään
- kyky suojata haavoittuva omaisuus hyväksikäytöltä
- haavoittuvaan omaisuuteen liittyvä kriittisyys (https://nigesecurityguy.wordpress.com/ 2013/06/20/threat-and-vulnerability-management/).

Muutokset liiketoimintaan tulee aina olla perusteltuja ja joissain tapauksissa muutosten juurisyyt on oltava selvitettävissä. Uhkaperusteisesti tehdyt muutokset antavat laajemman kuvan muutoksen vaikutuksista liiketoimintaan ja siten helpottavat myös päätöksentekijöiden valmiutta suuriinkin muutoksiin. Yhtälailla kun muutokset suunnitellaan uhkaperusteisesti, on muutosten toteutumista ja uuden toimintamallin mukaista toimintaa arvioitava säännöllisesti.

Arviointi

Kaikki muutokset jotka vahvistavat yrityksen turvallisuuskulttuuria ja vaikuttavat yrityksen arvomaailmaan parantavat yrityksen uhkien sietokykyä. Hy-

vään turvallisuuskulttuuriin kuuluu, että turvajärjestelyjä kehitetään jatkuvasti. Oleellista on, että organisaation ymmärrys turvajärjestelyistä, niiden ennaltaehkäisevästä merkityksestä ja estävästä merkityksestä kasvaa.

Kuten aiemmin todettiin, on uhkaperusteinen suunnittelu oltava linjassa liiketoiminnan tavoitteiden ja periaatteiden kanssa. Sellaisia kehittämistehtäviä, joille ei ole riittäviä liiketoiminnallisia tai uhkaperusteisia perusteita tulee välttää.

Turvajärjestelyt ovat normaalitilanteissa näkyvillä kaikessa yrityksen toiminnassa. Turvajärjestelyjä tulisi kehittää jatkuvasti siten, että ne olisivat osa yrityksen päivittäisiä lähes huomaamattomia toimintoja.

12 Yhteenveto

Tässä luvussa tiivistetään vielä keskeiset havainnot ja löydökset tutkittavasta aihealueesta.

12.1 Regulaation vaikutukset ja vaatimuspohja

Toimialaan liittyvällä regulaatiolla ja valvovan viranomaisen asettamilla vaatimuksilla tulisi olla vaikutus yrityksen arvoihin ja sitä kautta myös keskeisiin liiketoiminnan vaatimuksiin ja yrityksen johtamisjärjestelmään.

Viranomaisvaatimukset on yleisesti laadittu hyvin korkean tason vaatimuksiksi, joiden tulkinnassa yrityskohtaisessa toteutustavassa on paljon tulkinnanvaraa. Tämä asettaa yritykselle haasteen muodostaa tarkennetut vaatimukset toiminnalleen asetettujen viranomaisvaatimusten perusteella.

Tässä tutkielmassa esitetyt viranomaisen antamat ohjeet eivät tuota loogisesti järjestettyä esitystä siitä, miten viranomainen haluaa ohjata toimialalla toimivia yrityksiä. Viranomaisen edellyttämän tavoitetilan suunnittelu ja toteutus edellyttävät yritykseltä konseptien luontia, joilla viranomaisen yksittäiset vaatimukset kootaan yrityksen tavaksi toteuttaa vaatimukset omassa liiketoiminnassaan. Asioiden konseptointi auttaa myös viranomaisen kanssa käytävää keskustelua siitä, ovatko yrityksen ja viranomaisen tavoitteet samansuuntaiset.

Regulaatio pyrkii vaatimuksillaan asettamaan kaikille regulaation alaisille yrityksille saman vaatimuksellisen vähimmäistason. Tämä helpottaa sekä viranomaisen valvontatehtävää, että myös toimialan regulaation kehittymistä. Toimialan regulaation tulisi kehittyä niiden kokemusten myötä mitä regulaation alaisten yritysten toiminnasta on saatu kokemuksia.

Regulaatiossa ei ole riittävän hyvin eritelty missä ydinvoimalaitoksen rakentamisen ja käytön vaiheessa regulaation edellyttämät vaatimustenmukaisuus on oltava todennettavissa.

Yritykselle voi olla haastavaa täyttää viranomaisen antama todistamisvelvollisuus vaatimusten täyttymisestä. Regulaation perusteella jää paljon tulkinnan varaa siitä, onko turvajärjestelyt mitoitettu oikein.

Toiminnan jatkuvuus

Jatkuva uhkien ja riskien tunnistaminen ja niihin reagoiminen on perusedellytys jatkuvuudenhallinnalle. Regulaatio käsittelee hyvin niukasti jatkuvuuden hallintaa, mutta painottaa sen merkitystä ydinvoimalaitoksen elinkaaren hallinnassa.

On perusteltua, että turvajärjestelyihin liittyviä arviointeja suoritetaan ja niiden perusteella tehdyt analyysit toimitetaan viranomaiselle tiedoksi. Päätöstä turvajärjestelyjen toteutustavasta ei kuitenkaan tule antaa viranmaiselle. Viranomaisen tulee turvajärjestelyjä hyväksyessään arvioida vain turvajärjestelyjen vaatimustenmukaisuus, eikä viranomaisella pidä olla mahdollisuutta asettaa lisävaatimuksia, ellei erityisesti ole haettu poikkeamaan annetuista vaatimuksista. Turvajärjestelyjen ja yrityksen johtamismallin tulee perustua yrityksen omiin liiketoiminnan tavoitteisiin, eikä viranomainen voi olla päättämässä millaisella taloudellisella panostuksella ja toteutustavalla edellytetyt kyvykkyydet saavutetaan. Turvajärjestelyjen tarkoituksenmukaisuussääntöä tulisi noudattaa.

Regulaation olisi hyvä selkeästi määritellä ne asiat, jotka lisenssinhaltijan määrätään tarkasteltavan määräajoin, ja jotka tulee toimittaa viranomaisille arvioitaviksi.

Uhkienhallinta

Uhkaperusteinen suunnittelu on oltava linjassa liiketoiminnan tavoitteiden ja periaatteiden kanssa. Sellaisia kehittämistehtäviä, joille ei ole riittäviä liiketoiminnallisia tai uhkaperusteisia perusteita tulee välttää.

Regulaatiossa voisi vielä paremmin täsmentää, että uhkien- ja riskien hallinta ei ole erillinen toiminto, vaan uhkien- ja riskien tunnistaminen, arviointi ja niihin reagointi kuuluvat kaikkien yrityksen toimintojen tehtäviin.

Regulaatio olettaa, että suunnitteluperusteuhan mukaisiin uhkaskenaarioihin varautuminen on riittävä suojaamaan ydinvoimalaitosta sitä uhkaavilta lainvastaisilta toimilta. Suunnitteluperusteuhka on kuitenkin kooste vain keskeisimmistä kansalliseen uhkatilanteeseen vaikuttavista uhista. Tarkastelemalla uhkamaailmaa vain suunnitteluperusteuhan antamin perustein, ei riittäviä suunnitteluperusteita uhkien ennaltaehkäisyyn ja niiden toteutuksen valmisteluun estämiseen voida saavuttaa.

Regulaatio ei ota kantaa miten uhka-analyysit pitää suorittaa. Uhka-analyyseille ei ole myöskään mitään kansainvälisesti standardoitua tapaa uhkaskenaarion mallintamiseksi, joka yhtenäistäisi uhkien käsittelytapaa.

Toiminnan tarkastettavuuden kannalta, olisi hyvä määritellä vähintään ne vaiheet, ja tuotokset joita uhkien arviointimenettelyssä tulisi toteuttaa. Olisi myös hyvä tarkentaa, mitkä ovat uhka-analyysin lopputulokset, ja miten niitä tulisi jatkossa hyödyntää.

Riskienhallinta

Regulaatiossa tulisi painottaa voimakkaammin riskianalyysin riskinhallintatoimenpiteiden takaisinkytkentään liiketoimintaan. Takaisinkytkennällä tässä yhteydessä tarkoitetaan riskeistä johdettavien toiminnan muutosten kytkemistä yrityksen kehittämistehtäviin ja kehittämisvastuisiin.

Regulaatiossa painotetaan säteilypäästöjen estämistä ja lainvastaisella toiminnalla aiheutettujen päästöjen minimoimista. Regulaatio myös tunnistaa, että kaikkien riskien toteutumista ei voida estää, vaan on luotava menettelyt, joilla riskin toteutumisen todennäköisyyttä voidaan merkittävästi pienentää.

Tilannekuva ja harjoittelu

Turvajärjestelyjen tilannekuvan välittäminen ja viestinnän onnistuminen perustuvat jatkuvaan viestintään ja viestinnän harjoitteluun yrityksessä ja sen sidosryhmissä. Viranomaiselle viestiminen on tärkeä osa tätä kokonaisuutta. Regulaatiossa tulisikin painottaa voimakkaammin viranomaisviestinnän lisäksi yrityksen sisäisen viestinnän tärkeyttä ja sen harjoittelua normaali ja uhkatilanteissa.

12.2 Havaintoja tutkielmasta

Uhkaperusteinen toiminnan suunnittelu auttaa yritystä ennakoimaan liiketoimintaan kohdistuvia uhkatilanteita, ja hallitsemaan liiketoiminnan haavoittuvuuksia. Hyvä johtamiskulttuuri ja turvallisuuskulttuuri luovat pohjan jatkuvalle turvallisuuden kehittämiselle. Toimiva johtamisjärjestelmä ja siihen sovitetut toimintaprosessit muodostavat tarvittavan ympäristön uhkien hallintaan.

Toimialan regulaatio antaa toiminnalle reunaehtoja, mutta yritys on itse vastuussa liiketoimintansa kannattavuudesta ja siihen tehtävistä investoinneista. Regulaation määrittelemät vaatimukset tulee täyttää, mutta yrityksen täytyy itse arvioida se panostus, jota tarvitaan regulaation ja liiketoiminnasta syntyneiden vaatimusten täyttämiseksi.

Uhkaperusteisessa ajattelussa lähtökohtana on tunnistaa yrityksen suojattava omaisuus ja muodostaa sille riittävä suoja uhkia vastaan. Suojattavaan omaisuuteen kohdistuvat uhat tulee kartoittaa ja analysoida uhkien vaikutuksen pienentämiseksi. Uhkien vaikutuksen pienentämiseksi muodostetaan uhkaskenaariot ja analysoidaan niiden perusteella liiketoimintaan kohdistuvat riskit ja haavoittuvuudet. Riskianalyyseissä huomioidaan, että kaikkia riskejä ei voida poistaa, vaan liiketoimintaan jää aina jäännösriskejä, jotka pitää hallita riskienhallinnan menettelyin.

Riskianalyysejä hyväksikäyttäen muodostetaan liiketoiminnalle uhkaperusteisia vaatimuksia liiketoiminnan suojaamiseksi. Vaatimukset viedään liiketoiminnan eri osa-alueille toteutettaviksi kehittämis- ja muutoshallinnan menettelyin. Regulaation asettamiin vaatimuksiin vaikuttavat muutokset arvioidaan valvovan viranomaisen menettelyin tai kolmannen osapuolen katselmoinnein tai auditoinnein.

Toimintaa arvioidaan jatkuvasti, ja uusien uhkien ilmetessä uhka-analyysejä tarkastellaan uuden uhan näkökulmasta huomioiden uhan vaikutus turvallisuuskulttuuriin, johtamisjärjestelmään, organisointiin, prosesseihin, toimintoihin ja ohjeistukseen. Toiminnassa huomioidaan myös yrityksen liittyminen viranomaistoimintaan ja yrityksen alihankintaketjuihin.

12.3 Tutkimuksen opit

Tutkimusalueen rajaus osoittautui haasteelliseksi. Samalla rajaus antoi mahdollisuuden tutkia Uhkien ja riskienhallinnan merkitystä suhteessa yrityksen toimintamalliin. Mikäli yrityksen toimintaa ohjataan uhkaperusteisesti, voisi se poistaa merkittävästi sellaisia ongelmatilanteita, joihin yritys voi toiminnassaan törmätä valmistautumattomana.

Regulaatio ei voi olla kaiken kattava ohjeistus. Jos näin olisi, se rajoittaisi merkittävästi yrityksen mahdollisuuksia muodostaa oman liiketoimintansa kannata tehokkaimmat ratkaisut. On hyvä, että regulaatio ohjaa toimintaa ylätasolla ja jättää yritykselle mahdollisuuden innovatiivisiin ratkaisuihin.

13 Viiteluettelo

[1] Ydinenergialaki (990/1987).

[2] Valtioneuvoston asetus ydinenergian käytön turvajärjestelyistä (734/2008).

[3] Valtioneuvoston asetus ydinvoimalaitoksen turvallisuudesta (717/2013).

[4] Ydinvoimalaitoksen turvajärjestelyt, STUK YVL A.11 / 15.11.2013.

[5] Osakeyhtiölaki (624/2006).

[6] Säteilyturvakeskuksen määräys ydinvoimalaitoksen turvallisuudesta, STUK Y/1/2016

[7] Säteilyturvakeskuksen määräys ydinvoimalaitoksen turvallisuudesta (25-1)

[8] Turvallisuuden johtaminen ydinalalla, STUK YVL A.3 / 15.3.2019.

[9] SOPIMUS ydinaseiden leviämisen estämisestä, 11/1970.

[10] Nuclear security threat assessment, 11 design basis threats and 12 representative threat statements, IAEA NST058.

[11] Kansallinen turvallisuusauditointikriteeristö, versio II. Puolustusministeriö. KATAKRI II 2011.

[12] IAEA Nuclear Security Series No. 20, Objective and Essential Elements of a State's. Nuclear security regime.

[13] Ydinenergian käytön turvallisuusvalvonta, STUK YVL A.1 / 17.3.2020.

[14] IAEA Nuclear Security Series No. 24-G, Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control.

[15] Ydinvoimalaitoksen todennäköisyysperusteinen riskianalyysi ja riskien hallinta, STUK YVL A.7 / 15.2.2019.

[16] ISO 9001:2015 Laadunhallintajärjestelmät. Vaatimukset. 2015.

[17] Asetus ydinaineiden turvajärjestelyjä koskevista toimista tehdyn yleissopimuksen voimaansaattamisesta ja sen soveltamisesta (SopS 72/1989).

[18] Ydinlaitoksen tietoturvallisuuden hallinta, STUK YVL A.12 / 15.11.2013.

[19] Toiminnan jatkuvuuden hallinta, VAHTI 2/2016

[20] Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Rev.5).

[21] Nuclear Security Series No. 8 Preventive and Protective Measures against Insider Threats IAEA.

[22] Advisera.com https://advisera.com/27001academy/knowledge-base/threats-vulnerabilities/

[23] IAEA Nuclear Security Series No. 24-G, Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control.

[24] Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös. 2.11.2017.

[25] ISO/IEC 27001:2006. Information technology. Security techniques. Information security management systems.

[26] BSI Threats Catalogue – Elementary Threats. Federal Office of Information Security 2012.02.28.