Sähkömarkkinaosapuolen Palvelusopimus liite 5,
Valtuutetun Palvelusopimus liite 5,
Toimeksisaajan Palvelusopimus liite 5,
Muun verkonhaltijan Tiedonvaihtosopimus liite 4

TIETOTURVAVAATIMUKSET DATAHUB-JÄRJESTELMÄN KÄYTÖLLE

1 JOHDANTO

Tässä dokumentissa kuvataan Fingridin Datahub Oy:n (Datahub) tietoturvavaatimukset datahub-järjestelmää käyttäville asiakkaille. Vaatimuksissa painotetaan hyvän tietoturvan ylläpitoa ja kehitystä.

Tarvittaessa Datahubilla on oikeus tarkastaa joko itse tai kolmannen osapuolen toimesta vaatimusten toteutuminen. Datahubin on ilmoitettava Asiakkaalle tarkastuksesta vähintään 30 päivää etukäteen.

2 FINGRID DATAHUB OY:N VASTUUT

Sähkömarkkinalain 49 a § mukaan järjestelmävastaavan kantaverkonhaltijan on huolehdittava sähkökaupan keskitetyn tiedonvaihdon palvelujen tuottamisessa käyttämiinsä tietojärjestelmiin kohdistuvien riskien hallinnasta. Riskien hallinnassa on otettava huomioon mm. tietoturvauhkien ja häiriöiden käsittely.

Datahub on yleisen tietosuoja-asetuksen mukainen henkilötietojen rekisterinpitäjä, johon kuuluu yleisessä tietosuoja-asetuksessa sekä tietosuojalaissa määritellyt vastuut.

3 YLEISET TIETOTURVAVAATIMUKSET

Käyttäessään Datahubin palveluja Asiakkaan on huomioitava tietojen turvaaminen. Tämä kattaa sekä laitteita koskevat tekniset tietoturvavaatimukset, että henkilöiden toimintaan, materiaaleihin ja tietojen käsittelyyn liittyvät ei-tekniset toimenpiteet. Datahub vastaa datahub-järjestelmän riittävästä suojauksesta.

Asiakkaiden tulee noudattaa Datahubin laatimia tietoturvaan liittyviä ohjeita ja seurata tietoturvaan liittyviä tiedotteita. Tietoturvaohjeiden muutoksista Datahub ilmoittaa asiakkaille kirjallisesti.

Asiakas vastaa Asiakkaan laitteiden riittämättömän suojauksen seurauksena Datahubin tietojärjestelmiin tai ohjelmiin tulleista tietokonevirusten tai niihin rinnastettavien haittaohjelmien aiheuttamista välittömistä vahingoista. Fingrid voi käyttää ulkopuolista asiantuntijaa arvioimaan tietoturvan riittävyyttä. Vastuunrajoitukset on määritelty pääsopimuksen kohdassa 13. Asiakas ei saa toteuttaa datahub-järjestelmän käyttöliittymää käyttäviä automatisoituja ratkaisuja niiden toiminnallisuuksien osalta, joille on käytettävissä tekninen sanomarajapinta.

3.1 Pääsyn ja käyttäjäoikeuksien hallinta

Asiakas vastaa oman organisaationsa, mukaan lukien käyttämänsä palvelutoimittajien, osalta henkilöstön ja järjestelmien datahub-järjestelmään pääsyn ja käyttäjäoikeuksien hallinnasta.

3.2 Laitteistot ja ohjelmistot

Asiakkaan on huolehdittava niiden laitteiden, joilla käytetään datahub-järjestelmän palveluja, asianmukaisesta ja ajantasaisesta tietoturvasta. Asiakkaan tulee huolehtia siitä, että kyseiset laitteet ovat eri ohjelmistojen ja käyttöjärjestelmien suhteen päivitysten piirissä, ne on suojattu asianmukaisilla tietoturvatuotteilla (esim. virustorjunta, palomuuri) ja niissä tulee olla luotettava käyttäjähallinta. Käyttöoikeuksien suhteen on noudatettava vähimpien käyttöoikeuksien periaatetta, eli tietojärjestelmän käyttöoikeudet tulee rajata suppeimpiin mahdollisiin oikeuksiin, joilla käyttäjä tai prosessi kykenee suoriutumaan sille määrätystä tehtävästä

4 VARAUTUMINEN DATAHUB-YHTEYKSIEN KATKOON

Datahub-järjestelmän teknisiä rajapintoja hyödyntäviin järjestelmiin kohdistunut tietoturvahyökkäys tai -haavoittuvuus muodostavat tietoturvariskin myös datahub-järjestelmälle. Datahubilla on oikeus katkaista yhteydet järjestelmään, jonka epäillään aiheuttavan tietoturvauhan datahub-järjestelmälle. Datahubin tulee ilmoittaa Asiakkaalle yhteyden katkaisemisesta.

Asiakkaan tulee varautua tilanteeseen, joissa yhteydet datahub-järjestelmään joudutaan katkaisemaan tietoturvauhan takia. Asiakas tiedostaa, että sen sähkömarkkinalainsäädännössä määritellyt velvoitteet ovat voimassa, vaikka Asiakas ei pysty toimittamaan tai hakemaan tietoa datahub-järjestelmästä sen teknisten rajapintojen kautta.

5 VAATIMUKSET TIETOTURVAN HALLINTAAN

Asiakkaan on noudatettava sisäisesti omaa tietoturvan hallintamallia datahub-järjestelmän käyttöön liittyvissä asioissa. Hallintamalli voi perustua olemassa oleviin laatujärjestelmiin tai standardeihin esimerkiksi ISO27001:een. Sen on oltava jatkuvasti tarkentuva ja kehittyvä. Mallin on katettava mahdolliset käytettävät alihankkijat. Malli on dokumentoitava sekä katselmoitava ja tarvittaessa päivitettävä säännöllisesti.

Asiakkaan on kyettävä osoittamaan, että sen toiminnassa huomioidaan tietoturva. Asiakkaalla tulee olla tietoturvapolitiikka tai vastaava esim. toimintamalli, jolla yrityksen johto on määrittänyt toimintaperiaatteet tietoturvalle. Yrityksen johdon tulee myös olla sitoutunut tietoturvaan ja sen kehittämiseen. Tietoturva on oltava selkeästi vastuutettu yrityksen sisällä. Tietoturvapolitiikan periaatteet on myös oltava viestitetty omalle henkilöstölle sekä tarvittaessa käytettäville alihankkijoille.

Datahub ei kuitenkaan kerää tietoturvan hallintaan liittyvää dokumentaatiota asiakkailta.

Datahubin tulee vastaavasti noudattaa omaa tietoturvan hallintamallia.

Hallintamallin vähimmäisvaatimukset on esitetty kohdissa 5.1 - 5.4 .

5.1 Tietoturvan hallinnan suunnittelua koskevat vaatimukset

5.1.1 Riskiarvio

Asiakkaan tulee toteuttaa sisäinen riskiarvio roolistaan datahub-järjestelmän käyttäjänä sekä datahub-järjestelmään liittyvästä tietoturvastaan.

Riskiarviossa on tunnistettava ainakin seuraavat kohdat:

- Mitkä tahot ovat riippuvaisia Asiakkaan toimivasta ja luotettavasta datahub-järjestelmän käytöstä ja miten?
- Miten Asiakkaan oma liiketoiminta on riippuvainen toimivasta ja luotettavasta datahub-yhteydestä, sekä sen valtuuttamista kolmansista osapuolista datahub-järjestelmän käytössä?
- Mitä teknisiä ja organisatorisia haavoittuvaisuuksia Asiakkaan organisaatiossa tulee olemaan datahub-järjestelmän käyttöönoton jälkeen? Mitkä teknologiat ja palvelut sisältävät tai ovat osa näitä haavoittuvaisuuksia (esimerkiksi mitkä järjestelmät tuottavat tietoa datahub-järjestelmään)?
- Mitkä toimijat saattavat käyttää hyväksi todettuja haavoittuvaisuuksia ja miksi?
- Mille uhille organisaatio sekä siitä riippuvat osapuolet altistuvat, jos Asiakkaan yhteys datahub-järjestelmään joudutaan katkaisemaan? Uhkien arvioinnissa on otettava huomioon tilanteiden kehittyminen, jos Asiakkaan takaisinkytkentä datahub-järjestelmään pitkittyy.

5.1.2 Tietoturvaohjelma

Riskiarvion pohjalta Asiakkaan tulee luoda tietoturvaohjelma.

Tietoturvaohjelma on kommunikoitava asianmukaiselle henkilökunnalle ja otettava käyttöön viimeistään datahub-järjestelmän käyttöönoton yhteydessä.

Tietoturvaohjelman on otettava kantaa kaikkiin riskiarviossa ilmeneviin riskeihin ja joko hyväksyttävä ne tai määriteltävä tarpeelliseksi nähdyt varotoimenpiteet (suojaus, vastaus ja palautuminen) perustellusti.

Tietoturvaohjelman on otettava huomioon henkilöstön rooli tietoturvan toteuttamisessa.

Tietoturvaohjelman on otettava huomioon kohdissa 5.2 5.3 5.4 kuvatut vaatimukset.

Tietoturvaohjelma ja kaikki muutokset tietoturvaohjelmaan on dokumentoitava perusteluineen.

Tietoturvaohjelma on pidettävä ajan tasalla ja päivitettävä tarvittaessa.

Tietoturvaohjelman voi toteuttaa osana laajempaa, mahdollisesti jo olemassa olevaa tietoturvasuunnitelmaa.

5.1.3 Toipumissuunnitelma

Riskiarvion pohjalta on luotava toipumissuunnitelma sille tilanteelle, että Asiakas joudutaan kytkemään irti datahub-järjestelmästä.

Asiakkaan velvollisuus hoitaa lakisääteisiä tehtäviään säilyy Asiakkaalla, vaikka asiakkaalla ei ole pääsyä datahub-järjestelmän teknisiin rajapintoihin

Toipumissuunnitelman vaatimien käytäntöjen käynnistyessä Asiakkaan on kommunikoitava tilanteensa etenemisestä kaikille asianmukaisille tahoille perustuen sen riskiarvioissa ilmentyneisiin riippuvuussuhteisiin.

5.2 Teknisiä kontrolleja koskevat vaatimukset

5.2.1 Järjestelmien suojaus

Kaikki järjestelmät, jotka luovat datahub-järjestelmään tietosisältöä, tai hakevat siitä tietoa, on suojattava. Lisäksi suojauksen on katettava kaikki organisaation omassa hallinnassa olevat järjestelmät, joiden tieto kulkeutuu datahub-järjestelmään tai jotka osallistuvat datahub-järjestelmän B2B-rajapintaan lähetettävien sanomien muodostamiseen. Suojauksen on katettava myös kaikki yhteydet kyseisiin järjestelmiin.

Järjestelmiin tulee sallia kirjautuminen vain siten, että käyttäjän henkilöllisyys voidaan todentaa.

Käyttäjätunnuksiin on sovellettava vähimpien käyttöoikeuksien periaatetta.

Käyttäjätunnukset on hallittava ja katselmoitava säännöllisesti.

Järjestelmien valvontaan on kuuluttava ainakin:

- Riittävät menettelyt turvallisuuteen liittyvien tapahtumien jäljitettävyyteen sekä poikkeamien ja haavoittuvuuksien havainnointikykyyn, esimerkiksi toteuttamalla asianmukainen lokitusjärjestelmä.
- Valvontamenetelmien asianmukaisen aktiivinen käyttö niin, että tietoturvapoikkeamat ja mahdolliset haavoittuvuudet havaitaan ja selvitetään riskien minimoimiseksi
- Valvontamenetelmiin oleellisesti kuuluvien havaintojen tallennusjärjestelmien kuten lokituksen suojaus niin, että niiden sisältämän tiedon luvaton muuttaminen tai tuhoaminen estetään.

Järjestelmien käyttämien palvelinten kellot on oltava synkronoituja keskenään.

5.2.2 Datahub-järjestelmään välitettävien tietojen suojaus

Kaikki tieto, joka tulee muodostamaan datahub-järjestelmään välitettävän tietosisällön, on suojattava asianmukaisin keinoin.

Suojauksen on katettava tiedon säilytysaika, käsittely sekä tiedon kulku syntyhetkestään datahub-järjestelmään.

Suojaus on toteutettava niin, että suojeltava tieto ei vuoda oikeudettomien osapuolten käsiin eikä datahub-järjestelmään pääse oikeudettomasti muutettua tietoa.

5.2.3 Datahub-järjestelmästä vastaanotettujen tietojen suojaus

Kaikki datahub-järjestelmästä vastaanotettu tieto on suojattava asianmukaisin keinoin.

Suojauksen on katettava se ajanjakso, milloin tieto kulkeutuu datahub-järjestelmästä Asiakkaan järjestelmiin, sekä tiedon säilytyksen aika Asiakkaan järjestelmissä ja tiedon käsittely.

Suojaus on toteutettava niin, että suojeltava tieto ei vuoda oikeudettomien osapuolten käsiin eikä sitä muuteta oikeudettomasti.

5.2.4 SSL-sertifikaattien suojaus

Teknisen yhteyden muodostamisessa käytettävä SSL-sertifikaatti on Asiakkaan tekninen identiteetti. Asiakkaan tulee varmistaa, että tietoliikenteessä käytettävä sertifikaatti ei joudu asiattomien henkilöiden tai organisaatioiden käsiin. Kaikki Asiakkaan sertifikaatilla suoritetut toiminnot datahub-järjestelmässä tulkitaan Asiakkaan itsensä suorittamiksi.

5.3 Reagointikykyä koskevat vaatimukset

5.3.1 Tietoturvaloukkauksista ilmoittaminen

Tietoturvaloukkauksista ilmoittamiseen liittyvät vaatimukset on kuvattu pääsopimuksen kohdassa 10.2. Tietoturvaloukkauksista ilmoitetaan Datahubin Tukipalvelun kautta.

5.4 Henkilöstön tietoturvaosaamista koskevat vaatimukset

Asiakas vastaa datahub-järjestelmää käyttävän henkilöstönsä ja käyttämänsä palveluntoimittajien henkilöstön tietoturvakoulutuksesta tietoturvakäytäntöineen. Koulutuksen on annettava datahub-palvelua käyttäville henkilöille riittävät tiedot palvelun käyttöön sekä sen sisältämiin tietoihin liittyvistä tietoturva-, ja tietosuojavaatimuksista. Heidän on myös tiedostettava tietosuojaan liittyvät lainsäädännölliset vaatimukset.

Asiakkaalla on oltava tietoturvaohjelman jatkuvuudesta, toimivuudesta sekä päivityksestä vastaava henkilö sekä vähintään yksi varahenkilö

Henkilöillä on oltava välittömät oikeudet katkaista tai antaa lupa katkaista datahub-järjestelmän kanssa kommunikoivien järjestelmien yhteydet datahub-järjestelmään.

Henkilöiden on tunnettava riskiarvio, tietoturvaohjelma sekä toipumissuunnitelma niin, että he kykenevät suorittamaan tehtävänsä perustellusti ja ymmärtävät sen roolin laajemmassa kuvassa.

Turvallisuushavaintojen käsittely ja ulospäin kommunikointi tulee olla vastuutettu.

Henkilöiden on vastattava riskiarvion, tietoturvaohjelman sekä toipumissuunnitelman tarkistamisesta ja tarvittaessa niiden päivityksestä.