Liite 4 Hall 8-6-2018

Kouvolan Vesi

TIETOTURVAPOLITIIKKA

Versio: 1.0

Pvm: 5. Huhtikuuta 2018

Kouvolan Vesi

SISÄLTÖ

Tietoturvan tavoitteita ja siihen liityviä käsitteitä

Tämä tietoturvapolitiikka heijastaa Kouvolan Vesi Oy:n liiketoimintaan kohdistuvia lakisääteisiä, sopimussääteisiä ja liiketoimintapohjaisia tietoturvavaatimuksia. Tietoturvapolitiikka on myös omalta osaltaan vaatimusmäärittely, jota Kouvolan Vesi Oy:n organisaation, toimittajien ja ICT-palvelujen on noudatettava.

Tietoturvan tavoitteena on turvata Kouvolan Vesi Oy:n liiketoiminnan jatkuvuus, lainmukaisuus ja sopimustenmukaisuus sekä omalta osaltaan ennaltaehkäistä mahdollisia häiriöitä ja vahinkoja.

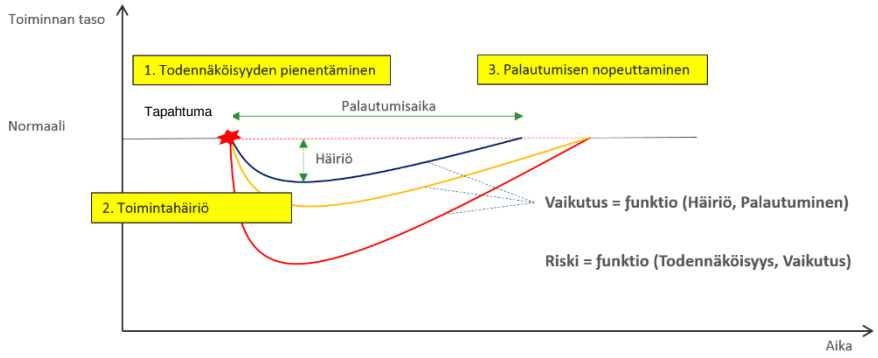
Tärkeitä mittareita tietoturvan onnistumisessa on:

1. Kouvolan Vesi Oy:n käsittelemien ja varastoimien tietojen luottamuksellisuuden, eheyden, saatavuuden ja jäljitettävyyden säilyttäminen kaikissa olosuhteissa
2. Auditoinneilla saatava varmuus siitä että tietoturvapolitiikan mukaiset säännöt toteutuvat Kouvolan Vesi Oy:n liiketoiminnassa, ICT-palveluissa ja niiden käytössä
3. Jatkuva tehostaminen tietoturvan laadussa ja kustannuksissa.
4. Turvata Kouvolan Vesi Oy:n liiketoiminnan jatkuvuus

Tietoturvan tavoitteissa käytetyt käsitteet:

1. Tiedon *luottamuksellisuudella* tarkoitetaan sitä, että tieto on ainoastaan siihen oikeutettujen käyttäjien saatavilla
2. Tiedon *eheydellä* tarkoitetaan sitä, että tietoa voi lisätä, muokata ja poistaa ainoastaan siihen oikeutetut henkilöt
3. *Saatavuudella* tarkoitetaan sitä, että järjestelmät ja palvelut sekä niiden sisältämät tiedot ovat käyttäjien saatavilla, eikä niissä esiinny tietoturvasta aiheutuvia palvelukatkoja
4. *Jäljitettävyydellä* tarkoitetaan sitä, että pystytään osoittamaan kuka on käsitellyt tietoa tai palvelua ja/tai kenellä on ollut mahdollisuus siihen

Alla oleva kuva havainnollistaa Kouvolan Vesi Oy:n tietoturvapolitiikan ja riskienhallinnan tavoitteita.



Toisaalta pyritään pienentämään todennäköisyyksiä, että tietoturvauhat toteutuvat ja toisaalta pyritään pienentämään mahdollisen toteutumisen aiheuttamaa häiriötä ja nopeuttamaan palautumista toiminnan normaaliin tilaan.

Kuvassa:

- Yrityksen toiminta häiriintyy tietoturvatapahtuman johdosta ja häiriön suuruudelle on piirretty kolme eri vaihtoehtoa. Punainen on suurin häiriö ja sininen on pienin häiriö.
- Palautuminen häiriöstä takaisin ns. normaalitasoon voi olla eripituista. Sinisestä häiriötilasta on palautuminen nopeampaa kuin keltaisesta ja punaisesta.
- Insidentin aiheuttama vaikutus yritykselle määräytyy häiriön suuruuden ja keston perusteella.
- Riski määräytyy insidentin todennäköisyyden ja sen aiheuttaman vaikutuksen perusteella.

Tietoturvan johtaminen

Tietoturvaa johdetaan tietoturvapolitiikalla ja riskienhallintapolitiikalla. Tietoturvapolitiikan tehtävänä on saada organisaatio, sen käyttämät palvelut[1] ja palveluntarjoajat toimimaan Kouvolan Vesi Oy:n kohtaamien vaatimusten mukaisesti noudattaen tietoturvan ”hyvää käytäntöä”.

Tietoturvapolitiikka ei aina kerro sitä konkreettista tapaa, jolla tietoturvapolitiikan mukaiset vaatimukset saavutettaisiin. Joissakin asioissa tietoturvapolitiikka on hyvinkin tarkka, säätäen esim. kuinka pitkiä salasanojen tulee olla tai kuinka usein näitä on vaihdettava. Tietoturvapolitiikan soveltamista varten voidaan tuottaa erillisiä ohjeistuksia.

Tietoturvapolitiikka ei myöskään voi huomioida kaikkia mahdollisia tietoturvaa vaarantavia tilanteita, joiden takia käyttäjillä on erityinen vastuu erilaisten uhkien torjumisessa ja mahdollisten tietoturvahäiriöiden tunnistamisessa. Aktiivinen riskienhallinta on myös erittäin

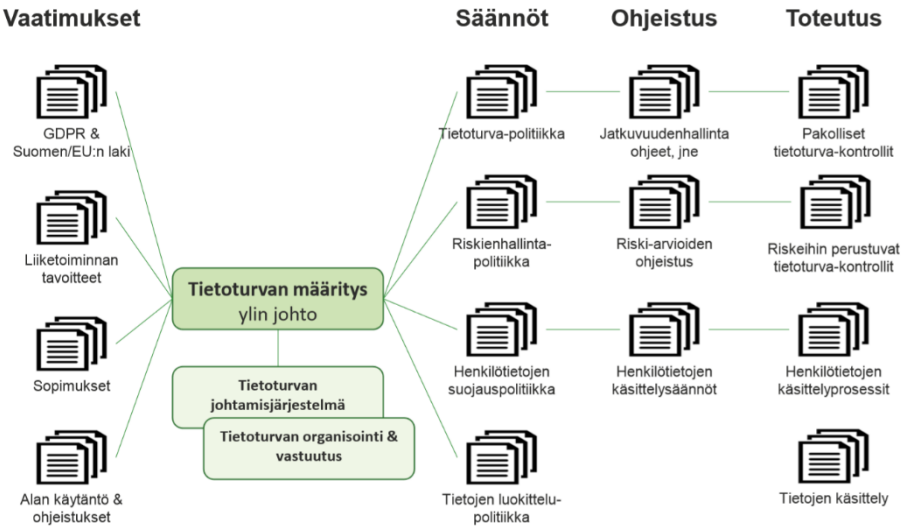
[1] Palvelu on yleisnimi kaikille niille toiminnoille, ICT-järjestelmille, jne. joita organisaatio käyttää toiminnassaan. Esimerkkejä palveluista ovat mm. henkilöstöhallinto, taloushallinto, tietoverkko, työasema(t). Palvelut koostuvat usein useasta eri kohteesta, kuten ohjelmistoista, sovelluspalvelimista, jne.

tärkeää, jotta kaikki uhat saadaan tunnistettua ja riittävästi mitigoitua. Riskienhallinnassa ei käytetä sanamuotoa ”riskien eliminointi”, koska riskejä voidaan harvoin kokonaan eliminoida – ja mitigointi tarkoittaa uhan toteutumisen todennäköisyyden alentamista ja/tai uhan toteutumisen aiheuttaman vahingon pienentämistä.

Seuraava esimerkki valottaa tietoturvapolitiikan ja riskienhallinnan välisestä yhteistyöstä:

- Tietoturvapolitiikan mukaisesti yhtiön palvelinten sähkönsaanti tulee turvata kaikissa olosuhteissa
- Riskiarviossa todetaan uhaksi sähkökatko yleisessä sähkönjakelussa. Riskiarvion mukaisesti yleisen sähkökatkon todennäköisyyttä ei voida pienentää, mutta sen aiheuttamaa vahinkoa voidaan pienentää käyttämällä UPS-akkuja ja diesel-generaattoreita. Riskianalyysin mukaisesti myös UPS-akuissa ja Diesel-moottoreissa voi olla häiriöitä, jolloin niitä tulee jatkuvasti huoltaa, koekäyttää ja kahdentaa.
- Lopputuloksena yrityksen palvelinten käytössä on kahdennetut UPS-akut, kahdennetut diesel-generaattorit, joita kaikkia huolletaan ja koekäytetään säännöllisesti, vaikka näitä turvamekanismeja ei ole erikseen määrätty tietoturvapolitiikassa.

Alla oleva kuva visualisoi kuinka yrityksen johto muuntaa yritykseen kohdistuvat ulkoiset ja sisäiset vaatimukset tietoturvaan liittyvien politiikkojen ja ohjeiden avulla käytännön työhön. Viime kädessä, kun kaikki toimivat annettujen tietoturvapolitiikkojen ja ohjeiden mukaisesti, varmistuu että yritys toimii kokonaisuudessaan lakien, sopimusten ja yritykseen kohdistuvien hyvien hallinto-odotusten mukaisesti.



Kuva 2: Tietoturvapolitiikka on osa ketjua, jolla yritys turvaa yhdenmukaisuutensa lakien, sopimusten, omistajien ja muiden sidosryhmien asettamien tavoitteiden mukaisesti

Tietoturvapolitiikka ja riskienhallintapolitiikka muodostavat kokonaisuuden, jolla pyritään eliminoimaan toistuvat uhat (tietoturvapolitiikan avulla) sekä uudet tai kertaluonteiset uhat (riskienhallintapolitiikan avulla).

Kouvolan Vesi

Ohjeistus auttaa organisaatiota toteuttamaan tarvittavan suojauksen, jotta saavutetaan yhdenmukaisuus tietoturvapolitiikan kanssa.

Tietoturvapolitiikan määritelmä

Tietoturvapolitiikka on yhtiön johdon hyväksymä ja sen noudattaminen on pakollista jokaiselle Kouvolan Vesi Oy:lle töitä tekevälle henkilölle riippumatta siitä mikä on henkilön työ- tai toimeksiantosuhde Kouvolan Vesi Oy:n kanssa. Vastaavasti jokaisen organisaation, joka tuottaa palveluita Kouvolan Vesi Oy:lle, on noudatettava tietoturvapolitiikkaa Kouvolan Vesi Oy:lle toimitetuissa palveluissa.

Tietoturvapolitiikan auditointi

Tietoturva-politiikka tulee auditoida vähintään kerran vuodessa, jolloin tulee arvioida mm. onko Kouvolan Vesi Oy:n toimintaympäristössä tapahtunut sellaisia muutoksia jotka edellyttävät muutoksia tietoturvapolitiikkaan tai onko ICT-järjestelmien operoinnissa tai käyttäjien kokemuksissa havaittu sellaisia asioita, jotka vaativat vastaavia muutoksia tietoturvapolitiikkaan.

ICT-järjestelmien, prosessien ja muiden käytäntöjen tietoturva-auditointi

Kouvolan Vesi Oy:n ICT-järjestelmät, prosessit, jne. tulee vähintään kerran vuodessa auditoida. Tavoitteena on turvata Kouvolan Vesi Oy:n toiminta ja varmistaa, että se noudattaa yrityksen hyväksymää tietoturvapolitiikkaa ja että näissä ei ole sellaisia tietoturvariskejä jotka vaarantavat Kouvolan Vesi Oy:n liiketoiminnan jatkuvuuden tai aiheuta mahdollisia häiriöitä siihen.

Tietoturva-auditointitiedon suojaaminen

Kaikki tietoturvaan liittyvät auditointitiedot ja riskiarviot ovat luottamuksellisia ja merkittäviä puutteita indikoivat tiedot ovat salaisia. Näin turvataan, ettei näitä tietoja tai niiden osoittamia heikkouksia pystytä hyödyntämään vahingollisessa tarkoituksessa ennen kuin Kouvolan Vesi Oy on ehtinyt korjaamaan havaitut heikkoudet.

Riskienhallintapolitiikka

Riskienhallinta koskee kaikkien mahdollisten uhkien mitigointia, eikä se siten rajoitu yksistään tietoturvaan kohdistuviin uhkiin. Tämän takia riskienhallintapolitiikka on kuvattu erillisessä dokumentissa.

Tietoturvaan liittyvässä riskienhallinnassa on noudatettava seuraavaa:

1. Tietoturvaan liittyvät riskiarviot on tehtävä palvelu/toimintokohtaisesti siten, että riskiarvio kattaa kaikki palvelussa/toiminnossa tarvittavat/käytetyt ICT-laitteet

2. Riskiarviot on tehtävä vähintään kerran vuodessa ja aina kun palvelussa/toiminnossa/laitteissa tehdään merkittävä muutos

3. Riskiarviot ovat luottamuksellisia ja jos niissä ilmenee merkittäviä riskejä – ovat nämä tiedot salaisia, jotta heikkouksia/haavoittuvuuksia ei pystyttäisi hyödyntämään vahingollisessa tarkoituksessa

Tietoturvan vastuuttaminen organisaatiossa

Tietoturvan toteuttamisesta vastaa yrityksen ylin johto tietoturvapolitiikan mukaisesti ja toteutus tapahtuu koko organisaatiossa, sen kaikilla eri tasoilla. Tämän takia vastuu tietoturvasta ja toiminnan jatkuvuuden turvaamisesta on vastuutettava niille henkilöille, jotka käytännössä pystyvät vaikuttamaan tietoturvan toteutumiseen.

Käytännössä tämä tarkoittaa, että jokainen Kouvolan Vesi Oy:n toimintaan osallistuva henkilö ja yritys on velvoitettu:

1. Noudattamaan Kouvolan Vesi Oy:n tietoturvapolitiikkaa
2. Havainnoimaan ja raportoimaan mahdollisista tietoturvapolitiikan rikkomuksista
3. Havainnoimaan ja raportoimaan oman toimialueensa riskeistä ja heikkouksista, jotka vaarantavat Kouvolan Vesi Oy:n tietoturvaa

Näiden koko organisaatiota koskevien vastuiden lisäksi on Kouvolan Vesi Oy:n johdolla ja tietoturvavastaavalla seuraavat nimetyt vastuut:

1. Hallitus
    a. Hyväksyy tietoturvaan liittyvät politiikat, kuten tietoturvapolitiikan, riskienhallintapolitiikan, henkilötietojen suojauspolitiikan, tietojen luokittelupolitiikan, jne.
2. Yrityksen johtoryhmä
    a. Nimittää tietoturvaorganisaation – tietoturvan ohjausryhmän
    b. Varaa riittävät resurssit tietoturvasta vastaavien käytettäväksi, jotta tietoturvapolitiikka ja sen tavoitteet toteutuvat
    c. Luokittelee liiketoiminnon tarvitsemat järjestelmät eri kriittisyysluokkiin, jotka heijastavat kunkin järjestelmän tärkeyttä Kouvolan Vesi Oy:n toiminnoille ja kuinka suurta vahinkoa tietomurrot voivat kussakin järjestelmässä aiheuttaa
    d. Nimeää palvelujen omistajat
3. Palvelujen omistajat
    a. Tunnistaa eri järjestelmien väliset riippuvuussuhteet
    b. Tunnistaa palveluihin liittyvät henkilörekisterit, rekisterinpitäjän ja käsittelijän roolit

c. Monitoroida palveluihin liittyviä riskejä, jotta riskit säilyvät riskienhallintapolitiikan sallimissa tasoissa

Tietoturvan huomioiminen projekteissa

Projektit heijastavat uuden kehittämistä tai muutosta johonkin olemassa olevaan. Uuden kehittämisessä ja muutoksissa ei ole kokemuksen antamaa turvaa, jolloin näissä on myös suurempi riski heikkouksien ja haavoittuvuuksien syntymiselle.

Tämän takia on tärkeää, että projektityössä tehdään laadukkaita riskiarvioita ja että niissä pyritään tunnistamaan kaikki mahdolliset tietoturva uhkat, näiden todennäköisyydet ja vaikutukset – ei sallittujen riskitasojen mitigoimiseksi.

Riskienhallinta ja tietoturvapolitiikan noudattaminen projektin tuotoksissa on oltava mukana projektin alusta lähtien.

Kouvolan Vesi Oy:n toiminnan suojaaminen tietoturvalla

Tietoturvakontrollit ovat keinoja ja ohjelmistoja, joilla pyritään turvaamaan tietojen luottamuksellisuus ja eheys, palvelujen saatavuus sekä tapahtumien jäljitettävyys. Palvelujen suojaamisessa on noudatettava seuraavaa menetelmää:

1. Palvelujen tunnistaminen ja tietoturvaluokittelu

    - Kouvolan Vesi Oy:n toiminta on riippuvainen erinäisistä tuotantoresursseista, kuten henkilökunnasta, veden tuottamisesta ja jakelussa käytettävästä automaatiosta, alihankkijoista, tietotekniikasta, jne. Palvelun tunnistamisessa tulee tunnistaa myös sen tuottamiseen tarvittavat resurssit. Esimerkiksi kun tunnistetaan ’Kouvolan Vesi Oy:n sisäinen tietoverkko’-palvelu, on myös tunnistettava mitkä kaikki reitittimet, kytkimet, tukiasemat, hakemistot ja muut laitteet/ohjelmistot osallistuvat tämän sisäverkko-palvelun tuottamiseen.

    - Kaikki tunnistetut palvelut tulee tietoturvaluokitella niihin mahdollisesti tulevien häiriöiden aiheuttamien vahinkojen perusteella. Vahinkoja ovat palvelun 1) sisältämien tietojen luottamuksellisuuden tai eheyden menetys, 2) saatavuuden menetys ja 3) tapahtumien jäljitettävyyden menetys. Mahdollisten vahinkojen perusteella tehtyä luokittelua tulee käyttää riskienhallinnassa, jatkuvuussuunnittelussa ja tietoturvan mitoituksen suunnittelussa.

2. Palvelujen välisten riippuvuussuhteiden tunnistaminen

    - Palvelujen väliset riippuvuussuhteet on tunnistettava. Riippuvuussuhteella tarkoitetaan sitä, että yhdessä palvelussa oleva häiriö vaikuttaa toisen palvelun toimivuuteen. Esim. sähköpostipalvelun saatavuus on riippuvainen internet-yhteyden (palvelusta) saatavuudesta.

    - Palvelujen välisiä riippuvuussuhteita tulee hyödyntää palvelujen jatkuvuussuunnittelussa ja palvelujen kriittisyysluokittelussa. Esim. useimmat liiketoimintasovellukset ovat riippuvaisia internet-yhteyden saatavuudesta ja luottamuksellisuudesta, jolloin Internet-yhteyden kriittisyys määräytyy siitä riippuvaisten muiden palvelujen kautta.

3. Palveluihin liittyvien riskien riskienhallinta

    - Riskienhallinnalla tulee palveluihin kohdistuvat riskit mitigoida[2] niin että riskit eivät ylitä Kouvolan Vesi Oy:n hyväksymiä riskitasoja[3].

4. Palvelujen suojaamiseksi soveltuvien tietoturvakontrollien tunnistaminen

[2] Mitigoinnilla tarkoitetaan kaikkia niitä keinoja, joilla uhan aiheuttavaa riskiä pienennetään, joko vähentämällä uhan toteutumisen todennäköisyyttä tai sen aiheuttaman vahingon suuruutta
[3] Riskitaso määräytyy arviosta uhan toteutumisen todennäköisyydestä ja arviosta sen aiheuttamasta vahingosta. Hyväksytyt riskitasot on määritelty Kouvolan Vesi Oy:n riskienhallintapolitiikassa

- Tuotantohäiriöiden ehkäisemiseksi ja tietoturvan ylläpitämiseksi on kaikki palvelut suojattava soveltuvin tietoturvakontrollein.
- Palvelun suojaamiseksi soveltuvista tietoturvakontrolleista on tehtävä kirjallinen soveltamissuunnitelma (statement of applicability, SOA)

5. Soveltuvien tietoturvakontrollien käyttöönotto

    - Soveltamissuunnitelman mukaiset tietoturvakontrollit tulee ottaa käyttöön ISO 27002 standardin mukaisesti. Poikkeamat käyttöönoton soveltamissuunnitelmasta tai ISO 27002 standardista tulee raportoida tietoturvan ohjausryhmälle.

6. Käyttöönotettujen tietoturvakontrollien seuranta, auditointi ja kehittäminen

    - Käyttöönotettujen tietoturvakontrollien toimintaa ja mahdollisia hälytyksiä tulee seurata niin että tietoturvakontrollien mahdollisiin toimintahäiriöihin ja hälytyksiin voidaan reagoida.

    - Mahdolliset toimintahäiriöt ja hälytykset tulee ilmoittaa tietoturvavastaavalle ja niihin on reagoitava asiaankuuluvalla tavalla.

7. Tietoturvavaatimusten seuranta ja niihin sopeutuminen

    - Kouvolan Vesi Oy:n toimintaympäristöä on seurattava, jotta siinä mahdollisesti tapahtuvat muutokset pystytään huomioimaan tietoturvassa. Sopivia lähteitä toimintaympäristön muutosten seurantaan on mm. kyberturvakeskuksen tiedotteet ns. huoltovarmuus kriittisille yrityksille, toimialajärjestö(t), lehdistö, jne. Toimintaympäristössä tapahtuvien muutosten vaikutukset tulee huomioida Kouvolan Vesi Oy:n tietoturvapolitiikassa ja tietoturvaan liittyvissä käytännöissä.

    - Kouvolan Vesi Oy:n tulee katselmoida tietoturvapolitiikka, palvelukohtaiset tietoturvakontrollien soveltamissuunnitelmat ja mahdolliset muutokset tietoturvakontrollien toteutusohjeissa (ISO 27002) vähintään kerran vuodessa.