KYBERTURVA ICT-SOPIMUKSISSA

– Vältä yleiset karikot

HUOLTOVARMUUSORGANISAATIO

KYBERTURVA ICT-SOPIMUKSISSA

– Vältä yleiset karikot

www.huoltovarmuus.fi

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa.

Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta.

Julkaisija:
Huoltovarmuuskeskus / Digipooli

Oppaan tekijä:
Jatkuvuuskonsultointi Oy

Kuvat: Shutterstock

Taitto: Up-to-Point Oy

Julkaisuvuosi: 2021

ISBN: ISBN 978-952-5608-88-5

Sisältö

VÄLTÄ ITC-SOPIMUKSEN KARIKOT

– Muista ainakin nämä

Määrittele tarpeesi selkeästi

- Suunnittele hankintasi osana kokonaisuutta
- Kuvaa mitä haluat saavuttaa ja mitkä ovat vaatimuksesi
- Sovita vaatimusten taso hankinnan mukaisesti
- Ota palveluntarjoajat mukaan, varmista yhteinen näkemys

Muista tarjouspyynnössä ja tarjouksissa

- Selkeät tavoitteet ja vaatimukset
- Kehityssuunnitelma ja toimintaympäristön muutokset
- Huomioi vakioprosessien rajoitukset
- Jätä tilaa palveluntarjoajan ehdotuksille

Huomioi sopimuksessa

- Muista hallinnointimalli
- Kokoa yhteinen näkemys kokonaisuudeksi ja tee muutokset aina kirjallisesti
- Varmista yhteinen ymmärrys palvelun sisällöstä ja vastuista
- Tarkista, että palvelu vastaa tarpeistasi ja vaatimuksiasi

Ylläpidä yhteistä näkemystä

- Muista säännölliset sopimuksen läpikäynnit
- Tarkista, vastaako toiminta sovittua
- Tarkista esimerkeillä vastuunjaon toimivuus ja yhteinen näkemys
- Tee muutokset aina kirjallisesti

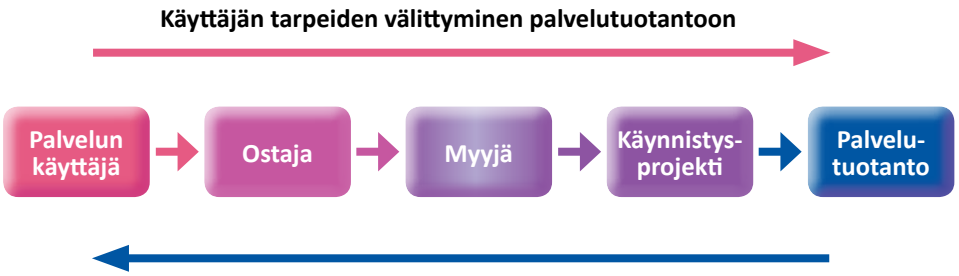
1 YHTEENVETO

Onnistuneiden tieto- ja viestintäpalvelusopimusten (ICT-palvelusopimusten) ja niiden palvelun toteutumisen perustana on kaikkien osapuolten samanlainen käsitys palvelun sisällöstä, vastuista ja tehtävistä. Pitkäkestoisten sopimusten velvoitteet määrittelevät osapuolten välisen yhteistyön pelisäännöt. Sopimuksen tarkoituksena ei ole vain kuvata hankinnan kohdetta, vaan ennen kaikkea taata, että sopimuksen osapuolet saavuttavat tavoittelemansa hyödyt.

Tämä opas antaa asiakkaalle malleja ja tukea ICT-palvelusopimuksien tekemiseen. Opasta varten haastateltiin kotimaisia yrityksiä, jotka raottivat kokemuksiaan epäonnistuneista sopimussuhteista ja esiin nousseista ongelmista yhteistyössä tai vastuunjaossa. Opas perustuu haastatteluissa esille nousseisiin tapauksiin. Yksittäisiä tapauksia on ohjeessa mukana esimerkkeinä sekä laajemmin kuvattuna ohjeen liitteessä. Useimmat esille nousseet haasteet liittyivät tietoturvavaatimuksiin ja tietoturvan huomioimiseen sopimuksissa.

Sopimuksen tavoitteen saavuttamiseksi on tärkeää, että asiakkaan ja palveluntoimittajan organisaatio muodostavat yhteisen näkemyksen sopimuksen sisällöstä. Sopimuksen laatimisen ja sopimuksen mukaisen palvelun toteuttamiseen eri vaiheisiin osallistuvat lukuisat eri henkilöt tai tiimit sekä asiakkaan että palveluntoimittajan organisaatioista.

Tyypillinen tilanne palvelujen hankinnassa on, että asiakkaan puolella palvelun ostaja on eri kuin sen käyttäjä. Palvelun toimittajalla on puolestaan usein erikseen myyjä ja palvelua tuottava organisaatio. Yksi tunnistetuista haasteista on palvelun käyttäjäorganisaation tarpeiden välittyminen koko ketjun läpi palvelutuotantoon ja vastaavasti palvelutuotannon rajoitteiden välittyminen tarjous- ja sopimusvaiheessa palvelun käyttäjäorganisaatiolle.



Yhteisen näkemyksen luominen ja ylläpitäminen sopimuksen sisällöstä koko sopimuksen voimassaoloajan on kaikkien osapuolten kannalta keskeinen asia. Palvelukuvausten, vastuumatriisien ja näitä testaavien ja konkretisoivien esimerkkitapauksiin perustuvien harjoitusten avulla kyetään saavuttamaan ja säilyttämään paremmin yhtenevä näkemys palvelun sisällöstä ja siihen liittyvistä vastuista. Tähän ohjeeseen on koottu keinoja yhteisen ymmärryksen varmistamiseksi, sopimussisällön

konkretisoimiseksi ja välittämiseksi operatiiviselle tasolle. Ohjeen liitteissä on ns. RACI-vastuumatriisin soveltamisohje esimerkkeineen sekä esimerkkejä ongelmatilanteista sekä mitä kuvattuihin tilanteisiin liittyen on sopimuksissa hyvä tarkistaa.

Ohjeessa kuvattuja käytäntöjä kannattaa soveltaa kaiken kokoisissa hankinnoissa ja sovittaa niiden taso ja työmäärä vastaamaan hankinnan kokoa ja kriittisyyttä.

2 ASIAKKAAN TARPEEN JA HANKINNAN MÄÄRITTELY

Muista huomioida asiakkaan tarpeen ja hankinnan määrittelyssä ainakin:

- ➔ Suunnittele hankinta osana liiketoimintasi kokonaisuutta, sovita muihin kokonaisuuteen liittyviin sopimuksiin ja itselle jääviin vastuisiin ja toimintoihin.
- ➔ Kuvaa sekä mitä haluat saavuttaa että mitä olet ostamassa.
- ➔ Kuvaa tietoturvavaatimuksesi hankinnan kohteen mukaisesti – mitä tärkeämpi asia, sitä enemmän panostettava.
- ➔ Muista myös ei-toiminnalliset vaatimukset, jotka vaikuttavat ratkaisun toteuttamiseen.
- ➔ Kuvaa kehityspolku ja miten toimintaympäristö tulee mahdollisesti muuttumaan.
- ➔ Hyödynnä markkinavuoropuhelua ja ota mahdollisuuksien mukaan palveluntoimittajat avuksi vaatimusten kuvaamiseen ja varmistamaan molemminpuolinen ymmärrys tarvettasi vastaavasta ratkaisusta.

2.1 Suunnittele hankinta kokonaisuuden osaksi ja sovita yhteen eri palvelusopimusten sisältö

Onnistuneen palvelusopimuksen perustana ovat sekä tavoitteen ja tarpeen selvä määrittely että kokonaisuuden huomioiminen. Palveluiden hankintaa on tarkasteltava osana yrityksen koko toimintaa ja kokonaisprosesseja. Tyypillisesti ICT- ja tietoturvapalveluiden tuottaminen jakaantuu usean kumppanin kesken. Eri palveluiden sopimusten sisältö sekä asiakkaan vastuulle jäävät tehtävät on katsottava kokonaisuutena ja varmistettava, ettei vastuisiin jää aukkoja. Tarkastelussa on syytä ottaa huomioon normaalitilanteiden lisäksi erilaiset häiriötilanteet, kuten tietomurrot.

Kuvaa ja piirrä kartta eri sopimusten ja palveluntuottajien, hankinnan kohteen ja omien tehtävien sekä vastuiden välisistä riippuvuuksista. Hyödynnä vastuumatriisia vastuujaon selventämiseen. Ohjeen liitteessä on esimerkkejä vastuumatriisin käytöstä usean palveluntuottajan vastuiden kuvaamisessa. Tarvittaessa järjestä työpöytäharjoitus kokeillaksesi, miten kokonaisuus toimii erilaisissa tilanteissa. Tavanomaisen toiminnan lisäksi erilaisten poikkeustilanteiden läpikäynti tuo hyvin esille mahdolliset epäjatkuvuuskohdat sopimusten välisissä rajapinnoissa. Esimerkkitapauksia on tämän ohjeen liitteessä ja voit myös hyödyntää esimerkiksi Kyberturvakeskuksen laatimia kyberharjoitusskenaarioita (Kyberharjoitusskenaariot 2020, Skenarioesimerkkejä harjoituksen järjestäjille).

Esimerkki:

Asiakkaalla oli useita palveluntarjoajia: kaksi palvelin- ja kapasiteettipalveluissa, yksi päätelaitesuojaukselle, yksi muille tietoturvapalveluille ja yksi sovellushallintapalveluille. Lisäksi asiakas käytti muutamia eri yrityksiä tietoturvakonsultointiin. Asiakkaan järjestelmät joutuivat vakavan tietoturvahyökkäyksen kohteeksi. Tietoturvahyökkäyksen havaitseminen ja torjunta ja siitä toipuminen vaati kaikkien osapuolten yhteistoimintaa. Häiriönhallinnan edetessä osapuolet toimivat hyvin yhteistyössä eivätkä vastuunjakoasiat nousseet esteeksi. Jälkikäteen todettiin joidenkin osien tuottaneen selvästi laajempaa palvelua kuin mitä palvelusopimukset edellyttivät. Joukko tehtäviä/vastuita ei sisältynyt sopimukseen eikä asiakkaallakaan ollut valmiutta hoitaa niitä. Tietoturvahyökkäyksen aiheuttama vahinko olisi ollut merkittävästi suurempi, mikäli palveluntoimittajat eivät olisi kyenneet tai suostuneet hoitamaan sopimuksen ulkopuolelle jääneitä heille kuulumattomia vastuita.

2.2 Kuvaa tavoitteet ja vaatimukset

Selvitä oman organisaatiosi hankittavaa palvelua koskevat tarpeet ja kuvaa selvästi mitä palveluita olet ostamassa ja mitkä ovat niihin liittyvät toiminnalliset ja laadulliset vaatimukset, mitä hyötyjä haluat saavuttaa ja miten hankinta tukee tavoitetta. Ole realistinen vaatimuksia kuvatessasi ja mitoita palvelun sisältö ja sen suojaukset suhteessa saamaasi hyötyyn.

Esimerkki:

Eräs esimerkkitapaus selkeästi ylimitoitetusta palvelutasovaatimuksesta on 2006 kilpailutettu julkinen hankinta, jossa vaadittiin puhelinpäivystykseltä kymmenen sekunnin vasteaika ja lisäksi sanktiovaatimukset olivat varsin kovat. Vaatimus on kovempi kuin esimerkiksi hätäkeskuksissa, joihin vuonna 2019 soittaneista 97 % sai vastauksen alle 30 sekunnissa.

Älä oleta jokaisen palveluntoimittajan ymmärtävän termien sisällön samalla tavoin tai samoin kuin mitä ne omassa organisaatiossasi tarkoittavat, vaan kirjoita termien määritelmät tarjouspyyntöön. Käytä tarvittaessa esimerkkejä selventämään mitä tarkoitat.

Kuvaa myös kehityssuunnitelmat ja se, miten toimintaympäristö mahdollisesti muuttuu, sillä muutoksiin sopeutuminen on otettava huomioon palvelusopimuksessa ja sen hallinnointimallissa. Kerro, mitkä kehitystoiveista ja muutoksista koskevat juuri tätä hankintaa ja mitkä asiat ovat vain taustoittamassa.

Tunnista, mikä on kyseisessä palvelussa käsiteltävän tiedon kriittisyys ja sovita tietoturvavaatimukset sen mukaisesti. Mitoita tietoturvavaatimukset järjestelmässä käsiteltävään tietoon liittyviin riskeihin. Vaativimmissa hankinnoissa varmista tietoturvavaatimusten kattavuus: mitä kriittisempää tietoa, sitä enemmän tietoturvavaatimusten määrittämiseen on panostettava.

Älä kuitenkaan aseta hankinnoille epärealistisen kovia vaatimuksia. Mieti myös, koskeeko koko hankintaa samat vaatimukset vai onko hankinta syytä jakaa osiin tietoturvavaatimusten osalta.

Esimerkki:

Ota erityisesti huomioon henkilötietojen käsittely ja vaatimukset tiedon maantieteellisestä käsittelypaikasta. Pilvipalveluissa tieto voidaan tallentaa ja sitä voidaan käsitellä Suomen ja EU:n ulkopuolella. On ymmärrettävä ero tiedon maantieteellisen sijainnin eli tallennuspaikan ja tiedon mahdollisten maantieteellisten käsittelypaikkojen välillä. Yleensä ympärivuorokautisen palvelun kustannustehokkuus saavutetaan, kun palvelua tuottava organisaatio on hajautettu eri aikavyöhykkeille niin sanotusti ”aurinkoa seuraamalla” (Follow the sun -periaate), jolloin palvelutuotannon henkilöstöllä on ainakin teoriassa käyttöoikeudet tietoihin Suomen/EU:n ulkopuolelta riippumatta tiedon tallennuspaikasta. Mikäli palvelutuotannon henkilöillä on pääsy tietoon Suomen/EU:n ulkopuolelta, se on otettava huomioon jo palveluratkaisua suunniteltaessa ja hankintaa tehdessä. Mahdolliset tiedon tallennus- tai käsittelypaikkaan liittyvät rajoitukset on kirjattava sopimukseen.

3 TARJOUSPYYNTÖ JA TARJOUKSET

Kiinnitä tarjouspyynnössä huomiota seuraaviin kohtiin:

- ➔ Tarjouspyyntö perustuu selviin hankinnan tavoitteisiin ja vaatimuksiin, kehityssuunnitelmaan sekä toimintaympäristön ennakoitujen muutosten kuvaukseen.
- ➔ Pyydä palveluntarjoajia tekemään itsearviointi tietoturvavaatimuksia vasten.
- ➔ Tarkista, vastaavatko tarjouksen mukana saadut palvelukuvaukset vaatimuksiasi. Ota huomioon mahdolliset palveluntoimittajan vakioprosessien ja toimintamallien tuomat rajoitukset.
- ➔ Hyvä tarjouspyyntö jättää tilaa myös toimittajan ehdotuksille

3.1 Hyvä tarjouspyyntö on laadukkaan sopimuksen pohja

Hyvällä tarjouspyynnöllä saa parhaiden palveluntarjoajien vertailukelpoiset ja realistiset tarjoukset. Hyvä tarjouspyyntö säästää aikaa niin asiakkaalta tarjousten vertailussa kuin toimittajilta tarjousten tekemisessä sekä luo hyvän pohjan sopimusneuvottelulle.

Tarjouspyynnön pohjana on selkeä asiakkaan tarpeen kuvaus (ks. kappale 2: Asiakkaan tarpeen ja hankinnan määrittely): Mitä hyötyjä hankinnalla tavoitellaan, mitä ja millaista palvelua ollaan ostamassa ja mitkä ovat hankintaan liittyvät vaatimukset? Hankinnan taustoittaminen, kehityspolku sekä toimintaympäristön tulevien muutosten kuvaaminen helpottavat asiakkaalle sopivan tarjouksen tekemistä. Tarjouspyynnössä on muistettava kuvata myös mahdolliset hankintaan liittyvät rajoitteet.

Mieti, millä perusteilla teet hankinnan, ketä palvelutoimittajia haluat mukaan ja ketkä palveluntoimittajat haluat karsia pois. Päätä millä kriteereillä ja millä painotuksilla teet valinnan, miten huomioit hinnan ja palvelun eri ominaisuudet päätöksenteossa. Varmista tarjouspyynnössä, että saat päätöksenteossa tarvitsemasi tiedot.

3.2 Palveluntoimittajan vaihtamiseen liittyvät seikat

Mikäli kyseessä on palveluntoimittajan vaihto, tarjouspyynnössä ja tarjouksessa on määriteltävä selvästi ja tarkasti, miten ja milloin vastuu siirtyy valittavalle uudelle toimittajalle. Huomioi vastuun siirron määrittelyssä miten uuden palveluntoimittajan kyky ja mahdollisuus tuottaa sopimuksen mukaista palvelua kehittyy palvelun siirtämisen aikana. Kuvaa myös mikä on luovuttavan osapuolen

vastuu osaamisen siirrossa ja uuden palveluntoimittajan kouluttamisessa. Määrittele osaamiselle kriteerit, jotka uuden palveluntoimittajan on saavutettava. Muista myös huomioida mahdolliset edellisen palveluntoimittajan virheistä tai laiminlyönneistä aiheutuvat ongelmat ja niiden vaikutukset palvelutuotantoon.

Esimerkki:

Asiakas päätti kilpailutuksen jälkeen hankkia sovellushallintapalvelun uudelta toimittajalta. Palvelu sisälsi sovellusten ylläpidon, viankorjauksen, pienkehityksen sekä erikseen sovittavat kehitysprojektit. Ylläpidosta ja viankorjauksesta oli sopimukseen kirjattu kiinteä hinta ja pienkehitystoimenpiteistä tuntihinta.

Haasteeksi muodostuivat edellisen palveluntoimittajan virheet. Miltä osin uusi toimittaja voi vastata järjestelmässä valmiiksi olevista virheistä ja puutteista ja miltä osin näiden virheiden korjaaminen sisältyy palvelun kiinteään hintaan? Miltä osin virheiden korjaaminen sekä järjestelmän parantaminen on erikseen laskutettavaa kehitystyötä? Miten nämä virheet huomioidaan palvelutasojen seurannassa ja mahdollisessa sanktiolaskennassa?

3.3 Varmista vaatimusten ja palvelun sisällön yhdenmukaisuus

Palveluntuottajan ja asiakkaan ymmärrettävä samoin asiakkaan tarpeet sekä palvelukuvaukset ja se, miten ne vastaavat toisiaan. Ylätason kuvaukset ja yleisten termien tai palvelunimien sisältö on syytä avata riittävän yksityiskohtaisesti. Tarkista, että palvelun sisältö, vastuunjako ja palveluntoimittajan mahdollisuudet palvelun tuottamiseen vastaavat määriteltyjä vaatimuksia. Varmista palvelun käyttäjäorganisaatiolta, että he ymmärtävät tarjotun palvelun sisällön ja siihen liittyvän vastuunjaon sekä esittävät tarvittavat tarkentuvat kysymykset tarjouksen tehneelle palveluntuottajalle.

Palvelukuvauksessa palveluntuottaja yksilöi tuottamansa palvelun sisällön ja toteutustavan. Palvelukuvauksen laatu kertoo usein myös yrityksen kyvystä tuottaa lupaamansa palvelu hyvin.

Palvelukuvauksen tulisi sisältää mm. seuraavat asiat:

- Palvelun yleisesittely, palvelun tavoitteet ja tuotokset
- Palvelun yksityiskohdat: perustoiminnallisuus, tuetut teknologiat, lisäpalvelut ja lisäominaisuudet jne.
- Mahdolliset rajaukset palvelun sisällössä
- Palveluarkkitehtuuri
- Palvelun tietoturvakuvaus
- Palvelun käyttöönoton kuvaus
- Miten palvelua tuotetaan, palvelu- ja muutospyyntöjen käsittely, häiriönhallinta
- Palvelun mittarit, palvelutasot ja niiden laskentaperiaatteet sekä raportointi
- Vastuut (esim. RACI-vastuumatriisi)
- Mitkä ovat edellytykset (mm. tekniset edellytykset) palvelun käyttöönotolle ja tuottamiselle
- Hinnoittelu- ja laskutusmallit
- Miten palvelukuvausta päivitetään ja miten palvelua kehitetään
- Miten palvelun muuttaminen tai lopettaminen tapahtuu ja näihin liittyvät toimienpiteet sekä vastuut

Palveluntuottaja toimii usein tehokkuussyistä omien määriteltyjen vakioprosessiensa ja -käytäntöjensä mukaisesti. Mikäli mahdollista, arvioi yhdessä palveluntoimittajan kanssa heidän vakioprosesseja siitä lähtökohdasta, onko palvelun tuottajan mahdollista tuottaa esitettyjen vaatimusten mukaista palvelua.

Arvioinnin lopputuloksena saadaan vakioprosessien ja asiakasvaatimusten puuteanalyysi (ns. GAP-analyysi), jonka pohjalta on tarkasteltava sekä asiakkaan vaatimusten todellista tarvetta sekä sitä, voidaanko poikkeamat hyväksyä tai voidaanko niiden vaikutus poistaa muilla ratkaisuilla. Arvioinnissa on hyvä tarkastella myös miltä osin vakioprosesseja on mahdollista ja järkevää räätälöidä. Läpikäyntiin osallistuvat myyjien ja ostajien lisäksi palvelua tuottavan ja käyttävän organisaation sekä tietoturvaorganisaation edustajat.

Esimerkki:

Asiakas oli määritellyt tarjouspyynnössä esitetyt vaatimukset, joiden pohjalta palveluntoimittajat olivat tehneet tarjoukset. Valitun toimittajan tarjouksen pohjalta tehtiin sopimus, jonka liitteenä olevissa palvelukuvauksissa oli mainittu häiriöiden korjaamisen alkavan, kun asiakas itse ilmoittaa viasta. Valvonnan hälytykset olivat asiakkaalla nähtävissä. Palvelukuvauksen mukaisesti toimittaja ei oma-aloitteisesti reagoinut kaikkiin valvontasovelluksen ilmoituksiin, vaan ainoastaan merkittävimpiin. Vaikka tämä oli kuvattu palvelukuvaukseen, asiakas ei ollut mieltänyt reagoinnin vaativan heidän omaa ilmoitustaan. Ympärivuorokautisessa valvonta- ja viankorjauspalvelussa on kiinnitettävä huomiota myös siihen, millaisissa tapauksissa korjaus aloitetaan välittömästi ja milloin esimerkiksi seuraavana työpäivänä. Mikäli korjaus aloitetaan aina seuraavana työpäivänä, on harkittava onko ympärivuorokautiselle valvonnalle oikeasti tarvetta.

Varmista ainakin tietoturvan kannalta kriittisimpien hankintojen osalta, että tarjouspyynnössä kuvatut tietoturvavaatimukset ja tarjotun palvelun vaatimuksen mukaisuuden tarkastaa tietoturva-asiantuntija. Tarjouspyyntöön on sisällytettävä selkeät tietoturvavaatimukset. Laajojen tai kriittisten laajojen tai kriittisten sopimusten palveluntuottajien kanssa on hyvä tehdä turvallisuussopimus (ks. liite 1: Esimerkkitapaukset).

Varmista yhdessä palveluntoimittajan kanssa, että ymmärrätte tietoturvavaatimukset samalla tavoin ja että palveluntoimittaja pystyy toteuttamaan ne. Selvittäkää yhdessä hankittavan palvelun riskit tai puutteet, jotka mahdollisesti vaativat lisätoimia tai korjaavia toimenpiteitä halutun tietoturvan toteuttamiseksi.

Esimerkki:

Yksi tapa on tarjousvaiheessa pyytää palvelutoimittaja täyttämään tietoturvan itsearviointilomake. Arvioinnin tulokset toimivat keskustelun pohjana eivätkä suoraan sulje pois toimittajia. Vaatimuksista uupumaan jäävät kohdat käsitellään yhdessä ja varmistetaan vaatimusten yhtenäinen ymmärtäminen, tarkoituksenmukaisuus, vaatimusten merkitys kyseisessä hankinnassa sekä mahdollisuudet paikata kyseiset puutteet korvaavilla toimenpiteillä tai suojauksilla. Itsearviointi on ennemmin pohja riskien hallitsemiseksi kuin ehdoton vaatimuslista palveluntarjoajille.

Pilvipalveluiden turvallisuuden arviointiin sopii Kyberturvakeskuksen julkaisema Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Kriteeristöä voidaan käyttää myös palveluntarjoajien oman turvallisuustyön tukena. Kriteeristö on laadittu tukemaan erilaisia pilvipalveluita ja erilaisia käyttötapauksia.

Hyvä tarjouspyyntö jättää palveluntoimittalle myös tilaa esittää näkemyksiään ja ehdottaa soveltuvinta kokonaisuutta hankinnan tavoitteen kannalta. Palveluntoimittajaa ei useimmiten kannata pakottaa käyttämään tiettyä tuotetta tai poikkeavaa prosessia, sillä poikkeava toimintatapa nostaa epäonnistumisen riskiä erityisesti poikkeustilanteissa. Vastaavasti riskiä pienentää sellaisen palvelutoimittajan valitseminen, jonka vakioitu ja tuotteistettu palvelu vastaa mahdollisimman hyvin tarpeitasi.

4 SOPIMUKSEN SOLMIMINEN JA SOPIMUSMUUTOKSET

Huomioi sopimuksessa ainakin seuraavat asiat:

- ➔ Muista, mitä sopimuksella tavoitellaan
- ➔ Määrittele mittarit, joilla seuraat sopimuksen toteutumista
- ➔ Määrittele sopimuksen hallinnointimalli joka salli sopimuksen mukauttamisen toimintaympäristön ja vaatimusten muuttuessa.
- ➔ Sisällytä hallinnointimalliin säännöllinen sopimuksen, toimintatapojen ja vastuiden katselmointi.
- ➔ Kokoa lopuksi sopimusneuvotteluiden tulos yhdeksi riidattomaksi kokonaisuudeksi
- ➔ Tee sopimusmuutokset ja tulkinnat aina kirjallisesti

4.1 Muista mitä sopimuksella tavoitellaan ja määrittele mittarit

Sopimuksessa vastuunjaon ja tehtävien lisäksi hyvä kuvata selvästi, mitä tavoitellaan ja mikä on sopimuksen tarkoitus. Yhteisen tahtotilan ja tavoitteen kirjaaminen auttaa niin sopimusneuvotteluissa yksityiskohtaisemman yhteisen näkemyksen muodostamista kuin sen säilyttämistä koko sopimuksen voimassaolon ajan.

Liitä sopimukseen palvelutasosopimus (SLA), jonka mittareiden avulla seurataan sopimuksen tavoitteiden ja sovittujen palvelutasojen toteutumista. Palvelutasosopimus sisältää asiakkaan odotukset, niille mittarit ja mittaustavat sekä seuraamukset palveluntoimittajalle mikäli tavoitteista jäädään. Hyviä tuloksia on saatu käyttämällä sanktioiden lisäksi palkkiota palveluntarjoajalle hyvästä palvelutasosta.

4.2 Määrittele hallinnointimalli

Palvelusopimuksen sisällön ja vastuiden läpikäynti sekä muiden palveluun ja palvelusopimukseen liittyvien yksityiskohtien yksiselitteinen kuvaaminen vaatii osapuolilta tarkkuutta ja vaivannäköä. Ympäristön muuttumisen takia kaikkia asioita ei pystytä sopimaan tai kuvaamaan.

Esimerkki:

Toimintaympäristön tietoturva ja uhkakuvat muuttuvat varsin nopeasti, eikä sopimuksiin ole mahdollista kuvata koko sopimuksen voimassaoloajan toimivia tietoturvakäytäntöjä. Sopimukseen kirjattu tietoturvallisuuden tahtotila toimii johtoajatuksena tietoturvan toteutuksen kehittämisessä sopimuksen aikana. Sopimukseen on hyvä kirjata yksiselitteisesti, mitkä ovat tietoturvan kehittämisen vastuut, miten palveluiden tietoturvaan tehtävät muutokset liitetään sopimukseen, miten niistä koituvat mahdolliset lisäkustannukset jakaantuvat jne. Samoin on otettava kantaa siihen, miten toimitaan ja mitkä ovat vastuut kun tietoturvauhat, lait tai asetukset muuttuvat sopimuksen aikana niin, ettei palvelu enää vastaa muuttunutta tilannetta. Tärkeätä on myös kirjata, miten haluttu tietoturvataso sekä laatuvaatimukset saavutetaan ja säilytetään sekä miten tietoturvaa ylläpidetään uhkakentän jatkuvasti muuttuessa. Hyvä on kuvata myös, miten toimitaan mikäli jälkikäteen havaitaan, ettei palvelu enää täytä sopimusvaiheessa käsiteltyjä vaatimuksia.

Sisällytä sopimukseen hallinnointimalli, joka sallii sopimuksen ja palveluiden sisällön mukauttamisen ja mahdollisten uusien palveluiden ja vastuiden lisäämisen tai muuttamisen sekä huomioi sopimuksen epäjatkuvuuskohdissa tiedon ja yhteisen ymmärryksen säilyttämisen. Sovi hallinnointimallissa miten palveluita kehitetään yhteisesti vuosittain ja miten esitetyt kehitystoiveet käsitellään.

Hallinnointimalliin on hyvä sisällyttää säännöllinen, vähintäänkin vuosittainen sopimuksen katselmointi, jolla varmistetaan palveluiden ajantasaisuus sekä sopimuksen mukainen toiminta. Vastuutaulukon ylläpitäminen ja säännöllinen päivittäminen auttaa sekä varmistamaan sopimuksen mukaisen toiminnan että vahvistaa yhteistä näkemystä. Vastuutaulukkoon kuvatut vastuut ja yhteinen näkemys voidaan varmistaa käymällä ns. työpöytäharjoituksissa läpi monipuolisesti erilaisilla esi-

merkkitapauksilla, jolloin osallistujat havaitsevat, mitä vastuut käytännössä kullekin tarkoittavat. Vastuunjakotaulukoiden hyödyntämisestä ja työpöytäharjoituksessa käytettävistä skenaarioista on esimerkkejä tämän ohjeen liitteissä.

Esimerkki kolmitasoisesta hallinnointimallista:

- **Kuukausittaiset operatiiviset seurantakokoukset:** esim. palvelutasojen seuranta ja operatiivisten sekä teknisten asioiden käsittely.
- **Neljännesvuosittaiset seurantakokoukset:** esim. kustannusten seuranta, sopimusmuutokset ja -päivitykset ja sopimuksen mukaisen toiminnan varmistaminen.
- **Vuosittaiset yhteistyö- ja kehityskokoukset:** esim. sopimuksen tavoitteiden toteutumisen seuranta ja sopimuksen ajantasaisuuden varmistaminen, toimintaympäristön odotettavissa olevat muutokset ja niiden vaikutukset sopimukseen, osapuolten tulevaisuuden suunnitelmat, sopimuksen kehittäminen, yhteisen näkemyksen testaaminen, ylläpitäminen ja vahvistaminen.

Sopimuksen voimassaolon aikana on useita epäjatkuvuuskohtia: liiketoiminnan tarpeiden määrittely, mahdollinen markkinavuoropuhelu, hankinnan valmistelu, tarjousvaihe, sopimusneuvottelut, käyttöönottoprojekti sekä palvelutuotanto ja sen aikana tapahtuvat henkilövaihdokset. Sopimuksen allekirjoittamisen jälkeen vastuu siirtyy usein käyttöönottoprojektille ja sitten palvelutuotannolle jatkuvan palvelun tuottamiseksi. Lisäksi sopimuksen aikana vastuuhenkilöt vaihtuvat, tulee palvelumuutoksia tai lisäyksiä sekä toimintaympäristö muuttuu.

Aiemmissa vaiheissa löydetty yhteinen näkemys katoaa helposti joko osin tai kokonaan näissä epäjatkuvuuskohdissa tiimien tai henkilöiden vaihtuessa. Yhteisen näkemyksen kadotessa se luodaan uudelleen uusien henkilöiden välillä, eikä uusi yhteinen näkemys välttämättä ole sama kuin aikaisemmin tai yhteinen näkemys jää kokonaan puuttumaan. Epäjatkuvuuskohdissa molempien osapuolten on varmistettava tiedon eheä siirtyminen. Pelkästään sopimusta lukemalla yhteinen ymmärrys ei välity vaan tiedon siirtyminen on hyvä varmistaa käytännön tekemisen kautta.

Esimerkki:

Vaativissa tai laajoissa tehtävien siirrossa voidaan hyödyntää vaiheittaista siirtymistä:

1. Perehtyminen: Tehtävän vastaanottava tutustuu materiaaliin ja ympäristöön
2. Tehtävän vastaanottava perehtyy toimintaan seuraamalla kaikkea tekemistä tehtävän luovuttavan rinnalla
3. Tehtävän vastaanottava ottaa vastuun tekemisestä, tehtävän luovuttava puolestaan seuraa ja vain tarvittaessa osallistuu. Luovuttavan vastuulla on varmistaa oikea toiminta ja laatu.
4. Tuki: Luovuttava tukee tarvittaessa pyynnöstä yksittäisissä asioissa
5. Täysin itsenäinen tekeminen: Vastuu ja tekeminen kokonaisuudessaan siirtynyt vastaanottavalle osapuolelle.

Sisällytä sopimukseen myös selkeä kuvaus toiminnasta, toimenpiteistä ja vastuista palvelun päättyessä tai siirtyessä toiselle toimittajalle.

4.3 Päätä sopimusneuvottelut ja kokoa yhteinen näkemys yhdeksi kokonaisuudeksi

Laajojen ICT-sopimusten sopimusneuvottelut kestävät yleensä pitkään. Sopimukset voivat olla laajoja kokonaisuuksia ja useat eri henkilöt ovat mukana sopimusneuvottelun eri vaiheessa. Sopimusneuvotteluiden aikana syntyy useita eri dokumentteja, kuten pöytäkirjoja, muistioita jne. Eri sopimuksen osia tai dokumentteja työstävät ja neuvottelevat mahdollisesti eri henkilöt, mikä osaltaan voi myös johtaa joiltain osin erilaisiin käsityksiin vastuujaosta ja palvelun sisällöstä. Joissain tapauksissa sopimusneuvotteluiden venyessä palvelutuotanto on saatettu aloittaa ennen kuin sopimukset ovat kaikilta osin valmiit, jolloin tuotannosta vastaavalle organisaatiolle on voinut muodostua oma sopimuksesta poikkeava näkemys palvelun sisällöstä.

Sopimusneuvottelut on syytä päättää selvästi ja koota yhteen materiaali, jossa on kuvattu yksiselitteisesti, mikä on sopimuksen tarkoitus, palvelun sisältö sekä vastuut ja velvollisuudet. Sopimuksen allekirjoittamisen jälkeen on varmistettava palvelutuotannon sopimuksenmukaisuus sekä tiedotettava palvelun sisällöstä niin palvelua käyttävään kuin tuottavaan organisaatioon. Sopimukseen voidaan sisällyttää lause, jossa todetaan allekirjoitettavan sopimusdokumentaation sisältävän ainoan yhteisen näkemyksen sopimuksen tavoitteista ja sisällöstä.

Esimerkki yhden sopimuksen sopimusneuvottelut päättävästä sopimuskohdasta:

”Tämä Sopimus Liitteineen käsittää Osapuolten välisen sopimuksen ja yhteisymmärryksen kokonaisuudessaan liittyen Sopimuksen kohteeseen ja sulauttaa itseensä aiemmat Osapuolten tai tiettyjen Osapuolten väliset kaikki suulliset ja kirjalliset välipuheet ja sopimukset. Kaikki muutokset tähän Sopimukseen ja sen Liitteisiin tulee tehdä kirjallisesti.”

4.4 Tee sopimusmuutokset ja -tulkinnat aina kirjallisesti

Toiminnan vakiinnuttua osapuolet voivat huomaamattaan muuttaa sopimuksen sisältöä ilman varsinaista kirjallista sopimusmuutosta. Sopimuksen sisällön ja vastuiden tulkintaa kirjataan pöytäkirjoihin, muistioihin tai sähköpostikeskusteluihin, jolloin yhteinen näkemys hajoaa eri puolille eikä kaikilla välttämättä ole samaa käsitystä sovituista asioita. Joissain tilanteissa toisen osapuolen voidaan katsoa hiljaisesti luopuneen jostakin oikeudestaan. Ristiriitatilanteessa tämän kaltaisten sopimuksen tai sopimusmuutosten osoittaminen edellyttää aina vahvaa näyttöä. Esimerkiksi pitkään jatkunut vakiintunut toiminta voi osoittaa sopimuksen tai sopimusmuutoksen olemassaolon.

Vertaa hallintomallin mukaisissa sopimuksen katselmoinneissa vakiintuneita toimintatapoja palvelun tavoitteisiin ja sopimukseen. Vahvista molempien hyväksymät muuttuneet, sopimuksessa sovitusta poikkeavat toimintatavat kirjallisesti tai sovi korjaavista toimenpiteistä.

Sopimuksen muutokset, tulkinta ja lisäykset on syytä tehdä kirjallisesti ja koota palvelun sisältö ja vastuut yhdeksi riidattomaksi kokonaisuudeksi. Mikäli näitä ei ole yksiselitteisesti sovittu ja kirjattu, ongelmatilanteissa tai epäjatkuvuuskohdissa tulkintaerojen ja riitojen todennäköisyys kasvaa selvästi. Ilmoita tai sovi myös kirjallisesti mikäli yksittäisessä tapauksessa luovut kertaluonteisesti oikeuksistasi. Vastaavasti, mikäli asiakkaan pyynnöstä toimitaan toisin kuin alun perin sovittu, niin palveluntoimittajat monesti ilmoittavat kirjallisesti poikkeavan toiminnan vaikutuksista ja mahdollisista riskien siirrosta asiakkaalle.

5 SOVELTUVUUSSELVITYS YHTEISEN YMMÄRRYKSEN LÖYTÄMISESSÄ

Mikäli hankinta aloitetaan soveltuvuusselvityksestä tai koetuotannosta (Proof of concept, PoC), onnistuneen PoC:n jälkeen voi tulla esiin hyvinkin erilaisia odotuksia kaupallisesta yhteistyöstä ja sopimusehdoista. Näin voi käydä erityisesti, jos näistä ole keskusteltu jo ennen PoC:n aloittamista. Usein toimittajan kanssa sovitaan vain soveltuvuusselvityksen teknistä sisältöä koskevat asiat, mutta muita ehtoja tai vaatimuksia ei käydä läpi. Toisaalta ei myöskään ole realistista ajatella, että laaja kaiken kattava sopimus saataisiin aikaan ennen yhteistyön alkua.

Parasta on, että ennen PoC:n aloittamista sovitaan etukäteen tärkeimmät perusasiat. Erityisen tärkeää on sopia aineettomien oikeuksien jakautumisesta, mikäli lopputuloksena saadaan jommankumman osapuolen liiketoiminnan kilpailukyvyn kannalta merkittäviä tuotoksia. Yksi vaihtoehto on tehdä palvelun teknisen PoC:in rinnalla ”sopimusneuvottelun PoC”, jossa käsitellään kummankin osapuolen valitsemat merkittävimmät sopimuskohdat ja vastuut, jotka eivät liity palvelun sisältöön tai toiminnallisuuteen. Tämän tarkoituksena on varmistaa yhteisymmärryksen löytyminen tärkeimpien sopimusehtojen ja vastuiden keskeisistä kohdista ja periaatteista ennen tarkempia sopimusneuvotteluita ja varsinaisen sopimustekstin muotoilua.

LIITE 1:
VASTUUMATRIISIT OSANA PALVELUN ELINKAAREN HALLINTAA

1 RACI-vastuumatriisi

Vastuumatriisi on yksinkertainen ja tehokas työkalu roolien ja vastuiden dokumentointiin sekä näiden viestintään kaikille osapuolille. Vastuumatriisi auttaa varmistamaan, että kaikki tietävät sekä omat että muiden vastuut, mitä tehtäviä kenellekin kuuluu ja kenen kanssa tehtävät tehdään.

Ostettaessa ICT-palveluita vastuumatrsiiseja kannattaa hyödyntää kaikissa sopimuksen ja palvelun elinkaaren vaiheissa asiakkaan tarpeen määrittelystä ja tarjouspyynnöstä aina palvelun käyttämiseen ja palvelun päättämiseen tai siirtämiseen toiselle toimittajalle tai toiseen ympäristöön.

Yleisimmin käytetty vastuumatriisi on RACI-matriisi. RACI muodostuu termeistä:

R = Responsible: Toteutusvastuu: Rooli / henkilö, joka vastaa tehtävän suorittamisesta

A = Accountable: Valvonta ja ohjausvastuu, päätöksen tekijä: Rooli / henkilö, joka vastaa siitä että tehtävä tulee tehdyksi.

C = Consulted: Konsultoiva, osallistumisvastuu: Rooli / henkilö, jolta pyydetään neuvoja tai apua tehtävän tekemiseen. Viestintä kaksisuuntaista.

I = Informed: Tiedotettava: Rooli / henkilö, joka pidetään tietoisena asioista. Viestintä yksisuuntaista.

Vastuumatriisin käyttäminen mm.

- Selkeyttää ja auttaa ymmärtämään roolit ja vastuut paremmin niin oman organisaation sisällä kuin yhteistyökumppaneiden välillä.
- Parantaa viestintää, tiedotettavat tahot selvästi määritelty.
- Varmistaa oikeiden henkilöiden osallistumisen tehtävien tekemiseen.
- Nopeuttaa päätöksentekoa kun päätöksentekovastuut ovat kaikkien tiedossa.
- Auttaa hahmottamaan tehtävien päällekkäisyyksiä sekä tehtävien väliin jääviä harmaita alueita.
- Helpottaa eri roolien ja henkilöiden työkuorman hahmottamisessa.
- Helpottaa uusien henkilöiden perehdytystä.

Vastuumatriisi sopii hyvin useamman sopimusosapuolen muodostaman sopimus- ja palvelukokonaisuuden vastuiden ja rajapitojen kuvaamiseen, jolloin vastuumatriisi kannattaa luoda niin sanotusti ylhäältä alaspäin hierarkkisesti. Tällöin mietitään ja kuvataan ensin, mitkä ovat eri sopimusten

ja palveluntuottajien roolit ja rajapinnat, sen jälkeen tarkemmalla tasolla yksittäisten sopimusten ja palveluiden sisäinen roolijako ja tehtävät. Seuraavissa kappaleissa on kuvattu tarkemmin esimerkkeineen eritasoisten vastuumatriisin käyttämistä sopimuksen elinkaaren eri vaiheissa. Ohjeen esimerkkejä kannattaa soveltaa vastaamaan omaa tilannetta ja sopimuksia.

2 Hankinnan suunnittelu, tarjouspyyntö ja tarjous

Onnistuneen palvelusopimuksen perustana ovat sekä tavoitteen ja tarpeen selvä määrittely että kokonaisuuden huomioiminen. Palveluiden hankinta on tarkasteltava osana yrityksen koko toimintaa ja kokonaisprosesseja. Käytä vastuumatriisia kuvaamaan eri sopimusten ja palveluntuottajien, hankinnan kohteen ja omien tehtävien sekä vastuiden välisistä riippuvuuksista. Määrittele kokonaisuutta kuvaavassa vastuumatriisissa tehtävät suurempina kokonaisuuksina kuin yksittäisen palvelusopimuksen tehtäviä määrittelevät vastuumatriisit. Testaa vastuumatriisia työpöytäharjoituksella varmistaaksesi ettei tehtäviä ja vastuita jää nimeämättä tai harmaalle alueelle.

Liitä kokonaisuutta ja rajapintoja toisiin palveluntuottajiin kuvaava ylätason vastuumatriisi tarjouspyyntöön. Alla on esimerkki tietoturvan valvontapalvelun (SOC-palvelu) osalta vastuumatriisista, jossa on kuvattu asiakkaan ja useamman palveluntarjoajan vastuut. Vastaavalla tavalla on hyvä kuvata vastuut kaikkien palveluiden osalta.

Edellytä tarjouspyynnössä palveluntuottajalta tarjoukseen palvelukuvaukset ja niihin sisältyvät tarkemmat vastuumatriisit. Tarjousvaiheessa palvelukohtaiset vastuumatriisit eivät ole vielä lopulliset, vaan tarkentuvat sopimus- ja käyttöönottovaiheissa. Palveluntuottajan vastuumatriiseihin on hyvä sisällyttää myös kolmansiin osapuoliin liittyvät vastuut ja rajapinnat. Tarjouksessa olevan palvelukuvauksen ja vastuumatriisin on oltava riittävän tarkalla tasolla jotta pystyt tarkistamaan vastaako palvelun sisältö tarpeitasi esittämiäsi vaatimuksia.

Muista myös sopimuksen päättämiseen tai palveluntarjoajan vaihtumiseen liittyvien vastuiden kuvaaminen.

3 Sopimus

Ota sopimuksen liitteeksi aina palvelukuvaus vastuumatriiseineen. Sopimuksessa oleva vastuumatriisi voi joiltain osin olla ylätasolla. Sitä voidaan vielä tarkentaa palvelun käynnistämisen yhteydessä. Lopputuloksena sinulla on sekä aiemmin kuvatut toimintaasi ja kaikkia palveluntoimittajiasi yhdistävät ylemmän tason vastuumatriisit sekä tarkemmat palvelusopimuskohtaiset vastuumatriisit.

Edellytä sopimuksessa palvelutoimittajalta vastuumatriisin ulottamista mahdollisiin alihankkijoihin ja alihankintasopimuksiin. Velvoita sopimukseen kirjattavassa hallinnointimallissa molempia osapuolia päivittämään ja yhdessä hyväksymään muuttuneet palvelukuvaukset ja vastuumatriisit aina, kun sopimuksen kohteena olevaan palveluun tai sen toteuttamistapaan tulee muutoksia.

Alla esimerkki palveluntoimittajia yhdistävästä vastuumatrisiisista sekä palvelu- ja sopimuskohtaiset vastuumatriisiesimerkit kapasiteettipalveluun, palvelinten hallintaan sekä varmistus- ja palautuspalveluun liittyen.

TEHTÄVÄ	Asiakas	SOC-palvelujen toimittaja	Palomuuripalvelujen toimittaja	Työasemapalvelun toimittaja	Tietoliikennepalvelujen toimittaja	Käyttö- ja kapasiteettipalvelujen toimittaja	
Prosessivastuut, Tietoturvan valvonta (SOC)							
Toimintatapojen määritys	A,R	C,I	I	I	I	I	
Tietoturvatapahtumien tunnistaminen ja käsittely	I	A,R					
Tietoturvatapahtuman kirjaaminen	I	A,R					
Tietoturvatapahtumien validointi	I	A,R					
Tietoturvatapahtuman ratkaisuvastaavien määrittäminen ja eskalointi	C	A,R	R	R	I	I	
Tiedottaminen sovittujen viestintäkäytäntöjen mukaisesti	I	A,R	R	R	I	I	
Tietoturvatapahtuman ratkaisu - juurisyyn etsintä	C	A,R	R	R	R	R	Tuotevastuiden mukaisesti
Tietoturvatapahtuman ratkaisu - ratkaisun määrittäminen	C	A,R	R	R	R	R	Tuotevastuiden mukaisesti
Tietoturvatapahtuman ratkaisun seuranta ja koordinointi	I	A,R	C	C	C	C	
Ratkaisun hyväksyminen	A,R	C	I	I	I	I	
Ratkaisun toteutus	A,R	R	R	R	R	R	Tuotevastuiden mukaisesti
Toimenpiteiden jälkiarviointi	I	A,R	R	R	R	R	Tuotevastuiden mukaisesti
Toimenpiteiden raportointi	I	A,R	C	C	C	C	
Tietoturvatapahtuman perusteella kehitystehtävän ehdottaminen	I	A,R	C	C	C	C	
Kehitystehtävän hyväksyminen	A,R	C	I	I	I	I	
Kehitystehtävän toteutus	A,R	R	R	R	R	R	Tuotevastuiden mukaisesti
Tietoturvatuotekohtaiset vastuut							
Tuote xxxx: tapahtumien hallinta	I	A,R					
Tuote xxx ennakoiva ylläpito, valvonta, konfigurointi	C,I	A,R					
Tuote xxx Lokilähteiden liittäminen	C,I	A,R	R				
Tuote xxx Lokilähteiden liittäminen	C,I	A,R		R			
Tuote xxx Lokilähteiden liittäminen	C,I	A,R			R		
Tuote xxx Lokilähteiden liittäminen	C,I	A,R				R	
xxx-tuotteiden asennukset	I	C			A,R		
xxx-tuotteiden asennukset	I	C				A,R	
Prosessivastuut, palomuuripalvelut							
xxxxvastuut							
xxxxvastuut							
xxxxvastuut							

Tehtävä Kapasiteettipalvelu	Asiakas	Toimittaja	3. osa-puoli	Huomiota
Tukipyyntöjen vastaanotto (puhelin email, web-lomake) ja sen kirjaaminen järjestelmään	I	R/A		
Tukipyyntöjen hallinnointi ja ongelman ratkaisu	C	R/A		
Ongelmanratkaisuun liittyvien tietojen välittäminen ja raportointi	I	R/A		
Häiriöiden juurisyiden selvittäminen	I	R/A		
Juurisyiden korjaamisen vaatimien muutosten ehdottaminen	I	R/A		Incident-tiketin perusteella tehdään tarpeen mukaan Problem-tiketti
Hankintojen hyväksyntään oikeutettujen henkilöiden luettelon toimittaminen ja ylläpito	R/A	I		
Luettelon toimittaminen ja ylläpito henkilöistä, joilla on valtuudet hyväksyä tietoturvaan liittyviä muutoksia	R/A	I		
Käyttöjärjestelmälisenssit (dedikoituun kapasiteettiin)	C	R/A		
Alustojen virtualisointikerrosten valvonta, hallinta, mittaus ja raportointi		R/A		
Palvelinalustojen firmware-päivitykset, palvelinkonfiguraatioiden luonti, testaus ja ylläpito		R/A		
Käyttäjätunnusten ja käyttöoikeuksien ylläpito	C/I	R/A		
Varmistuspalvelu, palvelinten hallintapalvelu, automaattihälytyksen lähettäminen asiakkaalle	C/I	R/A		
Lokitietojen tallennus ja säilytys	C/I	R/A		
Palvelun raportointi	C/I	R/A		Palveluntarjoajan vakioraportit
Palvelun tietoturvakäytäntöjen määrittely ja toteutus	I	R/A		Kapasitettipalvelussa noudatetaan palveluntarjoajan vakioituja käytäntöjä
Tietoturvavaatimusten ja lainsäädännön muutosten seuranta, muutosten määrittely ja toteutus	I	R/A		Palveluntarjoajan vakioraportit
Palvelun päättyessä asiakkaan tietojen toimittaminen asiakkaalle ja toiselle palveluntarjoajalle	I	R/A	I	Sopimukseen määritellyn mukaisesti
Palvelun pättyessä asiakkaan tietojen ja tallenteiden poistaminen	I	R/A		Sopimukseen määritellyn mukaisesti
Palvelun auditoinnissa avustaminen, auditoinnissa vaadittujen tietojen toimittaminen	I	R/A	I	Sopimukseen määritellyn mukaisesti

Tehtävä Palvelinten hallintapalvelu	Asiakas	Toimittaja	3. osa-puoli	Huomiota
Ympärivuorokautinen palvelinten valvonta ja häiriöiden ratkaisu		R/A		
Häiriöiden juurisyiden selvittäminen	I	R/A		
Juurisyiden korjaamisen vaatimien muutosten ehdottaminen	I	R/A		Incident-tiketin perusteella tehdään tarpeen mukaan Problem-tiketti
Palvelimiin tehtävien muutosten hyväksyminen	R/A	C		
Muutokset toteuttaminen palvelimiin	C/I	R/A		
Automaattisten korjaustoimenpiteiden määrittäminen	C	R/A		
Palvelinten muutokset/lisäykset/poistot	C	R/A		
Tietoliikenneyhteys asiakkaan ja toimittajan välillä	R/A			

Palvelinkonfiguraation luonti, testaus ja ylläpito sekä CMDB-päivitykset ja palvelinten korjauspäivitykset		R/A		
Palvelinten versionpäivitykset, service packien päivitykset	C	R/A		Erillisveloitus
Teknisten parannusten ja päivitysten suosittelu	C	R/A		
Tekniten parannusten hyväksyntä	R/A	I		
Määriteltyjen palvelinten suorituskyvyn optimoinnin (konfiguraatiomuutokset) suunnittelu ja toteuttaminen	C	R/A		
Halittavien ympäristöjen toipumissuunnitelmat ja niiden säännöllinen testaus	C	R		Toipumissuunnitelman testaus erikseen veloitettavaa
Lokitietojen tallennus ja säilytys	C/I	R/A		
Palvelun raportointi	C/I	R/A		Palveluntarjoajan vakioraportit
Tietoturvavaatimusten määrittely (ml. viranomaisvaatimuksiin perustuvat tarpeet)	R/A	C/I		
Tietoturvamuutosten toteutus	I	R/A		Erillisten tarjousten perustella
Sopimuksen päättyessä palvelinten siirrossa avustaminen	I	R/A	I	Sopimuksessa määritellyn mukaisesti
Asiakaskohtaisten tietojen, tallenteiden, määrittelyiden ja konfiguraatioiden toimittaminen pyydettäessä	I	R/A	I	Tietojen tomitus asiakkaalle ja 3. osapuolelle sopimuksen mukaisesti
Palvelun auditoinnissa avustaminen, auditoinnissa vaadittujen tietojen toimittaminen	I	R/A	I	Sopimukseen määritellyn mukaisesti

Tehtävä Varmistuspalvelu ja palautuspalvelu	Asiakas	Toimittaja	3. osapuoli	Huomiota
Palvelun tuottamisessa käytettävien laitteiden toimivuus ja huolto		R/A		
Suunnitelman mukaiset varmistukset		R/A		
Varmistusten onnistumisen valvominen	C	R/A		
Palvelinjärjestelmän varmistus- ja palautussuunnitelma sekä testaus	C	R/A		Testaus erillisveloituksella
Asiakkaan pyytäminen tietojen palautukset	C/I	R/A		Erillisveloitus
Sovelluskohtaisten varmistus- ja palautustietojen määrittely	R/A	C/I		
Palveluun tulevien muutosten tekeminen muutoksenhallintaprosessin mukaisesti	C/I	R/A		
Varmistusten ja palautusten automaattinen testaus	R	A		
Varmistusten säilytys	C	R/A		
Palveluraportointi	I	R/A		Palveluntarjoajan vakioraportit
Asiakaskohtaisten tietojen, tallenteiden, määrittelyiden ja konfiguraatioiden toimittaminen pyydettäessä	I	R/A	I	Tietojen toimitus asiakkaalle ja 3. osapuolelle sopimuksen mukaisesti
Palvelun auditoinnissa avustaminen, auditoinnissa vaadittujen tietojen toimittaminen	I	R/A	I	Sopimukseen määritellyn mukaisesti
Palvelun päättyessä asiakkaan tietojen ja tallenteiden poistaminen	I	R/A		Sopimukseen määritellyn mukaisesti

Tehtävä Verkon turvallisuusvalvontapalvelu	Asiakas	Toimittaja	3. osa-puoli	Huomiota
Tapahtumanhallinta: tunnistus, luokitus, kirjaus, priorisointi, tiketöinti	C/I	R/A		
Palvelupyyntöjen vastaanotto (puhelin, email, web-lomake) ja niiden tiketöinti	C/I	R/A		
Palvelupyyntöjen luokittelu kiireellisyyden, vaikutusten ja aiheuttajan perusteella	C/I	R/A		
Vastaanottoajan ja SLA:n mukaisen määräajan tallentaminen pyyntöihin	C/I	R/A		
Itsepalveluportaalin tarjoaminen loppukäyttäjille palvelupyyntöjen tekememiseen ja seuraamiseen	C/I	R/A		
Luettelon ylläpito henkilöistä hankintojen hyväksymisvaltuuksineen	R/A	C/I		
Määrittely noudatettavista käytännöistä (tietoturva ja tietosuoja, email, levytila yms.)	R/A	C/I		
Häiriön/ongelman kiireellisyyden ja priorisoinnin määrittely vaikutusanalyysin perusteella	C/I	R/A	I/C	kts. Palveluittain määritellyt 3. osapuolet
Asiakaskohtaisten tietojen, tallenteiden, määrittelyiden ja konfiguraatioiden toimittaminen pyydettäessä	I	R/A	I	Tietojen tomitus asiakkaalle ja 3. osapuolelle sopimuksen mukaisesti
Palvelun auditoinnissa avustaminen, auditoinnissa vaadittujen tietojen toimittaminen	I	R/A	I	Sopimukseen määritellyn mukaisesti
Palvelun päättyessä asiakkaan tietojen ja tallenteiden poistaminen	I	R/A		Sopimukseen määritellyn mukaisesti

4 Palvelun käynnistäminen ja palvelutuotanto

Täydentäkää ja tarkentakaa vastuumatriisi palvelun käynnistysprojektin aikana. Varmista, että jokaisen tehtävän kohdalla vain yhdellä on valvonta- ja ohjausvastuu (A). Varmista samoin, että kyseisissä rooleissa valta ja vastuu vastaavat toisiaan. Tarkista, että jokaisen tehtävän kohdalla on vähintään yhdellä toteutusvastuu (R). Mikäli jonkin tehtävän kohdalla on useita toteutusvastuita (R), kannattaa miettiä, voiko tehtävän pilkkoa useammaksi tehtäväksi roolien selkeyttämiseksi.

Uuden palvelun käynnistämiseen liittyen kannattaa järjestää työpaja, johon osallistuvat palvelun käyttäjäorganisaation ja palvelutuotannon edustajat. Työpajassa varmistetaan, että kaikilla osapuolilla on yhtenevä ymmärrys palvelun sisällöstä ja siihen liittyvistä vastuista. Tilaisuudessa on hyvä käydä muutaman esimerkkiin perustuvan harjoituksen avulla läpi toimintamallit normaalien ja poikkeavien tilanteiden osalta ja samalla varmistua mm. yhteydenpitomenettelyistä ja yhteystietojen ajantasaisuudesta. Työpajasta on syytä laatia muistio, jossa kuvataan miten vastuut jakautuivat ja toteutuivat harjoitelluissa tilanteissa ja määrittää mahdollisesti tarvittavat tarkennukset tai lisäykset vastuumatriisiin. Harjoitusmuistio tulee esitellä palvelun ohjausryhmässä ja kirjata hyväksytyksi ohjausryhmän pöytäkirjaan. Vastaavat vuosittaiset työpajat kannattaa sisällyttää sopimuksen hallinnointimalliin.

Laajempien, useamman palveluntuottajan muodostamien kokonaisuuksien osalta on hyvä järjestää erillinen työpaja, johon osallistuvat kaikki palveluntoimittajat. Työpajassa käydään vastaavalla tavalla esimerkkitapausten avulla läpi eri palveluntuottajien vastuut ja roolit.

Kaikki palvelukuvauksiin ja RACI-matriiseihin tehtävät muutokset tulee dokumentoida, hyväksyttää muutoshallintamenettelyn mukaisesti päätösvaltaisella taholla ja kirjata esimerkiksi palvelun ohjausryhmän pöytäkirjaan. Mikäli palvelukuvauksiin ja RACI-matriiseihin tulee suuria muutoksia, kannattaa muutosten toimivuus varmistaaa kevyen pöytäharjoituksen avulla.

LIITE 2: ESIMERKKITAPAUKSET

Esimerkkitapaus 1:

SOVELLUSHALLINTAPALVELU

Asiakkaalla oli käytössä toiminnanohjausjärjestelmä, jonka käyttöönotosta, integraatioiden toteutuksesta, parametroinnista ja räätälöintien toteutuksesta on vastannut eräs palveluntuottaja.

Sopimuskauden lähestyessä loppua asiakas päätti kilpailuttaa toiminnanohjausjärjestelmänsä sovellushallintapalvelun, joka sisälsi ylläpidon, viankorjauksen ja kehitystehtävät. Kilpailutuksen jälkeen asiakas päätyi vaihtamaan palveluntuottajaa.

Uusi sopimus sisälsi kiinteähintaisena järjestelmän ylläpidon ja viankorjauksen sekä erikseen tilattavana ja laskutettavana pienkehitystehtävät sekä kehitysprojektit.

Vastuu edellisen palveluntuottajan tekemistä virheistä

Kun palvelu siirtyi uudelle palveluntuottajalle, ongelmaksi muodostuivat edellisen palveluntoimittajan aiheuttamat virheet järjestelmässä. Virheitä todettiin olevan merkittävä määrä. Osapuolilla oli erilainen käsitys siitä, miltä osin uusi toimittaja vastasi haltuun ottamassaan järjestelmässä valmiiksi olevista virheistä ja puutteista, siitä, miltä osin näiden virheiden korjaaminen sisältyi palvelun kiinteään hintaan sekä siitä, miltä osin virheiden korjaaminen sekä järjestelmän parantaminen oli erikseen laskutettavaa kehitystyötä.

Lisäksi osapuolilla oli eriävä käsitys siitä, miten näiden virheiden korjausajat sekä niiden aiheuttamat käyttökatkokset huomioitiin palvelusopimukseen palvelutasoseurannassa ja sanktiolaskennassa. Osapuolilla ei ollut näiden osalta yhtenevää käsitystä kiinteähintaisen palvelun laajuudesta eikä palvelutasolaskennan perusteista.

Sopimuksesta puuttui selvä rajaus järjestelmässä jo olevista tai kolmannen osapuolen aiheuttamista virheistä sekä näiden vaikutuksesta palvelutasotavoitteisiin ja sanktioihin.

Sopimuksessa ei myöskään ollut yleisemmälläkään tasolla kuvattu tahtotilaa, vastuita ja velvollisuuksia, joita olisi pystynyt käyttämään apuna yhteisen näkemyksen löytämiseksi. Myöskään tarjouspyynnössä tai neuvotteluvaiheessa nämä asiat eivät olleet esillä.

Palvelusopimuksessa huomioitavia asioita:

- ← Rajaa selvästi mitä viankorjaus sisältää sekä selvyyden vuoksi myös, mitä se mahdollisesti ei sisällä.
- ← Kuvaa selvästi, miltä osin asiakkaan, aikaisemman palveluntuottajan, kolmansien osapuolten ja muiden ulkoisten, palveluntoimittajasta riippumattomien tekijöiden aiheuttamat virheet ja häiriötilanteet huomioidaan.
- ← Ota huomioon:
  - Mahdollinen poikkeava korjausvastuu ja toimintatapa
  - Vaikutus palvelutason ja sanktioiden laskentaan
  - Korjauksista aiheutuvien kustannusten vaikutus: Miltä osin se sisältyy kiinteään hintaan ja miltä osin se on erikseen veloitettavaa lisätyötä?
  - Mikäli korjaukset ovat erikseen veloitettavia, määrittele korjataanko virhe automaattisesti vai tilaako asiakas erikseen korjauksen kustannusarvion jälkeen.
  - Sovi mitkä asiat vaikuttavat viankorjauksen aloittamiseen (esim. kustannusarvion suuruus, korjauksen aiheuttamat riskit, virheen vakavuus)
  - Määrittele, ovatko vastuut ja palvelunsisältö samat sopimuksen elinkaaren eri vaiheissa (esim. palvelun käynnistäminen ja haltuunottovaihe, ensimmäinen vuosi, vakiintunut palvelutuotanto).

Vastuu tehtyjen muutosten kokonaisvaikutuksesta

Palveluntuottaja toteutti asiakkaan toivomia muutoksia toiminnanohjausjärjestelmään. Näiden muutosten määrittely tehtiin yhteistyössä ja palveluntuottaja vastasi työn ohjauksessa. Muutosten käyttöönoton jälkeen niiden huomattiin toimivan määritysten mukaisesti, mutta aiheuttavan ongelmia muissa järjestelmän toiminnoissa ja toisessa kohtaa asiakkaan prosessia. Ongelmien poistaminen edellytti uudelleen määrittelyn ja toteutustyön. Ongelma saatiin korjattua, mutta se aiheutti merkittäviä lisäkustannuksia.

Sopimuksen tai palvelukuvauksen perusteella ei ollut selvää, korjataanko nämä ongelmat virheenkorjauksena, muutostyön takuutyönä vai ovatko erikseen laskutettavaa kehitystyötä.

Palvelusopimuksessa huomioitavia asioita:

- ← Tarkista palvelun sisältö ja vastuut muutos- ja kehitystehtävien osalta: Mistä osuudesta vastaa asiakas ja mistä palveluntoimittaja?
- ← Varmista vastuiden selkeä rajaus kehitystehtävien virheenkorjauksen osalta: Mitkä virheet korjataan takuutyönä ja mitkä laskutettavana työnä?
- ← Huomioi erityisesti määrittelyvirheet tai toteutettavien muutosten vaikutus muualla järjestelmässä, prosessissa tai rajapinnoissa.

Esimerkkitapaus 2:

ICT-INFRA- JA DATA CENTER -PALVELU

Asiakas ja ICT-infra- / data center -palveluntarjoaja olivat usean vuoden ajan tehneet yhteistyötä. Palvelu tuotettiin palveluntarjoajan vakiomallilla, joka oli kuvattu palvelusopimukseen. Asiakkaan tietoturvavaatimukset olivat tiukemmat kuin mitä palveluissa oli vakiona. Sopimusvaiheessa asiakas ei huomannut, ettei palvelukuvauksen mukainen vakiopalvelu vastaa esitettyjä tietoturvavaatimuksia. Lisäksi tietoturvavaatimukset muuttuivat sopimuksen elinkaaren aikana.

Palvelun tietoturvan muutokset sopimuksen aikana

Asiakas teetti palveluihin tietoturvatestauksen, jonka seurauksen todettiin tietoturvapuutteita suhteessa asiakkaan tietoturvavaatimuksiin. Puutteiden korjaamiseksi sopimuksen sisältämiä palveluita piti laajentaa. Palvelun liittäminen sopimukseen edellytti pitkähköjä sopimusneuvotteluita.

Sopimuksessa huomioitavia asioita:

- Kuvaa tietoturvan tahtotila ja mitä tietoturvavaatimukset tarkoittavat sinulle. Huomioi suojattavat tiedot, käyttäjät, palvelun kriittisyys, erityisvaatimukset ja riskit liiketoiminnalle.
- Kuvaa tietoturvavaatimukset tarkasti. Varmista yhdessä palveluntuottajan kanssa, että palvelunsisältö vastaa tietoturvavaatimuksiasi.
- Määrittele sopimukseen tietoturvavaatimusten ja palvelukuvauksen pätemisjärjestys: Kumpi on määräävä, mikäli eivät ole yhdenmukaisia?
- Varmista, että hallinnointimallissa on sovittu tietoturvavaatimusten muutosten käsittely, miten muutokset otetaan osaksi sopimusta ja miten muutokset vaikuttavat hinnoitteluun.
- Huomioi vastuunjakotaulukossa kenen vastuulla on tietoturvapuutteiden ja kehitystarpeiden havaitseminen sekä korjaavien toimenpiteiden esittäminen.
- Varmista, että sopimuksessa on määritelty toimintatapa, mikäli palvelutuotannon aikana havaitaan, ettei palvelu vastaa esitettyjä tietoturvavaatimuksia. Sopimuksessa tulee määritellä, miten havainnot käsitellään, miten puutteet korjataan ja kenen vastuulla mahdolliset lisäkustannukset ovat.
- Kirjaa sopimukseen miten toimitaan ja mitkä ovat osapuolten vastuut, kun tietoturvauhat, lait tai asetukset muuttuvat sopimuksen elinkaaren aikana siten, ettei palvelu enää vastaa muuttunutta tilannetta. Kuvaa kenen vastuulla on havaita muutokset toimintaympäristössä tai lainsäädännössä.
- Huomioi hallinnointimallissa, miten ja kuinka usein muuttunutta tilannetta tarkastellaan sekä miten palvelun tietoturvaa kehitetään, hallinnoidaan ja raportoidaan.

Lisäksi laajojen tai kriittisten sopimusten palveluntuottajien kanssa on hyvä tehdä turvallisuussopimukset.

Varmista turvallisuussopimuksella mm. seuraavat seikat:

- Sitoutuminen asiakkaan sisäisiin ja ulkoisiin turvallisuusvaatimuksiin
- Tarvittaessa palveluun liittyvien henkilöiden vaitiolositoumukset ja turvallisuusselvitykset
- Luottamuksellisen tiedon suojaaminen ja tietosuojasta huolehtiminen
- Sitoutuminen valittuihin standardeihin ja käytäntöihin
- Turvaratkaisun sisältö ja palvelutaso
- Pyydettäessä palvelun turvallisuustason osoittaminen, mahdollisuus palvelun tarkastukseen ja auditointiin
- Palveluun liittyvien henkilöiden turvallisuusosaaminen
- Palvelun ja tietojen eriyttäminen muiden asiakkaiden palvelusta ja tiedoista
- Turvallisuuden huomiointi kehitystyössä, ”security by design”
- Palvelun jatkuvuussuunnittelu ja jatkuvuuden säännöllinen testaaminen
- Tietojen turvallinen poisto käytöstä poistettavilta laitteilta tai palvelun päättyessä
- Tietoturvan mittarointi ja säännöllinen raportointi, palvelutasot ja mahdollinen sanktiointi
- Turvallisuuden jatkuva kehittäminen yhteistyössä.

Palvelinten nollapäivähaavoittuvuus

Asiakas raportoi palvelun tuottajalle asiakkaan käyttämässä ohjelmistossa havaitusta nollapäivähaavoittuvuudesta ja pyysi ajamaan kiireellisen ohjelmistopäivityksen haavoittuvuuden korjaamiseksi mahdollisimman pian. Sopimuksen mukaisesti vain palvelun tuottaja pystyi tekemään päivityksiä data center -ympäristössä. Palvelun tuottaja ei kuitenkaan pystynyt tekemään päivityksiä riittävän nopeasti vaan haavoittuvuutta ennätettiin hyödyntämään.

Sopimuksessa, palvelukuvauksessa tai prosessiohjeessa ei ollut erikseen kuvattu mm. nollapäivähaavoittuvuuksiin tai vastaaviin kiireellisiin päivityksiin liittyviä vaatimuksia vastuita tai toimintaa.

Palvelusopimuksessa huomioitavia asioita:

- ← Tarkista, että sopimuksessa on määritelty erilaisille päivityksille vasteajat. Varmista yhdessä palveluntuottajan kanssa vasteaikojen realistisuus.
- ← Määrittele vastuujakotaulukkoon kenen vastuulla on haavoittuvuuksien seuranta, reagointi, päivitysten tilaus tai hyväksyntä sekä päivitysten toteutus eri ohjelmistojen osalta.
- ← Määrittele kriteerit hätäpäivitysten tekemiselle ja sekä hyväksymiskäytännöt hätäpäivityksiä varten.

24/7 valvonnan sisältö

Palvelusopimukseen sisältyi ympärivuorokautinen valvontapalvelu nopean reagoimisen varmistamiseksi häiriötilanteissa. Sopimuksen liitteenä olevassa palvelukuvauksissa oli kuitenkin todettu häiriöiden korjaamisen alkavan ***asiakkaan ilmoitettua häiriöstä***.

Automaattisen valvonnan tuottamat hälytykset olivat asiakkaan nähtävissä. Tarjouspyynnössä ei ollut erikseen edellytetty palveluntuottajan reagointia hälytyksiin tai muutenkaan mainintaa häiriöselvityksen aloittamisesta.

Palvelukuvauksen mukaisesti palvelutoimittaja ei oma-aloitteisesti reagoinut kaikkiin häiriöihin, ellei asiakas itse niistä erikseen ilmoittanut. Toiminta oli palvelukuvauksen mukaista, mutta asiakas ei ollut mieltänyt viankorjauksen vaativan heidän oman ilmoituksensa. Asiakkaan oletusarvona oli automaattinen reagointi, eikä asiakas sopimusvaiheessa kiinnittänyt huomiota palvelusopimuksessa olevaan mainintaan.

Palvelusopimuksessa huomioitavia asioita:

- Varmista, että palvelukuvauksessa on selvästi kuvattu vastuut häiriöihin reagoinnin ja korjaavien toimenpiteiden osalta: Kenen vastuulla on reagoida ja käynnistää korjaavat toimenpiteet ja miten reagointi- ja ratkaisuajat on määritelty?
- Tarkista palvelutasojen määrittely: Milloin reagointi- ja ratkaisuaikojen laskenta käynnistyy, huomioidaanko molemmat vai vain toinen ja miten reagointi on määritelty? Tarkoittaako reagointi esimerkiksi: ”Häiriö todettu” vai ”Häiriöselvitys aloitettu”?
- Varmista, että häiriöiden vakavuuden luokittelu on selkeästi määritelty ja kuka määrittelee häiriön vakavuuden.
- Tarkista, miten reagointi ja häiriöselvityksen käynnistäminen riippuu häiriöiden vakavuudesta.

Palomuuripalvelun sisältö

Asiakas sai muualta tiedon tietoturvauhasta. Asiaa tarkistettaessa selvisi, että palveluna ostettu palomuuripalvelu sisälsi tietoturvariskin: avattuihin portteihin kohdistuneita haitallisia yhteysyrityksiä ei torjuttu, vaikka ne tunnistettiin uhkiksi. Lisäksi havaituista haitallisista yhteyksistä tai yhteysyrityksistä ei raportoitu asiakkaalle ja lokitietojen toimittamisvelvollisuudesta ja -mahdollisuudesta asiakkaalle oli erilaisia käsityksiä palveluntuottajan organisaatiossa.

Palvelusopimuksessa huomioitavia asioita:

- Tarkista että palomuuripalvelun sisältö ja palvelulle asetetut vaatimukset selkeästi määritelty.
- Varmista, että palomuuripalvelun toiminnot kuvattu riittävän tarkasti ja että on selvää, millaisen suojan palvelu käytännössä tarjoaa.
- Sovi raportoinnista ja reagoinnista uhkiin ja varmista lokitietojen saanti tarvittaessa. Varmista myös, mitä tietoja tallennetaan lokille, mitä saa tallettaa lokille, kuinka kauan lokitietoja saa tai pitää säilyttää ja kenellä on oikeudet nähdä lokitiedot.
- Varmista kriittisten järjestelmien lokitietojen kattavuus: kerättävistä tiedoista pystyttävä selvittämään mitä palvelussa tapahtuu.
- Varmista erityisesti muiden asiakkaiden kanssa jaettujen ympäristöjen lokien hallinta ja saatavuus.
- Varmista, että on selkeästi sovittu kuka vastaa korjaavien toimenpiteiden käynnistämisestä ja kustannuksista mikäli palvelun tietoturvassa havaitaan puutteista.

YLEISET SOPIMUSEHDOT

Aineettomat oikeudet

Pitkän puitesopimusneuvottelun loppuvaiheessa todettiin, ettei aineettomista oikeuksista ollut yhteistä näkemystä. Asiakas ei ollut osannut tuoda neuvotteluiden alkuvaiheessa esille tarvitsevansa ratkaisun asiakaskohtaisen osuuden – räätälöinnit, parametroinnit, toimintatavan, tavan hyödyntää valmisohjelmistoa jne. – oikeudet itselleen. Lopputuotos oli kuitenkin keskeinen osa asiakkaan tuottamassa palvelussa ja toi merkittävän kilpailuedun. Yhteisen ymmärryksen löytäminen kesti kohtuullisen pitkään. Haasteena oli erotella sopimuksessa ostettavan tuotteen, toimitettavan palvelun ja sen soveltamisen ja räätälöintien aineettomat oikeudet.

Palvelusopimuksessa huomioitavia asioita:

- ← Esitä jo tarjouspyynnössä mahdolliset aineettomiin oikeuksiin liittyvät vaatimukset ja tarkista niiden kirjaaminen sopimukseen.

Hinnantarkistukset

Palvelusopimus oli ollut jo vuosia voimassa. Asiakas nosti esille hinnantarkistukset. Asiakkaan mielestä hinnantarkistuskohtaan kirjattu teksti olisi edellyttänyt, että toimittaja automaattisesti ehdottaa hintojen laskemista yleisen hintatason laskiessa. Tällä perusteella asiakas vaati taannehtivia hinnantarkistuksia.

Sopimukseen ja sen yleisiin sopimusehtoihin kirjattu menettely hintojen tarkistamiseen ei kuitenkaan vaatinut toimittajaa laskemaan hintaa vaan huomioimaan yleisen palveluiden kustannustason laskun, mikäli toimittaja ehdottaa sopimuksen mahdollistamia hinnan korotuksia.

Palvelusopimuksessa huomioitavia asioita:

- ← Kirjaa hallinnointimalliin, milloin toimittaja voi ehdottaa hintojen muutoksia, millä perusteella ja mitä hinnan tarkistuksessa on huomioitava, miten ehdotetut muutokset käsitellään sekä milloin ja millä perusteella asiakkaalla on oikeus olla hyväksymättä korotuksia.
- ← Varmista, onko automaattisesti hintoja muuttavia ehtoja (esim. valuuttakurssimuutokset), kenen vastuulla on esittää muutoksia näiden perusteella, miten toimitaan, mikäli muutoksia ei esitetä, ja voivatko muutokset tulla mahdollisesti voimaan takautuvasti.

HUOLTOVARMUUSKESKUS
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN
NATIONAL EMERGENCY SUPPLY AGENCY