Tietoturvavalvomo (SOC) ja tapahtumien hallinta (SIEM) -palveluiden hankinta ja käyttöönotto

Kaupunginhallitus 16.10.2023 § 284
2464/02.08.00/2023

Valmistelu- ja lisätiedot
Charlotta Grönqvist, kehitysjohtaja
Anssi Haapala, tietohallintopäällikkö
etunimi.sukunimi@porvoo.fi

Porvoon kaupungilla on tunnistettu tarve parantaa digitaalisen turvallisuuden havainnointia ja kyvykkyyttä reagoida poikkeamatilanteisiin. On tärkeää, että digitaaliseen turvallisuuteen (tietosuojaan ja tietoturvaan) kohdistuvat riskit tunnistetaan ja niiden edellyttämät hallintatoimenpiteet toteutetaan voimassa olevien lakien, sääntelyn ja yleisten hyvien käytänteiden mukaisesti. Kyberuhat muuntuvat jatkuvasti ja hyökkäykset ovat entistä kehittyneempiä ja tietoturvatapahtumien määrä lisääntyy jatkuvasti. Nykypäivän uhilta suojautuminen vaatii entistä nopeampaa vastetta ja vastatoimia organisaatioilta.

Tietoturvavalvomon (SOC, Security Operations Center) avulla pystytään muodostamaan ajantasainen kyberturvallisuuden tilannekuva ja mahdollistetaan ympärivuorokautinen seuranta, jonka avulla voidaan reagoida poikkeamiin, tunnistaa tietoturvauhat ja toteuttaa korjaavia toimenpiteitä ennakoivasti.

Suojaustiedot ja tapahtumien hallinta (SIEM, Security Information and Event Management) on keskeinen osa tietoturvavalvomokokonaisuutta. SIEM-työkalut keräävät, koostavat ja analysoivat tietoja organisaation sovelluksista, laitteista ja käyttäjistä reaaliaikaisesti ja pyrkivät tunnistamaan epänormaalia käyttäytymistä, joka voi viitata kyberhyökkäykseen. Näin tietoturvavalvomo (SOC) voi tunnistaa, analysoida ja vastata uhkatilanteisiin ennen kuin ne vahingoittavat organisaation ydintoimintaa.

HPK Palvelut Oy tarjoaa alkuvuodesta 2024 alkaen yhteistyössä Telia Oy:n kanssa kyberturvallisuuden SOC & SIEM -palvelua, joka mahdollistaa kyberuhkien nopean havaitsemisen ja torjumisen IT-ympäristössä.

HPK Palvelut Oy toimii julkisista hankinnoista ja käyttöoikeussopimuksista annetun lain (1397/2016) 15 §:n 1 momentin tarkoittamalla tavalla omistajiensa sidosyksikkönä. Porvoon kaupunki omistaa HPK Palvelut Oy:stä 55 prosenttia. Hankittavien palveluiden hankinnan kokonaisarvo on nykyisillä hinnoilla neljän vuoden ajalle yhteensä 597 168 euroa. Hankinnan arvo sisältäen kertaluontoiset käyttöönottokustannukset on yhteensä 618 168 euroa. Nyt hankittava palvelu on osa HPK Palvelut Oy:n kautta hankittua tietoliikenne- ja puhepalvelusopimusta, jonka HPK Palvelut Oy tulee kilpailuttamaan uudelleen vuoden 2025 aikana.

Hankittavan palvelun kustannukset jatkuvien palveluiden palvelumaksun osalta ovat 12 441 euroa kuukaudessa. Palvelu sisältää Telian tietoturvavalvomopalvelun (24/7) sekä tietoturvavalvomon tarvitsemat SIEM-työkalut.

Kaupunginjohtaja
Kaupunginhallitus päättää, että Porvoon kaupunki hankkii yllä esitetyt tietoturvavalvomo (SOC) ja suojaustiedot ja tapahtumien hallinta (SIEM) -palvelut HPK Palvelut Oy:ltä esitetyn mukaisesti. Porvoon kaupungin ja HPK Palvelut Oy:n välinen palvelusopimus, palvelukuvaukset, hinnastot sekä vastuunjakotaulukot päivitetään vuoden 2023 aikana vastaamaan laajennettua palvelua. Arvioidut käyttöönottokustannus 21 000 euroa ja kuukausikustannus 12 441 euroa budjetoidaan tietohallinnon käyttötalouteen.

Päätös
Kaupunginhallitus päätti yksimielisesti, että Porvoon kaupunki hankkii yllä esitetyt tietoturvavalvomo (SOC) ja suojaustiedot ja tapahtumien hallinta (SIEM) -palvelut HPK Palvelut Oy:ltä esitetyn mukaisesti.

Johan Söderberg, Nea Hjelt ja Mikko Valtonen olivat esteellisiä, eivätkä osallistuneet asian käsittelyyn.