Lahden kaupunki
Kaupunginhallitus

Päätöspäivämäärä
12.08.2019 § 183

Lahden kaupunkiin 11.6.2019 kohdistunut kyberhyökkäys

D/1532/07.01.00.01/2019

Asian valmistelija / Lisätietojen antaja: tietohallintojohtaja Marko Monni, puh. 050 559 4055

Päätös

Päätösehdotus: Kaupunginjohtaja Pekka Timonen

Kaupunginhallitus merkitsee annetun selvityksen tiedoksi.

Perusteluosa

Tapahtumien kulku

Lahden kaupunki joutui kyberhyökkäyksen kohteeksi 11.6.2019 iltapäivällä. Tapahtuma havaittiin noin kello 14:30 ja laajamittaiset toimenpiteet käynnistettiin kello 15:45. Illan aikana saatiin varmuus hyökkäyksen laajuudesta ja hyökkääjän pääsystä kaupungin järjestelmiin.

Kaupunki siirtyi tilannejohtamiseen klo 20:00. Tällöin kaupungintalolle perustettiin tilannehuone, josta käsin toimintaa kaupungin osalta johdettiin. Tilannehuoneeseen koottiin keskeiset toimijat ja sieltä käsin pidettiin kaupungin johto ajan tasalla tilanteen kehittymisestä.

Illan, yön ja seuraavan aamun aikana tehtiin ilmoitukset eri viranomaisille. Lisäksi illalla tehtiin päätös siitä, että hyvinvointikuntayhtymän yhteydet Lahden verkkoon katkaistaan. Päätös tehtiin yhtymässä ja perusteena oli turvata keskussairaalan toiminta sekä estää hyökkääjän pääsy yhtymän tietoliikenneverkkoon.

Keskiviikkoiltaan 12.6.2019 mennessä tekniset asiantuntijat olivat saaneet selville hyökkääjän käyttämien ohjelmistojen leviämismekanismit sekä keinon estää leviäminen. Keskiviikon ja torstain aikana valmistauduttiin hyökkääjän poistotoimenpiteisiin. Poistotoimenpiteet käynnistettiin perjantaina 14.6.2019 kello 18:00, jolloin kaupungin internet-liittymä suljettiin.

Internet-liittymän sulkemisen jälkeen tehtiin tarvittavat järjestelmien uudelleenasennukset ja tekniset ratkaisut tietoturvan parantamiseksi. Yhteyksien hallittu avaaminen aloitettiin seuraavana päivänä tärkeimpien yhteyksien osalta. Avaamista on jatkettu läpi kesän

järjestelmäpalveluista tehdyn priorisointilistan määräämässä järjestyksessä

Tapahtuman kustannukset

Tapahtuman suorat kustannukset ovat olleet heinäkuun loppuun mennessä 685 670 euroa. Kustannus muodostuu IT-palvelutuottajan tekemästä työstä, asiantuntijapalveluiden hankinnasta sekä erityisohjelmistojen lisensseistä.

Välillisiä kustannuksia mm. toimimattomien järjestelmien ja yhteyksien osalta ei ole arvioitu. Kustannus on kuitenkin merkittävä johtuen erityisesti siitä, että hyökkäys on ollut laaja-alainen, jolloin sen vaikutus on ulottunut kaupungin lisäksi ulkopuolisiin toimijoihin (mm. konserniyhtiöt ja kuntayhtymät) sekä siitä, että tietojärjestelmien toimivuuden palauttaminen on kestänyt pitkään.

Jatkotoimenpiteet

Jatkotoimenpiteiden osalta on suunniteltu sekä teknisiä että kaupungin toimintaa muuttavia muutoksia. Teknisen tietoturvan parantamiseksi parannetaan tietoliikenneverkon turvallisuutta jakamalla verkkoa pienempiin hallinnollisiin osiin, ottamalla käyttöön automaattista ja aktiivista liikenteen valvontaa tukevia järjestelmiä sekä kasvatetaan mahdollisten tietoturvapoikkeamien jäljitettävyyttä parantamalla lokituskäytäntöjä. Lisäksi kaikkiin kaupungin käyttäjiin tulee vaikuttamaan pääsynhallinnan koventaminen muuttamalla salasana- ja käyttöoikeuksien hallinnan käytäntöjä.

Kaupungin toimintaa muuttavia toimenpiteitä ovat tietoturva-auditointien ottaminen osaksi tietohallinnon vuosikelloa, uusien järjestelmien käyttöönoton yhteydessä tehtävät tietoturvatarkistukset sekä tietoturvallisuuden valmiuden ylläpitäminen jatkuvan, automaattisen seurannan avulla.

Tietohallintojohtaja Marko Monni on kokouksessa antamassa selvityksen tapahtumista.

Muutoksenhaku muutoksenhakukielto

Toimenpiteet -