Samuli Pekkola
professori, Jyväskylän yliopisto

Maija Ylinen
tutkijatohtori, Tampereen yliopisto

Kyberhyökkäys voi uhata sairaaloitakin

Sairaaloiden resilienssi vaatii vielä kehittämistä toimiakseen hyvin.

SIDONNAISUUDET
Ei sidonnaisuuksia.

KYBERHYÖKKÄYKSISTÄ on tullut merkittävä uhka kaikille tietojärjestelmäriippuvaisille organisaatioille. Yhteiskunnallisesti merkittävät toimijat, kuten sairaalat, ovat houkuttelevia hyökkäyskohteita, sillä hyökkäyksen seuraukset ovat merkittäviä.

Kyberhyökkäyksessä järjestelmiä saatetaan kuormittaa niin, etteivät ne pysty tuottamaan pyydettyä tietoa, tietoa saatetaan varastaa, palvelimilla olevaa tietoa saatetaan muuttaa ja vääristellä, kiristysohjelmia hyödyntää tai erilaisten koneiden ja laitteiden toimintaa häiritä.

Näiltä uhilta pyritään suojautumaan erilaisin teknisin ja toiminnallisin keinoin. Lisäksi sairaalat valmistautuvat jatkamaan toimintaansa onnistuneesta hyökkäyksestä huolimatta.

Kriisitilanteissa sairaalat tarvitsevat resilienssiä eli kykyä ennakoida, reagoida ja palautua kohtaamistaan vaikeuksista. Resilienssi edellyttää teknisen kyvykkyyden lisäksi ei-teknisiä toimenpiteitä ja taitoja kuten henkilökunnan kouluttamista kyberuhkien tunnistamiseksi, kyberhyökkäyksen aikaisia toimintasuunnitelmia ja hyökkäyksen jälkeisiä toipumissuunnitelmia.

Esimerkiksi potilastietojärjestelmän joutuessa kyberhyökkäyksen kohteeksi – jolloin sen tarjoamat palvelut eivät ole käytössä – potilaiden hoidon on jatkuttava.

Tietohallinnon keskittyessä tietojärjestelmien tuottaminen palveluiden palauttamiseen, hoitohenkilökunnan on kyettävä tuottamaan hoitoa ilman aiemmin käytettävissä ollutta tietoa potilaan hoitohistoriasta, allergioista tai veriryhmästä.

Valmius ja kyky toimia

Keskeistä on hoitohenkilökunnan valmius ja kyky toimia niin poikkeuksellisissa tilanteissa kuin normaaliin toimintatapaan palatessa. Onko hoitajilla ja lääkäreillä taitoa hoitaa potilaita ilman tavallisia työkaluja tai onko paperille tehtyjen muistiinpanojen potilastietojärjestelmään kirjaamiseen olemassa aikaa ja resursseja?

Sairaalan henkilöstön läpileikkaavan tutkimuksemme mukaan sairaaloiden resilienssi vaatii kehittämistä. Sairaalat ovat suojautuneet kyberhyökkäyksiltä niin teknisillä kuin ei-teknisillä toimenpiteillä. Kuitenkin hyökkäyksiin valmistautumisessa ja niistä toipumisessa on paljon tehtävää.

Asenne ratkaisee

Erityisen haasteen resilienssin parantamisessa muodostavat rutiiniprosessit ja henkilökunnan asenne. Sairaalan johto ja hoitohenkilökunta tiedostavat kyberuhkien uhat ja todennäköisyyden. Hoitotyön loputtomat vaatimukset eivät kuitenkaan jätä aikaa varautumiselle, joten se jää herkästi jonkun muun, usein tietohallintoyksikön vastuulle. Tietohallinto ei kuitenkaan voi yksin parantaa hoitoyksiköiden toimintaa ja hyökkäyksestä toipumista, mikäli sen rakentama suoja on pettänyt.

Sairaalat valmistautuvat kyberuhkiin tyypillisesti johdon ja tietohallinnon keskisissä harjoituksissa. Niissä käydään läpi esimerkiksi, miten kyberuhasta viestitään, miten toimenpiteitä johdetaan ja mistä on kunkin vastaa.

Muistilista ei riitä

Harjoitukset eivät useinkaan kosketa sairaalan hoitoyksiköitä. Niiden avuksi on laadittu erilai-

> *”Hyökkäyksiin valmistautumisessa paljon tehtävää.”*
> Samuli Pekkola ja Maija Ylinen

ADOBE/AOP

Sairaaloissa olisi tärkeää, että koko henkilökunta on koulutettu mahdollisiin uhkiin.

sia ohjeita ja muistilistoja, jotka ovat kuitenkin vain harvojen tiedossa. Lisäksi niissä keskitytään lyhytaikaisista poikkeamista selviämiseen, ei monimutkaisempiin, pitkittyneisiin kriiseihin.

Sairaalan resilienssin parantaminen painottuukin johdon toiminnan kehittämiseen ja ennaltaehkäiseviin toimenpiteisiin. Hyökkäyksiin varaudutaan teknisin keinoin ja yleistä kyberturvallisuustietoisuutta parantaen. Varautuminen vaikuttaa olevan kohtuullisella tasolla.

Sen sijaan hyökkäyksen aikainen toiminta ja hyökkäyksestä palautuminen ovat valtaosin kokonaisvaltaisesti harjoittelematta. Ohjeet auttavat teoriassa, mutta mikäli niiden olemassaoloa ei tiedetä tai niitä ei ole sisäistetty, niiden käytännön vaikutus jää minimaaliseksi.

Hyökkäyksestä palautumisen ajatellaan sujuvan osana normaalia toimintaa.

Yhteinen ponnistus

Kyber-resilienssin parantaminen edellyttää uhkatietoisuuden lisäämistä, yhteisen kyberturvallisuusasenteen jalkauttamista sekä kyvykkyyttä toimia oikein ja asianmukaisesti. Näitä keinoja voidaan parantaa ohjeilla ja harjoituksilla, jotka läpileikkaavat koko organisaation ja kaikki kyberhyökkäyksen vaiheet: ennen hyökkäystä, hyökkäyksen aikana ja hyökkäyksen jälkeen.

Harjoituksia ja ohjeita on myös aktiivisesti reflektoitava; mikä on kulloinkin heikoin lenkki ja parantamista kaipaava yksityiskohta? Aivan kuten hoidon parantaminen, resilienssi paranee vain yhteisillä ponnistuksilla.●

Näkökulma-palstalla julkaistavien kirjoitusten enimmäispituus on 5 000 merkkiä. Toimitus lyhentää kirjoituksia tarvittaessa. Palstalle tarkoitetut kirjoitukset lähetetään osoitteeseen laakarilehti@laakarilehti.fi