Diktamen
PUHUMALLA PARAS

F-Secure

LAPIN SAIRAANHOITOPIIRI
LAPPI BUOHCCEDIKŠUNBIIRE

Siun SOTE

Tietoturva ja kyberrikollisuus terveydenhuollossa

Suomalainen terveydenhuolto on jäänyt tietoturvan kehityksestä jälkeen

Asiantuntijoina

Mikko Hyppönen
Tutkimusjohtaja
F-Secure

Veli-Matti Tolonen
Tietohallintojohtaja
Lapin SHP

Tomi Tikkanen
ICT-pääsuunnittelija
Siun sote

Olavi Valkama
Toimitusjohtaja
Diktamen

Diktamen

Tietoturva ja kyberrikollisuus terveydenhuollossa

Suomalainen terveydenhuolto on jäänyt tietoturvan kehityksestä jälkeen, toisin kuin tuoreessa kyberturvallisuusselvityksessä pärjännyt finanssiala. Rahamme ovat siirtyneet pankkiholveista digitaalisiin palveluihin ja potilastietomme arkistokaappien kortistoista ensin suljettuihin potilastietojärjestelmiin ja lopulta pilvipalveluihin.

Vastaamon tapaus on osoitus siitä, että terveydenhuollossa digitalisoitumista ei ole tehty tietoturva edellä kuten finanssialalla.

"Kyberrikollisuus on digitalisaation kääntöpuoli. Internet on tuonut huimat määrät kaikkea hyvää, mutta se on pysyvästi muuttanut uhkia. Varhaisissa internetin vaiheissa asialla olivat yksittäiset hakkerit, mutta nykyään valtaosa hyökkäyksistä tehdään raha mielessä", kuvaa F-Securen tutkimusjohtaja Mikko Hyppönen.

Kansainvälisen kyberrikollisuuden arkkityypit

F-Secure

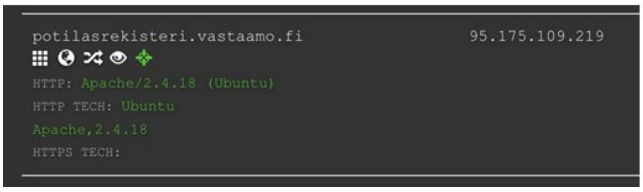
Case Vastaamo

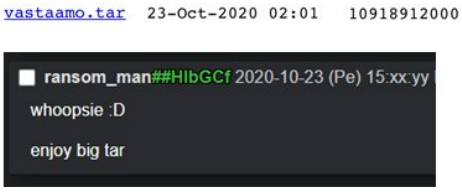
Kiristysviestin sisältö:
"Hyvaa paivaa.

Mina olen hakkeri. Olen kopioinut Vastaamo potilaiden tietokanta.

I have attached a small sample of your patient database to this email. If you reply within the next 6 hours we are prepared offer you a very special discount. Any price you'll pay us will be small compared to the damage that would be inflicted to your business if we release this information on the internet. We have over a gigabyte of your most sensitive patient data.

If you have any questions or difficulty understanding what's happening, I'm here to help."





Vastaamon tietomurto, jossa kymmenien tuhansien ihmisten arkaluontoisia potilastietoja vuodettiin internetiin, on poikkeuksellinen. Siitä on pian nousemassa Suomen suurin rikos, jossa rikosilmoituksia on tehty jo 26 000.

Hyppösen mukaan motiivina rikoksen takana oli raha: "Vastaamon tapauksessa kyseessä oli kiristyshyökkäys, joka kohdistui puutteellisesti suojattuun potilastietojärjestelmään. Hyökkääjä oli varastanut tiedot jo vuonna 2018, ja hän vaati puolen miljoonan lunnaita ensin Vastaamolta ja ryhtyi sen jälkeen julkaisemaan potilastietoja verkossa.

Lopulta hyökkääjä päätyi kiristämään rahaa myös yksityisiltä ihmisiltä, jotka olivat joutuneet tietomurron uhreiksi. **Tämä on kansainvälisesti poikkeuksellinen rikos.** Meillä on tiedossa kaikkiaan vain neljä vastaavaa tapausta, joista tämä on ensimmäinen terapiatietoihin liittyvä."

Vastaamo nosti tietoturvan kaikkien potilastietojen kanssa toimivien huulille. Diktamenin toimitusjohtaja Olavi Valkama näkee, että suhtautuminen tietoturvaan tulee muuttumaan.

"Olemme yhden aikakauden lopussa, jossa tietoturvaan liittyvät vaatimukset ovat olleet suhteellisen pieniä, ja tietoturva on perustunut luottamukseen enemmän kuin tiukkoihin vaatimuksiin."

"Olemme yhden aikakauden lopussa"

Tietoturvan hallinnan ISO27001-sertifikaatti

Diktamenissa käsitellään miljoonia saneluja ja potilasdokumentteja vuosittain, joiden tietoturvan vakuutena on yritykselle myönnetty alan tiukin kansainvälisesti tunnustettu ISO27001-sertifikaatti.

“ISO27001 on alan tiukin sertifikaatti”

“Meille myönnettiin ISO27001-standardin mukainen tietoturvan hallintajärjestelmän sertifikaatti jo vuonna 2018. Sitä vaadittiin, kun olimme laajentamassa toimintaamme Englantiin, jossa tietoturva on ollut pinnalla pidempään ja kyberrikollisuus laajempaa. **Tietoturvaan liittyviä vaatimuksia tullaan varmasti tiukentamaan hankinnoissa** ja sopimuksissa erityisesti silloin, jos palveluntuottajan tietojärjestelmiin tallennetaan tai niissä käsitellään tilaajan asiakkaiden potilastietoja”, arvioi Valkama.

“ISO27001 on alan tiukin sertifikaatti ja erinomainen tapa osoittaa organisaation kyky huolehtia tietoturvaan liittyvistä asioista. Sertifikaattia ei ole helppo saada. Prosessin läpikäynti on työlästä, koska siinä ei pelkästään dokumentoida kaikkia tietoturvan hallintakäytäntöjä, siinä myös läpikäydään ja auditoidaan käytännön toiminta ml. laitteisto. Sertifikaatti on aika harvinainen, sitä ei ihan helposti saa. Ne jotka kykenevät oman toimintakykynsä näillä sertifikaateilla osoittamaan, ovat todella ansainneet sen”, Hyppönen kuvaa.

“F-Secure on 1200 ihmisen yritys, meillä on konttoreita 29 eri maassa. **Meidän pitää myös pystyä osoittamaan oma toimintamme nimenomaan sertifiointien kautta.** Kävimme prosessin läpi ja meille myönnettiin ISO27001-sertifikaatti 2018 eli samana vuonna kuin Diktamenille”, Hyppönen jatkaa.

Valkama tunnistaa työlään prosessin: “Sertifikaatin saaminen edellytti sitä, että olemme koko toimintahistorian ajan kehittäneet palvelujamme, tietojärjestelmiämme ja organisaatiotamme tietoturva-asiat keskiössä.”

Diktamenin toimintaa ohjaa tietoturvan hallintajärjestelmän **ISO27001**-sertifikaatti, säännöllinen **auditointi** ja tietoturvatestaukset.

ISO27001-sertifikaatti on siis tietoturvan hallintajärjestelmä, joka ohjaa tietoturvaan liittyviä toimintoja organisaatiossa. Tietoturvan hallintajärjestelmän avulla tietoturvan taso on standardin mukaista. Sertifikaatin ylläpito vaatii jatkuvaa tietoturvan hallintaa ja organisaation johtamista tietoturvastandardin vaatimusten mukaisesti. Käytännössä tämä tarkoittaa dokumentointia, auditointeja sekä kouluttautumista.

Sertifikaatin ylläpito on työlästä

Sertifikaatti edellyttää yksityiskohtaisesti dokumentoitua tietoa siitä, miten tietoturvaan liittyvät asiat tehdään, oli kyse sitten tietojärjestelmistä, laitteista tai henkilöistä, jotka asiakkaan tai potilaiden tietoja käsittelevät.

"Tietoturvamme taso haastetaan säännöllisesti myös auditoinneilla, joissa t**ietoturvamme auditoidaan ulkopuolisen tahon toimesta.** Tällä testataan, vastaako dokumentaatio sitä, miten organisaatiomme toimii", kuvaa Valkama.

Sertifikaatin ylläpito on työlästä: vuosikellossa on joka kuukaudelle useampia sisäisiä ISO27001 liitännäisiä palavereja, joissa dokumentaatiota ja toimenpiteitä määritellään.

ISO27001 PERIAATTEET

Luottamuksellisuus
tieto on saatavilla vain niille, joilla on siihen oikeus

Koskemattomuus
tiedon ja sen käsittelytapojen tarkkuus ja täydellisyys

Saatavuus
ne, joilla on oikeus tietoihin, saavat tiedot tarvittaessa

Lisäksi Diktamenilla pidetään säännöllisiä tietoturvakoulutuksia koko henkilöstölle, ja Diktamen-tietojärjestelmä käy säännöllisesti läpi tietoturvatestaukset ja auditoinnit.

Diktamenille myönnetty tietoturvan hallintajärjestelmän ISO27001 sertifikaatti siis osoittaa, että yrityksessä on otettu käyttöön tunnetut parhaat käytännöt tietojen suojaamiseen sekä tietoturvariskien hallintaan.

Diktamenin ISO27001-sertifikaatti koskee koko Diktamen-konsernin toimintaa, ja koko henkilöstömme on sitoutunut käsittelemään kaikkea tietoa sertifikaatin vaatimusten mukaisesti.

Luottamuksen arviointi perustuu vaatimuksiin

Toimittajien luotettavuutta ja tietoturvan tasoa arvioidaan aina, kun hankintoja tehdään palveluista ja järjestelmistä, joilla potilastietoja käsitellään. Lapin sairaanhoitopiirin tietohallintojohtaja Vesa-Matti Tolosen mukaan kumppanien sekä palveluprosessien luotettavuuden ja tietoturvan tason arviointi tapahtuu organisaatiotasolla, ja siihen vaikuttavat erilaiset sopimukset ja vaatimusmäärittelyt:

"Olemme käyneet ja tarkentaneet standardivaatimuksia tietoturva huomioiden. Meillä on yli 100 vaatimusta ja määrittelyä tietoturvan ja tietosuojan osalta. Vastaamon tapauksen jälkeen ISO27001 on tullut voimakkaammin esille."

Lunnastroijalaisia sairaaloissa

Case Wannacry
NHS, Merck, etc **2017**
DCH Health System
Alabama USA **2019**
South West Alliance of Rural Health
Australia **2019**
Rouen University Hospital-Charles Nicolle
France **2019**
Brooklyn Hospital Center,
New York, USA **2019**
Hackensack Meridian Health,
New Jersey, USA, **2019**
Michael Garron Hospital,
Toronto, Canada, **2019**
Listowel Wingham Hospitals Alliance ,
Canada **2019**
Pleasant Valley Hospital West Virginia,
USA, **2020**
Universitätsklinikum Düsseldorf,
Germany **2020**
United Health Service,
USA **2020**

Tietoturvavaatimusten noustessa kasvaa myös toimittajan työmäärä, mikä näkyy hinnoissa. Siun Soten ICT-pääsuunnittelija Tomi Tikkanen näkee kehityksen luonnollisena jatkumona yhden aikakauden päätökseen:

"Vaatimustason nostaminen tietoturvassa tai laadussa yleisemmin on tarkoittanut korkeampaa hintaa. Näin se on ollut ja tietoturvatason vaatimusten nostaminen ei mielestäni tee tästä poikkeusta. Tässä on kysymys yksinkertaisesti siitä, että olemme tulleet yhden aikakauden päätökseen. Myös tietoturvan osalta vaatimuksia tullaan kiristämään, ja tällöin se tietysti tulee maksamaan enemmän, ja eurot pitää siihen saada allokoitua muualta."

"Kyllä hinnat tulee nousemaan."

Asianmukaisesta tietoturvan hallinnasta ei kuitenkaan kannata tinkiä. Tikkanen näkee positiivisena, että Vastaamon tapaukseen on suhtauduttu vakavasti ja vaatimustason täyttämiseen ollaan valmiita laittamaan euroja:

"Kyllä hinnat tulee nousemaan. Vastaamon jälkeen julkinen paine on luonut paineita nostaa tietoturvan vaatimustasoa. Meillä budjettia on annettu enemmän ensi vuodelle, jotta vaatimuksia voidaan kiristää hankinnoissa tietoturvan osalta."

"On nähtävissä, että erityisesti alihankintasopimusten sopimusehdot tiukkenevat. Alihankkijoiden kenttä on laaja. Esimerkiksi vanhusten asumispalvelut on suureksi osaksi ulkoistettu ja toimijat käyttävät omia tietojärjestelmiään. Siun Sotessa on aiemminkin ollut tietojenkäsittelyn vaatimukset ja ohjeet alihankkijoille. **Jatkossa otetaan kantaa myös fyysisiin ratkaisuihin ja vaikkapa siihen, onko palveluntuottajalla käytössään esimerkiksi pilvipalvelu** ja miten sen tietoturva on varmistettu", Tikkanen pohtii.

Mitä on tietoturva?

Diktamenin toimitusjohtaja Olavi Valkaman mukaan toimittajien luotettavuuden ja tietoturvan tason arviointiin on selvät askeleet.

“Mielestäni jokaisen organisaation tietoturvan heikoin lenkki on ostopalvelu- ja tietojärjestelmätoimittajat, sillä oman organisaation tietoturvaa on helpompi hallita ja hoitaa omien tietojärjestelmien tietoturvataso riittäväksi. Myös toimittajan tietoturvan tulee vastata riittävää tasoa niin organisaation kuin käytettyjen tietojärjestelmien osalta.”

“Sertifikaatti on paras ja selkein osoitus siitä, että palvelua tuottavan organisaation tietoturva on riittävällä tasolla. Se on ulkoisesti ja säännöllisesti auditoitu. Tietojärjestelmien tulee myös olla auditoitu ja todistetusti tietoturvatestattu”, Valkama jatkaa.

“Meillä tulee aina olemaan bugeja, koska ihmiset tekevät virheitä.

F-Securen tutkimusjohtaja Mikko Hyppönen näkee myös, että luotto ei yksin riitä. On myös varmistuttava siitä, että asiat hoidetaan niin kuin luvataan.

“Jos ajatellaan toimittajien tietoturvan tasoa niin testaus tarkoittaa nimenomaan testausta. Pitää vaatia tietoturvaa ja dokumentaatiota siitä, että asiat on hoidettu niin kuin on luvattu. **Pitää testata, että asiat on hoidettu niin kuin on dokumentoitu, ja sitten se pitää auditoida. Sillä luottamus syntyy.** Faktat pitää tarkistaa, jotta voidaan varmistua siitä, miten tietoturva-asiat on toimittajilla ratkaistu.”

Terveydenhuollossa tietosuoja ja tietoturva kulkevat käsi kädessä. **Tietoturva (security) ja tietosuoja (privacy)** ovat Hyppösen mukaan kuin kolikon kaksi puolta, ja Suomessa ne menevät usein sekaisin.

Potilastietojen kohdalla molemmat ovat yhtä tärkeitä: se että potilastiedot pysyvät turvassa ja yksityisinä eli eivät päädy vääriin käsiin.

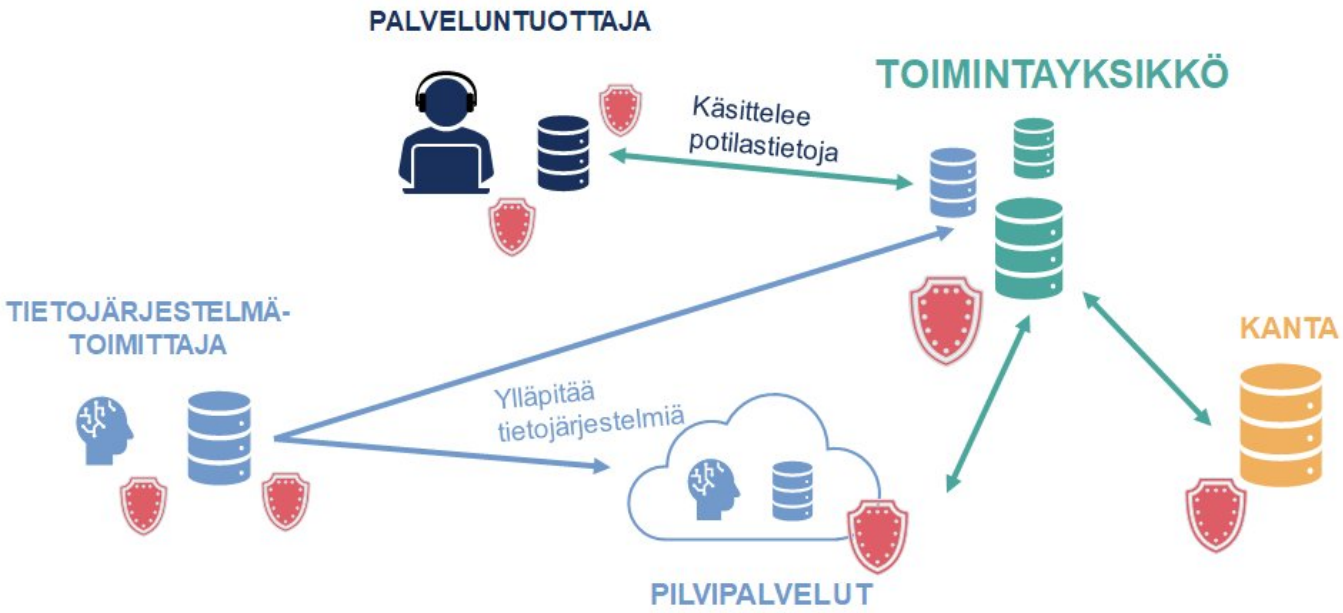
Mikko Hyppönen kertoo, että tietoturvariskien taustalta löytyy aina joko tekninen tai ihmisiin liittyvä aukko. Haavoittuvuus ja turvareiät järjestelmissä tarkoittavat, että on tapahtunut ohjelmointivirhe, eli siellä on bugi, jonka ansiosta tätä järjestelmää voidaan väärinkäyttää.

“Meillä tulee aina olemaan bugeja, koska ihmiset tekevät virheitä. Ennen bugi tarkoitti, että kone kaatuu. Konetta ei siis saanut kukaan haltuun, koska ei oltu verkossa. Nykyään samanlaiset bugit ovat turvareikiä, koska koneet ovat verkossa”, Hyppönen kertoo.

Teknisten ongelmien korjaaminen voi olla työlästä, hidasta ja kallista, mutta usein tehtävissä. Ihmistä ei toisaalta voi korjata samalla tavalla, mikä tekee ihmisen aiheuttamasta tietoturva-aukosta vielä haastavamman.

“Ihmisten aiheuttamat ongelmat liittyvät usein siihen, että klikataan sähköpostin jokaista linkkiä, käytetään samaa salasanaa joka paikassa, kompastutaan jokaiseen huijaukseen. **Tämä on vaikea ongelma - me emme voi vain etsiä bugia ihmisten aivoista ja päivittää softaa.** Ainoa keino on koulutus, ja se vasta hidasta onkin!” Hyppönen summaa.

Tietoturvan hallinta terveydenhuollon verkostoissa



Suojautuminen on kuitenkin mahdollista, jos organisaatio on pohtinut, millaiset tahot saattaisivat olla kiinnostuneita hyökkäämään niiden järjestelmään. Ulkoiset palveluntarjoajat ja pilvipalvelut ovat aiheuttaneet sen, että jokaisen yrityksen tulee miettiä suojautumiseen liittyviä kysymyksiä.

Tyypillinen ajattelumalli, jossa organisaation sisäistä verkkoa suojellaan isolta pahalta internetiltä laittamalla rautaa rajalle ja rakentamalla palomuureja, ei Hyppösen mukaan enää riitä.

"Emme enää voi ajatella niin, että pidetään paha ulkoverkossa, vaan meillä pitää olla näkymä siihen, missä meidän data on ja mitä sille tapahtuu. Silloin on helppo huomata, jos tapahtuu jotain epänormaalia. Vastaamossa ei seurattu, mitä tiedoille tapahtuu, muuten siellä olisi huomattu 2018, että gigatavun verran dataa kopioitiin ulkoiseen osoitteeseen. Verkon tilaa ei seurattu, joten sitä ei huomattu."

Tietoturva-asioita onkin hyvä lähteä pohtimaan tekemällä kartoitus kaikista palveluista ja järjestelmistä, mitä organisaatiolla on käytössä. Hyppösen mukaan ei ole itsestään selvää, että kattava listaus löytyisi kaikilta käden käänteessä:

"Harvalla on antaa suoraan lista, mitä kaikkea organisaatiolla on käytössä, minkä vuoksi on tärkeää tehdä kartoitus oleellisimmista järjestelmistä, siitä mitä kaikkia palveluntarjoajia on käytössä ja missä data kulkee. Tästä kun lähtee liikkeelle niin ollaan jo pitkällä."

Tietohallintojohtajana Vesa-Matti Tolonen vastaa siitä, että hän pystyy tuottamaan riittävän tilannekuvan organisaation johdolle myös tietoturvan osalta, ja hänen mukaansa sertifiointi on kiistattomasti paras tapa osoittaa, että tietoja käsitellään oikein:

"**Raamien löytäminen tietoturvan hallintaan on haasteellista ilman sertifikaattia.** Organisaatioiden tietoturvan osalta ihminen eli käyttäjä on monesti heikoin lenkki, siksi henkilöstön kouluttamiseen kannattaa panostaa. Koen, että tärkeintä on se, että tietoturvaa johdetaan oikein."

"Oman väen sisäinen johtaminen on helppoa, mutta ulkoisen toimittajan johtaminen onkin haastavampaa. Tarvitaan viitekehys ja selkeä menettely, jotta kaikille on samat minimivaatimukset", Tikkanen jatkaa.

Pankeistako malli terveydenhuoltoon?

Tietoturvan hallinnan tasosta kertoo parhaiten sertifikaatit ja todistukset sekä säännöllinen testaus hyökkäysten varalle.

“Ilman muuta tietoturvan hallintajärjestelmän ISO27001 sertifikaatti ja todistukset sen säännöllisestä ulkoisista auditoinneista on paras evidenssi, että tietoturva-asiat hoidetaan asianmukaisesti organisaatiossa. Käytettävästä tietojärjestelmästä, johon tilaajan potilastietoja tallennetaan, tulee olla säännölliset tietoturvatestaukset ja auditoinneista todistukset”, Valkama yhtyy muiden näkemyksiin.

Tulevaisuudessa terveydenhuollon tietoturvan tasolta tullaan vaatimaan yhä enemmän. Hyvä tavoite olisi saavuttaa finanssialan varmuus tietojen käsittelyssä.

“**Me emme yhteiskuntana ole suhtautuneet samalla vakavuudella terveystietoihin kuin pankkitietoihin.** Emme ole ymmärretty, miten ison ja tärkeän asian äärellä ollaan, kun puhutaan potilastiedoista. Niitä pitää suojata ikuisesti. Terapiatiedot eivät museoidu samalla tavalla kuin vanhat sähköpostiviestit. Ne ovat tulenarkoja vuosikymmeniä. Meidän pitää pystyä pitämään tiedot salattuna ja suojattuna samalla kun niiden on oltava saatavilla asianosaisille”, arvioi Hyppönen.

“**Toivon, että tietoturvaan liittyvät huolet eivät jää hetken huumaksi.** Samalla uskon, että sertifikaatit tulevat olemaan vaatimus hankinnoille tulevaisuudessa”, Tolonen arvioi.

Valkama toivoo, että muutoksia tullaan näkemään vaatimuksissa, mitä ulkoisen palveluntuottajan tietoturvatasosta odotetaan:

“Hankintayksikköjen kannattaa nostaa tietoturvan hallinnan tason vaatimusta, auditointi- ja

“Uskon, että sertifikaatit tulevat olemaan vaatimus hankinnoille tulevaisuudessa”

sertifikaattivaatimuksia hankinnoissa. ISO27001 tai vastaava tietoturvan hallintajärjestelmän vaatimus auditointeineen ja tietoturvatestauksineen voisi hyvin olla Suomessa pakollinen soveltuvuusvaatimus, kun hankitaan palveluita tai tietojärjestelmiä, joilla tai joissa tuotetaan tai käsitellään potilastietoja.”

Toiminnan turvaamiseen on Valkaman mukaan käytössä myös muita kriteerejä: “**Hyvä esimerkki on tietyn tason Rating Alfa tai vastaava luottoluokitus (esim. AA) -vaatimus**, joka on peruskamaa hankinnoissa: halutaan varmistaa toiminnan jatkuvuus, että tarjoajan talous on kunnossa. Samalla tavalla ISO27001-sertifikaatti on tietoturvan hallinnan osalta selkeä osoitus, että palveluntuottajan tietoturva-asiat ovat kunnossa.”

Siun soten Tomi Tikkasen mukaan Vastaamon tapaus on luonut uuden kiinnostuksen tietoturvaan liittyviin asioihin, mikä tuo tullessaan muutoksia vaatimuksiin.

“On anteeksiantamatonta, että meidän terveystiedot on huonommin suojattu kuin pankkitiedot. Onneksi tämä lähtee korjaantumaan: asenneilmapiiri on Vastaamon jälkeen muuttunut - nyt ollaan kiinnostuneempia kuin koskaan tietoturvakysymyksistä ja -mekanismeista.”

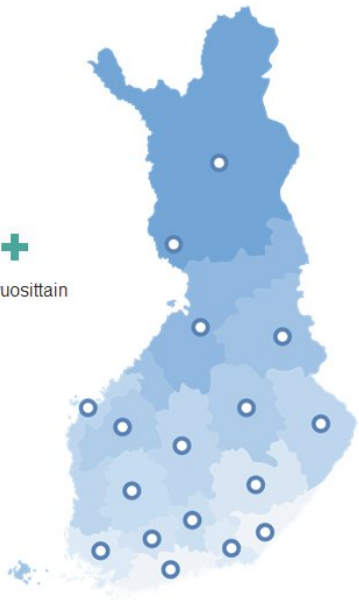
Ota avuksesi Diktamen

Diktamen on johtava potilastietojen dokumentointia nopeuttavien tietojärjestelmien ja sanelunpurku-palveluiden tarjoaja ja kehittäjä.

250+
asiakastoimipistettä

16000+
käyttäjää päivittäin

5 milj.+
potilasdokumenttia vuosittain



Terveydenhuollon tietoturva on vain niin vahva kuin sen heikoin lenkki. Jos sinulla heräsi aiheesta kysyttävää, ole meihin yhteydessä.
Autamme mielellämme.

Diktamen
PUHUMALLA PARAS

Olavi Valkama
olavi.valkama@diktamen.com

F-Secure

Mikko Hyppönen
mikko.hypponen@f-secure.com

LAPIN SAIRAANHOITOPIIRI
LAPPI BUOHCCEDIKŠUNBIIRE

Vesa-Matti Tolonen
vesa-matti.tolonen@lshp.fi

Siun SOTE

Tomi Tikkanen
tomi.tikkanen@siunsote.fi

Diktamen Oy
Itämerenkatu 1
00180 Helsinki

Vaihde: 010 420 8040
Myynti: 010 420 8048

myynti@diktamen.com
www.diktamen.com