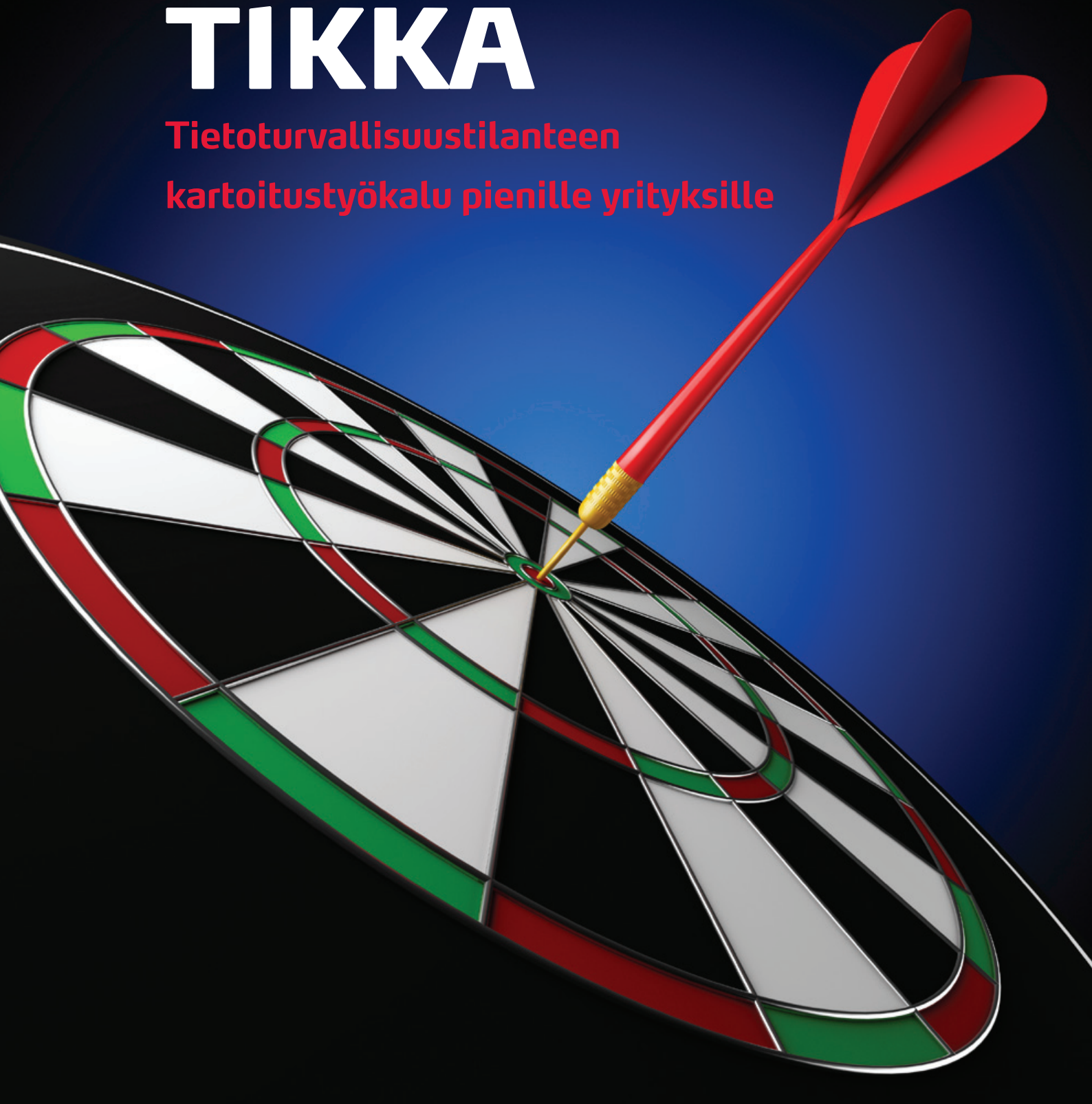
Viestintävirasto
Kyberturvallisuuskeskus

Elinkeinoelämän keskusliitto

Antti Kurittu

TIKKA

Tietoturvallisuustilanteen kartoitustyökalu pienille yrityksille



Riskien hallinta on aina helpompaa kuin vahingoista toipuminen!

Sisällysluettelo

Tervetuloa käyttämään Tikkaa – pienten yritysten tietoturvallisuustilanteen kartoitustyökalua

Jokaisella yrityksellä, niin pienellä kuin suurella, on suojaamisen arvoista tietoa. Tämä koskee kaikkia yrityksiä toimialasta riippumatta.

Tietoturvallisuudesta huolehtiminen on osa yrityksen välttämätöntä riskienhallintaa. Tietoturvaa koskevat väärinkäytökset, vahingot ja onnettomuudet voivat liittyä yrityksen hallintoon, fyysisiin toimitiloihin, henkilöstöön, tietoaineistoihin tai ohjelmistoihin ja laitteisiin.

Tässä julkaisussa esitelty Tikka-kartoitustyökalu on suunniteltu erityisesti tietoturvallisuustyötään aloittelevien yritysten tarpeisiin.

Julkaisu sisältää kuusi fiktiivistä esimerkkitapausta, joissa on hyödynnetty tyypillisiä piirteitä tosielämän tietoturvaonnettomuuksista, väärinkäytöksistä ja rikostapauksista. Jokaisen tapauksen yhteydessä analysoidaan tapahtumaan liittyneitä riskejä ja valotetaan tietoturvan ajankohtaisia ilmiöitä.

Tikka-työkalun kehittäminen on ollut minulle antoisa hanke, sillä olen perehtynyt tietoturvaan sekä opintojeni kautta että työssäni Kyberturvallisuuskeskuksessa.

Julkaisuvaiheen kumppaneinani ovat olleet Viestintäviraston Kyberturvallisuuskeskus ja Elinkeinoelämän keskusliitto EK. Molemmat tekevät työtä sen eteen, että myös pienet yritykset tiedostaisivat tietoturvariskejä entistä paremmin ja löytäisivät ennalta estäviä ratkaisuja niiden hallitsemiseksi.

Antti Kurittu
antti.kurittu@gmail.com

Näin käytät Tikka-kartoitustyökalua

- **Lue kukin esimerkkitapaus ja perehdy siihen liittyvään analyysiin. Poimi hyödylliset vinkit ja neuvot.**
- **Aseta tapahtumat oman yrityksesi kontekstiin ja esitä kysymykset:**
  Voisiko näin tapahtua meidän yrityksessämme?
  Miten meidän tulisi varautua tällaisen tilanteen varalle?
- **Käynnistä tarvittavat toimet, joilla yrityksesi tietoturvariskit saadaan aiempaa paremmin hallintaan.**

1 Myyntipäällikköä huijataan

Pentti työskentelee myyntipäällikkönä yrityksessä. Hän vastaa työtehtävissään asiakkaille laadittavien tarjousten laatimisesta. Pentillä on luonnollisesti pääsy yrityksen sisäverkkoon myös kotoaan, sillä hän matkustaa työnsä puolesta paljon ja tietoturvaohjeiden mukaan yrityksen tietoja saa tallentaa vain sisäverkkoon. Pääsy yrityksen sisäverkkoon on varmistettu käyttäjätunnuksella ja salasanalla, joka pitää vaihtaa kolmen kuukauden välein. Pentti pitää aina mukanaan yrityksen konetta, jonka kovalevy on salakirjoitettu. Tietoturvan pitäisi siis olla teknisesti kunnossa.

Yritys on ulkoistanut ylläpito- ja IT-tukipalvelut ja siirtänyt yrityksessä ennen IT-tukena toimineet henkilöt toisiin tehtäviin. Tällä tavoin yritys on säästänyt rahaa ja pystynyt keskittymään omaan ydinosaamisalueeseensa.

Pentti on työmatkalla Ikaalisissa, kun hän saa työsähköpostiinsa viestin IT-tuelta. Viestissä kerrotaan, että Pentin toimistolla sijaitsevalle työasemalle on tullut internetistä virus ja että IT-tukihenkilön tulisi kirjautua etäyhteydellä työasemalle virustorjuntaohjelman ajamista varten. Virustorjunnan ajamista varten Pentin pitäisi kirjautua verkkoon sähköpostissa annetusta linkistä.

Sähköposti on tullut IT-tuen sähköpostiosoitteesta ja siinä on oikean yrityksen logo. Viestikin on kirjoitettu siistillä ja selkeällä suomen kielellä.

Hän klikkaa sähköpostissa olevaa linkkiä ja syöttää sieltä aukeavalle verkkosivulle käyttäjätunnuksensa ja salasanansa.

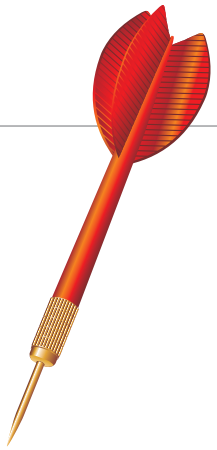
Sivusto antaa kuitenkin virheilmoituksen, ja Pentti sulkee sen.

Hetken kulutta Pentti saa toisen sähköpostin. Siinä kerrotaan, että virustorjunta onnistuttiin suorittamaan virheestä huolimatta ja ettei Pentin tarvitse enää huolehtia asiasta.

Muutamaa viikkoa myöhemmin käy ilmi, että kilpaileva yritys on voittanut tärkeän tarjouskilpailun yllättävän pienellä hintaerolla. Pentin yrityksessä uskottiin, ettei kilpailija pysty tuottamaan palvelua heitä halvemmalla ja tulisi häviämään kilpailun.

Asiaa selvittämään palkattu tietoturva-asiantuntija huomaa toimiston lähiverkon lokitiedoista, että Pentin käyttäjätunnuksella on kirjauduttu Maltalle johtavasta IP-osoitteesta yrityksen verkkoon ja ladattu kaikki tiedostot, mitä Pentin käytössä olevalta verkkolevyltä löytyi.

Yhteisellä verkkolevyllä oli tuoreimpien aineistojen lisäksi myös paljon Pentin työarkistoa. Vahingot hävitystä kilpailusta nousevat lopulta kymmeniin tuhansiin euroihin.



Analyysi ja johtopäätökset

Esimerkkiyritys joutui kohdennetun tietojenkalastelun uhriksi. Tietojenkalastelu (”phishing”) on tietoturvahyökkäys, jossa hyökkääjä erehdyttää uhriaan antamaan tälle käyttäjätunnuksen, salasanan tai muita tärkeitä tietoja. Näiden avulla rikollinen pyrkii murtautumaan uhrin tietojärjestelmään. Kohdennettu tietojenkalastelu (”spear phishing”) käyttää hyväkseen yksityiskohtaisia tietoja uhrista, kuten tämän kotiosoitetta, saadakseen urkinnan näyttämään uskottavammalta.

Kyse on ensisijaisesti hallinnollisen turvallisuuden ongelmasta, sillä ainoa keino torjua tietojenkalastelu on riittävä koulutus sen tunnistamiseksi. Etätyöskentelyä varten tehdyt tekniset suojaukset ovat hyödyttömiä, jos uhri luovuttaa itse kirjautumistunnuksensa hyökkääjälle. Kohdennettu tietojenkalastelu voi olla erittäin uskottavaa, eikä uhri välttämättä huomaa tulleensa huijatuksi eikä tieto tapahtuneesta koskaan tule ilmi.

Henkilöstön on syytä tietää, että henkilökohtaista salasanaa ei saa luovuttaa kenellekään missään olosuhteissa. Tekninen ylläpito voi suorittaa kaikki toimenpiteensä saamatta salasanaa tietoonsa. Ulkoistettujen IT-tukipalveluiden käyttö johtaa siihen, ettei IT-tukihenkilö ole työntekijälle tuttu, joten hyökkääjän on helppo esiintyä tällaisena. Kaikkiin tietokyselyihin pitää suhtautua äärimmäisellä varovaisuudella.

Työntekijät tulee kouluttaa tunnistamaan tietojenkalasteluhyökkäykset ja varmistamaan kaikki epäilyttävät viestit esimerkiksi puhelimitse IT-tukipalveluilta tai omalta esimieheltään. Salasanaa ei tule paljastaa kenellekään missään olosuhteissa. Tietokoneisiin liittyviin tukitoimintoihin on hyvä olla olemassa selkeä prosessi, jotta poikkeukselliset yhteydenotot erottuvat.

Kolme kysymystä sinun yrityksellesi

1.	Onko yrityksesi henkilökunta koulutettu tunnistamaan ja raportoimaan tietojenkalasteluyritykset esimiehelleen tai tietohallinnolle?
2.	Tietävätkö työntekijät, että IT-tuki ei kysy koskaan käyttäjien salasanoja eikä pyydä heitä kirjautumaan puolestaan järjestelmiin?
3.	Onko etätyöhön käytettävä yhteys suojattu esim. VPN-salauksella tai muilla teknisillä ratkaisuilla?

2 Murtovarkaat toimistolla

Insinööritoimisto Mynttinen & Pesonen on perustanut konttorinsa Helsingin Töölöön, katutasoon. Kaverukset ovat löytäneet valoisat tilat vanhasta, kauniista rakennuksesta ja päässeet toteuttamaan omaa sisustussilmäänsä tilojen suunnittelussa. Toimistossa on isot, kauniit ikkunat, jotka antavat pienelle tilalle suuren toimiston tuntua.

Työ sujuu hyvin ja asiakkaita riittää taantumasta huolimatta. Mynttinen ja Pesonen asuvat kumpikin lähistöllä ja nauttivat siitä, että voivat joka päivä kävellä kauniin Helsingin katuja pitkin työpaikalleen.

Toimisto sijaitsee sivukadulla poissa pahimmasta kaupungin melskeestä, jolloin työrauhakin säilyy.

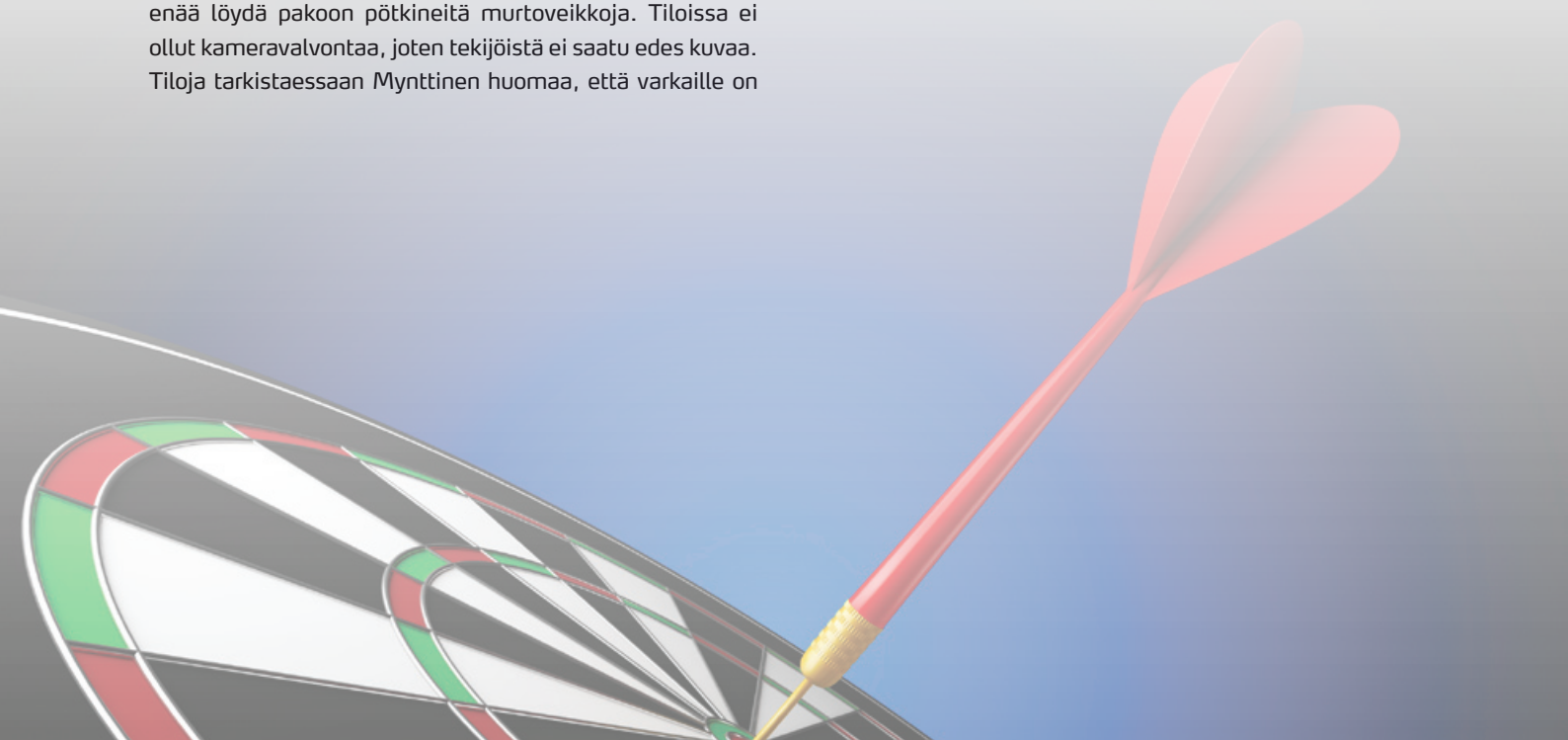
Eräänä yönä Mynttisen puhelin soi ja ruudulla näkyy outo numero. Vartioimisliikkeen hälytyskeskuksen päivystäjä soittaa kertoakseen, että toimistolta on aamuyöstä tullut lasirikkohälytys. Vartija on ehtinyt paikalle viidessätoista minuutissa hälytyksen vastaanottamisesta, mutta oli paikalle saavuttuaan vain todennut ammottavan reiän toimiston etuoven lasissa.

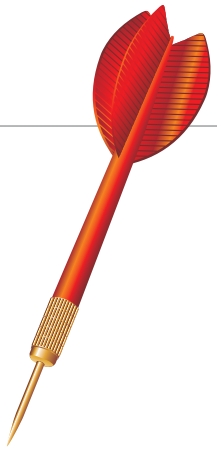
Paikalle kutsutaan poliisi, ja Mynttinen rientää itsekin kotoaan tarkistamaan tuhoja. Poliisi tekee alueella lähietsintöjä mutta ei kuitenkaan hyvistä yrityksistä huolimatta enää löydä pakoon pötkineitä murtoveikkoja. Tiloissa ei ollut kameravalvontaa, joten tekijöistä ei saatu edes kuvaa. Tiloja tarkistaessaan Mynttinen huomaa, että varkaille on kelvannut ainakin uusi videotykki, kahvihuoneen kolikkopurkki, Mynttisen pöydällä ollut avonainen tupakka-aski, pöydällä lojunut ulkoinen kovalevy sekä kaksi kannettavaa tietokonetta Mynttisen ja Pesosen työpöydiltä. Tietokoneilla oli Mynttisen ja Pesosen työtiedostoja, perheen valokuvia, sähköpostikirjeenvaihtoa kolmen vuoden ajalta ja iso liuta Mynttisen omia, henkilökohtaisia tiedostoja.

Ajantasaisia varmuuskopioitakaan ei ollut olemassa, koska varmuuskopiointia tehtiin epäsäännöllisesti ulkoiselle levylle, jota säilytettiin toimistolla. Senkin varkaat veivät. Osa tiedostoista oli tallessa sähköpostissa ja Mynttisen entisellä koneella, osa taas katosi pysyvästi varkaiden matkaan.

Mynttinen palaa kotiin pää painuksissa ja kaivaa komerosta vanhan tietokoneensa. Aamulla olisi edessä soitto asiakkaalle, että ensi viikoksi sovittua suunnittelupalaveria olisi lykättävä ja projekti myöhästyisi.

Mynttisellä oli edessään monta unetonta yötä kun jo kertaalleen tehdyt työt piti aloittaa alusta. Lisäksi Mynttistä vaivasi tietokoneella olevat intiimit valokuvat, joita he olivat vaimonsa kanssa ottaneet muutaman viinilasillisen jälkeen. Etteivät nyt vaan päätyisi internetiin...





Analyysi ja johtopäätökset

Yritys joutui aivan tavallisen liikemurron uhriksi. Vaikutukset kohdistuivat ensisijaisesti omaisuuteen, mutta omaisuuden mukana varastettiin myös arvokasta tietoaineistoa. Toimiston murtosuojaus oli puutteellinen ja sen lisäksi isoista ikkunoista oli selkeästi nähtävillä arvokasta, varkaita houkuttavaa omaisuutta.

Kyseessä on ensisijaisesti fyysiseen turvallisuuteen liittyvä ongelma. Toimistotilat sijaitsivat katutasossa ja niihin pääsi sisälle ikkunan rikkomalla. Syrjäinen sijainti sivukadulla antoi varkaille työrauhan. Arvokas omaisuus oli helposti ja nopeasti anastettavissa, eikä hälytinkään pelottanut vikkeliä varkaita.

Liiketilojen murtosuojauksessa tulee huomioida omaisuuden menetyksen lisäksi myös tiedon menetyksen mahdollisuus. Tärkeä tieto on kahdennettava myös sen varalta, että tietoa sisällään pitävät laitteet varastetaan tai tuhotaan. Paikallinen verkkotallennuslevy voidaan sijoittaa sellaiseen paikkaan, josta sitä ei ulkopuolinen helposti löydä.

Näkyvyys katutason liiketiloihin on hyvä rajata esimerkiksi verhoilla tai vaihtoehtoisesti maitokalvoilla, jolloin valo pääsee sisään. Ikkunoiden murtolujuutta voi lisätä turvakalvoilla tai panssarilasilla. Helposti anastettava arvo-omaisuus on syytä kiinnittää paikalleen tai ainakin nostaa pois näkyvistä, kun tiloissa ei oleskella. Kannettavat tietokoneet tulee suojata siten, ettei tietoja saa auki ilman salasanaa.

Kolme kysymystä sinun yrityksellesi

1.	Onko yrityksesi tiloihin asennettu hälytyslaitteet, valvontakamerat, murtosuojauskalvot tai turvalukot?
2.	Onko yrityksesi tiloissa säilytettävä omaisuus kiinnitetty rakenteisiin ja mahdollisuuksien mukaan poissa ulkopuolisten silmistä?
3.	Onko yrityksessäsi tietoa, joka menetetään, jos yksittäinen tietokone varastetaan tai tuhoutuu?

3 Vakoilija sähköpostilaatikossa

Tuomas työskentelee toimitusjohtajana pienessä yrityksessä, joka tuottaa ja suunnittelee pienyritysten toimistokalusteratkaisuja. Tuomas on perustanut yrityksen osakeyhtiönä lapsuudenystävänsä Henrin ja tämän vaimon Riitan kanssa. Yrityksessä on kolmikon lisäksi kuusi vakituista työntekijää, jotka tekevät pääsääntöisesti myyntityötä.

Tuomaksen ja yhtiökumppaneiden välit ovat viime aikoina kuitenkin kiristyneet bisnestä koskevien erimielisyyksien takia. Tämän lisäksi Henri epäilee, että Tuomaksella on silmäpeliä Riitan kanssa.

Riidat eivät ratkea, joten kolmikko sopii yhdessä, että Henri ja Riitta ostavat Tuomaksen ulos yrityksestä lunastamalla Tuomaksen osakkeet. Osakekauppa sujuu ongelmitta ja Tuomas vaihtaa maisemaa.

Tuomas saa työpaikan kilpailevasta yrityksestä ja etenee nopeasti esimiesasemaan. Kiireessään päästä Tuomaksesta eroon ei huomattu laatia kilpailukieltosopimusta, mutta Henri ja Riitta olettavat, ettei Tuomas kuitenkaan kehtaisi käyttää hyväkseen entisen yrityksen asiakastietoja.

Henri ja Riitta huomaavat kuitenkin pian, että asiakkaita alkaa kadota Tuomaksen uudelle työnantajayritykselle. Tuomas tuntuu olevan muutenkin yllättävän hyvin perillä siitä, mitä Henrin ja Riitan yrityksessä tapahtuu.

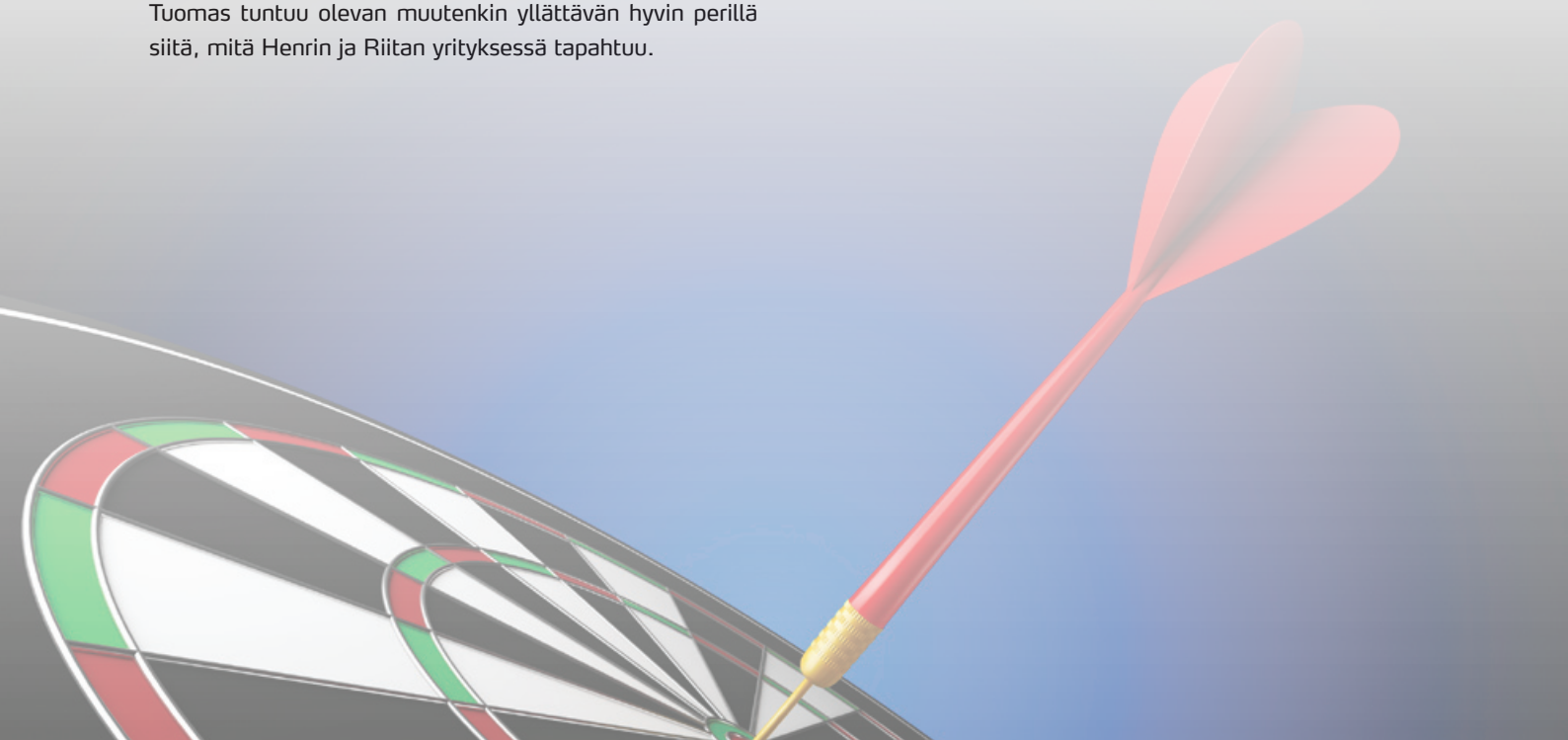
Eräänä päivänä yrityksen asiakaspalvelun sähköpostilaatikosta katoaa viestejä, ja Riitan epäilykset heräävät. Lähtiessään Tuomas oli vienyt töissä käyttämänsä tietokoneen mukanaan, sillä se oli hänen omansa. Lukeeko Tuomas vielä yrityksen sähköposteja?

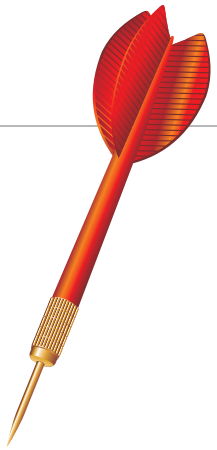
Asiasta tehdään rikosilmoitus. Rikostutkinnassa selviää, että Tuomas on tosiaankin lukenut edelleen kaikki viestit, joita yrityksen sähköpostilaatikkoon tulee. Ollessaan vielä perustamassaan yrityksessä töissä Tuomas oli vastuussa työntekijöiden sähköpostilaatikoiden luomisesta – ja niiden salasanoista.

Tuomaksen lähdettyä Henri vaihtoi asiakaspalvelun sähköpostin salasanan. Hän informoi työntekijöitä uudesta salasanasta – lähettämällä sen sähköpostilla. Tuomas sai tämän uuden salasanan tietoonsa erään asiakaspalvelijan sähköpostista.

Salasanoja ei siis vaihdettu turvallisesti, joten Tuomas oli pystynyt seuraamaan entisen työnantajansa sähköposteja monen kuukauden ajan.

Tuomas jäi kiinni vasta poistettuaan vahingossa viestejä laatikosta, jolloin rikos huomattiin.





Analyysi ja johtopäätökset

Entinen työntekijä sai viedä mukanaan työkäytössä olleen tietokoneen ilman, että sen sisältö tuhottiin. Kaikkia hänen luomiaan salasanoja ei vaihdettu. Sähköpostin uudet salasanat ilmoitettiin samaan sähköpostiin, jota entinen työntekijä pääsi yhä seuraamaan. Työntekijät laiminlöivät ohjeen, jossa heitä kehotettiin vaihtamaan salasana henkilökohtaiseksi.

Kyseessä on niin henkilöstöturvallisuuden kuin tietoaineistoturvallisuudenkin ongelma. Yrityksellä ei ollut olemassa ohjeistusta siitä, miten salasanoja hallitaan ja miten poistuvien työntekijöiden pääsy yrityksen tileille estetään. Asiakaspalvelusähköpostiin pystyi kirjautumaan internetistä eikä kirjautumislokeja seurattu.

Salasanojen luomisen jälkeen jokaisen käyttäjän on vaihdettava ne yksilöllisiin, vain itse tietämiinsä salasanoihin. Uudet salasanat yhteisiin sovelluksiin pitää jakaa sellaisella tavalla, etteivät ne leviä muiden tietoon. Tällaiset salasanat voidaan kirjata esimerkiksi muistioon, jota säilytetään kassakaapissa.

Yrityksen tulee laatia selkeät ohjeet siitä, miten tietoaineistojen turvallisuus varmistetaan irtisanoutumistilanteessa. Vanhat tilit tulee poistaa käytöstä siten, että niillä olevat yrityksen tiedot saadaan haltuun. Omien laitteiden käyttöä työpaikalla tulee rajoittaa, eikä niitä saa käyttää työhön liittyvän materiaalin tallentamiseen.

Kolme kysymystä sinun yrityksellesi

1. Onko yrityksellläsi selkeät, kirjalliset ohjeet käyttäjien ja ylläpitäjien salasanojen hallitsemiselle?
2. Onko yrityksellläsi kirjallinen toimintasuunnitelma niin aloittavien kuin poistuvienkin työntekijöiden varalta?
3. Vaihdetaanko toiminnan kannalta keskeisten tietojärjestelmien salasanat määräajoin?

4 Potilastiedot verkossa

Sakari perustaa kotisairaanhoitopalveluita tarjoavan yrityksen yhdessä sairaanhoitajavaimonsa kanssa. Sakari on pitkän linjan yrittäjä ja kaipaa elämäänsä uusia haasteita.

Uuden yrityksen liiketoiminta lähtee kasvamaan nopeasti ja pian yrityksellä onkin 34 työntekijää. Sakari on tyytyväinen. Suurin osa asiakkaista tulee yritykselle kaupungin sosiaalitoimen kautta, ja maksu hoidetaan maksusitoumuksen avulla.

Sakari vie eräänä päivänä kotiin vanhan kannettavan tietokoneensa, jota hän on käyttänyt töissään. Hän kuitenkin haluaa käyttöönsä uudemman mallin ja antaa vanhan tietokoneensa 12-vuotiaalle pojalleen. Poika on kiinnostunut tietokoneista, ja Sakari katsookin tyytyväisenä poikansa harrastusta. Ehkä poika joskus työllistyisi arvostetulle IT-alalle.

Poika formatoi tietokoneen kovalevyn ja asentaa siihen uuden käyttöjärjestelmän. Sakari palauttaa varmuuskopioista uudelle tietokoneelleen vanhat työtiedostonsa, jotka on asianmukaisesti varmuuskopioitu toimiston verkkolevylle.

Eräänä päivänä poika tulee kuitenkin itku silmässä kotiin ja kertoo hukanneensa uuden tietokoneensa. Poika oli jättänyt tietokoneen koulussa käytävälle reppuun, josta se oli oppitunnin aikana varastettu. Sakari lohduttelee poikaansa, ja myöhemmin samana päivänä he käyvät ostamassa pojalle uuden koneen kadonneen tilalle.

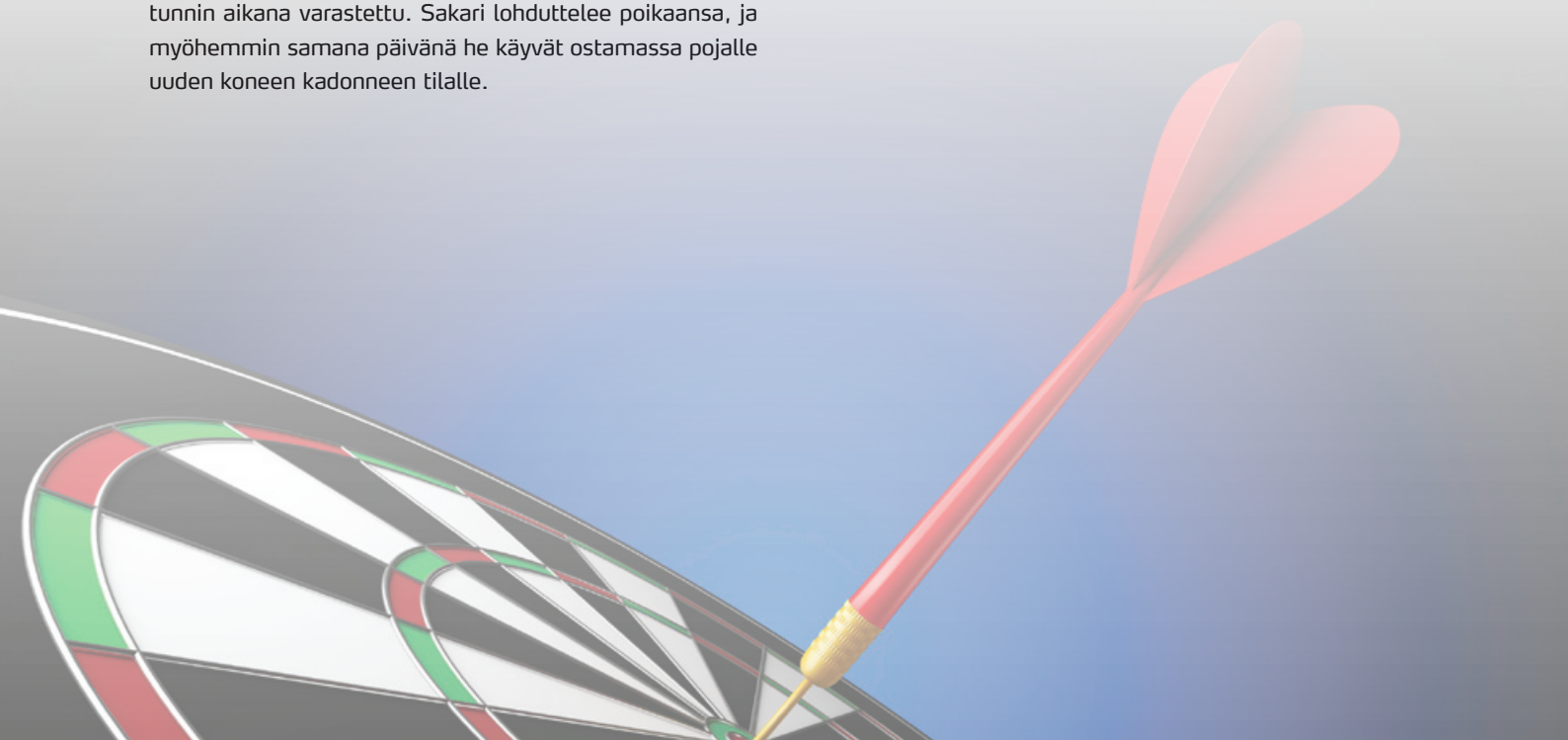
Muutaman viikon päästä poliisista otetaan yhteyttä Sakariin kuulustelukutsun merkeissä. Asema on ”rikoksesta epäilty”. Sakari on hämmentynyt, mistä häntä nyt epäillään?

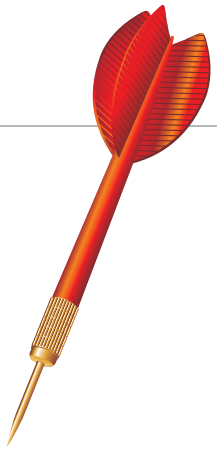
Kuulusteluissa poliisi kertoo löytäneensä internetistä listan sadoista potilaista, joiden kaikkien yhteinen nimittäjä on se, että he olivat Sakarin asiakkaita. Listalla oli potilaiden yksityisiä terveystietoja - kaikki taudinkuvauksista henkilötunnuksiin ja osoitteisiin asti. Tiedoilla oli tehty jo muun muassa petoksia ja otettu pikavippejä potilaiden nimiin. Sakaria epäillään ainakin henkilörekisteririkoksesta.

Myöhemmin selviää, että koulutoveri oli varastanut tietokoneen pojan laukusta. Hän oli myynyt koneen verkossa eteenpäin muutamalla kympillä.

Tietokoneen ostanut rikollinen oli kokeillut ilmaiseksi saatavia tiedonpalautustyökaluja ja huomannut, että koneen kovalevy oli tyhjennetty puutteellisesti. Suurin osa tiedostoista oli vielä palautettavissa. Näin rikollisen käsiin päätyi henkilörekisterin tunnusmerkit täyttäviä potilastietoja, jotka levisivät internetiin. Teon motiivi jäi epäselväksi.

Sakarin huolimaton toiminta johti siihen, että sosiaalitoimi purki yrityksen kanssa solmimansa sopimuksen ja yritystoiminta kärsi valtavan tappion.





Analyysi ja johtopäätökset

Yrityksessä oli laiminlyöty henkilötietojen käsittelyyn liittyvä huolellisuus. Käytettävien laitteiden elinkaarta ei ollut ajateltu yrityksen tarpeita pidemmälle, eikä tietojen turvallisen poistamisen merkitystä ollut ymmärretty. Yrittäjä oli myös siinä uskossa, että formatointi tyhjentää levyn niin, ettei tietoja voi enää palauttaa.

Kyseessä on tietoaineistoturvallisuuden ongelma. Tietokoneella olevat tiedostot eivät poistu levyn formatoinnin yhteydessä, vaan tallennusväline pitää joko päällekirjoittaa tai tuhota lukukelvottomaksi. Kaikki laitteet, joilla arkaluontoista tietoa käsitellään, pitää poistaa käytöstä tietoturvallisilla menetelmillä.

Laitteet, joilla käsitellään arkaluontoisia tietoja, tulee merkitä selkeästi ja niitä ei pidä tarpeettomasti kuljettaa yrityksen tiloista pois. Laitteiden jälleenmyynti-, kierrätys- tai edelleenluovutustilanteissa tallennusmediat tulee poistaa ja tuhota tai ylikirjoittaa. Sama koskee ulkoisia tallennusvälineitä, kuten USB-tikkuja tai irtokovalevyjä. Myös kopiokoneet tallentavat usein kopioitavia dokumentteja kovalevyilleen.

Käsiteltävät tiedot on syytä luokitella esimerkiksi neljään eri luokkaan julkisiksi, sisäisiksi, luottamuksellisiksi ja salaisiksi. Tietojen käsittelyohjeissa on otettava huomioon tietojen koko elinkaari niiden luomisesta niiden tuhoamiseen. Julkisten tietojen poistamisessa ei tarvitse olla erityisen tarkkana, mutta salaisten tiedostojen poistaminen edellyttää huolellisuutta ja tietoturvallisia toimintatapoja.

Kolme kysymystä sinun yrityksellesi

1. Onko tallennusvälineistänne laadittu elinkaarisuunnitelma, joka ottaa huomioon välineille tallennetun aineiston turvallisen hävittämisen?

2. Onko salassa pidettävät tiedot selkeästi erotettu julkisista tai sisäisistä tiedoista, joiden erityinen suojaaminen ei ole tarpeen?

3. Jos yrityksessäsi käsitellään henkilötietoja, onko niistä muodostuvasta henkilörekisteristä laadittu rekisteriseloste?

5 Päivittämättömät laitteet

Automaatiosuunnittelualan yritys on toiminut kohta vuosikymmenen toimitusjohtaja Matin ja uskollisen miehistön voimin. Yritys tekee tasaisen varmaa tulosta, ja työtä tuntuu tulevan samaa tahtia kuin sitä saadaan valmiiksi. Yrityksen operaatiot toimivat rutiinilla, ja muutamista yritystoimintaa uhkaavista riskeistä on toivuttu hyvän jatkuvuussuunnittelun ja sinnikkään yritysjohdon ansiosta.

Yrityksen perustamisvaiheessa hankittiin koneellista piirtämistä varten tietokoneita, jotka korvasivat käsin tehtävän suunnittelutyön. Työntekijätkin olivat saaneet koulutuksen ohjelmistoon ja työ sujui hyvin.

Työasemiin kului rahaa, mutta suurin investointi oli ohjelmiston lisenssi, joka maksoi 15 000 euroa ja sisälsi viiden vuoden ylläpitosopimuksen.

Ylläpitosopimuksen päätyttyä ohjelmistoyhtiö ilmoitti, että yrityksen käyttämää ohjelmistoversiota ei enää jatkossa tueta, sillä se perustuu vanhaan ohjelmistoarkkitehtuuriin.

Matille tarjottiin siirtymistä uuteen ohjelmistoon, mutta tämä olisi edellyttänyt myös kalliita laite- ja käyttöjärjestelmäpäivityksiä. Tällöin Matti katsoi, että työt sujuvat vanhallakin ohjelmistolla, joten päivitykseen ei ollut tarvetta.

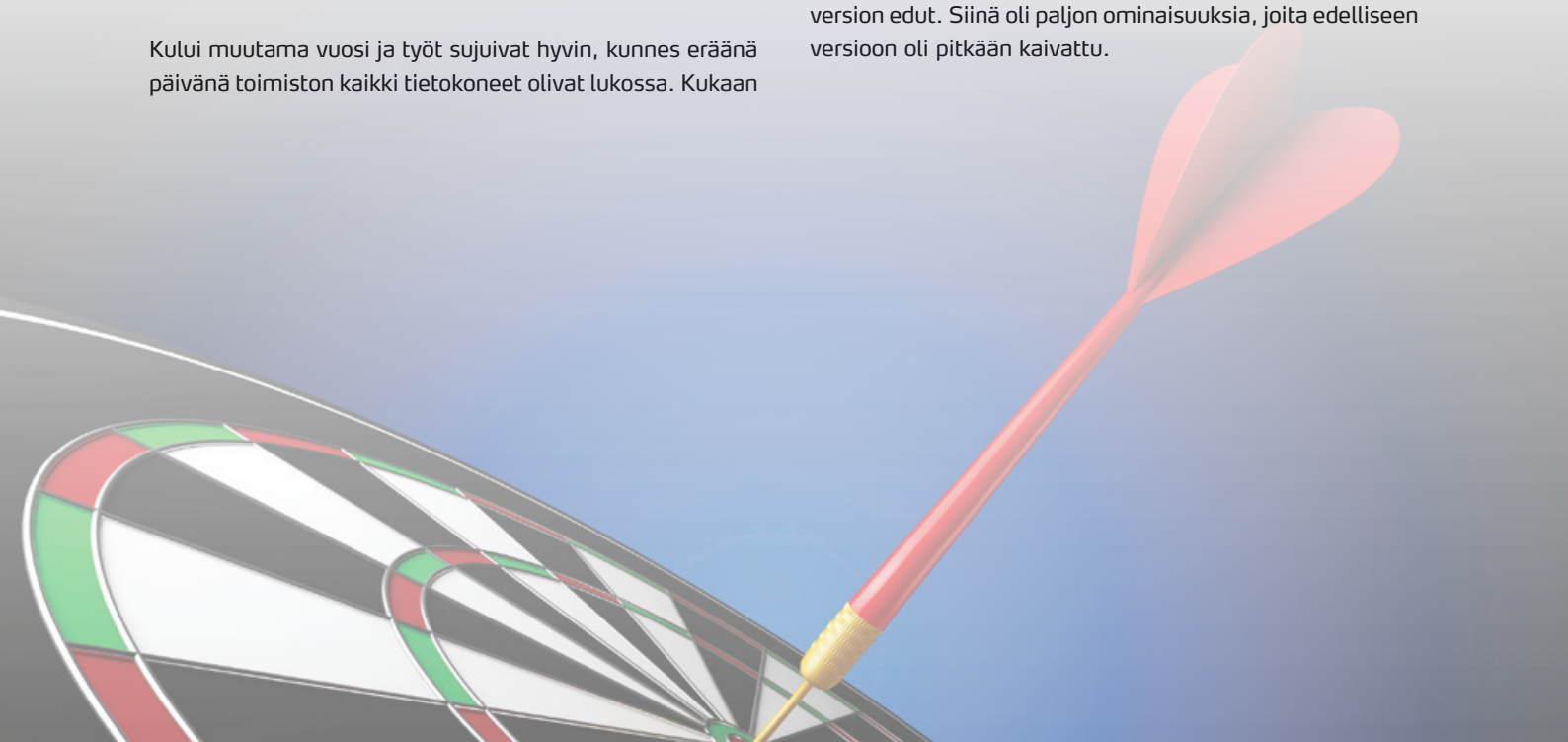
Kului muutama vuosi ja työt sujuivat hyvin, kunnes eräänä päivänä toimiston kaikki tietokoneet olivat lukossa. Kukaan toimistolla ei saanut yhtäkään konetta auki, ja mystiset virheilmoitukset eivät auttaneet asiassa laisinkaan.

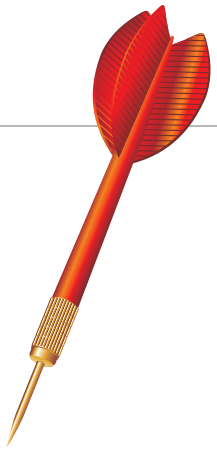
Matin yritys kääntyi tietoturva-asiantuntijapalveluita tarjoavan yrityksen puoleen, ja yritykseltä tuli paikan päälle asiantuntija tarkistamaan tilanteen.

Ongelman syyksi ilmeni se, että vanhoihin ohjelmistoihin ei enää ollut julkaistu tietoturvahaavoittuvuuksia korjaavia päivityksiä. Eräs yrityksen työntekijä oli saanut verkkosivuilta koneelleen viruksen, joka levisi koko sisäverkossa kaikkiin koneisiin. Suunnitteluohjelman sisäinen tietoliikenneprotokolla oli avannut lähiverkosta ulkoverkkoon reitin, jota pitkin virus pääsi koneeseen. Ohjelma tarvitsi tätä reittiä tiedonsiirtoon muiden koneiden kanssa, mutta siitä hiljattain löydetty haavoittuvuus oli jäänyt paikkaamatta toimittajan siirryttyä tukemaan uutta versiota.

Virus lukitsi koneet ja pyyhki niiltä järjestelmätiedostoja. Matin ei auttanut muu kuin sammuttaa kaikki laitteet ja lähettää ne huoltoon. Samalla oli marssittava tietokoneliikkeeseen hankkimaan uusia laitteita ja ohjelmistolisenssiä.

Uusien laitteiden asennuksen ajan työt seisoivat ja työtiedostojen palauttaminen varmuuskopioilta vei kaksi viikkoa. Uusien laitteiden myötä huomattiin myös uuden ohjelmistoversion edut. Siinä oli paljon ominaisuuksia, joita edelliseen versioon oli pitkään kaivattu.





Analyysi ja johtopäätökset

Yrityksessä laiminlyötiin ajantasaisten ohjelmistojen käyttäminen ja uskottiin vanhojen olevan käyttökelpoisia vielä pitkään. Vanhoista ohjelmistoista löytyy usein tietoturva-aukkoja, eikä ohjelmistontoimittajilla ole usein resursseja tai halua paikata vanhoja versioita samalla tarkkuudella kuin uusia. Tämä altistaa vanhat ohjelmat haavoittuvuuksille ja väärinkäytöksille.

Kyseessä on ohjelmistoturvallisuuden ongelma. Yrityksen olisi pitänyt laatia ohjelmistoille päivityssuunnitelma ja uusia laitteistonsa ajantasaiseksi hallitusti. Nettisurffaamisen rajoitukset pitää suunnitella työtehtävien ja suojattavan datan mukaan. Sellaisia koneita ei tule kytkeä verkkoon lainkaan, jotka sisältävät erityisen suojattavaa tietoa. Verkon turvallisuuteen liittyvät ohjelmat, kuten tietokoneiden käyttöjärjestelmät, verkkoselaimet, niiden liitännäiset ja virustorjunta on pidettävä ajan tasalla.

Ohjelmistojen toimittajien kanssa on käytävä läpi uusien ja vanhojen versioiden erot ja laadittava suunnitelma isommille versiopäivityksille. Lisenssienhallintaan liittyy myös riittävien ylläpito- ja tukipalveluiden hankkiminen. Tukipalvelut huolehtivat päivitysten jakelemisesta ohjelmistojen loppukäyttäjille.

Tietotekniset laitteet eivät ole ikuisia. Sama koskee myös ohjelmistoja. Niiden elinkaari mitataan muutamissa vuosissa. Erityisesti raskaat teollisuusohjelmistot edellyttävät tietokoneilta paljon tehoa, ja investoimalla riittäviin ja ajantasaisiin työkaluihin myös työn tulokset – ja turvallisuus – pysyvät laadukkaina.

Kolme kysymystä sinun yrityksellesi

1. Onko toimintanne kannalta olennaisten laitteiden ohjelmisto- ja laitetuki sovittu palveluntuottajan kanssa?
2. Onko yrityksessänne sovittu pelisäännöt sille, miten vapaasti työkoneilla saa surfata netissä?
3. Ovatko laitteidenne turvallisuusohjelmistot ja -asetukset ajantasaisia?

6 Suunnittelijan laiterikko

Sani on perustanut yrityksen, joka tuo maahan ja tuottaa omaan mallistoonsa laukkuja, kodintekstiilejä, sisustus- ja muotituotteita. Tavaraa on sekä omasta mallistosta että tunnettujen ulkomaalaisten tuottajien luetteloista.

Sani on aloittanut liiketoiminnan kotoaan ompeluhuoneestaan sivutoimena, mutta yrittäjän ahkeruuden ja lahjakkuuden ansiosta liiketoiminta on kasvanut joka vuosi huimasti. Pian Sani siirtyy toimistotiloihin Helsingin keskustaan ja palkkaa avukseen varastonhoitajan, toisen suunnittelijan sekä myyntimiehen. Liiketoiminnan keskipiste siirtyy omaan mallistoon, joka myy hyvin ja saa kehuja maailmalla.

Sani tekee suunnittelutyön pääasiassa omalla tietokoneellaan ja käyttää paljon sähköpostia sekä sosiaalista mediaa viestintään.

Yrityksen menestyessä sähköistä materiaalia alkaa kertyä niin paljon, että sen jakaminen työntekijöiden kesken käy vaivalloiseksi. Sani käy ostamassa elektroniikkaliikkeestä ulkoisen kovalevyn, jonka saa kytkettyä yrityksen lähiverkkoon. Hän vertailee hintoja ja päätyy noin 200 euron hintaiseen laitteeseen.

Sanin ystävä käy asentamassa kovalevyn ja verkottaa työntekijöiden tietokoneet niin, että kaikilla on omilta tietokoneiltaan pääsy uudelle verkkolevylle. Nyt kaikki tieto saadaan kätevästi jaettua toimiston väen kesken ja työ sujuu helpommin.

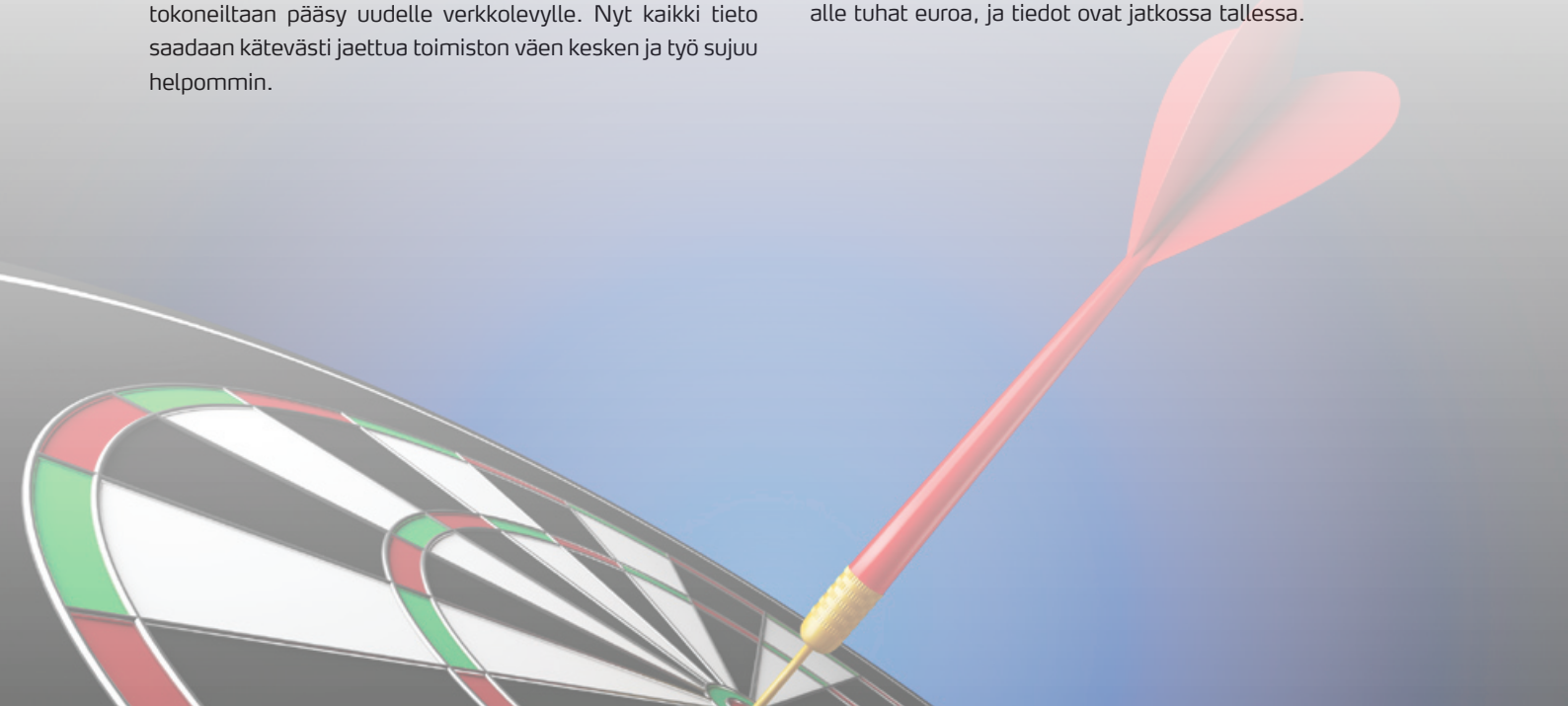
Eräänä aamuna Sani saapuu työpaikalleen ja käynnistää tietokoneensa. Verkkolevy-yhteys ei kuitenkaan käynnisty, eikä hän saa avattua uuden käsilaukkumalliston suunnittelutiedostoja. Kukaan toimistolla ei osaa korjata levyjärjestelmää, joten Sani soittaa ystävälleen, joka tulee tarkistamaan sen toiminnan.

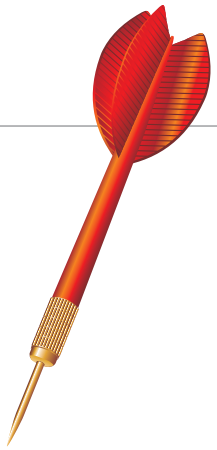
Ystävän tarkistaessa levyä käy ilmi, että yöllä raivonnut ukkosmyrsky on antanut sähköverkon ylitse jännitepiikin, joka on tuhonnut ulkoisen kovalevyn täysin. Tietojen palauttaminen edellyttäisi kovalevyn lähettämistä asiantuntijayritykselle. Korjausarvio liikkuu tuhansissa euroissa, mikäli tiedot on ylipäänsä mahdollista palauttaa.

Kylmä hiki kohoaa Sanin otsalle, kun hän muistaa, että uuden malliston suunnittelutiedostot ovat vain verkkolevyllä. Omalla koneellaan hän ei niitä säilytä, sillä hän pelkää, että kone varastetaan.

Sani joutuu aloittamaan kuukausia hiomansa työn alusta. Samalla hän menettää entisten projektiensa tiedostot, tärkeitä yhteystietoja sekä muita tiedostoja, joita levylle oli tallennettu.

Sani ottaa yhteyttä asiantuntijaan, joka suosittelee Sanille varmuuskopioivaa verkkotallennuslevyä sekä pilvipalvelua, johon tiedot varmistetaan automaattisesti. Ratkaisu maksaa alle tuhat euroa, ja tiedot ovat jatkossa tallessa.





Analyysi ja johtopäätökset

Kovalevyn vaurioituminen on tietoturvallisuuden kannalta ongelma. Levylle taltioitu tieto on fyysisesti levyn pinnalla, jolloin sen vaurioituminen on realistinen tietoturvauhka. Pahimmassa tapauksessa tietojen menetys voi johtaa liiketoiminnan loppumiseen. Tiedonpalautus hajonneilta levyiltä ei aina onnistu, ja onnistuessaankin se on kallista.

Kyseessä on sekä fyysisen turvallisuuden että laitteistoturvallisuuden ongelma. Fyysinen turvallisuus voidaan varmistaa suojaamalla yritystoiminnan kannalta kriittiset laitteet ulkoisilta häiriöiltä esimerkiksi vikavirtasuojalla tai virransyöttöä tasaavalla varavirtalaitteella. Myös tulipalon ja vesivahingon varalta on tehtävä riittäviä suojausjärjestelyitä. Tietoaineistoturvallisuus voidaan varmistaa varautumalla laitteiden vioittumiseen varmuuskopioimalla tärkeät tiedot. Vikasietoiset laitteet ovat kalliimpia, mutta halvempia kuin vahingosta aiheutuvat kulut.

Kaikki yrityksen toiminnan kannalta tärkeä tieto pitää vähintään kahdentaa paikallisesti eri levyille. Lisäksi ne on syytä varmuuskopioida fyysisesti eri paikkaan, esimerkiksi pilvipalveluun tai toiseen rakennukseen. Sähköverkon virranjakelun häiriöiltä voi suojautua käyttämällä siihen suunniteltuja laitteita. Vikasietoisten laitteiden käyttö on käytännössä yhtä helppoa kuin helposti vioittuvienkin.

Tiedontallennusratkaisuja suunniteltaessa kannattaa panostaa siihen, että hankitaan vikasietoisia laitteita ja seurataan aktiivisesti niiden toimintaa. Aloituskustannukset ovat suuremmat, mutta kokonaiskustannukset matalammat. Yrityksen toiminnan kannalta tärkeää tietoa ei saa koskaan säilyttää vain yhdessä paikassa.

Kolme kysymystä sinun yrityksellesi

1. Onko yrityksesi kaikki tärkeä tieto varmuuskopioitu ajantasaisesti?

2. Ovatko tallennus- ja tietojärjestelmänne suojattu sähkönjakeluverkon häiriöiltä?

3. Onko kaikki tieto keskitetty verkkolevylle vai säilytetäänkö työasemilla tärkeitä tietoja?

Lopuksi

Olet nyt läpikäynyt Tikka-kartoitustyökalun. Toivottavasti nämä tosielämään perustuvat esimerkkitapaukset valaisivat, millaisista käytännön asioista tietoturvallisuuden hallinnassa on kyse.

Kyse on ehkä yllättävänkin arkipäiväisistä riskeistä, joiden hallitseminen ei edellytä syvällistä teknistä osaamista. Joidenkin tietoturvallisuuden osa-alueiden kuntoon saattamisessa kannattaa turvautua luotettavan asiantuntijan apuun.

Tärkeintä on kuitenkin saada tietoturvallisuustyö käyntiin – ennen kuin vahinko ehtii tapahtua. Riskien torjuminen on aina parempi vaihtoehto kuin jälkien korjaaminen.

Onnea ja menestystä yrityksesi tietoturvatalkoisiin!

Antti Kurittu

Viestintäviraston Kyberturvallisuuskeskus

Elinkeinoelämän keskusliitto EK

Lisätietoja

Viestintäviraston tietoturvaopas pienyrityksille:
www.tietoturvaopas.fi

Ajantasaista tietoa tietoturvauhista:
www.kyberturvallisuuskeskus.fi

EK:n aineistoja yritysturvallisuudesta:
www.ek.fi/yritysturvallisuus

Tietosuojavaltuutetun ohjeet henkilötietojen käsittelystä:
www.tietosuoja.fi

Valtionvarainministeriön VAHTI-ohjeet kattavaan tietoturvaan:
www.vahtiohje.fi

Kirjoittaja:
© Antti Kurittu 2015
antti.kurittu@gmail.com

Julkaisu internetissä:
www.ek.fi/tikka
Kesäkuu 2015

Ulkoasu: Arja Nyholm, Jumo Oy

Julkaisijat:
Elinkeinoelämän keskusliitto EK
PL 30, (Eteläranta 10), 00131 Helsinki
Puhelin 09 420 20
ek@ek.fi
www.ek.fi
Twitter: @Elinkeinoelama

Viestintävirasto
Kyberturvallisuuskeskus
PL 313, Itämerenkatu 3 A, 00181 Helsinki
www.kyberturvallisuuskeskus.fi
Twitter: @CERTFI

Valokuva: iStock, Deliormanli