ASIANTUNTIJARAPORTTI

AVOIMET OVET

TUTKIMUS OSOITTAA, ETTÄ TOIMISTOLAITTEET JÄTETÄÄN USEIN ALTTIIKSI KYBERHYÖKKÄYKSILLE

Yritysten verkkotulostimien ja monitoimilaitteiden tietoturvassa on puutteita IT-tiimien keskittyessä muihin päätelaitteisiin

Toimistolaitteet ovat helppoja maalitauluja: Verkkoon liitettyjen ulostimien ja monitoimilaitteiden käyttörajoitukset ja lukituskäytännöt ovat usein puutteellisia.

Uhka on kuitenkin todellinen, eikä sitä tule jättää huomiotta. Suuryritysten käyttämät tulostimet ja monitoimilaitteet ovat nykyään tehokkaita verkkoon liitettyjä laitteita, jotka ovat alttiita samoille uhkille kuin verkon muut päätelaitteet. Nämä yleensä suojaamattomat kohteet ovat alttiita kyberhyökkäyksille. Niiden kautta voidaan myös päästä yrityksen sisäisiin ja taloudellisiin tietoihin, millä voi olla vakavia seurauksia yrityksen liiketoiminnalle.

Spiceworksin hiljattain suorittamassa kyselyssä havaittiin, että yli 300:sta IT-alan päätöksentekijästä vain 16 % pitää toimistolaitteita korkeana tietoturvariskinä. Luku on merkittävästi pienempi kuin työasemien, kannettavien tietokoneiden ja mobiililaitteiden kohdalla.[1] Tämä näkemys heikentää tapaa, jolla IT-henkilöstö lähestyy verkon tietoturvaa. Vaikka lähes kahdella kolmasosalla yrityksistä on verkkotulostimia ja monitoimilaitteita koskevat suojauskäytännöt, tämä prosenttiluku on huomattavasti pienempi kuin muilla verkon päätelaitteilla. Se altistaa laitteet hyökkäyksille, vaikka niiden suojaamista varten on saatavilla helppoja ratkaisuja.

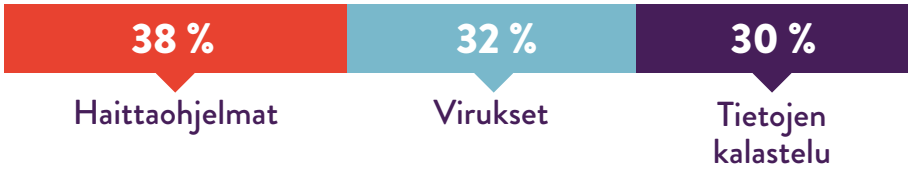
Tämä asiantuntijaraportti tarjoaa Spiceworksin toteuttaman kyselyn perusteella saatua tietoa toimistolaitteiden tietoturvasta, tietoturvarikkomusten vaikutuksista sekä nykyaikaisten verkkotulostimien ja monitoimilaitteiden sisäänrakennetuista suojausominaisuuksista.

VAIN 16 % VASTAAJISTA PITI TOIMISTOLAITTEITA MERKITTÄVÄNÄ TIETOTURVAUHKANA.[1]

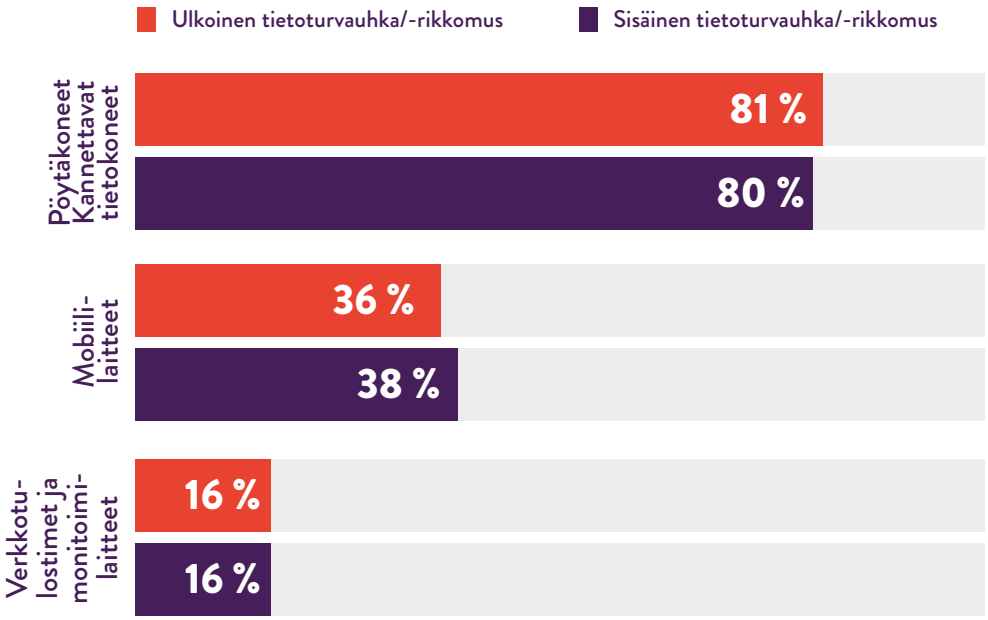
AVOIN OVI HYÖKKÄYKSILLE

Spiceworksin suorittamassa kyselyssä 74 % vastaajista (netto) sanoi organisaationsa joutuneen jonkinlaisen ulkoisen tietoturvauhkan tai -rikkomuksen kohteeksi viime vuoden aikana. 70 % vastaajista (netto) ilmoitti kokeneensa organisaation sisäisen tietoturvauhkan tai -rikkomuksen. Ne johtuivat yleensä käyttäjän virheestä, omien laitteiden käyttämisestä työtehtäviin tai työntekijöiden kotiverkkojen tai julkisten verkkojen käyttämisestä työtehtäviin.[1]

IT-AMMATTILAISTEN YLEISIMMIN KOHTAAMAT TIETOTURVAUHKAT/-RIKKOMUKSET



Yleisimmät uhkat aiheutuivat pääasiassa pöytätietokoneiden ja kannettavien tietokoneiden kautta, ja muut puolestaan mobiililaitteiden sekä verkkotulostimien ja monitoimilaitteiden kautta.[1] (16 % uhkista aiheutui verkkotulostimien ja monitoimilaitteiden kautta, mikä on merkittävästi enemmän kuin vuonna 2014, jolloin Spiceworksin vastaavassa tutkimuksessa lukema oli 4 %.) On myös mahdollista, että toimistolaitteisiin kohdistuvien hyökkäysten määrää on aliarvioitu, sillä verkkotulostimia ja monitoimilaitteita ei valvota yhtä tarkasti kuin tietokoneita ja mobiililaitteita.



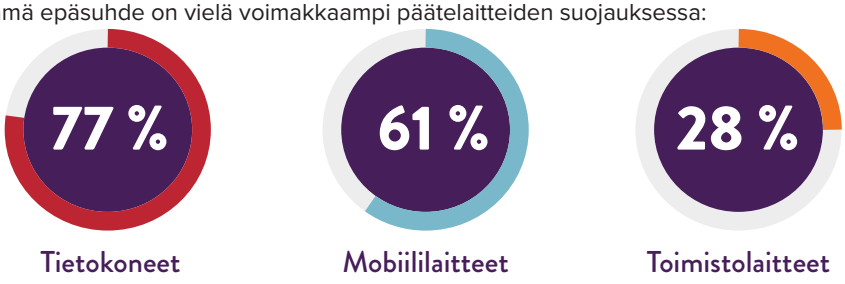
TOIMISTOLAITTEET JÄÄVÄT USEIN HUOMIOTTA

Spiceworksin suorittaman kyselyn perusteella voidaan todeta, että verkkotulostimien ja monitoimilaitteiden tietoturvaa ei usein ajatella riittävästi.

Organisaatiot tietävät hyvin, kuinka tärkeää verkon, päätelaitteiden ja tietojen suojaus on. Yli kaksi kolmasosaa kyselyn vastaajista ilmoittikin käyttävänsä verkon suojausta, pääsynvalvontaa/-hallintaa, tietojen suojausta tai päätelaitteiden suojausta – tai niiden yhdistelmiä.[1]

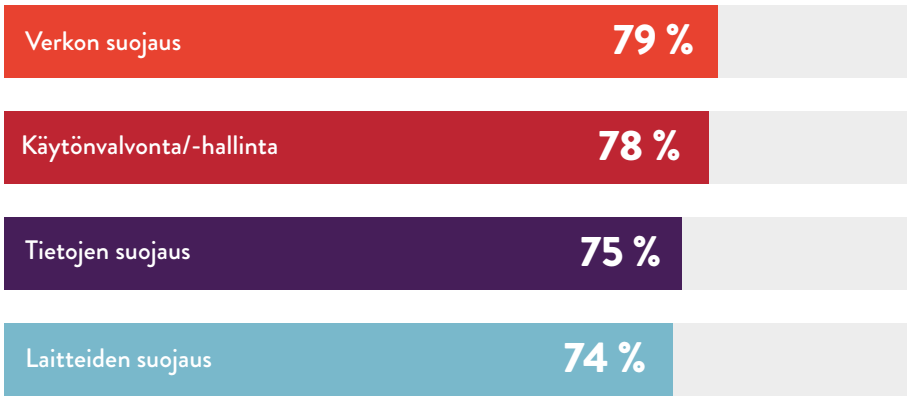
Näitä ratkaisuja käytetään kuitenkin paljon harvemmin verkkotulostimien ja monitoimilaitteiden kanssa. 83 % vastaajista ilmoitti käyttävänsä verkon suojausta pöytätietokoneissa ja kannettavissa tietokoneissa, 55 % mobiililaitteissa, ja vain 41 % tulostimissa ja monitoimilaitteissa.[1]

Tämä epäsuhde on vielä voimakkaampi päätelaitteiden suojauksessa:



alle yksi kolmasosa (28 %) vastaajista ilmoitti käyttävänsä verkkotulostimien ja toimistolaitteiden tietoturvasertifikaatteja – tietokoneiden osalta vastaava luku oli 79 % ja mobiililaitteiden osalta 54 %.[1]

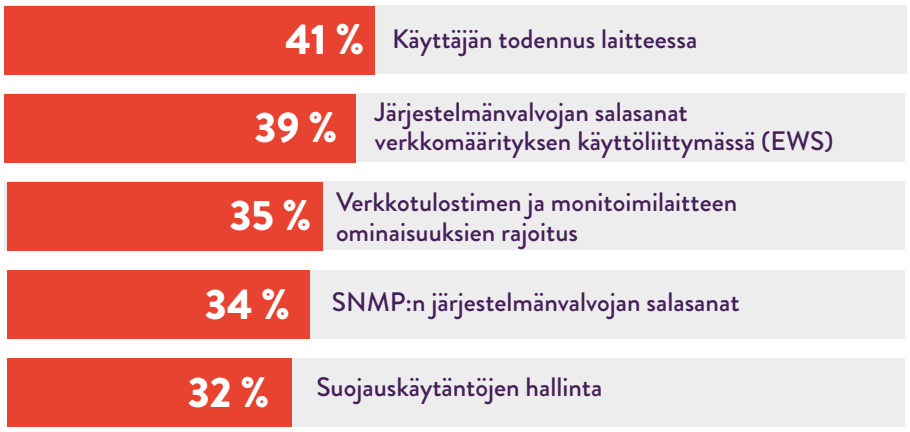
YLEISIMMÄT PÄÄTELAITTEIDEN SUOJAUSKÄYTÄNNÖT



Yleisistä päätelaitteiden suojaustavoista suosituimpia verkkotulostimien ja monitoimilaitteiden osalta olivat asiakirjojen suojaus, verkon suojaus ja pääsynvalvonta, mutta vain alle puolet vastaajista ilmoitti organisaationsa käyttävän näitä suojaustapoja toimistolaitteissaan.[1]

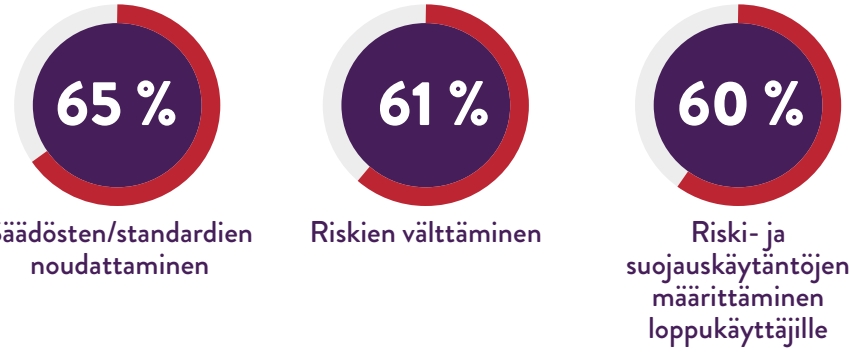
Joillakin yrityksillä on verkkotulostin- ja monitoimilaitekohtaisia suojauskäytäntöjä, mutta niissäkin on huomattavia eroja. Vain hieman yli 40 % organisaatioista ilmoitti käyttävänsä käyttäjien todennusta, ja alle 40 % ilmoitti käyttävänsä järjestelmänvalvojan salasanoja verkkomäärityksen käyttöliittymässä.[1] Tehokkaan suojauksen saavuttamiseksi organisaatioiden tulisi käyttää kaikkia näitä tapoja – ja lisäksi vielä muitakin.

YLEISIMMÄT TOIMISTOLAITEKOHTAISET SUOJAUSKÄYTÄNNÖT



Päätelaitteiden vaatimustenmukaisuus- ja tarkastuskäytäntöjen osalta verkkotulostimien ja monitoimilaitteiden tietoturva on heikommalla tasolla lähes kaikkiin muihin päätelaitteisiin verrattuna. Lähes 90 % organisaatioista käyttää suojauskäytäntöjä, mutta ne eivät yleensä kata toimistolaitteita. Esimerkiksi 57 % vastaajista ilmoitti käyttävänsä tietokoneissa haittaohjelmien torjuntaratkaisuja, mutta vain 17 % käyttää niitä verkkotulostimissa ja monitoimilaitteissa.[1]

LÄHES 90 % IT-AMMATTILAISISTA KERTOI ORGANISAATIOLLAAN OLEVAN TIETOJEN SUOJAUSKÄYTÄNNÖN SEURAAVISTA SYISTÄ:



Organisaatiot eivät siten suhtaudu toimistolaitteiden tietoturvaan asiaankuuluvalla vakavuudella.

”Monissa toimistolaitteissa on edelleen oletussalasanat tai ei lainkaan salasanoja, ja kymmenellä käyttäjällä voi olla myös sama salasana”, totesi HP:n tietoturva-asiantuntija Michael Howard kesäkuun Computerworld-julkaisussa. ”Verkkotulostin tai monitoimilaite ilman salasanaa on kuin kultakaivos hakkerien silmissä. Yksi yleinen hyökkäystapa on välistävetohyökkäys (man-in-the-middle), jossa hyökkääjä ottaa verkkotulostimen tai monitoimilaitteen haltuunsa ja ohjaa sitten kaikki laitteeseen saapuvat asiakirjat omalle tietokoneelleen ennen niiden tulostusta. Näin he näkevät kaiken, mitä toimitusjohtaja tulostaa.”[2]

TOIMISTOLAITTEISIIN KOHDISTUVIEN HYÖKKÄYSTEN MAHDOLLISET VAIKUTUKSET

Bitdefenderin vanhempi kyberturvallisuusanalyytikko Bogdan Botezatu pitää toimistolaitteita merkittävänä tietoturvariskinä. ”Saamme paljon telemetriatietoja haavoittuvuuksien arviointikokeissamme. Reitittin ei ole enää internetin haavoittuvaisin laite. Nyt se on verkkotulostin tai monitoimilaite.”[3]

Näillä haavoittuvuuksilla voi olla merkittäviä vaikutuksia yritysten liiketoimintaan. Yksikin suojaamaton toimistolaite voi altistaa kaikki verkkoon liitetyt laitteet hyökkäyksille, jolloin hakkerit voivat vakoilla koko verkkoa ja sen kaikkia laitteita vaarantaen koko verkon turvallisuuden.

Olemme kaikki nähneet, millaisia vaikutuksia tietoturvarikkomuksilla voi olla. Spiceworksin kyselyssä vastaajat ilmoittivat, että tietoturvarikkomuksen viisi tärkeintä vaikutusta ovat:[1]

Toimistolaitteisiin kohdistuvan hyökkäyksen vaikutukset voivat olla vieläkin vakavampia, erityisesti, jos käytössä on monitoimilaite, johon voidaan tallentaa tietoa sähköi-

sessä muodossa. Laitteen välimuistiin tallennetut tulostustyöt mahdollistavat hakkerien pääsyn arkaluonteisiin henkilötietoihin tai liiketoimintaan liittyviin tietoihin.

Vielä huolestuttavampaa on se, että suojaamattoman toimistolaitteen kautta hakkerit voivat päästä yrityksen verkkoon ja varastaa esimerkiksi henkilötunnuksia, taloustietoja, sisäisiä muistioita ja asiakirjoja. Nämä varastetut tiedot eivät vaikuta ainoastaan yksittäisiin työntekijöihin, vaan kilpailijat voivat käyttää niitä yritystä vastaan ja aiheuttaa merkittäviä haittoja.

HELPPO RATKAISU: SISÄÄNRAKENNETUT SUOJAUSOMINAISUUDET

On siis selvää, että yritysten on huomioitava myös verkkotulostimien ja monitoimilaitteiden tietoturva. Monissa nykyaikaisissa suuryritystason toimistolaitteissa on sisäänrakennetut, helppokäyttöiset suojausominaisuudet, jotka auttavat torjumaan verkkotulostimia ja monitoimilaitteita koskevat uhkat. Niitä ovat esimerkiksi seuraavat:

- Automaattinen hyökkäysten tunnistus, torjunta ja korjaus
- Käytön seuranta luvattoman käytön estämiseksi
- Helppo sisäänkirjautuminen esimerkiksi PIN-koodilla tai älykortilla
- Tunnuskortin lähikenttälukija, jonka avulla käyttäjät voivat todentaa henkilöllisyytensä ja käyttää laitetta turvallisesti omalla tunnuskortillaan
- Arkaluonteisten tulostettavien asiakirjojen salaus

Kun olet hankkimassa seuraavaa toimistolaitettasi, olipa kyseessä sitten pöytätulostin tai monitoimilaite, perehdy sen sisäänrakennettuihin suojausominaisuuksiin ja muista ottaa ne käyttöön. Tässä kuvattujen toimistolaitekohtaisten ja helppokäyttöisten ominaisuuksien ansiosta verkkotulostimien ja monitoimilaitteiden suojaus uhkilta onnistuu vaivattomasti. Esineiden internetin yleistyessä sinulla on monia muita päätelaitteita, joiden tietoturva aiheuttaa päänvaivaa – älä anna verkkotulostimiesi tai monitoimilaitteidesi olla yksi niistä.

ETSITKÖ TURVALLISEMPIA TOIMISTOLAITTEITA?

LISÄTIETOJA ›

Lähteet:

[1] Spiceworksin HP:n puolesta tekemä kartoitus, joka koski 309:ää IT-alan päätöksentekijää Pohjois-Amerikassa sekä EMEA- ja APAC-alueilla marraskuussa 2016.

[2] "Printer Security: Is your company's data really safe?" *Computerworld,* 1.6.2016. http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] "Printers Now the Least-secure Things on the Internet", *The Register*, 8.9.2016. http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/