Kyberkatsaus

6/2025

LOIHDE

Tiivistelmä

Kesäkuun raportissa on nostettu esille kriittisiä ja erittäin todennäköisesti pian aktiivista hyväksikäyttöä kohtaavia haavoittuvuuksia Citrix NetScalerista sekä Veeamin varmuuskopiointiratkaisusta. Näiden osalta korjaavien päivitysten asentaminen sekä korjaustoimenpiteet suositellaan tehtäväksi välittömästi.

Tunnusten kalastelua on tapahtunut aktiivisesti koko vuoden aikana, etenkin M365-tunnusten osalta. Uhkatoimijat käyttävät yhä enemmän jo vaarantamiaan tunnuksia lähettämään uusia kalastelusähköposteja. Lisäksi viesteihin sisällytetään mm. OneDrive-jakoja hämäämään vastaanottajaa ja vastaanottavan organisaation sähköpostisuojauksia. Kompensoivia kontrolleja, kuten Conditional Access Policyt, on syytä harkita otettavaksi käyttöön, jotta onnistuneista tunnusten kalasteluista syntyneet vahingot saadaan minimoitua tai estettyä kokonaan.

Kiristyshaittaohjelmarintamalla Broadcom on raportoinut havainneensa epätavallisten työkalujen käyttöä kiristyshaittaohjelmatapauksessa. Ransomware-kentällä on lisäksi nähty uusia toimijoita, kuten Anubis, jonka kiristyshaittaohjelmaan on rakennettu wiper-ominaisuus tiedostojen sisällön pyyhkimiseksi, mikäli lunnaita ei makseta.

Ruotsalainen kuorma-autoja valmistava Scania joutui tietomurron uhriksi, kun ulkoinen taho pääsi varastamaan dokumentteja Scanian vakuutuksia käsittelevästä verkkosovelluksesta.

Onnettomuustutkintakeskus julkaisi Helsingin kaupungin 2024 tapahtuneesta tietomurrosta suoritetun tutkinnan tutkintaselostuksen. Itsenäisen ja riippumattoman tutkintaryhmän suorittama tutkinta tunnisti puutteita Helsingin kaupungin IT-järjestelmien ylläpidossa, valvonnassa ja prosesseissa.

Kyberkatsauksessa on lisäksi nostettu esille Loihteen CSOCin kesäkuun kolme suositusta, joita hyödyntämällä organisaatiot kykenevät havaitsemaan epäilyttävää toimintaa ja suojautumaan ympäristöissään tapahtuvilta tietoturvapoikkeamilta. Riittävä näkyvyys ympäristöihin on perusedellytys tietoturvapoikkeamien ennaltaehkäisemiseen, havaitsemiseen ja niistä palautumiseen.

Alkuvuoden perusteella voidaan kyberturvallisuuteen liittyvien uhkien osalta odottaa aktiivista kesää. Rikollisten toiminta on aktiivista ja tähän trendiin ei näytä tulevan muutosta. Geopoliittinen tilanne aktivoi valtiollisia toimijoita, mutta mahdollistaa myös rikollisille erilaisia keinoja käyttää kyvykkyyksiään omien päämääriensä ajamiseksi. Suomalaisten yritysten on myös syytä tunnistaa oma potentiaalinsa hyökkäyksen mahdollistavana kohteena; yrityksen kautta vaikuttamalla hyökkääjä voi päästä käsiksi esimerkiksi kriittisen infrastruktuurin tai huoltovarmuuden kannalta tärkeisiin toimijoihin.

KUUKAUSIRAPORTTI 6/2025

Tämä raportti sisältää kuvauksen kesäkuun 2025 kybertapahtumista. Raportin sisältö pohjautuu avoimiin lähteisiin, joita ovat esimerkiksi uutiset, sosiaalisen median palvelut ja muut aiheeseen liittyvät verkkolähteet. Raportti tuo esille kyberturvallisuuteen liittyviä merkittäviä tapahtumia ja trendejä, jotka vaikuttavat meidän ja asiakkaidemme toimintaan.

Kyberkatsaus on heinäkuun tauolla. Seuraava raportti julkaistaan taas syyskuun alussa.

Sisällys

1. Yleistilanne

Suomalaisissa yrityksissä kyberturvallisuuteen liittyvät uhat ovat läsnä päivittäisessä toiminnassa eikä niiden vähenemisestä ole merkkejä. Suomalaisille yrityksille ja organisaatioille keskeisin kyberuhka ovat taloudellisesti motivoituneet rikolliset toimijat. Näiden lisäksi tietyille tahoille uhkaa muodostavat myös haktivistit ja valtiolliset toimijat. Edellä mainittuihin uhkiin vastaaminen vaatii organisaatioilta aktiivisia toimia ja jatkuvaa kyberturvallisuuden kehitystyötä.

Tilanne Suomen lähialueella on ollut jännitteinen jo muutamien vuosien ajan. Itämeren valtiot ovat joutuneet toistuvasti Venäjän aggressiivisen retoriikan ja toiminnan kohteeksi. Harjoitustoiminnan häiritseminen, alueloukkaukset, mahdollisesti vaurioitettu infrastruktuuri ja negatiivinen retoriikka ovat vakiintuneet osaksi Suomen lähialueen arkipäivää. Lisäksi Itämeren vedenalaista infrastruktuuria on vahingoitettu toistuvasti Suomen lähialueella. Suomalaisten organisaatioiden on syytä ottaa tämä huomioon omassa toiminnassaan ja riskiarvioissaan.

Tietoturvaan liittyvät uhat voivat olla sekä paikallisia että kansainvälisiä. Paikallisiin uhkiin vaikuttaa Suomen geopoliittinen asema ja kohdennetut kampanjat rikollisten taholta. Kansainvälistä uhkaa edustavat esimerkiksi globaalisti hyväksikäytettävät verkon reunalaitteiden haavoittuvuudet. Näihin uhkiin varautuminen edellyttää jatkuvaa työskentelyä ja kehittämistä tietoturvaan liittyen. Valvonta, reagointikyky ja poikkeamiin valmistautuminen ovat keskeinen osa jatkuvuuden varmistamista.

Lähi-Idän tilanne vaikuttaa myös globaaliin turvallisuustilanteeseen. Yhdysvaltojen ja Israelin suorittamat ilmaiskut Iranin ydinlaitoksiin, Iranin vastaiskut ja uhkaukset sulkea Hormuzinsalmi lisäävät vastakkainasettelua. Suojelupoliisin mukaan terrorismin uhka on kohonnut Suomessa ja esimerkiksi Iranin suhteet länsimaihin ovat heikentyneet.[1] Tämä voi näkyä Suomessa lisääntyneenä vihamielisenä toimintana ja kybervaikuttamisena.

[1] YLE, 23.6.2025, https://yle.fi/a/74-20169031

2. Haavoittuvuudet

2.1 CVE-2025-5349, CVE-2025-5777 & CVE-2025-6543: Critical Citrix NetScaler Vulnerabilities

Citrix julkaisi 17.06.2025 vakavuudeltaan kriittisen tiedotteen kahdesta haavoittuvuudesta koskien Citrix NetScaler ADC ja NetScaler Gateway -tuotteita.[2] CVE-2025-5349 on pääsynhallinnan ohittava haavoittuvuus ja CVE-2025-5777 puolestaan mahdollistaa hyökkääjälle arkaluontoisen datan lukemisen muistista. Haavoittuvuutta hyväksikäyttämällä hyökkääjä kykenee varastamaan laitteen muistista istuntoevästeet ja tätä kautta saamaan pääsyn laitteelle kaapatulla käyttäjäistunnolla.[3] Noin viikko tiedotteen jälkeen 25.6. julkaistiin vielä kolmas kriittinen haavoittuvuus, CVE-2025-6543, jonka aktiivista hyväksikäyttöä Citrix ilmoitti jo havainneensa.[4]

Citrix on julkaissut korjaavat päivitykset ja suosittelee ne asennettavaksi välittömästi. Päivitysten asentamisen lisäksi Citrix suosittelee katkaisemaan kaikki aktiiviset ICA- ja PCoIP-istunnot päivityksen jälkeen, jotta mahdollisesti varastetut istunnot keskeytyvät. NetScalerin aiemmat vastaavat haavoittuvuudet, kuten CVE-2023-4966 (nk. CitrixBleed), ovat olleet hyvin aktiivisen hyväksikäytön kohteita ja uhkatoimijoiden tehokkaassa käytössä.[5] On odotettavaa, että myös tämä haavoittuvuus päätyy etenkin kiristyshaittaohjelmatoimijoiden kohteeksi.

2.2 CVE-2025-23121: Veeam Backup & Replication authenticated RCE

Veeamin Backup & Replication -ratkaisusta on löydetty jälleen kriittinen haavoittuvuus. Veeam julkaisi 17.06.2025 tiedotteen päivityksestä, joka korjaa kriittisen haavoittuvuuden koskien tuotteen versiota 12.3.1.1139 ja sitä vanhempia version 12 koontiversioita. Haavoittuvuus mahdollistaa mielivaltaisen koodin suorittamisen etänä autentikoituneella domain-käyttäjällä.[6]

Haavoittuvuudesta ja sen hyväksikäytöstä ei ole vielä julkaistu yksityiskohtia, mutta sen epäillään olevan tapa ohittaa korjaus maaliskuun Kyberkatsauksessakin nostetulle vastaavalle haavoittuvuudelle CVE-2025-23120. Haavoittuvuuden löysivät WatchTowr:n ja CODE WHITE:n tutkijat, jotka jo maaliskuussa kertoivat haavoittuvuuden CVE-2025-23120 korjauksen olevan mahdollisesti ohitettavissa.[7]

[2] Citrix, 17.06.2025, NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-5349 and CVE-2025-5777, https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420
[3] Dark Reading, 23.06.2025, Citrix Patches Critical Vulns in NetScaler ADC and Gateway, https://www.darkreading.com/vulnerabilities-threats/citrix-patches-vulns-netscaler-adc-gateway
[4] Citrix, 25.06.2025, NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-6543, https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788
[5] CISA, 21.11.2023, #StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a
[6] Veeam, 17.06.2025, Vulnerabilities Resolved in Veeam Backup & Replication 12.3.2, https://www.veeam.com/kb4743
[7] CODE WHITE GmbH, 28.03.2025, Post on infosec.exchange Mastodon server, https://infosec.exchange/@codewhitesec/114241026482611250

Vaikuttaa siltä, että myös tässä tapauksessa kuka tahansa domainin käyttäjä kykenee hyväksikäyttämään haavoittuvuutta domainiin liitetyllä Veeam-palvelimella. Korjaava päivitys suositellaan asennettavaksi välittömästi, sillä Veeamin haavoittuvuudet ovat erittäin usein etenkin kiristyshaittaohjelmatoimijoiden kohteena.[8]

2.3 CVE-2025-33053: Internet Shortcut Files Remote Code Execution Vulnerability

Microsoftin kesäkuun päivitykset korjasivat liudan haavoittuvuuksia, joista yhtä on havaittu jo hyväksikäytettävän APT-uhkatoimijan, Stealth Falconin, toimesta nollapäivä-haavoittuvuutena. Check Pointin tutkijoiden raportoima CVE-2025-33053 mahdollistaa hyökkääjälle mielivaltaisen koodin suorittamisen uhrin laitteella haitallisen .url-tiedoston kautta.[9]

Haavoittuvuus piilee URL-tiedostojen parametreissa, joiden avulla verkkolinkkitiedoston saa suorittamaan binäärin hyökkääjän kontrolloimalta WebDAV-palvelimelta hyväksikäyttäen Windowsiin oletuksena asennettua Internet Explorerin iediagcmd.exe-diagnostiikkatyökalua. URL-tiedoston WorkingDirectory-parametrin voi ohjata ulkoisen WebDAV-palvelimen tiedostopolkuun, jolloin iediagcmd.exen diagnostiikan keruun käyttämät työkalut, kuten route.exe, haetaan hyökkääjän palvelimelta, koska sovellusta suorittava prosessi etsii sitä ensin prosessin omasta kansiosta ”%SystemRoot%\System32” -polun sijaan.[9]

[8] Rapid7, 17.06.2025, Critical Veeam Backup & Replication CVE-2025-23121, https://www.rapid7.com/blog/post/etr-critical-veeam-backup-replication-cve-2025-23121/
[9] Check Point, 10.06.2025, CVE-2025-33053, Stealth Falcon and Horus: A Saga of Middle Eastern Cyber Espionage, https://research.checkpoint.com/2025/stealth-falcon-zero-day/

3. Kalastelu ja huijaukset

CloudFlare raportoi SVG-tiedostojen lisääntyneestä käytöstä kalasteluviesteissä. Niitä erehdytään monesti luulemaan pelkiksi kuvatiedostoiksi, mutta ne voivat sisältää skriptejä ja esimerkiksi JavaScript-koodia. Tämä on mahdollista, koska SVG-tiedostot perustuvat XML:ään, joka tukee mm. HTML:ää ja JavaScriptiä. CloudFlaren mukaan monet sähköpostisuodattimet eivät tee tiedostoformaatille syvempää tarkistusta, joka johtaa siihen, että haitalliset tiedostot menevät niistä läpi. SVG-tiedostojen avaaminen johtaa sen sisältämän koodin suorittamiseen. Kalastelun kontekstissa tämä tarkoittaa monesti uudelleenohjausta kalastelusivustolle, kuten väärennetylle M365-kirjautumissivulle tai haittaohjelman suorittamiseen päätelaitteella.[10]

M365-käyttäjätunnusten kalastelu on ollut aktiivista koko vuoden 2025 ajan, eikä ilmiö näytä hiipumisen merkkejä. Perinteisen kaksivaiheisen tunnistautumisen ohittaminen AiTM:n[11] avulla on arkipäivää, eikä se yksistään tarjoa riittävää suojaa kalastelua vastaan. Kalasteluissa käytetään yhä enemmän aiemmin kaapattuja tunnuksia, joilta lähetetään kalasteluviestejä muihin suomalaisiin organisaatioihin. Lisäksi viesteissä hyödynnetään laajasti Microsoftin palveluita, kuten PowerBI ja Microsoft Forms, haitallisten linkkien toimittamiseen. Näiden avulla monet kalasteluviestit läpäisevät sähköpostisuojauksen helpommin, eivätkä viestien vastaanottajat välttämättä osaa epäillä luotetulta lähettäjältä tulevaa viestiä kalasteluviestiksi.

Onnistuneen kalastelun tapahtuessa uhkatoimijat kirjautuvat lähes reaaliajassa käyttäjän tunnuksilla Microsoft 365 -palveluun ja suuntaavat etsimään mielenkiintoisia asiakirjoja ja sähköposteja OneDriveen, SharePointiin ja Outlookiin. Arkaluontoisia tietoja voi näin ollen vaarantua minuuttien sisään ensimmäisestä haitallisesta kirjautumisista. Uhkatoimijat pyrkivät myös useimmiten lisäämään käyttäjälle uuden MFA:n, sähköpostiin uudelleenohjaussääntöjä tai lisäämään Azure/M365-ympäristöön haitallisia OAuth-sovelluksia, joilla he pystyvät pitämään jalansijan käyttäjätunnuksella. Tällaisissa tapauksissa on syytä suorittaa perusteellinen tutkinta käyttäjällä tehtyihin toimiin, jotta mahdolliset jalansijat pystytään poistamaan. Pelkkä istuntojen katkaisu tai salasanan vaihtaminen ei poista jälkikäteen lisättyä MFA:ta tai OAuth-sovelluksia.

Tämä alleviivaa kerroksittaisen suojauksen tärkeyttä. Kaikkia kalasteluviestejä ei pystytä estämään, joten on tärkeää kyetä minimoimaan vahingot onnistuneen kalastelun tapahtuessa. M365-tunnusten tapauksessa olennaisessa roolissa ovat Conditional Access -policyt ja kalastelun kestävä MFA (FIDO2). Kirjautumisten rajaaminen ainoastaan luotettuihin laitteisiin estää kirjautumisen onnistuneen kalastelun tapahtuessa. Tässä on kuitenkin syytä huomioida se, että salasana vaarantuu joka tapauksessa ja se on syytä vaihtaa. FIDO2 vähentää käyttäjän virheestä syntyneen kalastelun riskiä merkittävästi, koska onnistuneeseen kirjautumiseen vaaditaan MFA-mekanismin fyysinen läsnäolo eli fyysinen turva-avain, joka on

[10] CloudFlare, 6.5.2025. https://www.cloudflare.com/threat-intelligence/research/report/svgs-the-hackers-canvas/
[11] Kyberturvallisuuskeskus. 27.5.2025. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-tietoturva-ammattilaisille/aitm-adversary-middle

kiinni työasemassa (esim. Yubikey) tai Bluetooth-yhteys matkapuhelimen ja työaseman välillä (Passkeys).

4. Kiristyshaittaohjelmat ja -toimijat

Broadcom raportoi poikkeuksellisesta kiristyshaittaohjelmatapauksesta, jossa Fog-kiristyshaittaohjelmaa levittävä uhkatoimija käytti useita hyvin poikkeuksellisia työkaluja osana hyökkäystä. Hyökkäyksessä käytettiin useita harvinaisia penetraatiotestaustyökaluja, kuten Google Sheetsia C2-palvelimena käyttävää GC2-sheetsia, avoimen lähdekoodin Cobalt Striken vaihtoehtona tunnettua AdaptixC2, mutta mielenkiintoisin lienee Sytecan sovellusten käyttö. Syteca valmistaa muun muassa työntekijöiden aktiivisuusseurantaan käytettäviä sovelluksia, joita uhkatoimijan uskotaan käyttäneen näppäinten tallennukseen (keylogging) ja ruudunkaappaukseen. Todennäköisesti kaupallinen aktiivisuusseurantasovellus menee helpommin EDR:n ja muiden suojauksien ohi, kuin tunnettu haittaohjelma. [12]

Trend Micro on kirjoittanut analyysin melko tuoreesta kiristyshaittatoimijasta Anubiksesta. Poikkeuksellisena ominaisuutena Anubis on lisännyt kiristyshaittaohjelmaansa myös mahdollisuuden tyhjentää levyn sisällön. Tyhjennys ei poista tiedostoja, vaan tekee niistä 0KB kokoisia, käytännössä tyhjentäen tiedostojen sisällön. Tyhjennysominaisuus on todennäköisesti lisätty pelotteeksi uhrille, koska neuvottelujen kariuduttua Anubis kykenee poistamaan salatut tiedostot, tehden palautuksesta mahdotonta.[13]

[12] Broadcom, 12.06.2025, Fog Ransomware: Unusual Toolset Used in Recent Attack, https://www.security.com/threat-intelligence/fog-ransomware-attack

[13] Trend Micro, 13.06.2025, Anubis: A Closer Look at an Emerging Ransomware with Built-in Wiper, https://www.trendmicro.com/en_us/research/25/f/anubis-a-closer-look-at-an-emerging-ransomware.html

5. Muuta

5.1 Scanian tietoturvapoikkeama

Ruotsalainen rekkayhtiö Scania on vahvistanut joutuneensa tietomurron kohteeksi. Uhkatoimija julkaisi hakkerifoorumille ilmoituksen, jossa he yrittivät myydä murrossa varastettua dataa. Hyökkäys tapahtui Scanian mukaan toukokuun lopulla ja se kohdistui Scanian vakuutuksia käsittelevään ulkoisen IT-kumppanin toimittamaan sovellukseen. Hyökkäys sai alkunsa varastetuilla ulkoisen IT-kumppanin tunnuksilla, jota hyödyntäen hyökkääjä sai ladattua vakuutuskorvauksiin liittyviä dokumentteja. Uhkatoimijan julkaisun mukaan varastettuja tiedostoja olisi 34 000 kpl, joista he ovat jakaneet pienen osan näytteeksi yritettyään kiristää Scaniaa lähettämällä sähköpostia Scanian työntekijöille.[14]

5.2 Helsingin kaupungin tietomurron tutkintaselostus

Onnettomuustutkintakeskus (OTKES) julkaisi 17.06.2025 verkkosivuillaan 92-sivuisen tutkintaselostuksen Helsingin kaupunkiin keväällä 2024 tehdystä tietomurrosta, jossa hyökkääjä onnistui varastamaan n. kaksi teratavua asiakirjoja kaupungin verkkolevyltä, jonka seurauksena merkittävä määrä henkilötietoja päätyi hyökkääjän haltuun. Riippumattoman ja itsenäisen tutkintaryhmän tekemästä tutkintaselostuksesta käy ilmi, että Helsingin kaupungin VPN-palvelimena toimivan Cisco ASA -palomuurilaitteen ylläpidossa sekä verkon tietoturvavalvonnassa oli merkittäviä puutteita.[15]

Hyökkääjä onnistui kirjautumaan kahdella oppilaan tunnuksella ja VPN-reitittimen konfiguraatiossa ollut riskialtis asetus antoi tunnuksille IT-tuen oikeudet. Tämän jälkeen hyökkääjä eteni verkossa, saaden haltuunsa järjestelmänvalvojatunnukset sisäverkon palvelimiin. Raportin mukaan hyökkääjän etenemistä verkossa helpotti se, että monilla Helsingin kaupungin palvelimilla käytettiin samaa salasanaa paikallisilla järjestelmänvalvojatunnuksilla. Verkkolevyn lisäksi hyökkääjä sai raportin mukaan haltuunsa kahden AD-domainin käyttäjätiedot. Verkon valvonta oli tutkinnan mukaan vajavaista, eikä esimerkiksi keskitettyä lokienhallintaa tai kehittynyttä päätelaitesuojausta (EDR) ollut.

[14] Bleeping Computer, 17.06.2025, Scania confirms insurance claim data breach in extortion attempt, https://www.bleepingcomputer.com/news/security/scania-confirms-insurance-claim-data-breach-in-extortion-attempt/
[15] Onnettomuustukintakeskus, 17.06.2025, P2024 01 Helsinki tutkintaselostus, https://turvallisuustutkinta.fi/material/sites/otkes/otkes/hlsztol3t/P2024-01_Helsinki_tutkintaselostus.pdf

6. Suositukset

Tässä kuussa suosittelemme:

- Käyttäjien ohjeistaminen kalasteluviesteistä kesälomakaudella
- Verkkoliikenteen sääntöjen tarkastelu ja rajaaminen
- Ajantasainen laitelistaus

Kesälomakausi on otollista aikaa tietojenkalastelulle. Käyttäjät ovat kiireisiä ennen kesälomalle siirtymistään, koska keskeneräiset työtehtävät pyritään saamaan mahdollisimman valmiiksi ennen lomille siirtymistä. Uhkatoimijat tiedostavat tämän ja pyrkivät käyttämään tilanteen hyväkseen. Käyttäjiin kohdistetaan kalasteluviestejä juuri ennen lomien ja juhlapyhien alkamista, jolloin riski joutua tietojenkalastelun uhriksi kasvaa merkittävästi. Kalasteluviesti voi tulla tutultakin lähettäjältä, jonka tunnukset ovat vaarantuneet aiemmin.

Viesteissä pyritään luomaan kiireellisyyden tuntua, vastaanottajaa uhkaillaan tai luodaan katteettomia lupauksia. Näissä tapauksissa jossain vaiheessa pyritään kalastelemaan tunnukset esimerkiksi väärennetyn M365-kirjautumisnäkymän avulla. Organisaatioiden on suositeltavaa ohjeistaa käyttäjiään ja muistuttaa heitä olemaan erityisen valppaina avatessaan sähköposteja kesälomakaudella.

Kirjautuminen, erilaisten palveluiden käyttö ja esimerkiksi hyökkääjän komentokanava vaativat verkkoliikennettä toimiakseen. Organisaation verkossa olevien laitteiden ja etenkin palvelimien liikennettä onkin syytä tarkastella kriittisesti sallittujen yhteyksien osalta. Tarpeettomat palvelut ja portit on syytä sulkea ja niiden käyttö estää. Lisäksi on hyvä arvioida sitä, onko kaikilla palvelimilla tarve käyttää esimerkiksi kaikkia verkkoprotokollia. Kriittisten palvelimien, kuten domain controllereiden tai tuotantopalvelimen sallittujen verkkoyhteyksien rajaaminen vain tarvittuihin pienentää hyökkääjän toimintamahdollisuuksia huomattavasti. Yhteydet internetiin sekä muualle verkkoon tulisi olla rajattu vain tarvittaviin, poikkeuksina tehtyihin avauksiin.

Organisaatioilla tulisi olla ajankohtainen laitelistaus ja prosessi sen ylläpitämiseen.[16] Työasemien ja palvelinten kohdalla voidaan käyttää keskitettyä hallintaa, esimerkiksi EDR-tuotetta tai Microsoft Intunea. Kaikkia laitteita ei kuitenkaan voida seurata näitä järjestelmiä hyödyntämällä. Organisaation verkon ja verkossa olevien laitteiden tunnistamiseen voidaan käyttää esimerkiksi siihen tarkoitettua skanneria. Laitelistauksen olemassaolo ja ylläpitäminen on ensisijaisen tärkeää, jotta mahdolliset haavoittuvuudet saadaan korjattua ja hyökkäyspinta-ala minimoitua. Jos organisaatio ei tiedä jonkin laitteen olemassaolosta ympäristössään, on sen suojaaminen erittäin haastavaa.

[16] Palo Alto Networks, what is IT asset inventory? 25.6.2025, https://www.paloaltonetworks.com/cyberpedia/what-is-it-asset-inventory

Tämän raportin koostaa
Loihteen asiakkaille
kuukausittain
Loihteen CSOC:n eli
kyberturvakeskuksen
asiantuntijat hyödyntäen sekä
avoimia lähteitä että omaa
tietämystään.

Kellon ympäri miehitetty
kyberturvakeskuksemme valvoo
ja reagoi tietoturvatapahtumiin
pitäen huolen siitä, että
asiakkaamme voivat rauhassa
keskittyä liiketoimintaansa.

LOIHDE