

Kyberkatsaus

01/2026

LOIHDE



Tiivistelmä

Vuoden ensimmäisessä kyberkatsauksessa palaamme jälleen verkon reunalaitteisiin liittyviin vakaviin haavoittuvuuksiin. Loihteen CSOC:n arvio on, että vuoden 2026 aikana reunalaitteisiin liittyviä haavoittuvuuksia tullaan näkemään reilusti lisää. Organisaatioiden on syytä tarkistaa julkiverkkoon näkyvät palvelut ja rajata näkyvyyttä tarpeen mukaan.

Microsoft 365 -tunnuksiin liittyvissä kalasteluissa hyödynnetään enenevässä määrin automaatiota, jota on jalostettu pelkämästä kalastelutapahtumasta pidemmälle aina sähköpostien käsittelyyn ja edelleen lähettämiseen saakka. Loihteen CSOC:n havaitsemien tapahtumien perusteella käy ilmi, että murretuilta käyttäjätileiltä on havaittu satoja sähköpostien ja asiakirjojen käsittelyyn liittyviä tapahtumia muutamia sekunteja ensimmäisen haitallisen kirjautumisen jälkeen.

Tietoturvayhtiö SentinelOne arvelee, että tekoälyn ja kielimallien käyttö vauhdittaa kirstyshaittaohjelmatoimintaa ja madaltaa kynnystä osallistua siihen. Lisäksi paikallisten kielimallien käytön epäillään lisääntyvän kirstyshaittaohjelmien käytössä.

Huoltovarmuuskeskus on julkaissut selvityksen liittyen suomalaisten toimialojen kyberkypsyyteen. Selvityksessä tuodaan ilmi mm. kyberturvallisuuden kehittämiseen liittyviä haasteita.

Kyberkatsauksessa on lisäksi mukana Loihteen CSOC:n tammikuun kolme suositusta, joita hyödyntämällä organisaatiot kykenevät havaitsemaan epäilyttävää toimintaa ja suojautumaan paremmin ympäristöissään tapahtuvilta tietoturvapoikkeamilta. Riittävä näkyvyys ympäristöihin on perusedellytys tietoturvapoikkeamien ennaltaehkäisemiseen, havaitsemiseen ja niistä palautumiseen.


LOIHDE 0 1 - 2 0 2 6 

Vuosi 2025 lukuina



2x Kyberturvallisuuskeskuksen selvittämät vakavat tapaukset ovat kaksinkertaistuneet vuodesta 2024.

Tammikuu 2026

Loihteen CSOC arvioi, että...

-  ...tänä vuonna reunalaitteisiin liittyviä haavoittuvuuksia nähdään reilusti lisää.
-  ...M365-tunnuksiin liittyvissä kalasteluissa hyödynnetään yhä enemmän automaatiota.

Loihteen CSOC:n suositukset

-  Reunalaitteiden näkyvyyden rajaaminen julkiverkosta.
-  Päätelaitesuojauksen käyttöönotto kaikille yhteensopiville laitteille.
-  Suojaa NTLM-autentikointia käyttävät protokollat.

KUUKAUSIRAPORTTI 01/2026

Tämä raportti sisältää kuvauksen joulukuun 2025 ja tammikuun 2026 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.

Sisällys

Tiivistelmä	1
KUUKAUSIRAPORTTI 01/2026	2
1. Yleistilanne	3
2. Haavoittuvuudet	4
2.1 CVE-2025-55182: React Server Components pre-auth remote code execution ("React2Shell")	4
2.2 CVE-2025-59718 & CVE-2025-59719: Fortinet FortiCloud SSO login authentication bypass	4
3. Kalastelu ja huijaukset	6
4. Kiristyshaittaohjelmat ja -toimijat	7
4.1 Tekoäly vauhdittaa kiristyshaittatoimijoiden toimintaa	7
4.2 FinCEN-raportti kiristyshaittatoimijoista USA:ssa	7
5. Muuta	8
5.1 Huoltovarmuuskeskus: Toimialojen kyberkypsyyden selvitys 2025	8
5.2 Kimwolf-haittaohjelma saastuttanut Android TV Box -laitteita	8
6. Suositukset	9

1. Yleistilanne

Suomalaisissa organisaatioissa kyberturvallisuuteen liittyvät uhat ovat läsnä päivittäisessä toiminnassa eikä niiden vähenemisestä ole merkkejä. Suomalaisille yrityksille ja organisaatioille merkittävimmät kyberuhat 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.

Vakavien tietoturvapoikkeamien määrät suomalaisissa organisaatioissa pysyvät korkealla tasolla vuonna 2025. Kyberturvallisuuskeskuksen selvittämät vakavat tapaukset ovat kaksinkertaistuneet vuodesta 2024. Myös vakavien tietoturvaahaavoittuvuuksien määrä sekä niiden nopea hyväksikäyttö aiheuttavat huolta. Tekoälyn nopea kehittyminen tuo lisäksi mukanaan uusia haasteita kyberturvallisuuteen.

Kyberturvallisuutta pyritään parantamaan koko EU:n tasolla uusilla direktiiveillä ja säädöksillä. NIS2-direktiivin velvoitteet astuivat voimaan 8.4.2025, mikä toi mukanaan uusia velvoitteita sen piirissä oleville toimijoille. Kyberkestävyyslainsäädös (Cyber Resilience Act, CRA) tulee vaikuttamaan laitteisiin ja ohjelmistoihin, joihin liittyy digitaalinen elementti ja joita on mahdollista kytkeä toiseen laitteeseen tai verkkoon.¹

¹ <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/kyberkestavyyslaadon-cyber-resilience-act-cra#82703-1>

2. Haavoittuvuudet

2.1 CVE-2025-55182: React Server Components pre-auth remote code execution (“React2Shell”)

Joulukuun 3. päivä julkaistiin korjauksineen kriittinen, täyden 10.0 CVSS-pisteityksen saanut haavoittuvuus web-palveluiden käyttämässä React Server Componentsissa ja siihen liittyvissä frameworkeissa. Haavoittuvuuden hyväksikäyttö antaa hyökkääjälle mahdollisuuden suorittaa mielivaltaista koodia kohdepalvelimella vain yksittäisen HTTP-pyynnön lähettämällä.²

Itse haavoittuvuus piilee tavassa, jolla React käsittelee React Server Function -päätteisiin lähetettyjä tietosisältöjä. Hyväksikäyttö on triviaalia, eikä se vaadi hyökkääjältä esim. ennalta autentikointia tai valideja käyttäjätunnuksia. Koska React on hyvin laajasti käytetty organisaatioissa ympäri maailman, mm. osana Next.js frameworkia, ja koska ohjelmisto on haavoittuvainen oletuskonfiguraatioilla, on siihen kohdistunut hyvin aktiivista ja laajamittaista hyväksikäyttöä heti haavoittuvuuden julkaisusta alkaen.²

Hyväksikäyttöä on eri tutkijoiden toimesta havaittu useilta eri toimijoilta aina kryptolouhijoiden levittäjistä APT-ryhmiin. Haavoittuvuuden nopeaa tunnistamista ja hyväksikäyttöä helpottamaan julkaistiin nopeasti myös esimerkiksi selainlaajennuksia.³ Korjaavat päivitykset suositeltiin asennettavan välittömästi.

2.2 CVE-2025-59718 & CVE-2025-59719: Fortinet FortiCloud SSO login authentication bypass

Fortinet julkaisi kriittiseksi luokitellun tiedotteen FortiCloud-tuotteesta joulukuun alussa löytyneestä kahdesta haavoittuvuudesta, jotka mahdollistavat FortiCloud SSO -kirjautumisen ohittamisen FortiOS-, FortiWeb-, FortiProxy- sekä FortiSwitch Manager -laitteille. Mikäli FortiCloud SSO on laitettu laitteelle päälle, voi hyökkääjä hyväksikäyttää haavoittuvuutta lähettämällä haitallisen SAML-viestin, joka ohittaa autentikoinnin.⁴

Arctic Wolf havaitsi haavoittuvuuden aktiivista hyväksikäyttöä hyvin pian sen julkistuksen 9.12.2025 jälkeen. Fortinetin FortiGate-palomuurilaitteisiin kohdistuneet hyökkäykset ovat heidän havaintojensa mukaan kohdistuneet tyypillisesti admin-käyttäjään, jolle päästyään uhkatoimijat ovat mm. ladanneet laitteen konfiguraatitiedostot itselleen.⁵

² Microsoft Defender Security Research Team, 15.12.2025, Defending against the CVE-2025-55182 (React2Shell) vulnerability in React Server Components, <https://www.microsoft.com/en-us/security/blog/2025/12/15/defending-against-the-cve-2025-55182-react2shell-vulnerability-in-react-server-components/>

³ RSC_Detector Github repository, N.d., RSC Fingerprint Detector, https://github.com/mrknow001/RSC_Detector

⁴ Fortinet PSIRT, 9.12.2025, Multiple Fortinet Products' FortiCloud SSO Login Authentication Bypass, <https://fortiguard.fortinet.com/psirt/FG-IR-25-647>

⁵ Arctic Wolf, 15.12.2025, Arctic Wolf Observes Malicious SSO Logins on FortiGate Devices Following Disclosure of CVE-2025-59718 and CVE-2025-59719, <https://arcticwolf.com/resources/blog/arctic-wolf-observes-malicious-sso-logins-following-disclosure-cve-2025-59718-cve-2025-59719/>

Fortinet on suositellut asentamaan korjaavat päivitykset välittömästi sekä workaroudina disabloimaan FortiCloud SSO -kirjautumisen. Tammikuun 22. päivä Fortinet kuitenkin ilmoitti havainneensa myös onnistunutta hyväksikäyttöä laitteilla, joiden versiot olivat ajan tasalla haavoittuvuuden hyväksikäytön aikaan.⁶ Muutama päivä myöhemmin 27.1., Fortinet julkaisi tiedotteen uudesta haavoittuvuudesta FortiCloud SSO:ssa: CVE-2026-24858. Estääkseen laajemman hyväksikäytön Fortinet ilmoitti hetkellisesti poistaneensa SSO-kirjautumisen käytöstä FortiCloudin päästä ja estäneensä sinne pääsyn laitteilta, jotka ovat haavoittuneessa versiossa.⁷

⁶ Fortinet PSIRT blog, 22.1.2026, Analysis of Single Sign-On Abuse on FortiOS, <https://www.fortinet.com/blog/psirt-blogs/analysis-of-sso-abuse-on-fortios>

⁷ Fortinet PSIRT, 27.1.2026, Administrative FortiCloud SSO authentication bypass, <https://www.fortiguard.com/psirt/FG-IR-26-060>

3. Kalastelu ja huijaukset

Loihteen CSOC on havainnut (AiTM) Adversary-in-the-Middle⁸-tunnustenkalastelutapauksia, joissa uhkatoimijan toiminta onnistuneen tunnustenkalastelun jälkeen on ollut poikkeuksellisen nopeaa. Kirjautumiset ovat tapahtuneet AiTM:lle tyypillisiin sijainteihin, kuten OfficeHome ja Office365. Poikkeuksellista on kuitenkin ollut se, että uhkatoimija on lokitietojen perusteella käsitellyt useita satoja sähköpostiviestejä lähes välittömästi haitallisen kirjautumisen jälkeen. Tämä viittaa ohjelmalliseen automatisoituun toimintaan kalastelun jälkeen.

Loihteen CSOC:n näkemys on se, että pidemmälle jalostetut automaatioavusteiset kalastelutapaukset tulevat lisääntymään jatkossa. Tämä tarkoittaa sitä, että reaktiiviset toimet kalastelujen ja tietovuotojen pysäyttämiseksi eivät ole riittäviä. Kalastelun jälkeen tapahtuva asiakirjojen ja viestien urkinta tapahtuu niin nopeasti, etteivät automaattiset vastatoimetkaan ehdi niihin reagoimaan riittävällä tasolla. Lokien syntymisessä on myös aina viivettä, joten puolustajat ovat nopeimmillaankin aina vähintään muutaman minuutin myöhässä tapahtumahetkestä. Tehokkaimmat tavat suojautua tunnustenkalasteluilta ovat rajata kirjautumiset luotettuihin laitteisiin Conditional Access Policyjen avulla sekä käyttää Phishing Resistant MFA:ta. Yksittäisenkin käyttäjätunnuksen onnistunut kalastelu voi äityä tietosuojan kannalta ikäväksi tilanteeksi, koska uhkatoimijan käsiin saattaa päätyä hyvinkin arkaluontoista sisältöä ja henkilötietoa. Uhkatoimijat hyödyntävät haltuun saamia tietoa kalastelukampanjoiden toteuttamiseksi muihin organisaatioihin sekä laskutuspetoksiin.

Microsoft raportoi tammikuussa AiTM-kampanjasta, jossa kalasteluviestien levittämisessä on hyödynnetty Sharepointia. Uhkatoimija on aluksi saanut haltuunsa käyttäjätunnuksen, jolta on lähetetty edelleen kalasteluviestejä sekä organisaation sisällä että ulkoisille vastaanottajille. Tätä tunnusta käyttäen toimija on jakanut vastaanottajille Sharepoint-linkkejä käyttäen SecureLink-toimintoa, joka vaatii vastaanottajalta sähköpostiosoitteensa syöttämisen. Tämän jälkeen tähän osoitteeseen lähetetään kertakäyttöinen koodi, jolla näkee Sharepoint-linkin sisällön.⁹ Vastaanottajalle tämä on näyttänyt samalta kuin mikä tahansa Sharepointin kautta jaettu tiedosto. Vastaanottavan organisaation sähköpostisuojaus ei myöskään todennäköisesti havaitse kalastelua, koska sille se näyttäytyy luotettavalta lähettäjältä tulevana Sharepoint-jakona, joka on piilotettu sisäänkirjautumisen taakse. Linkin avattuaan vastaanottaja uudelleenohjataan haitalliselle M365-tunnuksen kalastelusivulle, joka vaarantaa käyttäjätunnuksen, mikäli sisäänkirjautumistiedot syötetään sivustolle.¹⁰ Myös Loihteen CSOC on havainnut kasvavan trendin kalastelutapauksissa, joissa hyödynnetään Sharepointia.

⁸ <https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/>

⁹ <https://learn.microsoft.com/en-us/sharepoint/what-s-new-in-sharing-in-targeted-release>

¹⁰ <https://www.microsoft.com/en-us/security/blog/2026/01/21/multistage-aitm-phishing-bec-campaign-abusing-sharepoint/>

4. Kiristyshaittaohjelmat ja -toimijat

4.1 Tekoäly vauhdittaa kiristyshaittatoimijoiden toimintaa

Samalla tavalla kuin puolustajat ovat saaneet hyötyä tekoälystä, niin myös haittatoimijat ovat alkaneet käyttää tekoälyä tehostamaan toimintaansa. SentinelOne on seurannut jo tapahtunutta muutosta haittatoimijoiden keskuudessa ja myös ennustaa näiden pohjalta, kuinka asiat tulevat todennäköisesti muuttumaan tulevaisuudessa. Tiivistettynä, mitään mullistavia muutoksia ei ole tiedossa, mutta haittatoimijoiden toiminnasta tulee yhä nopeampaa ja tehokkaampaa, sekä kynnys mm. kiristyshaittaohjelmien tekoon pienenee tekoälyn myötä.¹¹

Jo nyt haittatoimijat käyttävät tekoälyä hyväkseen mm. kalasteluviestien luonnissa ja viestien kääntämisessä. Haittatoimijat käyttävät pääasiassa paikallisia kielimalleja, kuten Ollama, mutta jatkuvasti kehitetään myös uusia tapoja kiertää tehokkaampien kaupallisten mallien rajoituksia. Osa haittatoimijoista on myös koittanut automatisoida hyökkäysketjuaan. Näistä yrityksistä ei ole kovin tarkkaa tietoa, joten on hankala sanoa, miten onnistuneita ne ovat olleet.¹¹

Seuraavan muutaman vuoden aikana odotetaan yhä useamman kiristyshaittaohjelman käyttävän paikallista kielimallia osana haittaohjelman toimintaa, mikä tekee haittaohjelmien havainnoinnista ja estämisestä yhä hankalampaa. Kaupallisten kielimallien hyväksikäyttö haittaohjelmien luonnissa ja kehityksessä tulee todennäköisesti yleistymään, mahdollisesti luoden uuden ”prompt smuggling as a service” -palvelun, joka automatisoi rajoitusten ohittamisen.¹¹

4.2 FinCEN-raportti kiristyshaittatoimijoista USA:ssa

Financial Crimes Enforcement Network (FinCEN) julkaisi raportin, jossa käsitellään kiristyshaittatoimijoiden toimintaa USA:ssa vuosina 2022–2024. Raportin mukaan 2023 oli ennätysvuosi yli \$1,1 miljardin lunnasmaksuilla. Vuonna 2024 lunnaiden määrä tippui \$734 miljoonaan, todennäköisesti useampaan kiristyshaittatoimijaan kohdistuneen lainvalvonnan toimien vuoksi. Mediaanilunnasvaatimus vuosien aikana vaihteli \$124 097:n ja \$175 000:n välillä. Vähemmän yllättäen kaikki lunnasmaksut tehtiin kryptovaluutoilla, pääasiassa bitcoineilla.¹²

Lunnaiden määrässä on pientä heittoa kohteen alan suhteen. Eniten kiristyshaittaohjelmatapauksia oli teollisuudessa (456 kpl), finanssialalla (432 kpl) ja sairaanhoidossa (389 kpl). Lunnaita kuitenkin maksettiin eniten finanssialalla (\$366 m), sairaanhoidossa (\$305 m) ja teollisuudessa (\$287 m).¹²

¹¹ SentinelOne, 15.12.2025, LLMs & Ransomware | An Operational Accelerator, Not a Revolution, <https://www.sentinelone.com/labs/llms-ransomware-an-operational-accelerator-not-a-revolution/>

¹² FinCEN, 12.2025, Ransomware Trends in Bank Secrecy Act Data Between 2022 and 2024, <https://www.fincen.gov/system/files/2025-12/FTA-Ransomware.pdf>

5. Muuta

5.1 Huoltovarmuuskeskus: Toimialojen kyberkypsyyden selvitys 2025

Huoltovarmuuskeskus on julkaissut vuonna 2025 aloittamansa selvityksen toimialojen kyberkypsyydestä. Raportin mukaan eri toimialojen kyberkypsyys kehittyy hitaasti, eikä se ole pysynyt nopeasti muuttuvan uhkakentän mukana. Raportin mukaan tuloksissa on merkittäviä eroja toimialojen välillä. Esimerkiksi vahvan sääntelyn piirissä olevat finanssi- ja teleliikenneala ovat vertailun kärjessä, kun taas esimerkiksi elintarvikealalla sekä liikenne- ja logistiikka-alalla kyberturvallisuuden kehitys on maltillisempaa.¹³ Huoltovarmuuskeskus toteutti selvityksen edellisen kerran vuonna 2022. Vuoden 2025 raportin perusteella kyberkypsyydessä ei ole tapahtunut merkittäviä muutoksia vuoden 2022 selvitykseen. Haastateltujen yritysten mukaan haasteita ovat esimerkiksi riittämätön kyberosaaminen sekä resurssien puute.¹⁴

5.2 Kimwolf-haittaohjelma saastuttanut Android TV Box -laitteita

Kimwolf:ksi nimetty haittaohjelma ja bottiverkko nousi lokakuussa 2025 ensimmäisen kerran laajempaan tietoisuuteen. Tämän haittaohjelman väitetään saastuttaneen ~1.8 miljoonaa Android TV Box -mediatoistinta ja hyödyntää toiminnoissaan laitteiden mukana tulevaa residential proxy -palvelua. Residential proxy mahdollistaa verkkoliikenteen reitittämisen teleoperaattorin IP-osoitteen kautta. Näin ollen liikenne voidaan anonymisoida ja osoitteiden ollessa teleoperaattoreiden omistamia ovat ne luotettavuuspalveluiden mielestä monesti myös vaarattomia. Residential proxyjen käyttö avaa kuitenkin mahdollisuuksia myös haitallisille toimijoille, koska haitallista liikennettä voidaan reitittää niiden kautta.¹⁵

Monissa TV Box -laitteissa on oletuksena päällä Android Debug Bridge (ADB), joka kuuntelee paikallisesti porttia 5555. Kimwolf:ia levittävä toimija voi residential proxy:ä ja ADB:tä hyväksikäyttämällä ottaa laitteita haltuun ja käyttää niitä osana bottiverkkoa.¹⁶

Kimwolf-haittaohjelmalla on kyvykkyys välittää haitallista liikennettä saastuneiden laitteiden kautta, kuten haitallisten mainosten levittämistä tai laajamittaiseen tiedonkeruuseen verkkosivuilta. Saastuneita laitteina voidaan myös hyödyntää osana palvelunestohyökkäyksiä.¹⁷

¹⁴ <https://www.huoltovarmuuskeskus.fi/files/31c81e6d4cf1e2f64f96742932d1ad0e549abb2b/kyberkypsyys-toimialoilla-2025-kansallinen-raportti-final-suomeksi.pdf>

¹⁵ KrebsonSecurity, 2.1.2026, The Kimwolf Botnet is Stalking Your Local Network. <https://krebsonsecurity.com/2026/01/the-kimwolf-botnet-is-stalking-your-local-network/>

¹⁶ <https://www.esecurityplanet.com/threats/2m-devices-at-risk-as-kimwolf-botnet-abuses-proxy-networks/>

6. Suositukset

Tässä kuussa suosittelemme:

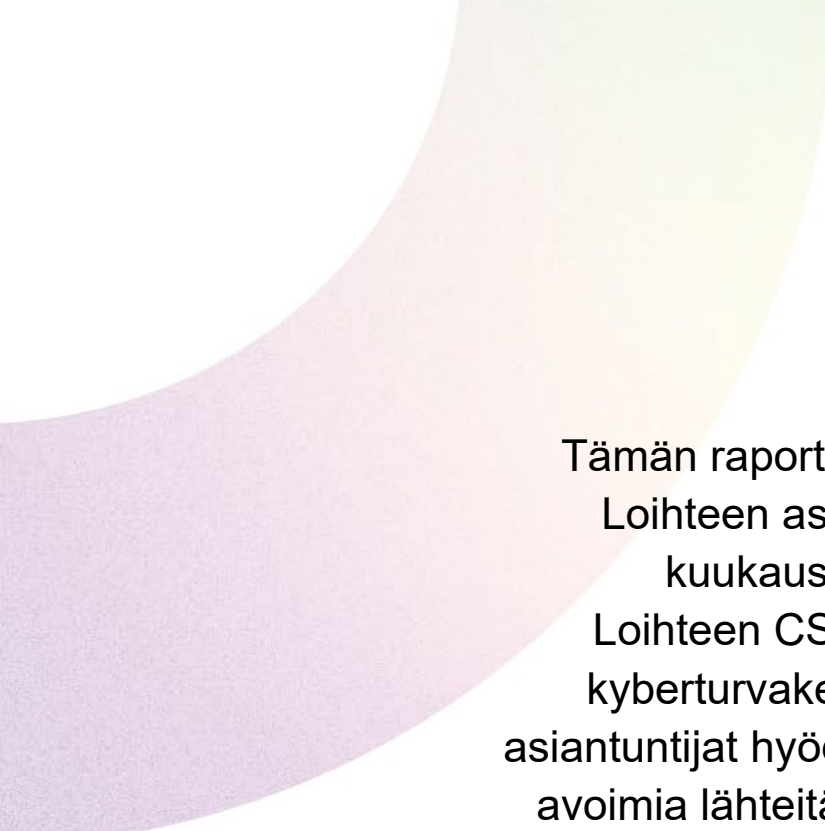
- Reunalaitteiden näkyvyyden rajaaminen julkiverkosta
- Päätelaitesuojauksen käyttöönotto kaikille yhteensopiville laitteille
- Suojaa NTLM-autentikointia käyttävät protokollat

Verkon reunalaitteiden näkyvyyttä julkiverkkoon tulisi rajata niin paljon kuin mahdollista. Erityisesti verkkolaitteiden hallintapaneelisiin liittyvät tietoturva-avoituvuudet ja niiden hyväksikäytöt ovat nousseet rajusti. Haavoittuvuuksia on esiintynyt monien tunnettujen verkkolaitteiden valmistajan ratkaisussa. Näkyvyys esimerkiksi hallintaportaaleihin olisi syytä poistaa julkiverkosta ja rajata ne luotettuihin IP-osoitteisiin. Lisäksi VPN:iin kirjautumiseen tulisi ottaa käyttöön monivaiheinen tunnistautuminen (MFA) kaikille käyttäjille. VPN:t ovat monesti julkiverkkoon näkyvillä, joten ilman MFA:ta uhkatoimijat pystyvät kirjautumaan suoraan organisaation VPN:iin tunnusten vuotaessa.

Suositlemme vahvasti päätelaitesuojauksen (EDR) asentamista kaikille yhteensopiville laitteille. Se on äärimmäisen tärkeä tietoturvakomponentti poikkeamien havaitsemiseen ja pysäyttämiseen päätelaitetasolla. EDR antaa näkyvyyden mm. päätelaitteiden prosesseihin, verkkoyhteyksiin ja muistiin. Lisäksi niissä on monesti sisäänrakennettuina haavoittuvuudenhallintaratkaisua. Ilman EDR:n tuomaa näkyvyyttä uhkatoimijat, kuten kiristyshaittaohjelmatoimijat, pystyvät toimimaan päätelaitteella huomaamatta. Mikäli EDR:n asentaminen jollekin kriittiselle päätelaitteelle luo liian ison riskin esimerkiksi suorituskykyongelmien muodossa, voi harkita päätelaitesuojauksen asettamista ns. monitorointitilaan tai vaihtoehtoisesti tapahtumalokien valvontaa esimerkiksi SIEM:n avulla, jotka kuormittavat laitetta vähemmän. Lisäksi kyseisen päätelaitteen verkkoliikennettä pitää rajata vain tarpeellisiin lähteisiin. EDR:n kokonaan pois jättämistä kannattaa kuitenkin pitää vasta viimeisenä vaihtoehtona.

NTLM-autentikointiprotokolla on edelleen monessa AD-ympäristössä sallittu. Tyypillinen ja hyökkääjille suosittu tapa hyväksikäyttää tätä ovat NTLM relay -hyökkäykset, joita hyväksikäyttäen hyökkääjä voi ottaa haltuun laitteita sekä liikkua lateraalisti verkossa. Esimerkiksi vasta viime kesänä julkaistu haavoittuvuus CVE-2025-33073 mahdollistaa laitteen täyden haltuunoton päivittämättömällä laitteella, jos SMB-allekirjoitusta (SMB signing) ei ole laitteella konfiguroitu vaadituksi. Suosittelemme varmistamaan, että NTLM-autentikointia käyttävät protokollat vaativat allekirjoituksen tai muuten todentavat autentikoinnin lähettävän laitteen oikeellisuuden. Allekirjoitus suositellaan asetettavan vaadituksi SMB- ja LDAP-protokollisiin. Lisäksi LDAP channel binding¹⁸ suositellaan laitettavan päälle. On myös erittäin suositeltavaa varmistaa, että vanha ja epäturvallinen NTLMv1 ei ole hyväksytty protokolla ympäristössä, sillä se kasvattaa relay-hyökkäysten potentiaalia.

¹⁸ TrustedSec, 29.1.2026, LDAP Channel Binding and LDAP Signing, <https://trustedsec.com/blog/ldap-channel-binding-and-ldap-signing>



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.

