LOIHDE

KYBERKATSAUS

1.2025

Tiivistelmä

Tammikuun aikana kyberturvallisuuteen liittyen tapahtui paljon Suomessa ja maailmalla. Verkon reunalaitteissa julkaistiin merkittäviä haavoittuvuuksia ja myös niiden aktiivista hyväksikäyttöä nähtiin tammikuussa. Tämän takia useat yritykset ovat joutuneet päivittämään ja tarkastamaan ympäristöjään potentiaalisen hyväksikäytön vuoksi.

Palomuureihin liittyen keskustelua herätti erityisesti luultavasti vuonna 2022 varastettujen Fortinet FortiGate -palomuurikonfiguraatioiden ilmestyminen pimeään verkkoon. Pimeästä verkosta konfiguraatiot siirtyivät nopeasti tutkittavaksi tietoturva-asiantuntijoiden toimesta ja tammikuun aikana nähtiinkin paljon analyysiä siitä, millaisia vaikutuksia vuoden 2022 konfiguraatioilla voi vuonna 2025 olla.

Suomalaisessa mediassa tietoturvan osalta erityisesti Valion tietomurto ja kiinalainen DeepSeek-yrityksen julkaisema laaja kielimalli nousivat esille ja herättivät keskustelua. Valion tietomurron tutkinnan myötä selvisi, että se koskee aikaisempaa arviota laajempaa joukkoa. Alun perin uutisoitiin tietomurron piirissä olevan noin 5000 henkilöä, mutta tutkinnan myötä määrä on laajentunut jopa 70 000 henkilöön. Kiinalainen kielimalli taas nosti keskustelua tietosuojan ja tietoturvan vuoksi. Lisäksi keskusteluun nousi sen käytön edullisuus.

Suomen lähialueella tilanne on edelleen Venäjän ja länsimaiden välillä kireä. Vuoden 2024 lopun kaapelikatkot eivät jääneet ainoiksi, sillä tammikuun lopussa katkesi Itämerellä jälleen yksi kaapeli. Kaapelin epäillään katkenneen Venäjältä lähteneen laivan toimien vuoksi. Itämeren tilanne ja esimerkiksi Venäjän retoriikka länsimaita kohtaan ei ole vuoden alussa näyttänyt lientymisen merkkejä.

Suomalaisten yritysten näkökulmasta tammikuun tapahtumat alleviivaavat proaktiivisen ja jatkuvasti kehitettävän tietoturvan merkitystä. Tämän lisäksi yritysten on syytä tarkistaa varautumissuunnitelmansa ja varautua esimerkiksi tietoliikenteen ja sähkönjakelun katkoksiin.

KUUKAUSIRAPORTTI 1/2025

Tämä raportti sisältää kuvauksen tammikuun 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.

Sisällys

Tiivistelmä 1
KUUKAUSIRAPORTTI 1/2025 2
1. Yleistilanne 3
2. Haavoittuvuudet 4
2.1 CVE-2024-55591: FortiOS: Authentication bypass in Node.js websocket module 4
2.2 CVE-2025-23006: SonicWall SMA1000 Pre-Authentication Remote Command Execution Vulnerability 4
2.3 CVE-2024-12084: rsync Remote Code Eexecution 4
3. Kalastelu ja huijaukset 5
4. Venäjä ja sitä tukevat ryhmät 6
5. Kiristyshaittaohjelmat ja -toimijat 7
6. Muuta 8
6.1 Kaapelikatkot Itämerellä 8
6.2 FortiGate-palomuurien konfiguraatiotietoja vuodettu 9
7. Suositukset 9

1. Yleistilanne

Suomalaisissa yrityksissä kyberturvallisuuteen liittyvät uhat ovat läsnä päivittäisessä toiminnassa ja näiden vähenemisestä ei ole merkkejä. Suomalaisille yrityksille ja organisaatioille keskeisin uhka 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 kehitystyötä kyberturvallisuuden kehittämiseksi.

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 yritysten on syytä ottaa tämä huomioon omassa toiminnassaan ja riskiarvioissaan.

Suomalaisten yritysten on hyvä huomioida toiminnassaan, että 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.

2. Haavoittuvuudet

Tammikuussa julkaistiin jälleen merkittäviä haavoittuvuuksia. Verkon reunalaitteet ja niiden haavoittuvuudet ovat olleet esillä jo pitkään, eikä tammikuu ollut poikkeus tämän osalta.

2.1 CVE-2024-55591: FortiOS: Authentication bypass in Node.js websocket module

Fortinet julkisti 14.1. FortiOS- ja FortiProxy-tuoteitta koskevan kriittisen haavoittuvuuden. FortiOS on käytössä Fortinetin verkkolaitteissa, kuten FortiGate-palomuureissa, joten haavoittuvuus koskettaa organisaatioita laajalti. Haavoittuvuus CVE-2024-55591 piilee laitteen webhallintaportaalin käyttämässä Node.js-moduulissa, jota hyväksikäyttämällä hyökkääjä voi saada ns. super-admin-tason pääsyn laitteelle.[1]

Haavoittuvuutta on aktiivisesti hyväksikäytetty ja Fortinet on havainnut uhkatoimijoiden mm. luovan uusia admin-tunnuksia sekä paikallisia käyttäjiä haavoittuvuuden kautta. Arctic Wolfin seuraama kampanja on alkanut jo marraskuussa 2024.[2]

2.2 CVE-2025-23006: SonicWall SMA1000 Pre-Authentication Remote Command Execution Vulnerability

Verkkolaitevalmistaja SonicWallin SMA1000-laitteista löydettiin kriittinen RCE-haavoittuvuus CVE-2025-23006. Tieto haavoittuvuudesta julkistettiin 22.1. ja haavoittuvuuteen on kohdistunut jo aktiivista hyväksikäyttöä. Kuten FortiOS-haavoittuvuus, myös tämä vaatii hyökkääjän pääsyä joko Appliance Management Console (AMC)- tai Central Management Console (CMC) -webhallintaportaaliin. Hyväksikäyttö mahdollistaa hyökkääjälle mielivaltaisen koodin suorittamisen etänä. Korjaava päivitys on julkaistu (hotfix) ja se suositellaan asennettavaksi pikimmiten.[3]

2.3 CVE-2024-12084: rsync Remote Code Eexecution

Tiedostojen siirtämiseen yleisesti käytetystä rsync-ohjelmistosta löytyi kriittinen haavoittuvuus. Haavoittuvuus on puskurin ylivuotohaavoittuvuus, jota hyväksikäyttämällä

[1] Fortinet, 14.1.2025, Authentication bypass in Node.js websocket module
[2] Arctic Wolf, 10.1.2025, Console Chaos: A Campaign Targeting Publicly Exposed Management Interfaces on Fortinet FortiGate Firewalls, https://arcticwolf.com/resources/blog/console-chaos-targets-fortinet-fortigate-firewalls/
[3] SonicWall, 22.1.2025, SNWLID-2025-0002, https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002

hyökkääjän on mahdollista suorittaa mielivaltaista koodia etänä kohteena olevalla rsync-palvelimella.[4]

Haavoittuvuus on korjattu versiossa 3.4.0, johon suosittelemme päivittämään. Lisäksi rsync:n kuuntelevan portin (oletuksena TCP-873) rajaamista palomuurilla on syytä harkita.[4]

3. Kalastelu ja huijaukset

Loihde CSOC on havainnut tunnusten kalastelua, jossa on käytetty Microsoft Sharepoint-linkkejä. Kalasteluviestit on pääsääntöisesti lähetetty kohteelle tutusta organisaatiosta. Viestit ovat sisältäneet suojatun linkin Sharepointiin. Vastaanottajan näkökulmasta nämä ovat siis olleet aivan tavallisia sähköposteja, koska viestit ovat saapuneet tutulta lähettäjältä ja ovat sisältäneet linkin lähettävän organisaation Sharepointiin. Varsinainen haitallinen tiedosto on sijainnut lähettävän organisaation Sharepointissa, jolloin vastaanottajan sähköpostisuojaukset eivät ole voineet analysoida ja estää näitä viestejä. Haitallinen tiedosto on sisältänyt linkin, joka on johtanut väärennetylle kirjautumissivulle. Käyttäjän tunnukset on saatu anastettua tämän kirjautumisen avulla. Mainitun kaltaisten viestien vahinkojen minimoimiseksi on tärkeää, että vastaanottaja suhtautuu kriittisesti vastaanottamiinsa sähköpostiviesteihin ja tarvittaessa varmistaa viestin aitouden ennalta määriteltyjä viestintäkanavia pitkin.

Microsoft Threat Intelligence raportoi venäläistaustaisesta Star Blizzard -uhkatoimijasta, joka on WhatsApp:ia hyödyntäen pyrkinyt varastamaan tietoa kohdistetuilla kalasteluviesteillä marraskuussa 2024. Viestejä on kohdistettu tahoihin, jotka ovat kytköksissä hallitukseen, diplomatiaan, turvallisuuspolitiikkaan ja kansainvälisiin suhteisiin. Lähettäjä on esiintynyt Yhdysvaltain hallituksen virkamiehenä ja viesteissä on valheellisesti pyritty saamaan koolle yksityinen WhatsApp-ryhmä, joka koostuisi Ukrainaa tukevista tahoista. Vastaanottajaa on pyydetty liittymään kyseiseen ryhmään viestissä toimitetun QR-koodin avulla. Tämä QR-koodi on ollut tarkoituksellisesti virheellinen ja uhri on houkuteltu vastaamaan viestiin, jolloin hänelle on lähetetty uusi, toimiva QR-koodi. Todellisuudessa tämä QR-koodi on mahdollistanut toimijalle pääsyn käyttäjätilille, jolta QR-koodi luettiin. Toimijan on näin ollen ollut mahdollista anastaa esimerkiksi uhrin WhatsApp-keskustelut. [5]

[4] Sysdig, 17.1.2025, Detecting and mitigating CVE-2024-12084: rsync remote code execution, https://sysdig.com/blog/detecting-and-mitigating-cve-2024-12084-rsync-remote-code-execution/
[5] Microsoft, 16.1.2025, New Star Blizzard spear-phishing campaign targets WhatsApp accounts, https://www.microsoft.com/en-us/security/blog/2025/01/16/new-star-blizzard-spear-phishing-campaign-targets-whatsapp-accounts/

Googlen nimissä on suoritettu edistynyttä tunnusten kalastelua. Kohde on saanut puhelinsoiton, jossa soittajana näkyy Google. Soittaja on ilmoittanut, että kohteen Google-tili on vaarantunut ja he ovat estäneet pääsyn tilille. Kohde on pyrkinyt varmistamaan tämän pyytämällä soittajaa lähettämään sähköpostin Googlen sähköpostiosoitteesta. Soittaja on lähettänyt viestin g[.]co:n alidomainista, joka on Googlen omistama domain. Tämän jälkeen kohdetta on pyydetty nollaamaan Googlen salasana hyväksymällä pyyntö, jonka soittaja on lähettänyt sähköpostitse.[6] Hack Club epäilee, että kyseessä on Google Workspacen bugi, joka mahdollistaa uuden Workspacen luomisen käyttäen mitä tahansa g[.]co:n alidomainia ja sähköpostin lähettämisen tästä domainista.[7]

4. Venäjä ja sitä tukevat ryhmät

Venäjän ja lännen vastakkainasettelussa ei ole tapahtunut tammikuun aikana merkittävää muutosta. Itämeren tilanne on kireä vuoden 2024 lopussa ja vuoden 2025 tammikuussa tapahtuneiden kaapelikatkojen vuoksi ja se näkyy myös Venäjän retoriikassa. Venäläisessä mediassa kaapelikatkoista on pyritty syyttämään Suomea ja muita Pohjoismaita ja niihin liittyviä toimia on luonnehdittu ylilyönneiksi. Samaan aikaan on nostettu esille vaihtoehtoja, joissa Venäjä rupeaisi suojaamaan laivojen kulkua Itämerellä. Tammikuun lopulla nousi esille myös ehdotus siitä, että Suomenlahden nimi vaihdettaisiin Pietarinlahdeksi.[8] Retoriikassa ei sinänsä ole mitään uutta, mutta se kuvastaa selkeästi kireää tilannetta.

Venäläisessä mediassa Suomesta ja länsimaista maalataan tällä hetkellä negatiivista kuvaa. Suomen ja Neuvostoliiton historiaa käsitellään aktiivisesti ja pääsääntöisesti Suomen kannalta negatiivisessa sävyssä. Tätä on perusteltu esimerkiksi sillä, että Venäjä on tähän mennessä halunnut kunnioittaa Suomea ja vaiennut näistä asioista, mutta Suomen ”aggressio ja russofobia” on syy nostaa asiat uudelleen esille.[9] Edellä kuvattujen narratiivien ja näkökulmien esille nostaminen on hyvin perinteinen tapa muokata kuvaa Suomesta ja muista länsimaista. Tällä pyritään luomaan negatiivista ja aggressiivista kuvaa Suomesta.

Informaatiovaikuttamisen lisäksi vaikuttaminen jatkuu myös kyberympäristössä. Näkyvin osa tästä tapahtuu esimerkiksi palvelunestohyökkäysten muodossa. NoName057(16) on jatkanut

[6] Zachlatta GitHub, https://gist.github.com/zachlatta/f86317493654b550c689dc6509973aa4
[7] Hack Club, lainattu 25.1.2025, https://hackclub.com/
[8] Tass, 31.1.2025, Historian Myagkov proposed renaming the Gulf of Finland to St. Petersburg, https://tass.ru/obschestvo/23011629
[9] AIF, 31.1.2025, Alexander Beglov called Finland's policy "overtly hostile", https://spb.aif.ru/politic/aleksandr-beglov-nazval-politiku-finlyandii-neprikryto-vrazhdebnoy

toimintaansa ja tammikuussa nähtiin hyökkäyksiä myös suomalaisia kohteita vastaan.[10] Hyökkäykset ovat pääosin lyhytkestoisia ja niiden vaikutukset jäävät vähäisiksi. Tammikuun lopulla Suojelupoliisi kertoi Venäjän tiedonhankinnan olevan aktiivista Suomessa. Tähän liittyen mainittiin myös, että erityisesti kybertiedustelu on aktiivista ja jatkuvaa. Perinteinen tiedonhankinta on myös käytössä, mutta se on hankaloitunut nykytilanteen vuoksi.[11]

Venäjän pääpainopiste on sekä fyysisen vaikuttamisen että informaatio- ja kybervaikuttamisen osalta Ukrainassa. Vaikuttamista toteutetaan myös muita maita kohtaan ja se tulee jatkumaan myös tulevaisuudessa. Suomalaisten yritysten näkökulmasta on varauduttava siihen, että myös Suomi joutuu vaikuttamisen kohteeksi. Tähän mennessä vaikuttaminen ei ole aiheuttanut merkittävästi haittaa esimerkiksi tietoliikenteeseen tai sähkönjakeluun, mutta viime vuosien trendi on ollut vaikuttamisen kiihtyminen ja edellä mainittuihinkin on syytä varautua.

5. Kiristyshaittaohjelmat ja -toimijat

Codefinger-nimellä tunnettu haittatoimija on alkanut kohdistaa kiristyshaittaohjelma-hyökkäyksiä AWS S3 -resursseihin. Poikkeuksellisen hyökkäyksistä tekee käytetty salaamistapa, joka tapahtuu käyttämällä hyväksi AWS S3:n sisäänrakennettua salausominaisuutta käyttäjän omilla salausavaimilla. Hyökkäyksissä käytetään hyväksi vuodettuja AWS-tunnuksia, joilla on kirjoitus- ja lukuoikeus S3-resursseihin. Tunnuksen oikeuksilla haittatoimija lisää oman salausavaimensa, jota AWS ei säilytä, eikä se lokitu kokonaisuudessaan mihinkään lokiviestiin. Käytännössä salauksen purku on mahdotonta ilman hyökkääjän käyttämää avainta. Vaikka hyökkäykset ovat kohdistuneet AWS:ään, on sama mahdollista myös muissa pilviympäristöissä, kuten Azuressa. [12]

Helsingin Sanomat uutisoi Valion joulukuisen tietomurrossa käytetyn tunnuksen vuotaneen Vincitin työntekijän henkilökohtaiselta tietokoneelta. Haittatoimija ehti salaamaan parikymmentä palvelinta ennen haittatoimijan pääsyn poistamista ympäristöstä. Haittatoimija sai kopioitua huomattavan määrän henkilötietoja, joka teoriassa mahdollistaa myös

[10] NoName057(16), Telegram
[11] MTV, 31.1.2025, Supo paljastaa: Näin Putinin kätyrit vakoilevat Suomessa – uusi laki ei olisi Kremlin mieleen, https://www.mtvuutiset.fi/artikkeli/supo-haluaa-uuden-vakoilulain-kohteena-venajan-katyrit-suomessa/9091762
[12] Halcyon, 13.1.2025, Abusing AWS Native Services: Ransomware Encrypting S3 Buckets with SSE-C, https://www.halcyon.ai/blog/abusing-aws-native-services-ransomware-encrypting-s3-buckets-with-sse-c

yksityishenkilöiden kiristämisen lunnailla. Yksikään haittatoimija ei ole julkisesti ilmoittanut olevansa tietomurron takana. [13]

Kiristyshaittatoimijat ovat alkaneet asentamaan yhä enemmän takaportteja suoraan VMware ESXi:lle. Yksi yleistynyt takaportti on SSH-tunnelin luonti ESXi-palvelimelta haittatoimijan palvelimelle. Todennäköisesti syy tälle on ESXi-palvelinten huonompi valvonta verrattuna esimerkiksi Windows- ja Linux-palvelimiin, koska ESXi:lle ei ole mahdollista asentaa mm. EDR-sovelluksia. [14]

Joulukuu oli kiireisin kuukausi kiristyshaittaohjelmatapausten määrän perusteella. NCC Groupin laskujen mukaan tapauksia oli 574 kappaletta ja niistä 18 % olivat Funksec-toimijan nimissä tehtyjä. Tapauksista 52 % kohdistui Pohjois-Amerikkaan ja 18 % Eurooppaan. [15]

6. Muuta

6.1 Kaapelikatkot Itämerellä

Itämerellä katkesi 26.1. jälleen merenalainen tietoliikennekaapeli. Katkoskohta sijaitsee Gotlannin saaren ja Latvian Ventspilsin kaupungin välillä. Katkoskohta on Ruotsin talousalueella. Tapahtuneen takia Latvian merivoimat tarkasti lähellä seilanneen Michalis San -aluksen, joka on rekisteröity Maltalle. Alukselta ei kuitenkaan löydetty viitteitä epäilyttävästä toiminnasta.[16]

YLE uutisoi 31.1, että Latvian poliisi on pyytänyt Silver Dania -nimisen, norjalaisomisteisen ja Norjaan rekisteröidyn laivan pidättämistä. Norjan viranomaiset pysäyttivät laivan 31.1. lähellä Tromssaa. Laivan miehistö on venäläinen.[17]

[13] Helsingin Sanomat, 9.1.2025, Valion laajan tietomurron syy selvisi, https://www.hs.fi/suomi/art-2000010952135.html
[14] Sygnia, 21.1.2025, ESXi Ransomware Attacks: Stealthy Persistence through SSH Tunneling, https://www.sygnia.co/blog/esxi-ransomware-ssh-tunneling-defense-strategies/
[15] NCC Group, 22.1.2025, NCC Group Monthly Threat Pulse – Review of December 2024, https://www.nccgroup.com/us/newsroom/ncc-group-monthly-threat-pulse-review-of-december-2024/
[16] MTV, 26.1.2025, Uusi kaapelirikko Itämerellä: Maltalaisalus tarkastettu Gotlannin lähellä, https://www.mtvuutiset.fi/artikkeli/juuri-nyt-uusi-kaapelirikko-itamerella/9089444
[17] YLE, 31.1.2025, Norja takavarikoi venäläismiehistöisen laivan – epäillään kaapelin vaurioittamisesta, https://yle.fi/a/74-20140643

6.2 FortiGate-palomuurien konfiguraatiotietoja vuodettu

Belsen Group-niminen uusi uhkatoimija julkaisi 14.1. pimeässä verkossa yli 15000:n FortiGate-palomuurin konfiguraatiot, IP-osoitteet ja VPN-tunnukset. Arkiston 1.6:n gigatavun kokoinen sisältö on lajiteltu maittain. Jokaisen maan kansiossa on myös oma kansio jokaiselle palomuurille, ja kansion nimeksi on annettu kyseisen palomuurin julkinen IP-osoite. [18] Tietoturva-asiantuntija ja bloggari Kevin Beaumont epäilee, että varastetut tiedot ovat peräisin vuonna 2022 hyväksikäytetystä FortiGaten haavoittuvuudesta CVE-2022-40684.[19] Vuodetut tiedot paljastavat tarkkoja tietoja organisaatioiden verkoista ja vuodettuja salasanoja voidaan väärinkäyttää, mikäli niitä ei vaihdeta. Analyysimme perusteella vuodettujen tietojen joukossa on myös suomalaisten organisaatioiden tietoja.

7. Suositukset

Tässä kuussa suosittelemme:

1. API-rajapintojen suojaaminen
2. Ajantasainen laitelistaus
3. Active Directoryn auditointi

Nykyään lähes jokaisessa sovelluksessa on API-rajapinta sen koneellista käyttöä ja hallintaa varten. Tämän takia ne ovat myös kiinnostavia kohteita uhkatoimijoille. Organisaation käyttämien API-rajapintojen avainten ja tunnusten hallintaan on syytä panostaa. Tyypillisesti API-tunnusten oikeudet sekä elinikä voivat olla liian laajat, ja tämä voi mahdollistaa hyökkääjälle kiinnostavan hyökkäysvektorin unohdettujen ja tarpeettomien tunnusten kautta. API-avainten ja salaisuuksien säilyttämiseen on myös syytä kiinnittää huomiota, sillä niiden löytyminen mm. julkisesti Githubista kovakoodattuna koodiin on harmillisen yleistä. API:n käytön auditointi ja sen valvominen on oleellista näiden havaitsemiseksi.

Organisaatioilla tulisi olla ajankohtainen laitelistaus ja prosessi sen ylläpitämiseen.[20] Työasemien ja palvelinten kohdalla voidaan käyttää keskitettyä hallintaa, esimerkiksi EDR-tuotetta tai Microsoft Intunea. Kaikkia laitteita ei kuitenkaan voida seurata näitä järjestelmiä

[18] Bleeping Computer, 15.1.2025, Hackers leak configs and VPN credentials for 15,000 FortiGate devices, https://www.bleepingcomputer.com/news/security/hackers-leak-configs-and-vpn-credentials-for-15-000-fortigate-devices/?utm_source=flipboard&utm_content=topic%2Fcybersecurity
[19] Kevin Beamont, 16.1.2025, 2022 zero day was used to raid Fortigate firewall configs. Somebody just released them., https://doublepulsar.com/2022-zero-day-was-used-to-raid-fortigate-firewall-configs-somebody-just-released-them-a7a74e0b0c7f
[20] PaloAlto Networks, lainattu 26.1.2025, What is IT Asset Inventory?, https://www.paloaltonetworks.com/cyberpedia/what-is-it-asset-inventory

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, niin sen suojaaminen on erittäin haastavaa.

Samaan tapaan kuin laitelistausta on pidettävä ajan tasalla, on myös tärkeää olla kartalla Active Directory -ympäristön tilanteesta. Esimerkiksi kiristyshaittaohjelmahyökkäyksissä hyödynnetään monesti tunnuksia, joilla on liian laajat käyttöoikeudet organisaation ympäristöön. Erityisesti palvelutunnukset (Service account) ovat uhkatoimijoiden suosiossa, koska näillä on monesti liian laajat oikeudet, kuten Domain Administrator -oikeudet. Näiden tunnusten käyttöoikeuksia olisi suositeltavaa rajata niin, että niillä on vain tarvittavat oikeudet. Huomioon tulisi ottaa mm. käyttöoikeudet ja käytöstä poistuneet, korkeat käyttöoikeudet omaavat tunnukset, jotka ovat edelleen olemassa AD:ssa.[21] Nämä ovat osa AD:n laajempaa tietoturvakatselmointia, joita organisaatioiden kannattaa suorittaa. Mm. Microsoftilla on laaja dokumentaatio aiheesta.[22] Auditointeihin löytyy paljon ilmaisia ja kaupallisia ohjelmistoja, kuten esimerkiksi PingCastle[23] ja PurpleKnight [24]. Hyvin hoidettu AD-ympäristö on yksi tehokkaimmista tavoista rajoittaa ja estää hyökkääjän liikehdintää ja toimia verkossa.

[21] Microsoft, Attractive Accounts for Credential Theft, https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/attractive-accounts-for-credential-theft
[22] Microsoft, Best Practices for Securing Active Directory, https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
[23] Pingcastle, https://www.pingcastle.com/
[24] Purple Knight, https://www.semperis.com/purple-knight/

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.

Lue lisää:
www.loihde.com/palvelut/kyberturva/

LOIHDE