

LOIHDE

KYBERKATSAUS

10.2024

Tiivistelmä

Kuukauden aikana on jälleen tapahtunut paljon kyberturvallisuuteen liittyen. Organisaatioiden uhkana ovat pääosin taloudellisesti motivoituneet rikolliset, mutta myös haktivistit ja valtiolliset toimijat. Hyökkäyksissä hyödynnetään esimerkiksi kalastelua ja verkon reunalaitteiden haavoittuvuuksia, Lokakuun aikana nähtiinkin esimerkiksi Fortinetin tuotteen 0-päivähaavoittuvuuden laajaa hyväksikäyttöä. Hyökkäysten torjuminen ja havaitseminen vaatii puolustajilta näkyvyyttä, riittäviä työkaluja ja kykyä nopeaan reagointiin.

Lokakuun aikana kalastelu ja huijaukset ovat jatkuneet totutulla tasolla. Kalastelun tavoitteena on yleensä saada pääsy yrityksen ympäristöön, jonka jälkeen voidaan toteuttaa esimerkiksi tiedon varastaminen, jalansijan laajentaminen tai laskutushuijaus. Kalastelua kohdistuu myös yksityisiin henkilöihin, jolloin tavoitteena on yleensä maksujen tai maksutietojen varastaminen.

Kuun aikana on tapahtunut kiristyshaittaohjelmahyökkäyksiä myös suomalaisiin organisaatioihin. Hyökkäykset tulevat mitä luultavimmin jatkumaan niin kauan, kun saavutettavissa oleva taloudellinen hyöty säilyy nykyisellä tasolla. Kiristyshaittaohjelmat ovat merkittävä uhka organisaatioille ja niiltä välttyminen vaatii jatkuvaa työskentelyä tietoturvan kehittämiseksi. Uhkatoimijat pyrkivät jatkuvasti löytämään uusia menetelmiä hyökkäysten toteuttamiseksi ja näin ollen yritystenkin on kyettävä kehittämään suojaustaan jatkuvasti.

Venäjä jatkaa vaikuttamista disinformaation, kyberoperaatioiden ja fyysisten toimien avulla länsimaissa. Venäjän toiminnan pääpainopiste on edelleen Ukrainassa, mutta se pyrkii vaikuttamaan länsimaihin resurssiensa puitteissa myös muualla. Venäjän keinovalikoima vaikuttamisen suhteen on joustava ja on oletettavaa, että jo nähtyjen lisäksi uusia keinoja vaikuttamisen osalta tullaan näkemään lähitulevaisuudessa.

Syksyn aikana pankkeihin on kohdistunut palvelunestohyökkäyksiä, jotka ovat näkyneet käyttäjille katkoksin. Palvelunestohyökkäyksistä on käyty myös aktiivisesti keskustelua mediassa, koska katkokset ovat olleet laajoja ja aiheuttaneet paljon haasteita organisaatioille. Hyökkäykset ovat olleet intensiivisiä ja niihin on käytetty esimerkiksi pohjoismaisia laitteita. Hyökkäykset ovat nyt keskittyneet pankkisektorille, mutta tulevaisuudessa on erittäin todennäköistä, että ne kohdistuvat myös muihin yhteiskunnan osa-alueisiin.

KUUKAUSIRAPORTTI 10/2024

Tämä raportti sisältää kuvauksen lokakuun 2024 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 10/2024	2
1. Yleistilanne	3
2. Haavoittuvuudet	4
2.1 Cisco	4
2.2 FortiManager FG-IR-24-423 (CVE-2024-47575)	4
2.3 VMWare vCenter	5
3. Kalastelu ja huijaukset.....	6
4. Venäjä ja sitä tukevat ryhmät	7
5. Kiristyshaittaohjelmat ja -toimijat	8
6. Muuta	9
7. Suositukset.....	10

1. Yleistilanne

Suomalaisissa yrityksissä kyberturvallisuuteen liittyvät uhat ovat läsnä päivittäisessä toiminnassa ja niiden 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.

Venäjän ja länsimaiden vastakkainasettelu on näkynyt uutisissa ja erilaisina poikkeamina kesän ja syksyn aikana. Suomen ja Itämeren alueen osalta keskeisimpänä ovat näkyneet esimerkiksi rajaloukkaukset merellä ja ilmassa sekä Venäjällä tapahtuva vihamielinen uutisointi Suomeen liittyen. Samoja ilmiöitä on ollut havaittavissa myös kyber- ja informaatiotilassa esimerkiksi palvelunestohyökkäysten ja informaatiovaikuttamisen muodossa. Tämä vastakkaisasettelu onkin syytä ottaa huomioon toiminnassa ja riskiarvioissa.

Suomalaisten toimijoiden 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

Lokakuun aikana julkaistiin useita haavoittuvuuksia, joiden vakavuus CVSS-asteikolla on kriittinen. Useat näistä haavoittuvuuksista kohdistuivat tuotteisiin tai palveluihin, jotka ovat laajalti käytössä. Seuraavat kolme on nostettu esille niiden merkittävyyden ja vakavuuden vuoksi.

2.1 Cisco

Cisco julkaisi lokakuussa useita kriittisiä haavoittuvuuksia tuotteissaan: Cisco ASA(CVE-2024-20329)¹, Firepower(CVE-2024-20412) ja Secure Firewall(CVE-2024-20424)². Näiden kaikkien osalta on julkaistu päivitykset, joissa haavoittuvuus on korjattu. Kaikki kolme haavoittuvuutta ovat kriittisiä, mutta näistä vain CVE-2024-20412:n hyväksikäyttö on mahdollista ilman autentikoitumista. Haavoittuvuus johtuu staattisten käyttäjätunnusten kovakoodatuista salasanoista, jotka ovat löydettävissä palvelusta. Hyväksikäyttö onnistuu kirjautumalla CLI:n kautta näillä tunnuksilla. Tämän jälkeen hyökkääjä voi suorittaa toimiaan järjestelmässä ja esimerkiksi varastaa tietoja.³

2.2 FortiManager FG-IR-24-423 (CVE-2024-47575)

Fortinetin palomuurien hallintaan tarkoitetussa tuotteessa, FortiManagerissa, havaittiin 0-päivähaavoittuvuus. Haavoittuvuuden avulla hyökkääjä on kyennyt suorittamaan mielivaltaista koodia etänä ilman autentikoitumista. Haavoittuvuus mahdollistaa hyökkääjälle esimerkiksi tietojen varastamisen ja konfiguraatioiden muokkaamisen.⁴

Fortinet ilmoitti rajatulle joukolle haavoittuvuudesta ja sen hyväksikäyttöön liittyvistä indikaattoreista ennen haavoittuvuuden julkaisemista. Fortinet viesti ylläpitäjille haavoittuvuuden hyväksikäytön estämiseen liittyen ja jakoi lisäksi tietoa haavoittuvuuden hyväksikäytön havaitsemisesta. Asiasta liikkui myös huhuja ja esimerkiksi aktiivisesta hyväksikäytöstä kirjoitettiin jo ennen haavoittuvuuden julkaisua. Lisäksi Fortinetin toimintaa

¹ Cisco, 23.10.2024, Cisco Adaptive Security Appliance Software SSH Remote Command Injection Vulnerability, <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssh-rce-gRAuPEUF>

² Cisco, 23.10.2024, Cisco Secure Firewall Management Center Software Command Injection Vulnerability, <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inj-v3AWDqN7>

³ Cisco, 23.10.2024, Cisco Firepower Threat Defense Software for Firepower 1000, 2100, 3100, and 4200 Series Static Credential Vulnerability, <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-statcred-dFC8tXT5>

⁴ Kyberturvallisuuskeskus, 23.10.2024, Fortinetin FortiManager-tuotteessa kriittinen haavoittuvuus, https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_25/2024

haavoittuvuuden julkaisematta jättämisen suhteen kritisoitiin.⁵ Haavoittuvuus CVE-2024-47575 julkaistiin lopulta Fortinetin toimesta 23.10.2024.⁶ Tässä vaiheessa haavoittuvuuden hyväksikäyttö oli jo laajalti tiedossa ja käynnissä.

Haavoittuvuuteen liittyen on havaittu massamaista hyväksikäyttöä, jossa hyökkääjä on liittänyt kohdelaitteelle uuden Fortimanagerin. Tämän lisäksi hyökkääjä on luonut *tgz*-tiedoston, johon on kerätty kohdelaitteen hallinnassa olevien palomuurien konfiguraatiot. Nämä tiedot on tämän jälkeen varastettu hyökkääjän toimesta. Hyökkäyksen toteuttajasta on erilaisia spekulatioita, mutta esimerkiksi Mandiant seuraa toimijaa uutena ryhmänä nimellä UNC5820.⁷

2.3 VMWare vCenter

VMware vCenter Server -tuotteessa julkaistiin syyskuussa kaksi kriittistä haavoittuvuutta: CVE-2024-38812 ja CVE-2024-38813. Haavoittuvuuksista uutisoitiin ja niihin liittyen julkaistiin päivitykset.⁸ Haavoittuvuus CVE-2024-38812 on muistin ylivuotohaavoittuvuus ja CVE-2024-38813 on oikeuksien korottamiseen liittyvä haavoittuvuus. Haavoittuvuuksien hyväksikäytön kautta hyökkääjällä on mahdollisuus suorittaa etänä koodia hyväksikäytön kohteessa. Haavoittuvuuksien hyväksikäytöstä ei ole ollut havaintoja niiden julkaisuajankohtana.⁹

Broadcom julkaisi 21.10. korjaavan päivityksen edellä mainittuihin haavoittuvuuksiin liittyen. Julkaistun päivityksen yhteydessä todetaan, että syyskuussa julkaistu päivitys ei korjannut tarvittavilta osin haavoittuvuutta CVE-2024-38812.¹⁰

⁵ Kevin Beamont, 22.10.2024, Burning Zero Days: FortiJump FortiManager vulnerability used by nation state in espionage via MSPs, <https://doublepulsar.com/burning-zero-days-fortijump-fortimanager-vulnerability-used-by-nation-state-in-espionage-via-msp-c79abec59773>

⁶ FortiGuard Labs, 23.10.2024, Missing authentication in fgmsd, <https://www.fortiguards.com/psirt/FG-IR-24-423>

⁷ Mandiant, 24.10.2024, Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575), <https://cloud.google.com/blog/topics/threat-intelligence/fortimanager-zero-day-exploitation-cve-2024-47575/>

⁸ Bleeping Computer, 17.9.2024, Broadcom fixes critical RCE bug in VMware vCenter Server, <https://www.bleepingcomputer.com/news/security/broadcom-fixes-critical-rce-bug-in-vmware-vcenter-server/>

⁹ Bleeping Computer, 22.10.2024, VMware fixes bad patch for critical vCenter Server RCE flaw, <https://www.bleepingcomputer.com/news/security/vmware-fixes-bad-patch-for-critical-vcenter-server-rce-flaw/>

¹⁰ Broadcom, 21.10.2024, VMSA-2024-0019:VMware vCenter Server updates address heap-overflow and privilege escalation vulnerabilities (CVE-2024-38812, CVE-2024-38813), <https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24968>

3. Kalastelu ja huijaukset

Useimpien käyttäjien siirtyessä käyttämään verkkopankkia mobiililaitteilla myös haittatoimijat kehittävät haittaohjelmia yhä enemmän mobiililaitteille, pääasiassa Androidille. Esimerkiksi viimeisin TrickMo-pankkitroijalainen kykenee mm. hallitsemaan saastunutta laitetta etänä ja myös kaappaamaan laitteen PIN-koodin, jonka avulla laitteen lukitus voidaan avata haittatoimijan toimesta.¹¹

Suomalaisiin verkkopankkeihin kohdistettuja pankkitroijalaisia on vielä vähän, mutta osa pankeista on alkanut jo nyt estää verkkopankin käytön, jos laitteelta löytyy mm. accessibility serviceä käyttäviä sovelluksia¹². Accessibility service on tarkoitettu Androidilla avustamaan laitteen esteettömyydessä, mutta sen antamia oikeuksia käytetään hyväksi myös haittaohjelmissa.

Matkailualalla on syys- ja lokakuussa tullut esille tapauksia, joissa kalastelun avulla on päästy käsiksi matkanjärjestäjän asiakkaiden tietoihin. Tämän jälkeen hyökkääjä on pyrkinyt hyötymään tilanteesta taloudellisesti ottamalla yhteyttä asiakkaisiin. Molemmissa uutisissa olleissa tapauksissa hyökkäys on tapahtunut onnistuneen kalastelun kautta. Työntekijän syötettyä tunnuksensa kalastelijan linkin kautta, on hyökkääjä päässyt käsiksi asiakkaiden tietoihin.^{13 14 15}

¹¹ Zimperium, 11.10.2024, Expanding the Investigation: Deep Dive into Latest TrickMo Samples, <https://www.zimperium.com/blog/expanding-the-investigation-deep-dive-into-latest-trickmo-samples/>

¹² Io-tech, 21.9.2024, Danske Bankin ja Nordean sovellukset kieltäytyvät toimimasta liikaa oikeuksia hamuavien tuntemattomista lähteistä asennettujen sovellusten rinnalla, <https://bbs.io-tech.fi/threads/danske-bankin-ja-nordean-sovellukset-kieltäytyvat-toimimasta-liikaa-oikeuksia-hamuavien-tuntemattomista-lahteista-asennettujen-sovellusten-rinnalla.559773/>

¹³ Yle, 28.10.2024, Visit Inarin asiakkailta huijattu satoja euroja – huijarit pääsivät järjestelmään Googlen kalastelulinkin kautta, <https://yle.fi/a/74-20120774>

¹⁴ Yle, 14.10.2024, Arctic SnowHotel & Glass Igloos kertoo mahdollisesta tietovuodosta, <https://yle.fi/a/74-20117901>

¹⁵ Visit Inari, 28.10.2024, Tärkeää: Tiedote tietomurrosta, <https://visitinari.fi/fi/tuoreimmat-uutiset/>

4. Venäjä ja sitä tukevat ryhmät

Venäjän ja lännen vastakkainasettelu jatkuu eikä lientymistä ole havaittavissa. Venäjä näkee länsimaat ja erityisesti NATO-jäsenet vastustajinaan. Länsimaat ovat pitäneet kiinni sanktioista ja pakotteista, joita Venäjää vastaan on asetettu Ukrainan sodan vuoksi. Suomen ja Venäjän välinen raja pysyy suljettuna. Länsimaat jatkavat tukeaan Ukrainalle.

Venäjä käyttää epäystävällisiksi katsomiaan maita kohtaan erilaisia vaikuttamisen keinoja. Näitä ovat esimerkiksi informaatiovaikuttaminen, kyberhyökkäykset ja infrastruktuuriin kohdistuvat iskut. Suomen osalta on viimeisen kahden vuoden aikana nähty kaikkia edellä mainittuja. Osa vaikuttamisesta on suoraa, kuten Kremlin viralliset lausunnot ja toimet. Osa taas on peiteltyä, kuten jatkuvat, haktivistien suorittamat palvelunestohyökkäykset tai kiinalaisen rahtialuksen katkaisema merenalainen putki.

Lokakuun aikana Venäjää koskevissa uutisissa on korostunut Ukrainaan liittyvät tapahtumat. Erityisesti esillä ovat olleet Venäjän Belgorodin alue¹⁶, jonka Ukraina on vallannut, sekä Venäjän ja Pohjois-Korean yhteistyö. Pohjois-Korea on useiden lähteiden mukaan lähettänyt joukkoja Venäjän tueksi. Tämänhetkisten tietojen mukaan joukkoja koulutetaan nyt Venäjällä.¹⁷ Samaan aikaan Venäjän on uutisoitu myös tukeneen hutheja heidän hyökkäyksissään rahtialuksia vastaan.¹⁸

Uutisissa on ollut esillä myös suomalainen disinformaatiota levittävä Johan Bäckman, joka on saanut Venäjän kansalaisuuden.¹⁹ Bäckman on viimeisen kymmenen vuoden ajan tuottanut päätoimisesti disinformaatiota sekä Venäjällä, Suomessa, että vallatuilla ukrainalaisalueilla.²⁰

Uutisissa on käsitelty myös Suomen tekemiä venäläisten omistusten takavarikoiteja. Omaisuutta on takavarikoitu sekä yksityisiltä henkilöiltä että erilaisilta organisaatioilta, viimeisimpänä valtion omistuksia. Venäjän viranomaiset ovat myös ottaneet asiaan kantaa ja syyttäneet Suomea lainvastaisesta toiminnasta.²¹

¹⁶ The New York Times, War May Be Distant in Moscow, but in One Russian Border City, It's Real, <https://www.nytimes.com/2022/09/14/world/europe/russia-ukraine-border-belgorod.html>

¹⁷ Reuters, 29.10.2024, No new limits on Ukraine's use of US arms if North Korea joins Russia's fight, Pentagon says, <https://www.reuters.com/world/europe/nato-chief-says-he-can-confirm-north-korean-troops-are-russias-kursk-2024-10-28/>

¹⁸ The Wall Street Journal, 24.10.2024, Russia Provided Targeting Data for Houthi Assault on Global Shipping, https://www.wsj.com/world/russia-provided-targeting-data-for-houthi-assault-on-global-shipping-eabc2c2b?mod=latest_headlines

¹⁹ Kommersant, 21.10.2024, Putin Grants Citizenship to 'First Political Refugee from the US' John Robles, <https://www.kommersant.ru/doc/7247853>

²⁰ Helsingin Sanomat, 10.7.2022, Venäjän uskollinen mediasoturi, <https://www.hs.fi/feature/art-2000008893252.html>

²¹ Helsingin Sanomat, 28.10.2024, Suomi alkoi takavarikoida Venäjän valtion omaisuutta: Yksi kohteista tontti Töölössä, <https://www.hs.fi/visio/art-2000010791415.html>

Kybertoimintaympäristöön liittyen TAG ja Mandiant ovat julkaisseet artikkelin Ukrainaa vastaan toteutetusta tiedustelu- ja vaikuttamisoperaatiosta, jossa Venäjään liittyvä uhkatoimija on levittänyt Android- ja Windows-haittaohjelmia Telegram-viestintäsovelluksen välityksellä. Ohjelmaa markkinoitiin viestipalvelussa potentiaalisille varusmiehille, jotta he voisivat jakaa rekrytointipisteisiin liittyviä tietoja. Ohjelman asentaminen Google Play Storen ulkopuolelta aiheutti laitteen saastumisen. Viestipalvelussa jaettiin myös materiaalia vaikuttamistarkoituksessa ja sen kautta pyrittiin häiritsemään liikekannallepanoa ja horjuttamaan puolustustahtoa. Tämä on hyvä esimerkki operaatiosta, jossa käytetään monia eri keinoja vaikuttamisen työkaluina.²²

5. Kiristyshaittaohjelmat ja -toimijat

Kyberturvallisuuskeskus julkaisi статистиikkaa heille tietoon tulleista kiristyshaittaohjelmaryhmistä. Muuhun maailmaan verrattuna Suomessa selvästi aktiivisin ryhmä on Akira, joka on tehnyt jopa 40 % vuoden 2023 kiristyshaittaohjelmatapauksista. Tapausten määrää todennäköisesti selittää 2023 aktiivisesti hyväksikäytetty Cisco ASA:n haavoittuvuus CVE-2023-20269. Toiseksi aktiivisin ryhmä Suomessa oli LockBit 13 % osuudella. Muualla maailmassa aktiivisin oli LockBit (26 %) ja BlackCat (11 %).²³

LockBitin verkkosivusto ja muu infra kaapattiin osana monikansallista poliisioperaatio Chronosta helmikuussa 2024. Operaatiossa saatua tietoa on käyty läpi eri organisaatioiden toimesta ja UK:n National Crime Agency julkaisi teknisiä lisätietoja alustan toiminnasta. Kiinnostavimpana tietona NCA listasi, kuinka LockBit oli toteuttanut varastettujen tietojen poistamisen lunnaiden maksamisen jälkeen. Tietojen poistaminen vaati manuaalisia toimia LockBitin ylläpitäjiltä, ja käytännössä yhdenkään organisaation tietoja ei ole poistettu 2022 jälkeen, vaikka lunnaat olisi maksettu.²⁴

²² Google Cloud, 28.10.2024, Hybrid Russian Espionage and Influence Campaign Aims to Compromise Ukrainian Military Recruits and Deliver Anti-Mobilization Narratives, <https://cloud.google.com/blog/topics/threat-intelligence/russian-espionage-influence-ukrainian-military-recruits-anti-mobilization-narratives>

²³ Kyberturvallisuuskeskus, 27.9.2024, Akira- ja Lockbit-kiristyshaittaohjelmat valokeilassa, <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/akira-ja-lockbit-kiristyshaittaohjelmat-valokeilassa>

²⁴ Databreaches, 1.10.2024, Did LockBit really delete your data if you paid them? Nope, and even the affiliates didn't know that?!, <https://databreaches.net/2024/10/01/did-lockbit-really-delete-your-data-if-you-paid-them-nope-and-even-the-affiliates-didnt-know-that/>

6. Muuta

Syksyn aikana on nähty laajoja katkoksia pankkipalveluissa, joiden on kerrottu johtuneen palvelunestohyökkäyksistä. Katkokset ovat aiheuttaneet haasteita sekä yksityisille käyttäjille, että organisaatioille. Erityisesti katkoksista on uutisoitu Nordean palveluissa. Pääosin kyse on ollut palveluiden saatavuudessa, mutta ongelmia on ilmennyt myös tilien näkyvyydessä. Nordea on kertonut hyökkäysten olleen erityisen intensiivisiä ja niiden tulevan myös pohjoismaisista IP-osoitteista. Samassa yhteydessä kerrottiin, että pääosa hyökkäyksistä on saatu torjuttua, mutta silti palveluissa on esiintynyt katkoksia.²⁵

Asia on herättänyt paljon keskustelua ja sitä on käsitelty myös eduskunnassa. Talousvaliokunta kuuli esimerkiksi Nordean, Suojelupoliisin ja Kyberturvallisuuskeskuksen puheenvuoroja lokakuun puolivälissä asiasta.²⁶ Lisäksi Kyberturvallisuuskeskus julkaisi tietoa palvelunestohyökkäysten tilanteesta ja muodoista Suomessa.²⁷ Koska hyökkäyksiä on tehty ilmeisesti hyödyntäen kodin laitteita, on Suojelupoliisin vuoden takainen ohje vahvistaa kodin tietoturvaa nostettu myös ajankohtaisena esille eri tilanteissa.²⁸

On oletettavaa, että palvelunestohyökkäykset tulevat jatkumaan osana vaikuttamisen keinoja, joten on syytä pyrkiä varmistamaan toiminnan jatkuvuus niistä huolimatta. Yksityisten henkilöiden on lisäksi syytä harkita varautumista esimerkiksi vaihtoehtoisen tunnistautumismenetelmän ja käteisen avulla.

²⁵ Helsingin Sanomat, 15.10.2024, Nordea: Verkko-hyökkäysten voima ja kesto täysin ennen-näkemätön, tarkoitus horjuttaa yhteiskuntaa, <https://www.hs.fi/talous/art-2000010761540.html>

²⁶ Helsingin Sanomat, 16.10.2024, Eduskunnan talous-valiokunta käsitteli turva-tiloissa Nordeaan kohdistuvaa hyökkäystä, <https://www.hs.fi/politiikka/art-2000010766558.html>

²⁷ Kyberturvallisuuskeskus, 10.10.2024, Palvelunestohyökkäystilanne Suomessa, <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaystilanne-suomessa>

²⁸ Yle, 12.10.2023, Supo varoitti reitittimien tietoturvauhasta – tarkista kotona ainakin nämä kuusi asiaa kuntoon, <https://yle.fi/a/74-20054897>

7. Suositukset

Tässä kuussa suosittelemme:

1. Varautumaan poikkeaman selvittämiseen ja DFIR-kumppanin kontaktointiin
2. Vahvan autentikoinnin käyttöönottoa kriittisiin palveluihin ja kriittisille käyttäjille
3. Lokitustason tarkistamista ja tarvittaessa laajentamista

Tietomurtoon varautuminen on tärkeää tehdä mahdollisimman hyvin ennen kuin mitään on tapahtunut, joten viime kuun suosituksemme kontaktoida potentiaalista DFIR-yhteistyökumppania säilyy myös tässä kuussa. Tämän lisäksi suosittelemme käymään läpi ja päivittämään suunnitelmat, jotka liittyvät poikkeamiin varautumiseen. Digipoolin DFIR-jaos on julkaissut ennakointiin, havainnointiin ja palautumiseen liittyen työkaluja. Suosittelemme tutustumaan myös näihin ja arvioimaan oman varautumisen tasoa näihin peilaten.²⁹

Suositlemme myös FIDO2:n tai muun vahvan autentikoinnin käyttämistä kriittisille palveluille ja käyttäjille. Pilviympäristöissä yleisin tapa kaapata tunnuksia on kalastelusivustot, jotka ohjaavat kirjautumisen proxy-palvelimen kautta. Tämän avulla perinteinen MFA saadaan kaapattua. Kalastelun riskiä voidaan pienentää ottamalla käyttöön kriittisille käyttäjille FIDO2-tasoisin kirjautumismenetelmä. Tällainen on esimerkiksi Yubikey tai Windows Hello for Business. Kriittiset käyttäjät vaihtelevat organisaatioittain, mutta hyvänä lähtökohtana voi käyttää sisäpiiriläisiä, ylläpitäjiä ja talousasioiden kanssa tekemisissä olevia.

Suositlemme tarkistamaan lokitustason ja lokien säilöntäajan sekä lokittamaan mahdollisuuksien mukaan kaikkia keskeisiä järjestelmiä. Lisäksi suosittelemme keräämään lokit keskitettyyn paikkaan, esimerkiksi SIEM-palveluun, vähintään kriittisten järjestelmien osalta. Lokien keskittäminen tekee mahdollisten poikkeamien tutkinnasta helpompaa, koska lokit löytyvät yhdestä paikkaa ja riski lokien muokkaamiselle tai poistamiselle on pienempi. Keskitetyssä lokienhallinnassa on myös helpompi määritellä lokeille tarvittava tallennusaika.

²⁹ Digipooli, 22.10.2024, Varautuminen tietomurtoon, <https://www.digipooli.fi/varautuminen-tietomurtoon/>

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