

LOIHDE

KYBERKATSAUS

12.2024

Tiivistelmä

Joulukuussa tapahtui jälleen paljon kyberturvallisuuteen liittyen. Suomessa merkittävimmät tapahtumat liittyivät kaupallisesti motivoituneisiin rikollisiin. Näiden kohteena olivat suomalaiset yritykset, mutta myös kuluttajat. Kalastelu, erilaiset huijaukset ja laajalti käytössä olevien tuotteiden haavoittuvuudet ovat hyökkääjien käytössä olevia työkaluja, joiden avulla he pyrkivät saavuttamaan taloudellista hyötyä.

Joulukuussa Suomessa uutisoitiin useita tietomurtoja, joista osa liittyi myös toisiinsa. Hyökkäysten kohteena olevat organisaatiot toimivat esimerkiksi IT-, ruoantuotannon ja median alalla. Ulkomailla otsikoihin nousivat laajalti käytössä olevat tiedostonjakopalvelut, joiden haavoittuvuuden kautta Clop-kiristyshaittaohjelmaryhmä sai kiristyksen kohteeksi jopa 66 eri organisaatiota.

Venäjän kybertoimintaan liittyen uutisoitiin merkittävästä ja laajasta hyökkäyksestä Ukrainan kansalaisiin liittyviä rekistereitä ja tietokantoja vastaan. Hyökkäyksen taustalla epäillään olevan Venäjän sotilastiedustelun ja sen vaikutukset ovat näkyneet laajalti Ukrainassa. Venäjään liittyvät palvelunestohyökkäykset jatkuvat edelleen.

Venäjä jatkaa aggressiivista retoriikkaa ja toimintaa Itämeren alueella. Keinovalikoimaa ei ole rajoitettu, joten vaikuttamista voidaan tehdä fyysisesti, informaatiotilassa tai kyberkeinoin. Joulukuun aikana on nähty Venäjän vaikuttamistoimintaa kaikissa edellä mainituissa. Venäjän toiminnan pääpainopiste säilyy Ukrainassa, mutta se jatkaa vaikuttamistaan myös lähialueellaan.

Joulupäivänä havaittiin Itämerellä jälleen kaapelikatko, kun Estlink 2 -sähkökaapeli irtosi verkosta puolenpäivän aikaan. Tapahtuneen käynnistämä tutkinta paljasti sähkökaapelin lisäksi vaurioituneen useita datakaapeleita. Suomen viranomaiset pysäyttivät ja ottivat haltuunsa tapahtuneeseen liittyen Cookinsaarten lipun alla seilaavan rahtialuksen, joka on nyt hinattuna Kilpilahteen tutkinnan ajaksi. Törkeän vahingonteon lisäksi alusta epäillään pakotteiden kiertoon liittyvästä toiminnasta.

KUUKAUSIRAPORTTI 12/2024

Tämä raportti sisältää kuvauksen joulukuun 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 12/2024	2
1. Yleistilanne	3
2. Haavoittuvuudet	4
2.1 CVE-2024-49112: Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	4
2.2 CVE-2024-11639, CVE-2024-11772, CVE-2024-11773: Ivanti Cloud Services Application	4
2.3 CVE-2024-3393 PaloAlto PanOS DoS	5
3. Kalastelu ja huijaukset	6
4. Venäjä ja sitä tukevat ryhmät	7
5. Kiristyshaittaohjelmat ja -toimijat	8
6. Muuta: Kaapelikatkot Itämerellä	9
7. Suositukset	10

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 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

Joulukuun osalta vältyttiin Log4shell kaltaisilta kaaoksilta. Microsoft julkaisi muutamia kriittisiä haavoittuvuuksia, joista laajalti käytettyä LDAP-palvelua koskevat on nostettu tähän. Tämän lisäksi nostona on Ivantin CSA-verkkolaitteista löytynyt haavoittuvuuskatras.

2.1 CVE-2024-49112: Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability

Microsoftin joulukuun päivityksissä julkaistiin korjaus kriittiseen haavoittuvuuteen CVE-2024-49112, joka piilee Windowsin Lightweight Directory Access Protocol (LDAP) -protokollassa. Onnistunut hyväksikäyttö mahdollistaa hyökkääjälle mielivaltaisen koodin suorittamisen etänä (RCE) LDAP-palvelun kontekstissa.¹

Hyväksikäyttö tapahtuu lähettämällä tietyllä tavalla rakennettuja RPC-kutsuja domain controllerille, jotka triggeröivät haun hyökkääjän domainista. Hyväksikäytön voi Mnemonic:n mukaan ketjuttaa kahteen muuhun haavoittuvuuteen (CVE-2024-49124 ja CVE-2024-49127), jotka mahdollistavat mielivaltaisen koodin ajamisen korkeimmilla SYSTEM-oikeuksilla.²

Tarkempia tietoja haavoittuvuudesta tai sen hyväksikäytöstä on hyvin niukasti.

Haavoittuvuuden mitätöimiseksi Windows-päivitykset tulee asentaa viipymättä. Tämän lisäksi domain controllerien yhteys internetiin tulisi olla rajattu.

2.2 CVE-2024-11639, CVE-2024-11772, CVE-2024-11773: Ivanti Cloud Services Application

10.12.2024 Ivanti julkaisi korjaukset kolmeen kriittiseen haavoittuvuuteen koskien Cloud Services Application (CSA) -tuotetta. CVE-2024-11639 (CVSS 10.0) mahdollistaa autentikoimattoman hyökkääjän ohittaa palveluun autentikoiminen ja saada järjestelmänvalvojan tasoiset oikeudet CSA:n web-käyttöliittymän hallintakonsolissa.³ Kaksi muuta haavoittuvuutta CVE-2024-11772 ja CVE-2024-11773 mahdollistavat (esim. edellä mainittua haavoittuvuutta hyväksikäyttäen) käyttöjärjestelmätason komentojen ja SQL-

¹ Microsoft, 10.12.2024, Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability, <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49112>

² Mnemonic, 13.12.2024, Advisory: Critical vulnerability in Windows LDAP (CVE-2024-49112), <https://www.mnemonic.io/resources/blog/advisory-critical-vulnerability-in-windows-ldap-cve-2024-49112/>

³ Ivanti, 10.12.2024, Security Advisory Ivanti Cloud Services Application (CSA) (CVE-2024-11639, CVE-2024-11772, CVE-2024-11773), https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Services-Application-CSA-CVE-2024-11639-CVE-2024-11772-CVE-2024-11773?language=en_US

lausekkeiden mielivaltaisen suorittamisen autentikoituneelle hyökkääjälle. Käytännössä hallintakonsoliin yhteyden saava hyökkääjä kykenee ottamaan laitteen hallintaansa.⁴

Julkista PoC-koodia tai laajaa hyväksikäyttöä ei ole maailmalla Ivantin mukaan esiintynyt. Ivanti CSA:n versio 5.0.2 ja sitä vanhemmat versiot ovat haavoittuvia. Korjaava päivitys 5.0.3 suositellaan asentamaan viipymättä.³

2.3 CVE-2024-3393 PaloAlto PanOS DoS

Palo Alto julkaisi 27.12. CVSS 8.7 arvion saaneen haavoittuvuuden PanOS käyttöjärjestelmässään. Haavoittuvuus mahdollistaa tunnistautumattomalle hyökkääjälle palvelun käytön estämisen tietyssä muodossa olevien pakettien lähettämisen avulla.⁵ Lähettämällä paketteja laitteelle hyökkääjä saa laitteen ylikuormittumaan ja käynnistämään itsensä uudelleen. Monesti toistettaessa tilanne johtaa laitteen käynnistymiseen ylläpitotilassa. Hyökkääjä pystyy näin estämään palvelun käytön ja aiheuttamaan katkoksia verkkoliikenteeseen.⁶

Jotta haavoittuvuutta on mahdollista hyväksikäyttää, on käytössä oltava DNS Security tai Advanced DNS Security lisenssi. Lisäksi DNS Security lokitus on oltava sallittuna. Haavoittuvuuden hyväksikäyttöä on valmistajan mukaan jo havaittu. Korjaava päivitys on olemassa ja sen asennusta suositellaan välittömästi.⁷

⁴ Sangfor, 24.12.2024, CVE-2024-11639: Ivanti Cloud Services Application (CSA) Authentication Bypass Vulnerability, <https://www.sangfor.com/farsight-labs-threat-intelligence/cybersecurity/cve-2024-11639-ivanti-cloud-services-applicationcsa>

⁵ Palo Alto, 27.12.2024, CVE-2024-3393 PAN-OS: Firewall Denial of Service (DoS) in DNS Security Using a Specially Crafted Packet, <https://security.paloaltonetworks.com/CVE-2024-3393>

⁶ Bleeping Computer, 27.12.2024, Hackers exploit DoS flaw to disable Palo Alto Networks firewalls, <https://www.bleepingcomputer.com/news/security/hackers-exploit-dos-flaw-to-disable-palo-alto-networks-firewalls/>

⁷ Palo Alto, 27.12.2024, CVE-2024-3393 PAN-OS: Firewall Denial of Service (DoS) in DNS Security Using a Specially Crafted Packet, <https://security.paloaltonetworks.com/CVE-2024-3393>

3. Kalastelu ja huijaukset

Käyttäjätunnusten kalastelu ja kalasteluviestien kautta leviävät haittaohjelmat ovat edelleen uhkatoimijoiden yleisin reitti organisaatioiden ympäristöihin. Yksityishenkilöihin kohdistuu erityisesti pankkien nimissä tekstiviestitse lähetettyjä kalasteluviestejä.⁸ Yritysten kannalta kalastelu on merkittävä uhka, sillä nykyaikaista kalastelua on vaikeaa tunnistaa ja se on erittäin yleistä. Käyttäjätunnuksen vaarantuminen johtaa nopeasti käyttäjän resurssien, kuten sähköpostien ja pilvipalveluiden tiedostojen vaarantumiseen. Kalastelun ennaltaehkäisyyn ja sen riskien minimointiin liittyen on syytä rajata kirjautumismahdollisuuksia, huolehtia lokituksesta ja toteuttaa jatkuvaa valvontaa.

Kyberturvallisuuskeskus raportoi tekijänoikeusteemaisista huijausviesteistä, joissa lähettäjä esiintyy suomalaisina toimijoina. Viesteissä vastaanottajan väitetään rikkoneen tekijänoikeuksia ja niissä kehoitetaan avaamaan viestin liitteenä oleva PDF-tiedosto. Todellisuudessa liitetiedoston formaatti on jotain muuta, kuten .exe tai .dll.⁹ Nämä viestit täyttävät tyypillisen kalasteluviestin tunnusmerkit, jossa pyritään saamaan vastaanottaja avaamaan liite kiireen, uhkailun tai viestin tärkeyden perusteella.

Joulukuussa uutisiin nousi myös FlowerStorm PhaaS-palvelu (Phishing-as-a-Service). Palvelun avulla hyökkääjät voivat suorittaa kalastelua helpommin ilman laajaa teknistä osaamista. Palvelut saa käyttöön maksamalla kuukausimaksun. Edellä mainittu palvelu on nostanut suosiotaan nopeasti ja siitä on povattu Rockstar2FA -palvelun korvaajaa. Rockstar2FA suljettiin aikaisemmin tänä vuonna.¹⁰

⁸ OP, lainattu 28.12.2024, Mistä tunnistaa huijausviestin – katso, millaisia huijausviestejä tietoomme on tullut, <https://www.op.fi/turvallinen-asiointi/mista-tunnistaa-huijausviestin>

⁹ Kyberturvallisuuskeskus, 20.12.2024, Kyberturvallisuuskeskuksen viikkokatsaus - 51/2024, <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-512024>

¹⁰ Bleeping Computer, 21.12.2024, New FlowerStorm Microsoft phishing service fills void left by Rockstar2FA, <https://www.bleepingcomputer.com/news/security/new-flowerstorm-microsoft-phishing-service-fills-void-left-by-rockstar2fa/>

4. Venäjä ja sitä tukevat ryhmät

Venäjä jatkaa vaikuttamista itselleen vihamielisiin lukemiinsa maihin niin kyber- ja informaatiotilassa, kuin myös fyysisesti. Toiminnan painopiste on Ukrainassa, mutta vaikutusta pyritään saamaan aikaan myös muualla. Kyberympäristössä vaikuttamiseen käytetään viranomaisten resursseja, rikollisia ja haktivisteja. Keinovalikoima on laaja ja esimerkiksi informaatio- ja kybervaikuttaminen sulautuvat monesti osaksi toisiaan.

Viime vuosina paljon mediatilaa saaneet palvelunestohyökkäykset eivät lähiaikoina ole nousseet enää uutiskynnyksen yli, vaikka niitä jatkuvasti tapahtuu. NoName057(16) on jatkanut toimintaansa ja toteuttaa palvelunestohyökkäyksiä länsimaita kohtaan DDoSia projekt-sovelluksensa ja joukkoistamisen avulla. Joulukuussa uutisoitiin ryhmän toteuttamista hyökkäyksistä italialaisen lentokentän verkkosivuja vastaan. Uutisten mukaan hyökkäyksillä ei ollut vaikutusta kentän toimintaan.¹¹

Joulukuussa Ukraina ilmoitti kohdanneensa merkittävän kyberhyökkäyksen, jonka takana on Venäjä. Hyökkäys lamautti merkittäviä rekistereitä ja tietokantoja, joita käytetään esimerkiksi syntyneiden, kuolleiden ja vihittyjen tietojen säilytykseen. Hyökkäyksen seurauksena näitä tietoja on jouduttu rekisteröimään nyt paperilla. Ukrainan turvallisuuspalvelun (SBU) mukaan hyökkäyksen uskotaan liittyvän Venäjän sotilastiedusteluun (GRU). Hyökkäyksen kerrottiin olleen ammattimaisesti ja pitkäjänteisesti toteutettu.¹²

Azerbaidžanilainen matkustajalentokone tuhoutui 25.12.2024 Venäjän ilmatilassa. Tapahtumasta syytettiin aluksi lintuparvea, mutta nopeasti havaittiin merkkejä mahdollisesta ilmatorjunta-aseen käytöstä. Tämänhetkisen tiedon perusteella näyttääkin sille, että lentokone on tippunut venäläisen ilmatorjunnan alas ampumana. Tapaus on tämänhetkisten tietojen mukaan voinut johtua siitä, että venäläinen ukrainalaisten lennokkien torjuntaan liittyvä osasto on ampunut koneen alas erehdyksessä. Putin on pahoitellut tapausta, mutta ei ole myöntänyt asiaa.¹³

Venäjän ja länsimaiden välisessä diplomatiassa tai vastakkainasettelussa ei tällä hetkellä näy lientymisen merkkejä.

¹¹ DW, 28.12.2024, Pro-Russian hackers target Italian airport websites, <https://www.dw.com/en/pro-russian-hackers-target-italian-airport-websites/a-71176385>

¹² The Record, 20.12.2024, Ukraine's state registers hit with one of Russia's largest cyberattacks, officials say, <https://therecord.media/ukraine-government-cyberattack-state-registers-russia>

¹³ Reuters, 29.12.2024, Russia's Putin apologises to Azerbaijan over 'tragic' airliner crash, <https://www.reuters.com/world/asia-pacific/putin-apologises-aliyev-over-tragic-incident-with-azerbaijan-airlines-plane-2024-12-28/>

5. Kiristyshaittaohjelmat ja -toimijat

Joulukuun alussa uutisiin nousi Cleo-tiedostonjakopalveluissa ilmenneen haavoittuvuuden hyväksikäyttö. Cleo LexiCom, VLTransfer ja Harmony sovellukset ovat melko yleisiä tiedostojen siirtoon käytettäviä ohjelmia. Näistä löytynyt haavoittuvuus CVE-2024-50623¹⁴ mahdollistaa hyökkääjän koodin suorittamisen sovellusta ajavalla palvelimella.¹⁵ Haavoittuvuuden hyväksikäyttö oli julkaisuajankohtana aktiivista, vaikka kyseessä oli aiemmin tuntematon haavoittuvuus. Pian haavoittuvuuden julkaisun jälkeen Clop-kiristyshaittaohjelmaryhmä ilmoitti olleensa hyväksikäytön takana. Kyseessä ei ole ensimmäinen kerta, kun Clop kohdistaa hyökkäyksiä tiedostonjakosovelluksia kohtaan. Esimerkiksi kesällä 2023 Clop hyökkäsi vastaavalla tavalla MOVEit-tiedostonjakosovellusta kohtaan.¹⁶ Myöhemmin Clop julkaisi haavoittuvuuteen liittyen jopa 66 uutta kiristyksen kohdetta vuotosivustollaan.¹⁷ Kiristyksen kohteista Blue Yonder on kuitenkin ilmoittanut, ettei sillä ole syytä uskoa Clopin saaneen pääsyä järjestelmiinsä Cleon haavoittuvuuden vuoksi. Yritys joutui kiristyshaittaohjelman kohteeksi marraskuussa ja Clop on väittänyt hyväksikäytön tapahtuneen Cleon sovelluksen avulla.¹⁸ Clopin uhrien osalta onkin siis vielä varmistamatta, ovatko kaikki todella kyseisen haavoittuvuuden vuoksi listalla.

Venäjän viranomaiset ilmoittivat joulukuun alussa pidättäneensä kiristyshaittaohjelmia kehittäneen henkilön, jonka uskotaan olleen ”Wazawaka” -nimimerkkiä käyttänyt hakkeri. ”Wazawaka” on tällä hetkellä myös FBI:n top10 rikollisen listalla ja hänen pidätykseensä johtavista tiedoista Yhdysvaltojen hallitus on ilmoittanut maksavansa 10 miljoonan dollarin palkkion. Pidätys voidaan nähdä poikkeavana Venäjän aikaisempaan linjaan nähden, sillä samankaltaisia verkkorikollisia on pidätetty vain harvoin. Pidätyksiä on tapahtunut harvoin varsinkin silloin, jos rikolliset ovat kohdistaneet hyökkäyksensä Venäjän rajojen ulkopuolelle.¹⁹

¹⁴ Cleo Solution Center, lainattu 28.12.2024, Cleo Product Security Advisory - CVE-2024-50623, <https://support.cleo.com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623>

¹⁵ Hunteres, 9.12.2024, Threat Advisory: Oh No Cleo! Cleo Software Actively Being Exploited in the Wild, <https://www.huntress.com/blog/threat-advisory-oh-no-cleo-cleo-software-actively-being-exploited-in-the-wild>

¹⁶ Bleeping Computer, 15.12.2024, Clop ransomware claims responsibility for Cleo data theft attacks, <https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-cleo-data-theft-attacks/>

¹⁷ Bleeping Computer, 24.12.2024, Clop ransomware is now extorting 66 Cleo data-theft victims, <https://www.bleepingcomputer.com/news/security/clop-ransomware-is-now-extorting-66-cleo-data-theft-victims/>

¹⁸ The Record, 27.12.2024, Blue Yonder says November ransomware attack not connected to Cleo vulnerability, <https://therecord.media/blue-yonder-ransomware-attack-not-connected-to-cleo-vulnerability>

¹⁹ Daryna Antoniuk, 2.12.2024, Ransomware suspect Wazawaka reportedly arrested by Russia, <https://therecord.media/wazawaka-mikhail-matveev-reportedly-arrested-russia>

Kiristyshaittaohjelmiin liittyen uutisoitiin myös Suomessa, kun Valio ilmoitti joutuneensa tietomurron kohteeksi.²⁰ Tapaukseen liittyen on julkisuuteen kerrottu hyökkääjän saaneen haltuunsa työntekijöiden tietoja. Lisäksi uutisoinnissa on kerrottu kiristysyrityksestä. Tapaukseen liittyen ei ole kerrottu, kuka hyökkäyksen takana on.²¹ Valio ja Vincit ovat kertoneet, että Valion järjestelmiin on päästy sen IT-kumppani Vincitin tietomurron avulla.²²

6. Muuta: Kaapelikatkot Itämerellä

Joulupäivänä 25.12. Suomen ja Viron välinen Estilink2 sähkökaapeli irtosi verkosta 12:26. Tapahtuneen jälkeen aloitettiin selvitystyö, jonka perusteella oli syytä uskoa alueella olleen rahtialuksen liittyvän yhteyden katkeamiseen. Myöhemmin selvisi, että sähkökaapelin lisäksi kolme datakaapelia on katkennut ja yksi vaurioitunut lievemmin. Kaikki edellä mainitut näyttävät liittyvän Cookinsaarten lipun alla seilaavan Eagle S rahtialuksen toimintaan.²³

Tapauksen ilmettyä poliisi, rajavartiolaitos ja tulli aloittivat yhteisoperaation asiaan liittyen. Myös puolustusvoimat antoivat tapahtumiin liittyen virka-apua edellä mainituille. Rajavartiolaitoksen partioalus Turva lähestyi rahtialusta ja havaitsi sen ankkuriketjun olevan alhaalla. Alus ohjattiin kansainvälisiltä vesiltä Suomen vesialueelle, jossa aamuyöllä 26.12. poliisin valmiusyksikkö ja rajavartiolaitoksen erikoisjoukot laskeutuivat helikoptereista alukselle ja ottivat sen komentoonsa.²⁴ Tämän jälkeen poliisi käynnisti rikostutkinnan törkeään vahingontekoon liittyen.²⁵

Joulukuun 28. päivänä alus siirrettiin hinaamalla Kilpilahteen sisäankkuripaikalle, jossa tutkinta jatkuu. Vuosina 2023 ja 2024 on tapahtunut kolme vastaavaa tapausta, jossa merenalaista infrastruktuuria on vahingoitettu raahaamalla ankkuria rahtialuksen perässä. Näistä viimeisin on ainoa, jossa laiva on pysäytetty ja otettu haltuun.

²⁰ Valio, 20.12.2024,

Valion ja maidonhan-kin-tao-suus-kuntien henkilöstön tietoihin kohdistunut tietoturva-hyökkäys, <https://www.valio.fi/uutiset/valion-ja-maidonhankintaosuuskuntien-henkiloston-tietoihin-kohdistunut-tietoturvahyokkays/>

²¹ MTV, 20.12.2024, Valioon tehty laaja tietoturvahyökkäys – nimet ja henkilötunnukset rikollisille, <https://www.mtvuutiset.fi/artikkeli/valion-tietoihin-kohdistunut-tietoturvahyokkays/9070714>

²² Yle, 20.12.2024, Valioon laaja tietomurto, tuhansien tiedot ovat saattaneet vuotaa – it-kumppani Vincitin tunnukset murrettu, <https://yle.fi/a/74-20132963>

²³ Helsingin Sanomat, 25.12.2024, Poliisi tutkii, liittykö ulkomaalainen alus Suomen ja Viron kaapeli-häiriöön – Suomalainen vartiolaiva saattoi Venäjän varjo-laivastoon liitetyn tankkerin Porkkalan edustalle, <https://www.hs.fi/talous/art-2000010926181.html>

²⁴ Helsingin Sanomat, 28.12.2024, Kamppailu aikaa vastaan, <https://www.hs.fi/tutkiva/art-2000010928353.html>

²⁵ Poliisi, 27.12.2024, Suomenlahden kaapelivauriot: Merenpohjan tutkinta alkamassa, <https://poliisi.fi/-/suomenlahden-kaapelivauriot-merenpohjan-tutkinta-alkamassa>

7. Suositukset

Tässä kuussa suosittelemme:

1. Kirjautumisten rajaaminen vain luotettuihin laitteisiin
2. Verkkoliikenteen sääntöjen tarkastelu ja rajaaminen
3. Varautumissuunnitelman harjoittelu

Käyttäjätilit ja niihin liittyvät resurssit ovat hyökkääjän kannalta kiinnostavia kohteita. Näihin pyritään pääsemään käsiksi usein esimerkiksi kalastelun avulla. Tähän liittyvää riskiä voi pyrkiä pienentämään rajaamalla mahdollisimman tarkasti kirjautumista esimerkiksi sijainnin ja laitteen osalta. Organisaation resursseihin ja palveluihin pääsy on hyvä rajata tapahtumaan ainoastaan organisaation laitteilta ja esimerkiksi ainoastaan tietystä maasta. Tällöin haitallinen kirjautuminen ei onnistu, vaikka käyttäjä vahingossa luovuttaisikin kirjautumistapahtumansa hyökkääjälle kalastelun tuloksena. Conditional Access -policyjen lisäksi identiteettien valvonta ja nopea reagointi poikkeamiin on oleellinen osa puolustautumista.

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 verkkoprotokolia. Kriittisten palvelimien kuten domain controllerien tai tuotantopalvelimen sallittujen verkkoyhteyksien rajaaminen vain tarvittuihin pienentää hyökkääjän toimintamahdollisuuksia huomattavasti. Yhteydet internetiin sekä muualle verkkoon tulisi olla rajattu vain tarvittaviin, poikkeuksina tehtyihin avauksiin.

Varautumissuunnitelman harjoittelu ja koeponnistaminen on syytä tehdä säännöllisesti. Harjoittelun kautta voidaan todentaa suunnitelman toimivuutta ja tarkistaa esimerkiksi, onko suunnitelman vaiheisiin tarve tehdä päivityksiä. Mikäli harjoittelua on jo tehty, voidaan sen painopistettä siirtää ja testata esimerkiksi vain osaa suunnitelmasta. On myös hyvä muistaa, että suunnitelmaa päästään toteuttamaan tositilanteessa harvoin samoilla, suunnitelluilla resursseilla ja yhtä rauhallisissa olosuhteissa, kuin alun perin on ajateltu. Tämän vuoksi voikin olla hyvä koestaa suunnitelmaa esimerkiksi siten, että osa henkilöstöstä puuttuu tai jokin tärkeä resurssi ei ole käytössä. Tällöin voidaan testata suunnitelman kestävyyttä myös poikkeavassa harjoitustilanteessa.

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