TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Maaliskuu 2026

Kybersää

Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä.

Tämä tuote on suunnattu ensisijaisesti eri tasoilla organisaatioiden tietoturvallisuuden parissa työskenteleville. Kybersää tarjoaa nopean kokonaiskuvan, mitä kyberturvallisuuskentällä on tapahtunut ja mitä on tulossa.

Kybersää voi olla:  rauhallinen  huolestuttava  vakava

Kuukauden tunnuslukuja

Kyberturvallisuuskeskus julkaisi maaliskuussa kolme haavoittuvuustiedotetta kriittisistä haavoittuvuuksista.[1]

Kyberturvallisuuskeskuksen Autoreporter-palvelu on ollut toiminnassa jo yli 20 vuotta. Autoreporter saa tietoja Suomesta lähtöisin olevasta haittaohjelmaliikenteestä lähes kaikkialta maailmasta. Havainnot välitetään teleyrityksille, jotka ilmoittavat havainnoista asiakkailleen laitteiden siivoamiseksi. Viimeisen yli 20 vuoden aikana Autoreporter on jakanut lähes kolme miljoonaa havaintoa.[2]

Kybersään yleistilanne maaliskuussa 2026

Kybersää jatkui sateisena

Sadepilviä keväiselle kybertaivaalle kerryttivät useammat ohjelmistokomponenttien kautta tehdyt toimitusketjuhyökkäykset. Uhkatoimija TeamPCP toteutti hyökkäykset avoimen lähdekoodin ohjelmistojen (Trivy, Kicks, ja Python-paketti LibLLM) kautta.[3]

M365-tilimurtojen aalto vaikuttaa pienentyneen edelliseen kuukauteen verrattuna.

Maaliskuussa julkaisimme kolme haavatiedotetta kriittisistä haavoittuvuuksista.[4]

Kyberturvallisuuskeskukselle on alkuvuonna ilmoitettu poikkeuksellisen vähän kiristyshaittaohjelmatapauksia. Kansainvälisesti kiristyshaittaohjelmien määrä kasvaa jatkuvasti, joten tilanne voi myös Suomessa muuttua nopeasti.

Valon pilkahduksia sadepisaroiden lomaan toi Kyberturvallisuuskeskuksen ja suojelupoliisin osallistuminen kansainväliseen operaatioon, jossa torjuttiin Venäjän sotilastiedustelupalvelu GRU:n vakoilutoimintaa. Operaatiossa estettiin murretuista TP-linkin reitittimistä muodostetun maailmanlaajuisen kybervakoiluverkoston käyttö.

GRU oli käyttänyt haavoittuvia reitittimiä ainakin käyttäjien vakoiluun muuttamalla laitteiden nimipalveluasetuksia. Tämä on mahdollistanut välimieshyökkäyksen (adversary-in-the-middle, AitM) toteuttamisen ja salatun verkkoliikenteen purkamisen.[5]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Kyberturvallisuuskeskus julkaisi tilannekortteja, jotka auttavat organisaatioita viestimään kyberpoikkeamista. Korteista saa yleiskuvan erilaisista poikkeamatapauksista ja konkreettista tukea niistä viestimiseen.[6]

Kutsumme organisaatioita osallistumaan maksuttomaan Vartijatonttu-kokeiluprojektiin, jolla kartoitetaan suomalaisten yritysten kykyä tunnistaa ja reagoida ajankohtaisiin kyberturvallisuusuhkiin. Osallistujat saavat vertailutietoa omasta kyberkypsyydestään, analyysin todellisista uhkaskenaarioista sekä konkreettisia kehityssuosituksia.[7, 8]

Kyberturvallisuuskeskuksen uusi opas Ohjelmistoturvallisuuden johtaminen - Roolit ja osaamistarpeet tarjoaa tukea ohjelmistoturvallisuuden systemaattiseen johtamiseen koko ohjelmiston elinkaaren ajan. Tällä turvataan organisaatioiden ja koko yhteiskunnan toiminnan jatkuvuutta ja häiriöttömyyttä digitaalisessa ympäristössä.[9]

Erityisesti ohjelmistokehittäjille suunnattu Kriittinen koodi -webinaarisarja alkaa 17.4. Kyberturvallisuuskeskuksen järjestämässä webinaarisarjassa käsitellään ohjelmistojen turvallisuutta käytännön näkökulmasta: miten parempaa ja turvallisempaa koodia tehdään.[10]

Kuukauden raekuuro
Pikaviestisovellusten tilit kaappausyritysten kohteena

Kyberturvallisuuskeskukselle on alkuvuoden aikana ilmoitettu lukuisia pikaviestisovellusten tileihin liittyviä poikkeamia. Kohteena ovat olleet Telegram-, WhatsApp- ja Signal-tilit.[11, 12]

Poikkeamia on ilmoitettu monenlaisia. Raportoiduissa tapauksissa tilejä on luotu toisen henkilön käytössä olevalla tai käytöstä poistetulla numerolla. Tilikaappauksia ja luvatonta käyttöä ollaan toteutettu ainakin linkitystoiminnolla, joka mahdollistaa saman tilin käyttämisen toiselta laitteelta. Linkitykseen vaadittava koodi pyritään huijaamaan kalastelulla.

Pikaviestisovellusten tilejä voi suojata monivaiheisella tunnistautumisella, sekä varmistamalla, ettei tuntemattomia laitteita ole yhdistetty tiliisi. Puhelinvastaajan oletusarvoinen pin-koodi tulee vaihtaa. Organisaatioiden on hyvä ohjeistaa työntekijöitä pikaviestisovellusten käytöstä työkontekstissa.

Kansainvälisesti raportoidut kampanjat osoittavat, että pikaviestisovellusten tilikaappauksissa on mahdollisuus vakaviinkin poikkeamiin.

Havaintoja pikaviestisovellusten poikkeamista kansainvälisesti

- Saksassa viranomaiset varottivat pikaviestisovelluksissa, etenkin Signalissa tehdystä kalastelusta, jonka taustalla on todennäköisesti valtiollinen toimija. Kalastelun kohteena on ollut korkea-arvoisia poliitikkoja, virkamiehiä, puolustusvoimien edustajia ja toimittaja.[13]
- Alankomaiden viranomaiset julkaisivat tietoja globaalista kampanjasta, jolla Venäjän valtioon yhdistetyt kyberuhkatoimijat pyrkivät saamaan merkkihenkilöiden Signal- ja WhatsApp-tilejä haltuun.[14]
- Italiassa Signal-kampanjassa ollaan pyritty kalastelemaan ihmisten henkilökohtaisia tietoja sosiaalisen manipuloinnin keinoin.[15]

Kybersään ilmiöt

Osiossa käymme läpi kyberturvallisuuden ilmiöiden kehitystä ja trendejä.

Kybersää
maaliskuu 2026

1 kk

Tietomurrot- ja vuodot

Maaliskuu oli tietomurtojen osalta melko tasainen. Kuukauden aikana tapahtui kuitenkin muutamia merkittävämpiä tietomurtoja ja tietovuotoja. Hyökkäykset toteutettiin pääasiassa hyödyntämällä haavoittuvuuksia.

Haittaohjelmat

Maaliskuussa uhkatoimijan tekemät avoimen lähdekoodin ohjelmistoihin kohdistuneet toimitusketjuhyökkäykset vaikuttivat laajalti niin kansallisesti kuin kansainvälisesti.

Haavoittuvuudet

Maaliskuussa raportoitiin edelleen paljon haavoittuvuuksia. Vaikutukset Suomessa olivat varsin rajallisia.

Huijaukset ja kalastelut

Maaliskuussa havaittiin runsaasti veroteemaisia huijausviestejä, jotka liittyvät veronpalautuksiin, veropäätöksiin tai jälkiveroon.

WhatsApp-ryhmäkeskustelujen avulla kerätään yrityksistä tietoja laskutuspetoksia varten.

Automaatio ja IoT

Yhdysvallat kielsi ulkomailla valmistettujen kuluttajareitittimien tuomisen Yhdysvaltojen markkinoille kansalliseen turvallisuuteen vedoten.

Verkkojen toimivuus

Maaliskuussa palvelunestohyökkäyksiä ilmoitettiin hieman alkuvuoden kuukausia enemmän, mutta merkittäviä vaikutuksia ei havaittu.

Teknisten palvelunestohyökkäysten rinnalle voi olla nousemassa inhimillisten rajapintojen häirintä.

Kybersää
maaliskuu 2026 1/2

1 kk

Tietomurrot ja -vuodot

- Viranomaisten yhteisoperaatiossa torjuttiin Venäjän sotilastiedustelun kybervakoilua, jossa hyödynnettiin TP-Linkin reitittimien haavoittuvuutta (CVE-2023-50224) laitteiden tietomurtoon. Tietomurron avulla hyökkääjät käyttivät vakoilun välineinä erityisesti päivittämättömiä reitittimiä, esimerkiksi ohjaamalla verkkoliikennettä oman infrastruktuurinsa kautta.[16]
- Digitalist Experience Oy:n järjestelmään kohdistui tietomurto, joka sisälsi Viking Linen asiakastietoja.
- M365-tilien tietomurroista ilmoitettiin Kyberturvallisuuskeskukselle lähes puolet vähemmän kuin helmikuussa.

Haittaohjelmat

- Uhkatoimija TeamPCP onnistui toteuttamaan toimitusketju-hyökkäyksen avoimen lähdekoodin ohjelmistoihin Trivy-tietoturva-skanneriin, LiteLLM:ään ja Checkmarxiin. Hyökkäyksellä uhkatoimija asensi ohjelmistoihin takaoven. Haitalliset versiot ohjelmista olivat julkisesti jaossa laajasti. Hyökkäys aiheutti tietomurtoja ympäri maailmaa.[17, 18]
- Haittaohjelmia ilmoitettiin Kyberturvallisuuskeskukselle maaliskuun aikana tavanomaista enemmän.

Haavoittuvuudet

- Maaliskuussa julkaistiin kriittinen haavoittuvuus Citrix NetScaler ADC ja Netscaler Gateway -tuotteissa (CVE-2026-3055), joka mahdollistaa muistissa olevien tietojen vuotamista haavoittuvasta järjestelmästä. Korjaamiseksi suositellaan välitöntä päivitystä.[19]
- Kriittinen haavoittuvuus julkaistiin myös F5 BIG-IP APM -pääsynhallintajärjestelmässä (CVE-2025-53521). Suosituksena on päivittää järjestelmä korjattuun versioon ja tarkistaa ympäristö hyväksikäytön varalta.[20]
- Kriittinen haavoittuvuus löydettiin myös Axios JavaScript -paketin npm-jakelussa.[21]

Kybersää
maaliskuu 2026 2/2

1 kk

Huijaukset ja kalastelut

- Veroteemaisia huijausviestejä on maaliskuussa lähetetty veronpalautuksen, veropäätöksen tai jälkiveron verukkeilla.
- Maksukortin tietoja on kalasteltu asuntovuokravälityspalveluiden nimissä.
- Yritysten sisäisiä tietoja on kerätty laskutuspetoksia varten WhatsApp-ryhmäkeskustelujen avulla. Huijari on väärentänyt johtajan nimiin sähköpostin, jossa pyydetään työntekijää perustamaan ryhmäkeskustelu ja lähettämään liittymislinkki vastausviestissä. Vastaavasta menetelmästä ei olla aiemmin ilmoitettu KTK:lle.

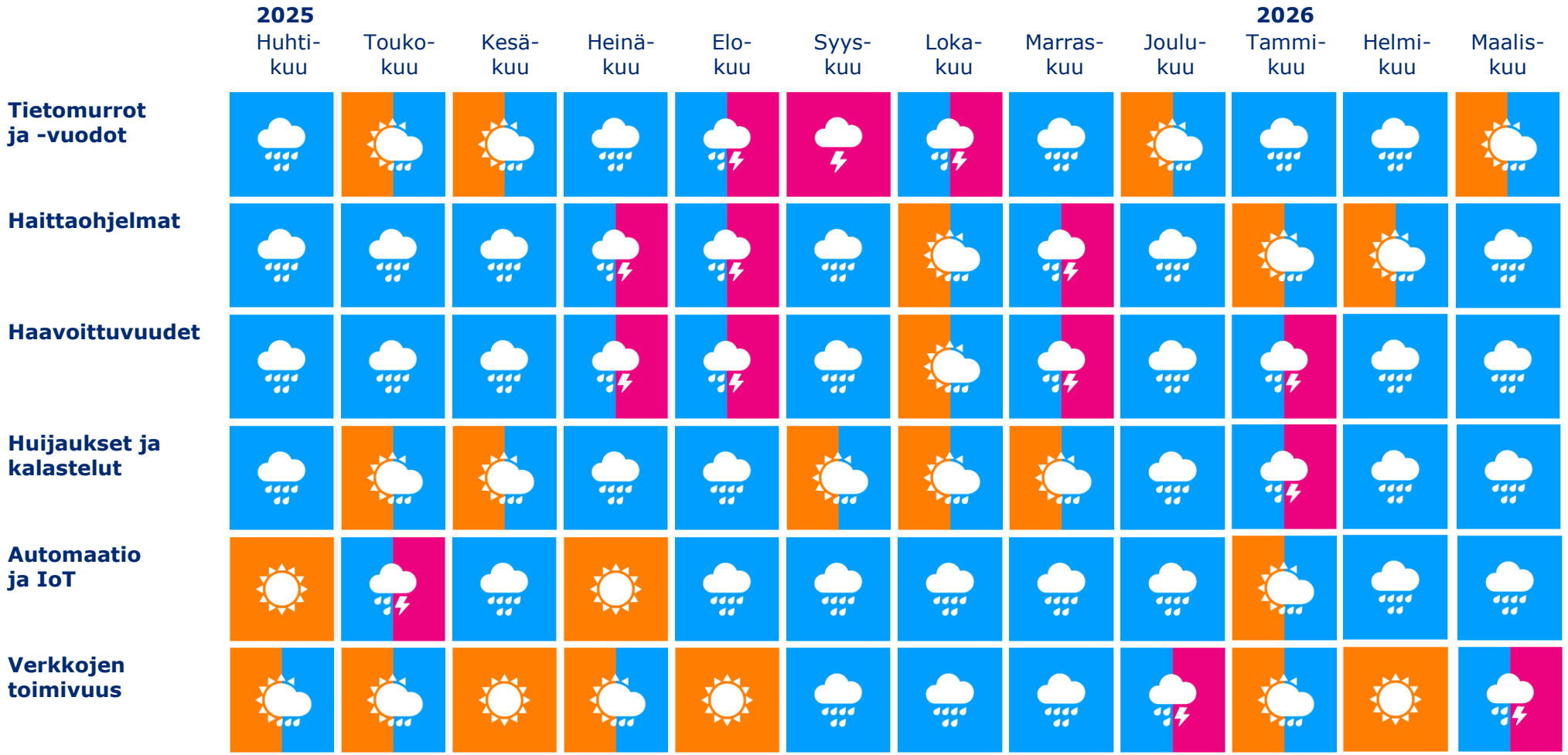
Automaatio ja IoT

- Yhdysvalloissa ulkomaisten reitittimien katsotaan aiheuttavan uhkia kotitalouksille ja tietoverkoille sekä mahdollistavan vakoilun ja tekijänoikeusvarkaudet.[22]
- Yhdysvaltain viestintäkomissio FCC kielsi muiden kuin kotimaassa valmistettujen kuluttajareitittimien maahantuonnin, markkinoinnin ja myymisen Yhdysvalloissa.
- Saadakseen myyntiluvan reitittimien täytyy läpäistä viranomaisarviointi ja valmistajan tulee esittää suunnitelma tuotannon siirtämisestä Yhdysvaltoihin.
- Kuluttajat voivat jatkaa nykyisten laitteittensa käyttöä.

Verkkojen toimivuus

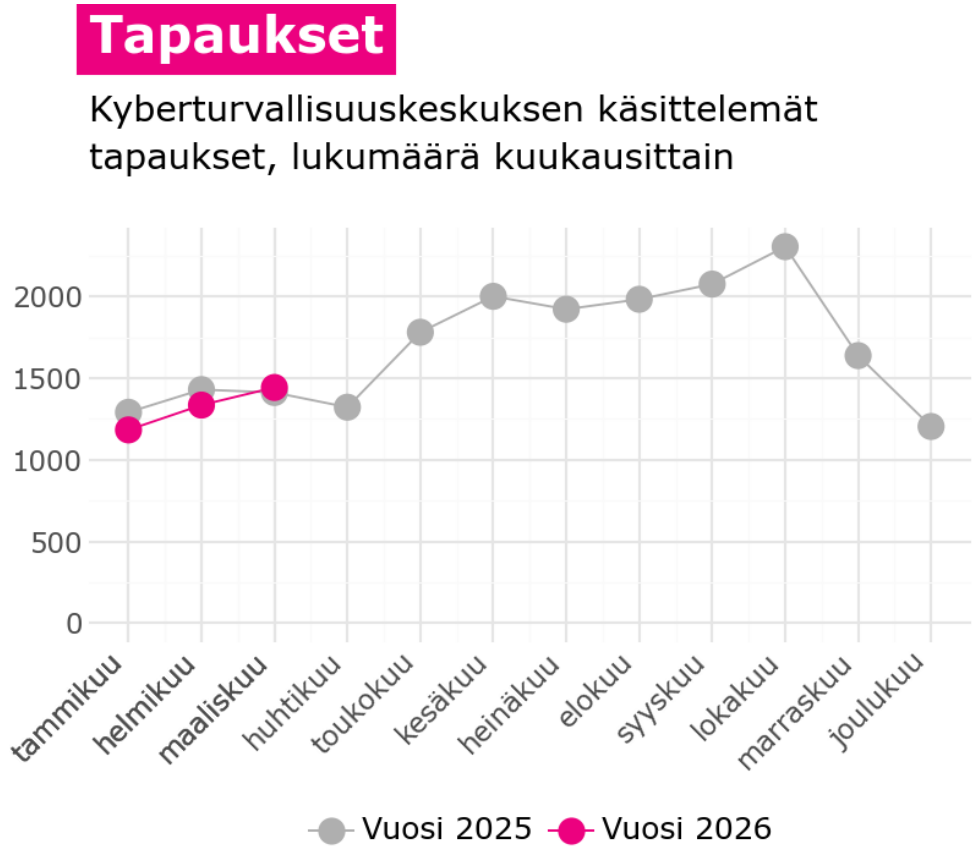
- Maaliskuussa uutisointiin käräjäoikeuksien ja hallinto-oikeuden kuormittuvan tekoälyllä tuotetusta materiaalista.[23, 24]
- Generatiivinen tekoäly mahdollistaa myös monien muiden palvelujen ruuhkauttamisen, kuten asiakaspalvelut tai viranomaisten kirjaamot.
- Kyberturvallisuuskeskukselle on ilmoitettu tapauksista, joissa asiakaspalvelua on ruuhkautettu muun muassa tehtailluilla valvontapyynnöillä.

Kybersään ilmiöt
kulunut 12 kk



Tapaukset

- Kyberturvallisuuskeskus käsitteli maaliskuussa 1443 tapausta.
- Ilmoitusten määrä on 12 kuukauden keskiarvoon nähden 14 % alhaisempi, mutta määrällisesti vastasi edeltävän vuoden maaliskuuta.
- Maaliskuun aikana ilmeni useita kriittisiä ja vakavia haavoittuvuuksia eri palveluissa ja tuotteissa. Haavoittuvuuksien runsaudesta huolimatta nämä eivät näkyneet paljoa Kyberturvallisuuskeskukselle tehdyissä ilmoituksissa.
- Eri avoimen lähdekoodin palveluihin tehdyt toimitusketjuhyökkäykset kuitenkin vaikuttivat Kyberturvallisuuskeskukselle tehtyjen ilmoitusten vakavuuteen.
- Vaikka haavoittuvuudet ja toimitusketjuhyökkäykset altistavat merkittäville kyberpoikkeamille, on näiltä kuitenkin vältytty organisaatioiden aktiivisen toiminnan ja varautumisen ansiosta Suomessa.



Kybersääennuste

Kybersääennuste on aiempiin havaintoihin perustuva yhteenveto ja suuntaa-antava arvio lähikuukausien kyberuhista ja niiden kehityskuluista.

Osiossa käsitellään myös puolivuosittain ilmiöiden pitkän aikavälin kehitysnäkymiä ja lähitulevaisuuden top 5 kyberuhat.

Kybersääennuste
Kyberuhat pysyvät tavanomaisina

1 kk

Ohjelmistoriippuvuuksiin liittyviin kyberriskeihin on varauduttava myös jatkossa. Maaliskuussa nähdyt toimitusketjuhyökkäysten kampanjat eivät varmasti jää viimeisiksi, mutta korostavat ilmiön vakavuutta.

Myös Lähi-idän nopeasti muuttuva tilanne voi edelleen aiheuttaa odottamattomia kerrannaisvaikutuksia Suomeen esimerkiksi monimutkaisten toimitusketjujen kautta.

Organisaation varautuminen

- Valistaminen ja monivaiheinen tunnistautuminen (MFA) eivät riitä suojaamaan työntekijöitä kehittyneiltä tilimurtoyrityksiltä, kuten AiTM-tekniikkaa käyttävältä kalastelulta.
- Organisaatioissa kannattaa ottaa käyttöön kehittyneitä turvallisuusominaisuuksia, kuten ehdollisen pääsyn (conditional access) käytäntöjä, riskipohjainen tunnistautuminen (risk-based authentication) ja jatkuva pääsyn arviointi (continue access evaluation).

Huolestuttava

Kyberuhkien määrä ja vakavuus ovat tavanomaisella tasolla.

Kybersääennuste on aiempiin havaintoihin perustuva yhteenveto ja suuntaa-antava arvio kyberuhkien tilasta. Arviota ei tule käyttää sellaisenaan kyberuhkiin varautumisessa, vaan sen tukena on käytettävä organisaatiokohtaista tietoa ja analyysiä. Kyberuhat voivat muuttua nopeasti, myös negatiiviseen suuntaan.

Pitkän aikavälin kybersää
Ilmiöiden seuraaminen yli viiden vuoden aikajänteellä

Murrokselliset teknologiat
esimerkiksi tekoäly, 6G, kvantti-teknologia

Infrastruktuuriin ja yhteiskunnan kriittisiin toimintoihin
kohdistuvat kyberuhat

Laaja-alaisiin kyber-hyökkäyksiin ja -häiriöihin
varautuminen

Tietoturva-loukkausten muutos
esimerkiksi tietomurrot ja -vuodot

Digitaalisen yhteiskunnan sääntelykehitys

Pitkän aikavälin kybersää
Heikosti suojatut verkkolaitteet 1/2

Globaalisti huolestuttavaksi ilmiöksi ovat nousseet heikosti suojatut verkkolaitteet, jotka muodostavat tietoturvariskin sekä niiden käyttäjille että laajemmin yhteiskunnalle. Kyseessä ovat etenkin kotitalouksien ja pienyritysten (nk. SOHO eli "*small office, home office*") käyttämät laitteet, kuten reitittimet.

Tyypillisimmin riskin muodostavat verkkokaupoista ostetut, hyvin edulliset verkkolaitteet, jotka eivät täytä kaikkia tietoturvavaatimuksia. Laitteisiin on jopa voitu asentaa haittaohjelma niiden valmistusvaiheessa.

Heikosti suojattujen verkkolaitteiden ongelma ei rajoitu vain yksittäisiin laitteisiin, vaan liittyy laajempaan ilmiöön, jossa jotkut valmistajat tai jakeluketjut eivät huolehdi laitteidensa tuotannon riittävästä turvallisuudesta ja laadunvalvonnasta.

Heikosti suojatut verkkolaitteet altistavat käyttäjät tietoturvariskeille, joita yksittäisen kuluttajan voi olla vaikea tunnistaa tai arvioida laitetta hankkiessa.

- Yleisesi nämä voivat mm. heikentää kuluttajien yksityisyyttä, koska laitteet keräävät jatkuvasti dataa, joka voi päätyä vääriin käsiin.

Heikosti suojatut verkkolaitteet muodostavat rikollisille ja valtiollisille toimijoille alustan haitallisen verkkoinfrastruktuurin rakentamiseen, jota voidaan hyödyntää erilaisiin kyberhyökkäyksiin, vakoiluun tai toiminnan peittämiseen.

- Kyberturvallisuuskeskus ja suojelupoliisi osallistuivat maalis-huhtikuussa kansainväliseen operaatioon, jolla ajettiin alas Venäjän sotilastiedustelupalvelun kybervakoiluun käyttämää infrastruktuuria, joka oli muodostettu murretuista reitittimistä.[25]

Laajempana ongelmana on, että markkinoille tulee jatkuvasti uusia verkkolaitteita, joiden tietoturvassa on puutteita, eikä yhden laiteverkoston hajottaminen siten poista uhkaa.

- Rikolliset lisäksi mukautuvat nopeasti ja muodostavat uusia murretuista laitteista muodostuvia verkostoja haitallisen toiminnan mahdollistamiseksi.
- Viranomaiset ovat varoittaneet heikosti suojattujen verkkolaitteiden tietoturvasta useasti viime vuosina.

Pitkän aikavälin kybersää
Heikosti suojatut verkkolaitteet 2/2

Kuluttajalaitteiden haittaohjelmahavainnot ovat lisääntyneet viimeisen vuoden aikana

Suomessa esimerkiksi kiinalaiseen IPIDEA-välityspalvelinverkkoon liittyvät havainnot ovat lähteneet nousuun kuluvana vuonna. IPIDEA kontrolloi miljoonia kotitalouksien verkkolaitteita ja levittää niillä haitallista koodia.[26]

- Haitallinen koodi käskee tartunnan saanutta laitetta välittämään verkkoliikennettä ja osallistumaan hajautettuihin palvelunestohyökkäyksiin.

Kesällä 2025 BadBox 2.0 -haittaohjelmaa alettiin havaita Suomessa erityisesti edullisissa ja tuntemattomampien valmistajien Android-laitteissa. Haittaohjelmalla laite voidaan liittää osaksi bottiverkkoa. Lisäksi se voi kerätä käyttäjästään tietoa, näyttää vääriä mainoksia ja välittää muita haittaohjelmia.[27]

- BadBox 2.0 voi olla valmiiksi esiasennettuna laitteeseen jo tuotantolinjalla, mutta sitä voidaan jakaa myös haitallisten sovellusten ja epäilyttävien verkkosivustojen kautta.

Uhkaan pyritään puuttumaan sääntelyllä

- EU:n kyberkestävyyssäädös CRA:n tavoitteena on parantaa EU:n markkinoille saatettujen tuotteiden tietoturvaa niin, että tuotteissa on vähemmän haavoittuvuuksia.
- EU:n markkinoille saatetut tuotteet on 11.12.2027 lähtien suunniteltava, kehitettävä ja tuotettava EU:n kyberkestävyyssäädöksen olennaisten kyberturvallisuusvaatimusten mukaisesti.[28]
- Tammikuussa annetussa kyberturvallisuusasetuksen päivityksen (CSA2) ehdotuksessa kiinnitetään huomiota mm. kyberturvallisuussertifiointiin sekä ICT-toimitusketjujen turvallisuuteen. Näillä toimilla on vaikutuksia verkkolaitteiden turvallisuuteen.[29]

Heikosti suojattujen verkkolaitteiden uhka tuskin katoaa lähitulevaisuudessa, eikä sääntely välttämättä riitä kitkemään heikosti suojattuja verkkolaitteita markkinoilta. Ilmiöön voidaan pystyä vaikuttamaan tiedon jakamisella heikosti suojattujen laitteiden uhkista sekä kuluttajien kyberhygieniataitojen kehittämisellä.

Top 5 uhat lähitulevaisuudessa

1 Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

Haavoittuvuuden korjaavan päivityksen asentamisen lisäksi on usein tarpeen tutkia, onko haavoittuvuutta hyödynnetty jo ennen päivityksen asentamista.

2 Tekoälyn käytön lisääntyminen edellyttää riskienhallintaa

Organisaatioiden varautuminen ja aktiiviset riskienhallinnan toimet ovat tärkeitä nopeasti lisääntyvän tekoälyn käytön myötä.

3 Toimitus- ja palveluketjujen tietoturva ja jatkuvuus

Alihankintaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä. Valtaosa organisaatioista on enemmän tai vähemmän riippuvaisia ulkoistetuista digitaalisista palveluista.

4 Kriittisen infrastruktuurin suojaamisen tärkeys korostuu

Nopeasti muuttuva kybertoimintakenttä vaikuttaa kriittisen infrastruktuurin suojaamiseen.

5 Kiristyshaittaohjelmat ovat merkittävä uhka organisaatioille

Kiristyshaittaohjelmien määrä kasvaa globaalisti jatkuvasti.

● = uusi uhka Top 5 -listalla

1 Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

Rikolliset ja valtiolliset toimijat pyrkivät hyväksikäyttämään haavoittuvuuksia ennen kuin niitä on ehditty korjata. Haavoittuvuuden aktiivinen hyväksikäyttö saattaa usein tapahtua jo ensimmäisen vuorokauden sisällä siitä, kun haavoittuvuudesta on tullut julkinen.

- Järjestelmien nopea päivittäminen on erityisen tärkeää. Valmius päivittämiseen on syytä ylläpitää jatkuvasti, myös loma-aikoina.
- Haavoittuvan järjestelmän päivittämisen lisäksi on tärkeää tutkia, onko haavoittuvuutta jo ehditty hyväksikäyttää ennen sen korjaamista.

Myös vanhoja haavoittuvuuksia hyödynnetään edelleen onnistuneesti. Hyökkääjät etsivät haavoittuvuuksia julkaistujen päivitysten sisällöstä. Haavoittuvuuksia etsitään aktiivisesti myös ohjelmistopäivitysten muistioista, mikä altistaa päivittämättömiä laitteita hyökkäyksille.

Haavoittuvuuksiin liittyvää uhkaa lisäävät uudet tekoälytyökalu, jotka mahdollistavat massamaisen ja automatisoidun haavoittuvuuksien etsimisen, tunnistamisen ja hyväksikäytön. Tekoälytyökaluilla kirjoitetaan haavoittuvuuksien hyväksikäyttökoodia.

Löydettyjen haavoittuvuuksien määrä kasvoi edelleen vuonna 2025.

Verkon reunalaitteet muodostavat merkittävän rajapinnan hyökkäyksille, joita toteutetaan usein nollapäivähaavoittuvuuksien kautta. Monien merkittävien laitevalmistajien verkon reunalaitteissa, kuten VPN-yhdyskäytävissä, on havaittu vakavia ja helposti hyödynnettäviä haavoittuvuuksia viimeisen vuoden aikana.

- Pääosa verkon reunalaitteisiin kohdistuvista hyökkäyksistä on opportunistisia. Reunalaitteet ovat kuitenkin viime aikoina korostuneet valtiollisten toimijoiden vaikuttamisen kohteena.
- Haavoittuvuuksiin liittyvien uhkien hallinnassa korostuvat sekä havainnointi että reagointikyky. Järjestelmäympäristön valvonta ja haavoittuvuuksien etsiminen edistää hyökkäysten rajoittamista. On hyvä seurata valmistajan ohjeita tietomurtojen ja hyväksikäytön havaitsemiseksi.
- Organisaatioilla tulee myös olla suunnitelma hyökkäyksestä ja sen vaikutuksista palautumiseen.

2 Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa

Erilaiset tekoälysovellukset saattavat aiheuttaa uusia ja yllättäviä tietoturvauhkia organisaatioille. Tekoälytyökalujen ja -ohjelmistojen käyttöönotto lisää organisaation hyökkäyspintaa.

Etenkin tekoälyn hallitsematon käyttöönotto, ”varjo-AI”, luo organisaatioille haasteen. Moniin tuotteisiin on integroitu yllättäviä tekoälytoiminnallisuuksia, joita työntekijät voivat ottaa käyttöön epävirallisesti, organisaation tietoturvapolitiikan vastaisesti.

Organisaatioiden on tekoälyn käytössä hyvä ottaa huomioon erityisesti tietosuoja- ja salassapitonäkökulmat, ja pohtia näihin liittyviä linjauksia organisaatiossa.

- Tekoälyn käyttöön tulisi laatia organisaation sisäinen käyttöpolitiikka ja ohjeistus henkilöstölle siitä, miten tekoälyä voi sallitulla tavalla hyödyntää työssä. Tekoälyn huoleton käyttö on yleinen riski. Arkaluontoista tietoa saattaa päätyä käyttäjien välityksellä erilaisiin tekoälypalveluihin.[30]
- Integroiduilla tekoälysovelluksilla saattaa olla laaja pääsy organisaation dataan. Riskit korostuvat, jos sovellus säilyttää tai käsittelee dataa organisaation ulkopuolisella palvelimella.[31]

Tekoälytyökalut mukana kyberrikollisten työkalupakissa

Kyberuhkatoimijat käyttävät yhä aktiivisemmin tekoälypalveluita haittaohjelmien ja hyökkäysten jalostamiseen. Tekoälyä hyödynnetään esimerkiksi kalasteluviestien laatimiseen, haittaohjelmien kehittämiseen tai haitallisen koodin tulkittavuuden hankaloittamiseen (obfuscation).

- Uudet tekoälytyökalut myös mahdollistavat massamaisen ja automatisoidun haavoittuvuuksien etsimisen, tunnistamisen ja hyväksikäytön.[32]

Rikolliset käyttävät syvävääreennöksiä eli deepfake-teknologiaa vakuuttavien huijauksien ja kalastelujen tekemiseen. Kyberturvallisuuskeskukselle tehtyjen ilmoitusten perusteella suomenkielisien syvä-väärennöksien käyttö ei kuitenkaan vielä ole yleistä.

3 Toimitus- ja palveluketjujen tietoturva ja jatkuvuus ovat yhä kriittisempiä

Alihankkijaketjun ymmärtäminen on organisaatioiden kyberturvallisuuden kannalta keskeistä. Valtaosa organisaatioista on enemmän tai vähemmän riippuvaisia ulkoistetuista digitaalisista palveluista.

- Toimitusketjuihin liittyvä uhka ei kohdistu pelkästään komponentteihin, vaan saattaa konkretisoitua esimerkiksi ohjelmistojen ja ohjelmointikirjastojen kautta.

Kyberturvallisuuskeskukselle ilmoitetuissa tapauksissa vaikuttaa usein siltä, että alihankintaketjuihin liittyvät vastuut ovat organisaatioille epäselviä. Vastuut tulisi määritellä selkeästi etukäteen myös mahdollisia poikkeamatilanteita varten.

- Toimintakulttuurilla ja prosesseilla on suuri merkitys uhkien havaitsemisessa, tunnistamisessa ja tiedon jakamisessa.

Tekoälyn käyttöönoton lisääntyessä myös toimitusketjuihin kohdistuva riski kasvaa, sillä tekoälyjärjestelmien integrointi organisaatioiden ympäristöihin luo uuden, potentiaalisesti haavoittuvan hyökkäyspinnan.

- Avoimen lähdekoodin ohjelmistot erityisen alttiita riskille, jonka tekoälytyökalujen automaattinen haavoittuvuuksien etsintä muodostaa. Jopa 80 % ohjelmistoista hyödyntää tavalla tai toisella avointa lähdekoodia.

Toimitusketjuhyökkäys voi vaikuttaa lamauttavasti organisaation toimintaan. Kriittistä on ymmärtää omat alihankkijaketjut ja olla tietoinen sopimusyksityiskohdista palveluntarjoajien kanssa. On tärkeä selvittää kolmannen osapuolen tietoturvan taso ja ulottaa tietoturvallisuuden hallinta myös palveluihin, kattaen esimerkiksi:

- Konsultit ja heidän organisaatioidensa sisäiset järjestelmät.
- Laitteistot ja palvelut, joita voidaan käyttää joko osana omaa tuotetta, palvelukokonaisuutena tai ostettuna palveluna.

Organisaation tulee ymmärtää koko alihankintaketju, sillä myös organisaation alihankkija voi hankkia tuotteen tai palvelun seuraavana ketjussa olevalta palveluntarjoajalta.

- Varautuminen on keskiössä: Hyökkäysten vaikutusten pienentämiseksi organisaatioiden kannattaa pohtia palveluntarjoajaan tai toimitusketjun osaan kohistuvan hyökkäysten mahdollisia vaikutuksia, sekä tapoja häiriötilanteiden hallintaan.

4 Kriittisen infrastruktuurin suojaamisen tärkeys korostuu

Kriittiseen infrastruktuuriin ja organisaatioihin kohdistuvat kyberuhat ovat toimintaympäristön jatkuvan ja nopeaan muutoksen kohteina.

Kansallinen kyberturvallisuuden uhkataso on ollut kohonneena syyskuusta 2022. Kyberturvallisuuskeskus ja suojelupoliisi nostivat uhkatasoa kiristyneen kansainvälisen tilanteen vuoksi.

Nopeasti muuttuva kyberuhkien kenttä vaatii kyberuhkilta suojautumisessa ja varautumisessa jatkuvaa valppautta ja proaktiivisia toimia.

Huoltovarmuuskeskuksen toimialojen kyberkypsyysselvityksen 2025 mukaan kansallisen kyberkypsyyden taso on kuitenkin kehittynyt vain maltillisesti vuodesta 2022.[33]

Kriittinen infrastruktuuri on keskeinen kiinnostuksen kohde muiden Kybersäähän nostettujen kyberuhkien kohdalla.

- Verkon reunalaitteiden suojaaminen, ohjelmistojen ja laitteiden päivittäminen ja toimitusketjujen tietoturvallisuuden varmistaminen ovat keskeisiä suojaamistoimia.

Toimitusketjuihin kohdistuvien poikkeamien kautta kriittisen infrastruktuurin turvallisuuteen voi vaikuttaa laajan organisaation tietoturvakäytännöt.

Viimeisten vuosien aikana Suomessa on tapahtunut useita tietoliikenneinfrastruktuuriin kohdistuneita vahinkoja ja luonnonilmiöitä, sekä ulkopuolisten tekijöiden aiheuttamia tahallisia häiriöitä.

- Häiriönsietoa voidaan parantaa esimerkiksi kahdentamalla kriittisiä järjestelmiä ja yhteyksiä, sekä varmistamalla niiden sähkönsaanti lyhyen sähkökatkoksen varalta.
- Kaikkien tietoliikenne- ja tietojärjestelmäinfrastruktuurin omistajien kannattaa huolehtia viestintäverkkojen ja -palveluiden fyysisestä suojaamisesta.

5 Kiristyshaittaohjelmat ovat merkittävä uhka organisaatioille

Kiristyshaittaohjelmien määrä kasvaa globaalisti jatkuvasti. Kiristyshaittaryhmien toiminta on opportunistista, ja sen kohteet voivat muuttua nopeasti esimerkiksi uusien haavoittuvuuksien mukaan.

Kiristyshaittaohjelmien tapausmäärät voivat myös Suomessa muuttua yllättävästi. Kiristyshaittaohjelmien uhka on säilynyt ennallaan, vaikka Kyberturvallisuuskeskukselle ilmoitetut tapausmäärät ovat viime vuosina laskeneet. Eurooppa on maantieteellisesti toisella sijalla verkkorikollisuuden kohdealueena.[34]

- Kiristystapaustoiminnan arviointiin pätee ns. Iceberg-viitekehys: tilastot eivät kerro koko totuutta. Toimintaa tapahtuu todennäköisesti enemmän kuin mitä sitä havaitaan ja raportoidaan.

Kiristyshaittaohjelmailmiö ja siihen liittyvä palvelutuotanto on jatkuvassa kehityksessä, ja esimerkiksi hyökkäysten eri osia on ulkoistettu palveluiksi.

- Yli 97 % identiteettihyökkäyksistä on salasanahyökkäyksiä. Valtaosa haitallisista kirjautumisyrityksistä tapahtuu laajamittaisten brute force -hyökkäysten kautta. Hyökkääjät saavat käyttäjätunnuksia ja salasanoja pääasiassa tunnistetietovuotojen kautta. Kyberrikollisten on myös havaittu käyttävän yhä enemmän tietoja varastavia haittaohjelmia.[35, 36]

Kiristyshaittaohjelma tartutetaan usein kalasteluviestin, vuotaneiden käyttäjätunnusten tai päivittämättömien haavoittuvuuksien kautta. Tiedostojen salaus ja muut hyökkääjän tekemät toimenpiteet saatetaan toteuttaa viipymättä sisäänpääsyn jälkeen.

Viime aikoina kansainvälisesti kiristyshaittaohjelma-hyökkäyksissä on korostunut tiedostojen salaamisen sijaan datan nopea varastaminen kohdejärjestelmästä. Tapauksissa kiristäjä lupaa lunnaita vastaan hävittää varastetun aineiston tai jättää sen julkaisematta.

Kiristyshaittaohjelmahyökkäys voi kohdistua toimitusketjuun ja levitä sitä kautta nopeasti useisiin organisaatioihin samalla kertaa. Varsinkin huoltovarmuuskriittisten organisaatioiden joutuessa uhriksi voivat yhteiskunnan elintärkeät toiminnot vaarantua.

- Kiristyshaittaohjelma saattaa pahimmassa tapauksessa lopettaa organisaation toiminnan kokonaan.
- Kiristyshaittaohjelmien torjunnassa ennaltaehkäisy, havainnointi ja nopea reagointi ovat avainasemassa. Varmuuskopiot voivat nopeuttaa kiristyshaittaohjelmahyökkäyksestä toipumista.

Tietoturva-alan kehitys, sääntely ja standardit

Tietoturva-alan kehitys -osiossa kerromme keskeisistä uudistuksista esimerkiksi alaa koskevan lainsäädännön tai asetusten päivityksiin liittyen. Kerromme kaikille tärkeää kyberturvallisuustietoa ja Kyberturvallisuuskeskuksen ajankohtaisista asioista.

Oikeudelliset asiat
Hallitus linjasi kantojaan EU-kyberturvallisuussääntelyyn

- Euroopan komissio antoi tammikuussa 2026 ehdotukset kyberturvallisuusasetuksen uudistamisesta (CSA2) ja kyberturvallisuusdirektiivin (NIS2) muuttamisesta.[37]
- Uutena asiana säädettäisiin ICT-toimitusketjujen turvallisuudesta, kriittisten ICT-osien tunnistamisesta ja korkean riskin toimittajien määrittämisestä EU-tasolla.
- ENISA:n tehtävät uudistettaisiin ja eurooppalainen kyberturvallisuuden sertifiointikehys (ECCF) selkeytettäisiin
- NIS2-direktiiviin esitetään kohdennettuja muutoksia ja joidenkin uusien toimijoiden lisäämistä.
- Hallitus antoi eduskunnalle 12.3.2026 kirjelmän valtioneuvoston kannasta komission ehdotuksiin. Valtioneuvosto pääosin kannattaa ehdotuksia ja niiden tavoitteita.
- EU-tasoisia ratkaisuja ICT-toimitusketjujen turvallisuudesta ja siihen liittyviä tavoitteita pidetään kannatettavina.
  - Toimenpiteiden tulisi kuitenkin olla oikeasuhtaisia ja riskiperustaisia.
- NIS2-muutosehdotuksien tavoitetta sääntelyn yksinkertaistamisesta ja sääntelystä aiheutuvien hallinnollisten kustannusten alentamisesta pidetään kannatettavana.

Oikeudelliset asiat
Hallitus kannattaa EU:n viestintäverkkoja koskevan sääntelyn nykyaikaistamista

- Euroopan komissio antoi 21.1.2026 ehdotuksen uudesta digitaalisia verkkoja koskevasta asetuksesta (Digital Networks Act).[38]
- Asetuksen tarkoituksena on yhdenmukaistaa ja nykyaikaistaa EU:n viestintäverkkoja koskevaa sääntelyä. Rajat ylittävää liiketoimintaa helpotetaan ja yritysten hallinnollista taakkaa pyritään keventämään.
  - Teleyritykset voisivat jatkossa yhdessä jäsenvaltiossa tehdyn rekisteröintimenettelyn kautta toimia myös muissa EU:n jäsenvaltioissa.
  - Satelliittiviestintäpalveluille annettaisiin jatkossa EU:n laajuinen valtuutus.
  - Taajuuksien käyttöön oikeuttavat verkkotoimiluvat olisivat toistaiseksi voimassa olevia ja niiden uusiminen olisi mahdollista ilman uutta lupaprosessia.
  - Hallinnollisia uudistuksia ehdotetaan Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelin BEREC:in ja sen sihteeristön, sekä radiotaajuuspolitiikkaryhmä RSPG:n osalta.
- Eduskunnalle 1.4. annetussa kirjelmässä valtioneuvosto kannattaa EU:n sähköisen viestinnän sisämarkkinoiden kehittämistä.
- Komission ehdotusta kannatetaan sääntelyn keventämisen ja joustavoittamisen osalta. Sääntelyä sujuvoittavia toimia voitaisiin toteuttaa komission ehdotustakin rohkeammin.
- Rajallisten, yhteiskunnallisesti ja taloudellisesti merkittävien radiotaajuuksien käytön on oltava tehokasta. Ennakoitava taajuussuunnittelu lisää toimintaympäristön investointimyönteisyyttä.
- Jäsenvaltioiden tulisi sitoutua taajuuksien nopeaan käyttöönottoon.
  - Valtioneuvosto pitää tärkeänä, että EU-sääntely mahdollistaa riittävän kansallisen liikkumavaran esimerkiksi toimilupaprosesseihin ja verkkotoimilupien ehtoihin liittyen.

Epäiletkö tietoturvaloukkausta?

Jos teihin on kohdistunut tai epäilette teihin kohdistuneen tietoturvaloukkauksen, olkaa yhteydessä Traficomin Kyberturvallisuuskeskukseen.

- Sähköinen lomake www.kyberturvallisuuskeskus.fi/fi/ilmoita
- Sähköposti: cert@traficom.fi
- Puhelin: 0295 345 630 (arkisin klo 9-15)

Muissa asioissa voitte olla meihin yhteydessä osoitteessa kyberturvallisuuskeskus@traficom.fi.

Kyberturvallisuuskeskuksen eri toimintojen ja hankkeiden yhteystiedot löydät keskitetysti osoitteesta www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot.

Lähteet

Lähdeluettelo
1/4

1. https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

2. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-102026#107448-0

3. https://www.sans.org/blog/when-security-scanner-became-weapon-inside-teampcp-supply-chain-campaign

4. https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

5. https://supo.fi/-/viranomaisten-yhteisoperaatio-torjui-venajan-kybervakoilua

6. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille/miten-viestimme-0

7. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-142026#97997-4

8. https://www.kyberturvallisuuskeskus.fi/fi/tonttu

9. https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/ohjelmistoturvallisuuden-johtaminen-roolit-ja-osaamistarpeet

10. https://www.kyberturvallisuuskeskus.fi/fi/tapahtumat/kriittinen-koodi-webinaari-ohjelmistoturvallisuusoppaiden-julkistustilaisuus-103

Lähdeluettelo
2/4

11. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/telegram-ja-whatsapp-pikaviestitilit-kaappausyritysten-kohteena

12. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-132026#97891-1

13. https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/praevention_wirtschafts-und_wissenschaftsschutz/2026-02-06-gemeinsame-warnmitteilung-phishing.pdf?__blob=publicationFile&v=3

14. https://english.aivd.nl/latest/news/2026/03/09/russia-targets-signal-and-whatsapp-accounts-in-cyber-campaign

15. https://www.acn.gov.it/portale/en/w/signal-campagna-attiva-finalizzata-all-account-takeover

16. https://traficom.fi/fi/uutiset/viranomaisten-yhteisoperaatio-torjui-venajan-kybervakoilua

17. https://www.wiz.io/blog/trivy-compromised-teampcp-supply-chain-attack

18. https://www.sans.org/blog/when-security-scanner-became-weapon-inside-teampcp-supply-chain-campaign

19. https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/kriittinen-haavoittuvuus-citrix-netscaler-adc-ja-netscaler-gateway-tuotteissa

20. https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/kriittinen-haavoittuvuus-f5-big-ip-apm-paasynhallintajarjestelmassa

21. https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/kriittinen-haavoittuvuus-axios-javascript-paketin-npm-jakelussa

Lähdeluettelo
3/4

22. https://www.bbc.com/news/articles/c74787w149zo

23. https://yle.fi/a/74-20212565

24. https://yle.fi/a/74-20212545

25. https://traficom.fi/fi/uutiset/viranomaisten-yhteisoperaatio-torjui-venajan-kybervakoilua

26. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ipidea-kotilaitteita-hyodyntava-valityspalveluverkko

27. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haittaohjelma-voi-lymyilla-laitteessa-jo-ostovaiheessa-laitteet-poistettava-kaytosta

28. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/kyberkestavyyssaados-cyber-resilience-act-cra

29. https://lvm.fi/-/komissio-antoi-ehdotukset-uudesta-kyberturvallisuussaantelysta-ja-digiverkkoasetuksesta

30. https://www.theregister.com/2025/10/07/gen_ai_shadow_it_secrets/

31. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ole-valppaana-tekoalyn-kanssa

32. https://pudgycat.io/ai-found-500-zero-days-open-source/

Lähdeluettelo
4/4

33. https://www.huoltovarmuuskeskus.fi/julkaisu/kyberkypsyys-toimialoilla-2025-kansallinen-koosteraportti
34. https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-2025-european-threat-landscape-report-ransomware
35. https://blogs.microsoft.com/on-the-issues/2025/10/16/mddr-2025/
36. https://www.fortinet.com/resources/cyberglossary/ransomware-statistics
37. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act
38. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-digital-networks-act-dna