TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Helmikuu 2025

#kybersää

Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä.

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

Kybersää voi olla:  rauhallinen  huolestuttava  vakava

Kuukauden tunnuslukuja

Haktivistit näyttävät siirtyvän perinteisistä palvelunestohyökkäyksistä kohti matalalla roikkuvia tietomurtoja. Esimerkiksi haktivistiryhmä PENTEST-Z:iin julkisuudessa liitetyissä hyökkäyksissä useisiin eurooppalaisiin teollisuusautomaatiojärjestelmien on korostunut kaksi toimialaa: vesi ja energia.[1]

Kyberturvallisuuskeskuksen kansallinen koordinointikeskus myönsi vuosina 2023 - 2024 mikro- ja pk-yrityksille rahoitustukea modernien tieto- ja kyberturvaratkaisujen käyttöönottoon ja innovointiin yhteensä noin 2 milj. euroa.[2]

Alue- ja kuntavaalit pidetään 13.4.2025. Kyberturvallisuuskeskus tukee puolueiden ja ehdokkaiden vaalien kyberturvallisuutta esimerkiksi uutiskirjein, sekä ohjeistamalla älylaitteiden ja sosiaalisien median tilien tietoturvallista käyttöä.[3]

Kybersää helmikuu 2025

Tietomurrot ja -vuodot

- M365-tilien murtaminen Dropbox-teemaisilla viesteillä jatkui runsaana. Murretuilta tileiltä tehtiin laskutushuijauksia ja lähetettiin uusia kalasteluviestejä.
- Organisaatioihin kohdistui brute force -hyökkäyksiä, joista muutama oli poikkeuksellisen massiivinen.
- Facebook-tilejä kaapattiin kysymällä puhelinnumeroa ja vahvistuskoodia kilpailun verukkeella Messengerissä.

Huijaukset ja kalastelut

- Suomalaiset luottavat poliisiin. Huijarit ovat hyödyntäneet tätä ja lähettäneet huijausviestejä poliisin nimissä, soittaneet puheluita Europolin virkamieheksi tekeytyneinä ja väärentäneet tekstiviestejä oikeuslaitoksen nimiin.
- Verottajan nimiin väärennetyillä huijauksilla on yritetty päästä käsiksi pankkitunnuksiin.

Haittaohjelmat ja haavoittuvuudet

- Useita ilmoituksia Magecart-hyökkäyksistä suomalaisiin verkkokauppoihin.
- Ilmoituksia sähköposteista joissa QR-koodin sisältäviä liitetiedostoja

Automaatio ja IoT

- Suomessa myydyimmät IoT-laitteet eivät täytä tällä hetkellä kaikkia radiolaitedirektiivin (RED) vaatimuksia[4]. Direktiivin soveltaminen alkaa 08/2025.
- IoT-laitteita unohtuu kentälle. Tilojen valvontasuunnitelma, asennettujen laitteiden elinkaaren dokumentointi sekä prosessit tiloihin kuulumattomien laitteiden havaitsemiseen auttavat.

Verkkojen toimivuus

- Helmikuussa yleisissä viestintäverkoissa havaittiin neljä toimivuushäiriötä.
- Ilmoitettujen palvelunestohyökkäysten määrässä on havaittavissa pientä laskua.
- Palvelunestohyökkäykset eivät aiheuttaneet merkittäviä häiriöitä suomalaisiin verkkopalveluihin helmikuun.

Vakoilu

- Venäjään julkisuudessa yhdistetyt APT-ryhmät hyödyntävät Microsoftin pilvisähköpostitileihin kohdistuvaa kalastelumenetelmää, jossa uhri huijataan vahvistamaan hyökkääjän laitetunnuksen yhdistäminen uhrin tiliin, jolloin hyökkääjä saa pääsyn tilille.[5] Venäläistoimijat ovat hyödyntäneet laitelinkitystä myös Signal-tileihin kohdistuneessa kalastelussa.[6]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Riskienhallinta on avain ohjelmistoturvallisuuteen – ja kilpailuetu. Turvallinen ohjelmistokehitys ei ole vain tekninen vaatimus, vaan varmistaa liiketoiminnan jatkuvuuden, ohjelmistojen luotettavuuden ja siten asiakkaiden luottamuksen ylläpidon. Ennakoiva riskienhallinta auttaa tunnistamaan ohjelmistokehityksen ja hankintojen riskit ajoissa, mikä vähentää korjauskustannuksia ja tietoturvauhkia.[7]

Kyberturvallisuuskeskus on saanut ilmoituksia suomalaisiin verkkokauppoihin kohdistuvista Magecart-hyökkäyksistä, joissa verkkokauppaan lisätään haitallisia lisäosia tai sen lähdekoodiin lisätään haitallista koodia. Jos pidät verkkokauppaa, huolehdi järjestelmänvalvojan admin-tunnuksistasi ja verkkokaupan päivityksistä. Tarkista verkkokauppasi tarvittaessa haitallisen koodin tai haitallisten lisäosien varalta.[8].

Yritysten sisäverkkoon tarkoitettujen laitteiden ja sertifikaattien näkyvyyttä julkiverkosta on hyvä tarkastella säännöllisesti. Esimerkiksi Censys-palvelussa voi etsiä omia laitteita. Tuloksissa kannattaa huomioida, miten laitteiden sertifikaatit on allekirjoitettu, mitä palveluita havaitaan ja missä laitteet sijaitsevat.

Selvitys: Satelliittilaajakaista tarjoaa merkittävän vaihtoehdon ja lisäresurssin organisaatioiden varautumisessa tietoliikenneverkkojen häiriötilanteisiin. KTK:n ja Huoltovarmuuskeskuksen tuoreen selvityksen tarkoituksena on luoda yleiskuva satelliittilaajakaistateknologioiden ja -palveluiden hyödyntämisestä huoltovarmuuskriittisten organisaatioiden varautumisessa. Selvitys on käyttökelpoinen myös muille organisaatioille, jotka haluavat hyödyntää satelliittilaajakaistateknologioita ja –palveluita.[9]

Helmikuun kyberturvallisuuden yleiskuva

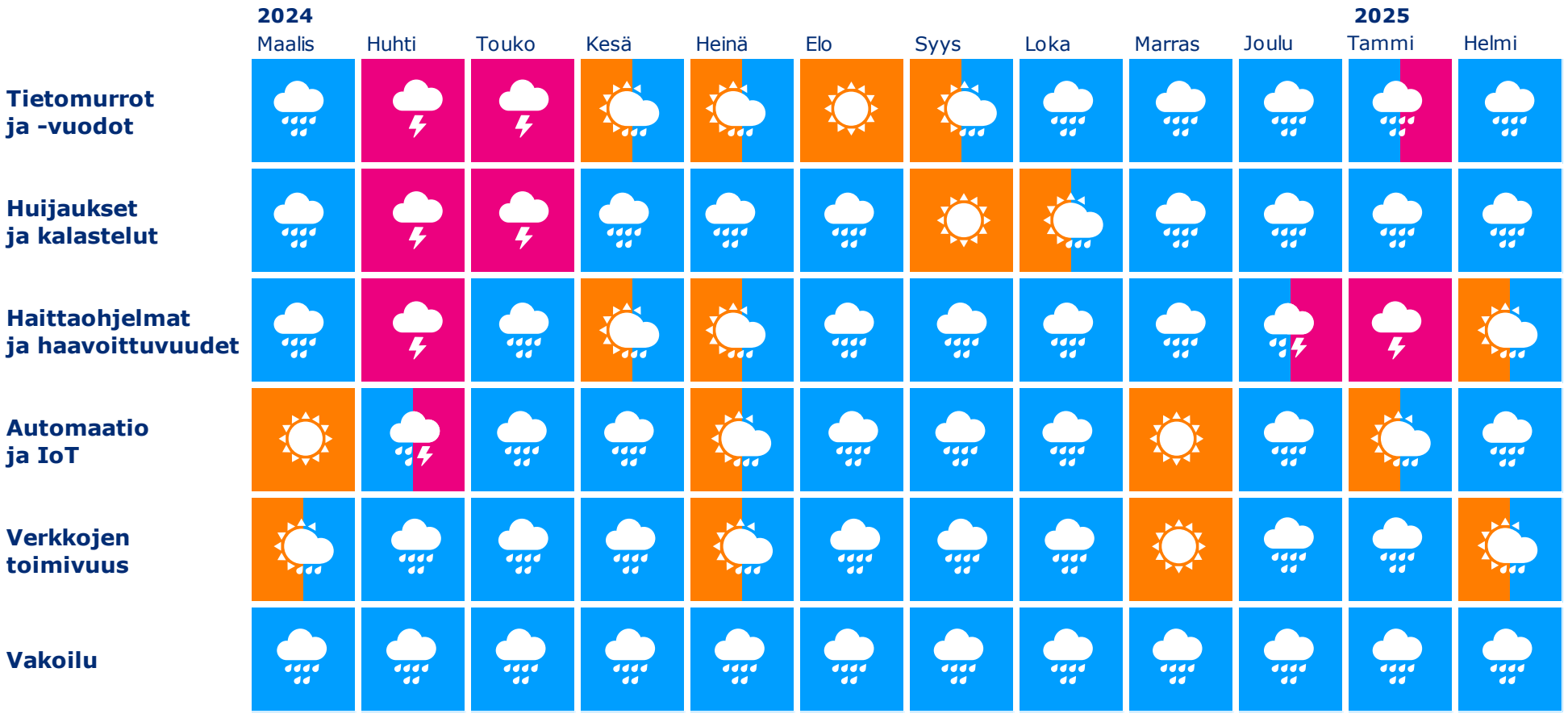
- Helmikuun räntäsateita ovat aiheuttaneet kriittiset haavoittuvuudet Ivantin Connect Secure ja Policy Secure – tuotteissa, jotka ovat mahdollistaneet mielivaltaisen koodin suorittamisen haavoittuvalla laitteella[10]. Vakava haavoittuvuus Palo Alton PAN-OS järjestelmässä on mahdollistanut tunnistautumisen ohittamisen ja komentojen suorittamisen laitteella.[11]
- TJ-huijauksia on liikkeellä osoitteista *etunimi.sukunimi.organisaatio/domain[at]outlook[.]com.*[12]
  - Huijausten suomenkieli on ollut aiempaa virheettömämpää ja niissä puhutellaan usein vastaanottajaa etunimellä. Huijaus lähtee liikkeelle viestillä, jossa pyydetään vastaanottajalta palvelusta ja pyydetään vastaamaan sähköpostilla tilanteen takia. Mikäli huijausviestiin vastaa, huijari pyytämää uhria hankkimaan lahjakortteja organisaatiolle yrityslahjoiksi.
- Viranomaisten nimissä tehtyjä kalasteluja runsaasti liikkeellä:[13]
  - Kyberturvallisuuskeskus sai helmikuussa useita ilmoituksia eri viranomaisten nimissä tehdyistä huijausviesteistä ja –puheluista. Huijauksien tavoitteena on ollut saada uhri luovuttamaan arkaluonteisia tietojaan, kuten pankkitietoja. Viranomainen ei koskaan pyydä puhelimessa luovuttamaan pankkitunnuksia tai maksukorttitietoja.
  - Viranomaiselta tulevan puhelinsoiton aitouden voi varmistaa esimerkiksi kyseisen viraston asiakaspalvelusta tai vaihteesta. Yhteystiedot löytyvät virastojen verkkosivuilta. Eri viranomaiset tiedottavat verkkosivuillaan aktiivisesti myös nimissään liikkuvista huijauskampanjoista. Ajankohtaisiin huijauksiin voit tutustua myös Kyberturvallisuuskeskuksen viikkokatsauksissa.
- M365
  - Kyberturvallisuuskeskuksen tietoon tulleissa M365-tietomurtotapauksissa käyttäjätilille on yritetty kirjautua jopa minuuttien sisällä siitä, kun tunnukset on syötetty kalastelusivulle. Useissa tapauksissa tietomurron jälkeen tililtä on haettu laskutukseen liittyviä tietoja ja yritetty laskutushuijausta vaihtamalla laskun vastaanottajan tilinumero rikollisen tilinumeroksi.[14]
  - Vaikka valtaosassa tapauksista havitellaan rahallista hyötyä, on hyvä muistaa, että käyttäjätileistä voivat olla kiinnostuneita muutkin kuin opportunistit. Muun muassa tietoturvayritykset Microsoft ja Volexity ovat kertoneet valtioon liitetyn kyberuhkatoimijan tuoreesta kampanjasta, jossa tavoitellaan Microsoft 365 -pilvipalvelutunnuksia. Kampanja on kohdistunut ainakin seuraaville sektoreille: valtionhallinto, ICT- ja telepalvelutarjoajat, terveydenhuolto, puolustus ja energia-ala.[15]

Ilmiöiden ja toimialojen trendit

Osiossa käymme läpi kyberturvallisuuden ilmiöiden kehitystä ja trendejä eri aikaväleillä. Toimialakohtaisissa nostoissa on esitelty eri toimialojen tilannetta yleistasolla.

Kyberturvallisuuden trendit
kulunut 12 kk

1 kk



Pitkä aikaväli ja lähitulevaisuus

Osiossa on esitelty pitkän aikavälin ja lähitulevaisuuden kyberturvallisuuden ilmiöitä. Seuraamiemme pitkän aikavälin ilmiöiden joukosta analysoidaan kuukausittain yksi ilmiö. Top 5 –kyberuhkat kertovat puolestaan lähitulevaisuuden uhkista.

Pitkän aikavälin (5v+) kybersää: ilmiöt joita seuraamme

Pitkän aikavälin kybersää: Toimitusketjujen tietoturva

- Toimitusketjuhyökkäykset ovat jatkuneet globaalisti vuoden 2025 alussa. IT-palveluntarjoajat ovat tällä hetkellä toimitusketjuhyökkäysten kärkikohteita. Noin 1/3 osaa kaikista toimitusketjuhyökkäyksistä kohdistuu IT-palveluntarjoajiin.[16]
- Muun muassa hyökkäyspinta-alan kasvun (mm. pilvipalvelut), haavoittuvuuksien, epätietoisuuden kolmannen osapuolen tuotteista ja prosesseista sekä tekoälyavusteisten hyökkäysten on havaittu vaikuttavan toimitusketjuhyökkäysten kasvuun.[17]
- Esimerkiksi NIS 2-direktiivin mukaan viestintäverkkoihin ja tietojärjestelmiin sekä niiden fyysiseen ympäristöön kohdistuvat riskit tulisi tunnistaa kaikki vaaratekijät huomioiden[18]. Uhkamallinnoksella ja riskienhallinnalla kyetään vähentämään esimerkiksi ohjelmistojen osalta toimitusketjuihin kohdistuvaa kyberuhkaa[19].
  - Ohjelmistoriippuvuuksien hallinta on kriittinen osa yrityksen kyberturvallisuutta. Kolmannen osapuolen komponentit ja kirjastot nopeuttavat ohjelmistokehitystä, mutta samalla ne voivat tuoda mukanaan haavoittuvuuksia, jotka altistavat koko järjestelmän kyberuhkille.
  - Riskienhallinta tulee aloittaa kartoittamalla kaikki käytössä olevat kolmannen osapuolen komponentit ja kirjastot sekä tutustumalla niiden lisenssiehtoihin. Tämä antaa pohjan tietoturvalliselle kehitystyölle ja auttaa varautumaan mahdollisiin riskeihin. Software Bill of Materials (SBOM) on hyödyllinen työkalu, jonka avulla voidaan systemaattisesti seurata ohjelmiston sisältämiä riippuvuuksia ja arvioida niiden turvallisuutta.
  - Jatkuvalla testaamisella automaattisilla työkaluilla voidaan tunnistaa ja korjata haavoittuvuuksia ennen kuin ne muodostuvat merkittäväksi uhkaksi. Uhkatekijöitä tunnistaessa kannattaa kyberuhkan lisäksi huomioida myös sisäpiirin uhka, ulkoinen uhka kuten sään ääri-ilmiöt tai yhteiskunnallinen tapahtuma sekä fyysinen uhka kuten murtovarkaus.

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

- Suomen avaruusstrategia 2030 on julkaistu[20]:
  - Suomen avaruusstrategia on uudistettu elinkeinoministeri Wille Rydmanin toimeksiannosta vastaamaan muuttunutta globaalia toimintaympäristöä.
  - Suomen avaruusstrategia on uudistettu vastaamaan muuttunutta globaalia toimintaympäristöä.
  - Avaruusstrategia määrittelee Suomen avaruustoiminnan vision ja päämäärät vuoteen 2030 asti.
  - Strategia korostaa avaruustalouden merkitystä, turvallisuus- ja puolustuspoliittisia näkökulmia sekä huoltovarmuutta.
  - Strategia on valmisteltu työryhmässä työ- ja elinkeinoministeriön yhteydessä toimivan avaruusasiain neuvottelukunnan pääsihteerin johdolla.

Oikeudelliset asiat

- Kriittisen infrastruktuurin tietojen avoin jakaminen arvioidaan uudelleen[21]:
  - Valtiovarainministeriö on asettanut työryhmän, jonka päätavoitteena on tunnistaa kansallisen turvallisuuden kannalta merkitykselliseen kriittiseen infrastruktuuriin liittyvä avoin tieto ja muodostaa ajantasainen tilannekuva tämän tiedon käsittelystä.
  - Arvioitaessa tietojen avointa jakamista kansallisen turvallisuuden näkökulmasta tulee pyrkiä tasapainoon tiedon suojaamisen ja avoimuuden välillä.
  - Julkisen hallinnon tietovarantojen avoimuus edistää demokratian läpinäkyvyyttä sekä hallinnon sisäistä tehokkuutta.
  - Hanke tarkastelee myös lainsäädännön muutostarpeita sekä valmistelee mahdollisia muita toimenpiteitä.
  - Kevään 2025 aikana luodaan alustava tilannekuva, joka samalla toimii työryhmän jatkotyön pohjana. Hankkeen toimikausi on 19.2.2025 – 31.3.2026.

Oikeudelliset asiat

- Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi - liikenne- ja viestintävaliokunnan mietintö valmistunut.[22]
  - Esityksessä ehdotetaan säädettäväksi kyberturvallisuuslaki sekä muutettavaksi useita muita lakeja.
  - Lain soveltamisalaan kuuluville toimijoille asetetaan useita uusia velvoitteita muun muassa riskienhallintaan, tietoturvaan ja raportointiin liittyen.
  - Liikenne- ja viestintävaliokunta kantaa mietinnössään huolta viranomaisresurssien riittävyydestä sekä pitää tärkeänä, että yrityksillä on riittävät resurssit pitämään huolta riittävästä kyberturvallisuudesta.
  - Valiokunta pitää toimijaluetteloon ilmoittamiselle tarkoituksenmukaisena siirtymäaikana yhtä kuukautta lain voimaantulon jälkeen. Riskienhallinnan toimintamallin laatimiselle valiokunta pitää tarkoituksenmukaisena siirtymäaikana kolmea kuukautta lain voimaantulon jälkeen.

Oikeudelliset asiat

- Liikenne- ja viestintävirasto Traficom pyytää lausuntoja verkkotunnusmääräysluonnoksesta[23]:
  - Voimassa oleva verkkotunnusmääräys 68/2016 M on tarkoitus korvata uudella verkkotunnusmääräyksellä ottaen huomioon verkkotunnustoimintoa koskeva uusi lainsäädäntö.
  - Päivitettävän verkkotunnusmääräyksen valmistelu perustuu hallituksen esitykseen kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi (HE 57/2024 vp).
  - Määräyksellä on tarkoitus lisätä valvonnan kannalta tarpeellisia tietoja välittäjäilmoituslomakkeelle, edistää verkkotunnusten käyttäjätietojen oikeellisuutta sekä ajantasaistaa tietoturvavaatimuksia.
  - Verkkotunnusmääräysluonnos on lausuttavana 18.3. asti.

Kybermittari

- Kybermittari-palvelu uudistuu:[24]
  - Kybermittariin on lisätty ja lisätään käytettävyyttä ja prosessia tukevaa materiaalia sekä toiminnallisuutta. Näihin kuuluvat mm. Arviointia tukevat kehityspolut ja käytäntökohtaiset kuvaukset.
  - Kybermittarin, Traficomin NIS2-suosituksen ja kyberturvallisuuden standardien keskinäisen vertailun helpottamiseksi on julkaistu ristiinviittaustaulukko:[25].
  - Raportointi on entistä paremmin muokattavissa organisaation tarpeisiin ja sisältää esimerkiksi NIS2-suosituksen perustason tietoturvakäytäntöihin pohjautuvan listaukseen.
  - Kybermittari-palvelun sisällöstä, uudistuksista ja kehitysideoista järjestetään kolme webinaaria 17.-18.3.2025. Ilmoittautumislomake Kybermittarin sivuilla, tervetuloa mukaan:

Onko teillä jokin Kybermittariin liittyvä idea, palvelu, hanke tai kokemuksia, joista haluaisit kertoa muille tai vaan meille? Jos on, niin ota yhteyttä Kybermittari@traficom.fi tai yhteydenottolomakkeella. Jos kiinnostusta on riittävästi, niin järjestämme aiheesta erillisen webinaarin.

Epäiletkö tietoturvaloukkausta?

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

- Sähköinen lomake: https://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 täältä: https://www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot

Lähdeluettelo

1) CISA ja NSA: Defending OT operatios against ongoing pro-Russia hactivist activity - https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3761830/urgent-warning-from-multiple-cybersecurity-organizations-on-current-threat-to-o/ , Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity - https://www.cisa.gov/resources-tools/resources/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity, Dragos Reports OT/ICS Cyber Threats Escalate Amid Geopolitical Conflicts and Increasing Ransomware Attacks - https://www.dragos.com/resources/press-release/dragos-reports-ot-ics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-attacks/, Targeting Operational Technology: The Hacktivist's Path to Public Attention and Disruption - https://www.dragos.com/blog/hacktivist-tactics-targeting-operational-technology/, Security Navigator 2025 reveals Europe as top target for hacktivism, with groups shifting focus to cognitive warfare - https://newsroom.orange.com/securitynavigator/, Z-PENTEST ALLIANCE - https://www.orangecyberdefense.com/fileadmin/global/CyberIntelligenceBureau/Gangs_Investigations/z-pentest/Z-Pentest_Alliance.pdf, New Russian Threat Group Z-Pentest Targets Energy System Controls - https://thecyberexpress.com/russian-threat-group-z-pentest/
2) Kyberturvallisuuskeskuksen haavoittuvuustiedotteet https://kyberturvallisuuskeskus.fi/fi/haavoittuvuudet?limit=20&offset=0&query=&sort=updated
3) Kyberturvallisuuskeskuksen viikkokatsaus 05/2025: Yhdistysten tietoturvaan on tärkeää panostaa - https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-052025#81928-1
4) D25] State of Union - Heikki Juva - https://www.youtube.com/watch?v=gXucurU5_iY
5) Multiple Russian Threat Actors Targeting Microsoft Device Code Authentication - https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/ ja Storm-2372 conducts device code phishing campaign - https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/
6) Signals of Trouble: Multiple Russia-Aligned Threat Actors Actively Targeting Signal Messenger - https://cloud.google.com/blog/topics/threat-intelligence/russia-targeting-signal-messenger
7) Kyberturvallisuuskeskuksen viikkokatsaus 06/2025 - https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-062025#82301-0]
8) Kyberturvallisuuskeskuksen viikkokatsaus 09/2 025 - https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-092025#83023-0) ja Digitaalinen skimmaus - vinkkejä verkkokaupan suojaamiseen: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/digitaalinen-skimmaus-vinkkeja-verkkokaupan-suojaamiseen
9) Satelliittilaajakaista auttaa tietoliikenneverkkojen häiriöihin varautumisessa - https://www.traficom.fi/fi/ajankohtaista/satelliittilaajakaista-auttaa-tietoliikenneverkkojen-hairioihin-varautumisessa
10) Kriittisiä haavoittuvuuksia Ivanti Connect Secure ja Ivanti Policy Secure - https://kyberturvallisuuskeskus.fi/fi/haavoittuvuus_6/2025
11) Vakava haavoittuvuus Palo Alton PAN-OS järjestelmässä - https://kyberturvallisuuskeskus.fi/fi/haavoittuvuus_7/2025
12) Kyberturvallisuuskeskuksen viikkokatsaus - 08/2025 - https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-082025
13) Kyberturvallisuuskeskuksen viikkokatsaus 08/2025 - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-082025#82609-4

Lähdeluettelo

14) Kyberturvallisuuskeskuksen viikkokatsaus - 06/2025 - https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-062025#82301-0
15) Esim. Multiple Russian Threat Actors Targeting Microsoft Device Code Authentication - https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/ ja Storm-2372 conducts device code phishing campaign
16) Why Supply Chain Attacks Are The Biggest Threat To Businesses? - https://securityboulevard.com/2025/03/why-supply-chain-attacks-are-the-biggest-threat-to-businesses-2/
17) Why Supply Chain Attacks Are The Biggest Threat To Businesses? - https://securityboulevard.com/2025/03/why-supply-chain-attacks-are-the-biggest-threat-to-businesses-2/ Ja Lessons From the Largest Software Supply Chain Incidents - https://www.darkreading.com/vulnerabilities-threats/lessons-largest-software-supply-chain-incidents
18) Suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä - https://www.kyberturvallisuuskeskus.fi/fi/saadokset/suositus-nis-valvoville-viranomaisille-kyberturvallisuuden-riskienhallinnan
19) Uhka-analyysi ja uhkamallinnus varautumisen työkaluina kyberturvallisuusriskien hallinnassa – https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uhka-analyysi-ja-uhkamallinnus-varautumisen-tyokaluina-kyberturvallisuusriskien, Toimitusketjujen riskienhallinta – miksi se on elintärkeää liiketoiminnan jatkuvuudelle? - https://kyberturvallisuuskeskus.fi/fi/toimintamme/hankkeet, -ja-projektit/ohjelmistoturvallisuus/toimitusketjujen-riskienhallinta-miksi-se Kyberturvallisuuskeskuksen viikkokatsaus 06/2025 - https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-062025#82301-0 ja https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/hankkeet-ja-projektit/ohjelmistoturvallisuus/uhkamallinnus-ja-ohjelmistoturvallisuus ja Kyberturvallisuuskeskuksen viikkokatsaus - 08/2025 - https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-082025
20) Avaruusstrategia 2030 - https://julkaisut.valtioneuvosto.fi/handle/10024/166042
21) Kriittisen infrastruktuurin tietojen avoin jakaminen arvioidaan uudelleen - https://vm.fi/-/kriittisen-infrastruktuurin-tietojen-avoin-jakaminen-arvioidaan-uudelleen
22) Asian käsittelytiedot HE 57/2024 vp: Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi - https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_57+2024.aspx
23) Lausuntopyyntö verkkotunnusmääräysluonnoksesta - https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=b13c7032-38a7-48f6-91e9-06b99722abb7
24) Kybermittari - https://www.kybermittari.fi/
25) Suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä - https://kyberturvallisuuskeskus.fi/fi/saadokset/suositus-nis-valvoville-viranomaisille-kyberturvallisuuden-riskienhallinnan

VERSIOHISTORIA
17.3.2025: Kosmeettisia korjauksia sivujen 4 ja 9 taulukoihin sekä footer-elementtiin.