TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Tammikuu 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

Microsoft 365 -tunnuksia on jälleen kalasteltu aktiivisesti. Dropbox-teema kalasteluviesteissä on syksyn tapaan jatkunut.[1]

Tammikuussa nähtiin piikki merkittävissä haavoittuvuuksissa ja julkaisimme viisi haavoittuvuustiedotetta. Tämä on jo viidesosa viime vuonna julkaistujen haavoittuvuustiedotteiden määrästä.[2]

Suomessa on yli 100 000 yhdistystä, joiden tietoturvaan panostamisesta muistutimme tammikuussa. Yhdistykset ovat suurimpia henkilötietojen käsittelijöitä, minkä vuoksi niiden on erityisen tärkeää panostaa jäsenrekisteriensä tekniseen suojaamiseen.[3]

Kybersää tammikuu 2025

Tietomurrot ja -vuodot

- Usean valmistajan verkon reunalaitteita on hyväksikäytetty osana tietomurtoja. Juurisyynä ovat usein käyttäjien heikot tietoturva-käytänteet, jotka altistavat haavoittuvuudet nopealle hyväksikäytölle.[4]
- M365-tunnuksia on murrettu onnistuneen Dropbox-välitteisen kalastelun avulla.[5]

Huijaukset ja kalastelut

- Verotusteemaiset huijaukset ovat vuodenvaihteessa jälleen yleistyneet. Veroteemaisilla tekstiviesteillä uhreja houkutellaan syöttämään pankkitunnuksensa huijarille.
- Huijarien ostamat hakukone-mainokset ovat johtaneet kalasteluun. Huijausmainoksia on nähty pankkien ja mm. Traficomin hakusanoilla.[6]

Haittaohjelmat ja haavoittuvuudet

- Fortinetin FortiOS- ja FortiProxy-tuotteissa kriittinen haavoittuvuus. Fortinet on kertonut, että haavoittuvuutta hyväksikäytetään aktiivisesti.[7]
- Ainakin Tori.fi- ja Facebookin Marketplace -alustoilla on liikkunut huijauksia, joissa tuotteen myyjä on houkuteltu asentamaan haittaohjelma.[8]

Automaatio ja IoT

- Komissio on hyväksynyt kyberkestävyyssäädöksen standardointipyynnön 20.1.2025.
- BlinkenCity-niminen tutkimus suojaamattomien radiosignaalien käyttämisestä Keski-Euroopassa energiasektorilla nosti esille riskejä ja tarpeen ottaa käyttöön paremmin turvattuja langattomia kommunikaatiomenetelmiä.[9]

Verkkojen toimivuus

- Tammikuussa yleisissä viestintäverkoissa havaittiin seitsemän toimivuushäiriötä.
- Ilmoitettujen palvelunesto-hyökkäysten määrä on kasvussa.
- Venäjämielinen haktivistiryhmä kohdisti palvelunestohyökkäyksiä suomalaisille verkkosivuille ja kertoi syyksi joulukuussa julkaistun puolustusselonteon. Hyökkäysten vaikutukset jäivät vähäisiksi.

Vakoilu

- Ivanti Connect Secure VPN:stä löydettyä haavoittuvuutta on maailmalla hyödynnetty nollapäivänä ainakin joulukuun puolivälistä asti organisaatioihin tunkeutumisessa.[10]
- Myös Suomessa on tutkittu murretuiksi epäiltyjä laitteita.[11]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Verkon reunalaitteiden näkyminen ja avoimuus internetiin avaa paljon hyökkäyspintaa pahantahtoisille toimijoille. Muistutimme Tietoturva Nyt! -artikkelissa jatkuvasti ajankohtaisesta verkon reunalaitteiden turvaamisesta.[12]

Internetin kauppapaikoilla levitetään parhaillaan puhelimiin asennettavaa haittaohjelmaa, jolla rikolliset voivat saada koko puhelimen haltuunsa. Muistutimme sovellusten lataamisesta vain virallisista sovelluskaupoista ja turvallisesta toiminnasta verkkokaupoissa.[13]

Kyberturvallisuuskeskus nosti valmiuttaan ja varautumistaan Helsingissä 14.1. järjestetyn Itämeren alueen Nato-maiden huippukokouksen vuoksi. Kyberturvallisuuden näkökulmasta tilanne sujui rauhallisesti.[14]

Tietoturva 2025 -seminaari järjestetään tänä vuonna 12. maaliskuuta teemalla digitaalisen yhteiskunnan suojaaminen. Traficomin ja Huoltovarmuuskeskuksen seminaariin voit ilmoittautua ja ohjelmaan tutustua osoitteessa tietoturvaseminaari.fi.[15]

Tammikuun kyberturvallisuuden yleiskuva

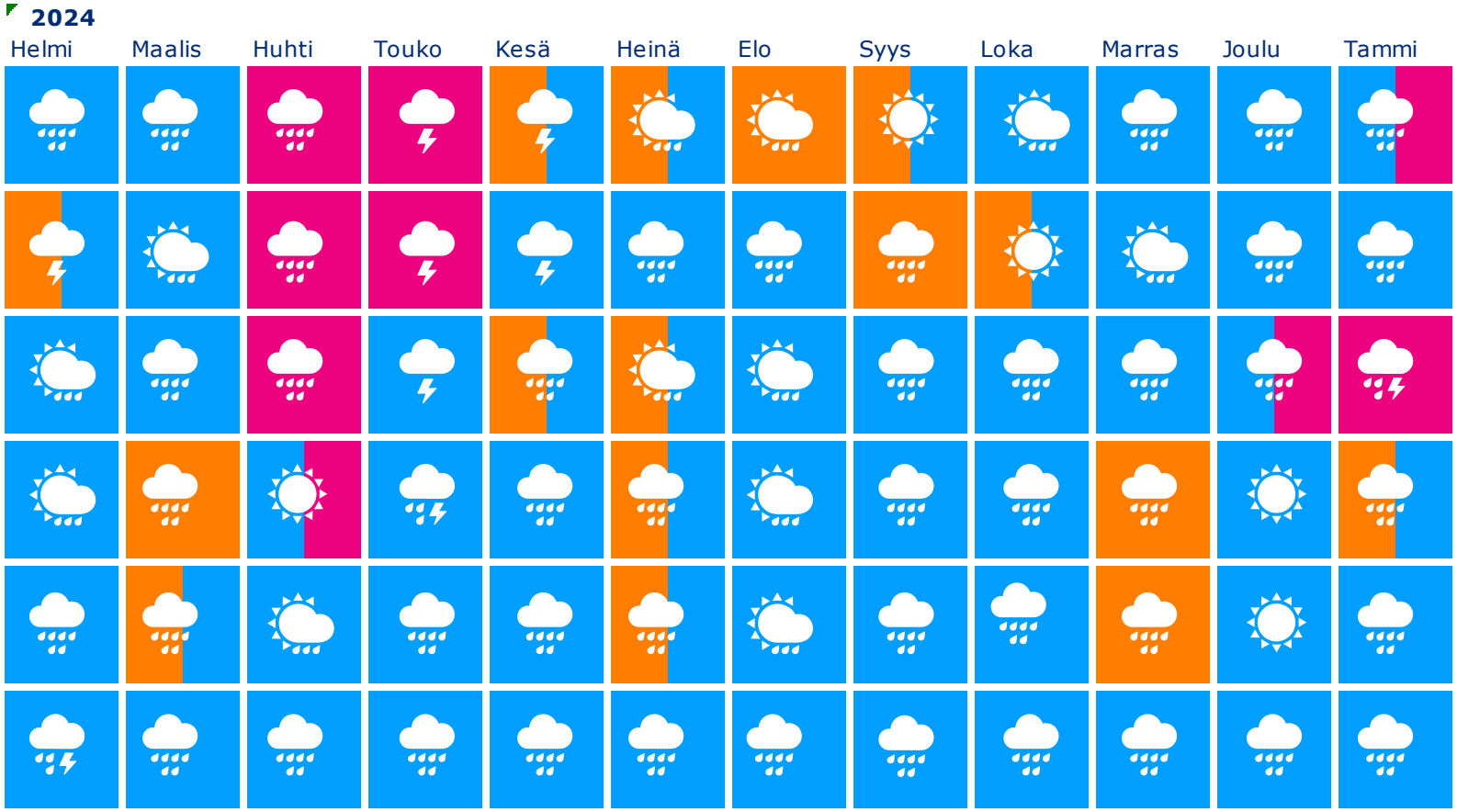
- Tammikuussa sadepilviä taivaalle keräsivät vakavat haavoittuvuudet Ivantin, Fortinetin ja SonicWallin tuotteissa. Kaikkia haavoittuvuuksia on hyväksikäytetty aktiivisesti. Kyberturvallisuuskeskuksen tietoon tuli useita kymmeniä Ivanti- ja Fortinet-laitteisiin liittyviä tietomurtoja.[16]
  - Osa haavoittuvuuksista on ollut hyökkääjien käytössä jo ennen kuin tuotteiden omistajat ovat saaneet tiedon haavoittuvuuksista.
  - Kahden haavoittuvuuden hyväksikäyttö voitiin kokonaan estää rajoittamalla hallintakäyttöliittymän näkyvyyttä julkisista verkoista.
- Dropboxia hyödyntävää Microsoft 365 -tunnusten kalastelua lähti jälleen tammikuussa runsain määrin liikkeelle. Kalastelut ovat johtaneet eri toimialoilla useisiin tietomurtoihin ja jatkokalasteluihin.[17]
  - Sähköpostitunnusten kalasteluissa rikolliset käyttävät hyväkseen erityisesti Dropboxista jaettavia PDF-tiedostoja esimerkiksi otsikolla "LASKU_INV_PO300125.PDF". Kyberturvallisuuskeskuksen tietoon tulleissa tapauksissa käyttäjätilille on yritetty kirjautua jopa minuuttien sisällä siitä, kun tunnukset on syötetty kalastelusivulle.
  - Kyberturvallisuuskeskuksen tietoon tulleissa tapauksissa kaapatulle sähköpostitilille on lisätty viestin käsittelysääntö, joka siirtää kaikki “dropbox”-sanana saapuvat viestit RSS Syöte -kansioon. Tavoitteena on salata käyttäjältä tilillä tapahtuva epäilyttävä toiminta.
  - Kyberturvallisuuskeskuksen ohjeessa tietomurtotilanteessa toimimiseksi neuvotaan ennaltaehkäisevät toimenpiteet ja oman M365-tilin varmistamisen askelmerkit.[18]

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: Haavoittuvuudet

- Ilmoitettujen haavoittuvuuksien määrä on viimeisen vuosikymmenen aikana kansainvälisesti kuusinkertaistunut.[19]
- Haavoittuvuuksien merkittävään uhkaan pyritään EU-tasolla puuttumaan esimerkiksi sääntelyn keinoin.
  - NIS2-direktiivin myötä Euroopan kyberturvallisuusvirasto ENISA tulee perustamaan Euroopan laajuisen haavoittuvuustietokannan.[20]
  - EU:n kyberkestävyyssäädös CRA puolestaan tuo syyskuusta 2026 alkaen velvoitteet tuotteiden valmistajille raportoida aktiivisesti hyväksikäytetyistä haavoittuvuuksista ja tuotteen tietoturvaan vaikuttavista vakavista poikkeamista EU:n markkinoilla olevissa, säädöksen soveltamisalaan kuuluvissa tuotteissa.[21]
- Viime aikoina tietomurroissa ovat pääasiassa korostuneet verkon reunalaitteissa ja niiden hallintaliittymissä olevat haavoittuvuudet. Valtiolliset toimijat ovat viime vuosina hyödyntäneet verkon reunalaitteiden haavoittuvuuksia kyberhyökkäyksissään.
  - Organisaatioiden tulee ennakoivasti tarkastella julkisesti verkkoon näkyvissä olevia palveluitaan ja varmistaa, ettei julkiseen verkkoon ole näkyvissä sellaisia palveluita, joille se ei ole välttämätöntä.

Top 5 uhat lähitulevaisuudessa (6kk–2v)

1.

Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

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

2.

Kiristyshaittaohjelmat - Merkittävä uhka organisaatioille

Viimeisen vuoden aikana usea organisaatio Suomessa on joutunut kiristyshaittaohjelman uhriksi, ja niiden määrä kasvaa jatkuvasti myös globaalisti.

3.

Toimitus- ja palveluketjujen tietoturva ja jatkuvuus ovat yhä kriittisempiä.

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

Uusi

Päivitetty

Symbolit

4.

Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa.

Organisaatioiden olisi hyvä tunnistaa tekoälyn tuomia haasteita, ja varautua niihin esimerkiksi kouluttamalla henkilöstöään.

5.

Tietoliikenneinfran suojaamisen tärkeys korostuu

Tietoliikenne- ja tietojärjestelmäinfran suojaaminen maailmalla ja kotimaassa on tärkeää, sekä siihen kohdistuvien vahinkojen ja luonnonilmiöiden että ulkopuolisten aiheuttamien tahallisten häiriöiden takia.

1. Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

- Haavoittuvuuden korjaavan päivityksen asentamisen lisäksi on usein tarpeen tutkia, onko haavoittuvuutta hyödynnetty jo ennen päivityksen asentamista, tai onko järjestelmään luotu takaovia eli piilotettuja sisäänpääsyreittejä.
- Rikolliset pyrkivät hyväksikäyttämään haavoittuvuuksia jo ennen kuin niitä on ehditty korjata. Haavoittuvuuden aktiivista hyväksikäyttöä aletaan yrittää viimeistään siinä vaiheessa, kun haavoittuvuudesta on tullut julkinen. Rikolliset etsivätkin ahkerasti verkosta päivittämättömiä järjestelmiä kohteikseen.
  - Microsoftin mukaan haavoittuvuuksien hyväksikäyttö järjestelmiin tunkeutumisen ensimmäisenä sisäänpääsyvektorina on yleistynyt. Aikaikkuna kriittisten haavoittuvuuksien paikkaamiseen on kaventunut viidessä vuodessa kuukausista ja viikoista keskimäärin 1-3 vuorokauteen, mutta hyväksikäyttöä on tapahtunut jopa kymmenissä minuuteissa hyväksikäyttömenetelmän julkaisun jälkeen.[22, 23]
  - Järjestelmien nopea päivittäminen onkin erityisen tärkeää ja valmius päivittämiseen pitäisi olla jatkuvasti, myös yleisinä loma-aikoina.
- Haavoittuvuuksien hallintaa on haastavaa tehdä, mikäli organisaatio ei tunne ympäristöään. Järjestelmien kartoitus ja dokumentointi on syytä tehdä viimeistään nyt.
- Haavoittuvia palveluita näkyy monesti myös julkisesti verkkoon. Organisaatioiden olisikin hyvä myös tarkastella omia palveluitaan säännöllisesti ja varmistaa, että mahdollisuuksien mukaan palveluita ei olisi näkyvissä julkisesti verkkoon.
  - Haavoittuvien ja muutoin verkkoon avoimena näkyvien palveluiden kartoitusta tarjoavat myös monet kaupalliset toimijat.
- Monien merkittävien laitevalmistajien verkon reunalaitteissa, kuten VPN-yhdyskäytävissä, havaittu vakavia ja helposti hyödynnettäviä haavoittuvuuksia viimeisen vuoden aikana.
  - Osa haavoittuvuuksista on ollut nollapäivähaavoittuvuuksia eli niitä on hyväksikäytetty ennen kuin korjaava päivitys on ollut saatavilla.

2. Kiristyshaittaohjelmat - Merkittävä uhka organisaatioille

- Viimeisen vuoden aikana usea organisaatio Suomessa on joutunut kiristyshaittaohjelman uhriksi, ja kiristyshaittaohjelmien määrä kasvaa jatkuvasti myös globaalisti.
  - **Akira on viimeiset kaksi vuotta ollut Kyberturvallisuuskeskukselle eniten ilmoitettu kiristyshaittaohjelma. Sen lisäksi on raportoitu useita kiristyshaittaohjelmia, joita ei ole ennen havaittu Suomessa.**
- **Kiristyshaittaohjelma saattaa pahimmassa tapauksessa lopettaa organisaation toiminnan kokonaan. Hyökkäys voi kohdistua myös toimitusketjuun ja levitä sitä kautta nopeasti useisiin organisaatioihin samalla kertaa. Varsinkin huoltovarmuuskriittisten organisaatioiden joutuessa uhriksi voivat yhteiskunnan elintärkeät toiminnot vaarantua.**
- **Organisaatioiden tulee ottaa kiristyshaittaohjelmahyökkäykset ja niistä palautuminen huomioon varautumisessa ja harjoitustoiminnassa.**
- Kiristyshaittaohjelma tartutetaan usein kalasteluviestin, vuotaneiden käyttäjätunnusten tai päivittämättömien haavoittuvuuksien kautta. Tiedostojen salaus ja muut hyökkääjän tekemät toimenpiteet saatetaan toteuttaa viipymättä sisäänpääsyn jälkeen, joten ennaltaehkäisy, havainnointi ja nopea reagointi ovat avainasemassa.
- **Osa kiristyshaittaohjelmista pyrkii etsimään ja tuhoamaan myös kohteensa varmuuskopiot, joten ainakin yksi varmuuskopio tulee säilyttää poissa verkosta. Kyberturvallisuuskeskuksen tiedossa olevista kiristyshaittaohjelmasta palautuneista organisaatioista suurin osa palautui varmuuskopioiden avulla.**
- Viime vuosina on yleistynyt ns. double extortion, jossa salaamisen lisäksi rikolliset myös varastavat tiedot ja kiristävät organisaatiota tietovuodolla. Kiristyshaittaohjelmatoimijoiden vaatimia lunnaita ei tule maksaa. Palautumisesta ei ole takeita, ja lunnaat maksamalla rahoittaa rikollista toimintaa.
- Kiristyshaittaohjelmia myydään yhä enenevissä määrin myös palveluna (RaaS). Tämän vuoksi hyökkääjän ei enää tarvitse olla teknisesti taitava toteuttaakseen hyökkäyksiä, ja RaaS-palvelua hyödyntäviä rikollisia voi olla enemmän. Europolin arvion mukaan tulevaisuudessa nähdään yhä enemmän rikollisia, jotka tarjoavat muille RaaS-palveluita. Kuinka kauan nämä ryhmät ovat aktiivisia on kiinni siitä, miten tyytyväisiä palveluita ostaneet ovat.

3. Toimitus- ja palveluketjujen tietoturva ja jatkuvuus on yhä kriittisempää

- Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä. Valtaosa organisaatioista on enemmän tai vähemmän riippuvaisia ulkoistetuista digitaalisista palveluista.
  - Esimerkiksi sähköisten asiointipalveluiden tarjoajat tunnistavat asiakkaansa vahvan tunnistautumisen avulla. Mikäli jokin tunnistautumisen keino ei toimi, kyseisen tunnistautumisvälineen käyttäjät voivat jäädä ilman palvelua, jos heillä ei ole varalla toista tunnistautumiskeinoa.
- Kyberturvallisuuskeskukselle ilmoitetuissa tapauksissa vaikuttaa usein siltä, että alihankintaketjuihin liittyvät vastuut ovat organisaatioille epäselviä. Vastuut olisikin hyvä määritellä aina siten, että poikkeamatilanteessa olisi selvää, mitä vastuunjaoista on sovittu.
  - Uudistetussa kansallisessa kyberturvallisuusstrategiassa muistutetaan, että yhteiskunnan kriittisten toimijoiden on varmistettava, että niiden palveluntuottajat ja toimitusketjut ovat kyberturvallisia.
- Organisaatioiden on keskeistä ymmärtää omat alihankkijaketjunsa ja olla tietoisia 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, koska myös organisaation alihankkija voi hankkia tuotteen/palvelun seuraavalta ketjussa olevalta palveluntarjoajalta.
- Maailmalla uutisoidaan jatkuvasti toimitusketjuihin kohdistuvista kyberuhista sekä niissä havaituista heikkouksista.

4. Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa

- Lyhyellä aikavälillä tekoälyn haasteisiin on liitetty skenaarioita esimerkiksi tekoälyn kyvystä kirjoittaa haittaohjelmia tai laatia paremmin kohdistettuja ja kielellisesti laadukkaampia tietojenkalasteluviestejä eri kielillä. Ainakin toistaiseksi tekoälyn kyvykkyyttä luoda aidosti toimivia haittaohjelmia on kuitenkin pidetty rajallisena.
- Organisaatioiden on hyvä ottaa huomioon erityisesti tietosuoja- ja salassapitonäkökulmat tekoälyn mahdollisessa käytössä, ja pohtia näihin liittyviä linjauksia organisaation sisällä.
  - Tekoälyn käyttöön tulisi laatia organisaation sisäinen käyttöpolitiikka ja ohjeistus henkilöstölle siitä, miten tekoälyä voi sallitulla tavalla hyödyntää työssä.
  - Iso-Britanniassa laaditun selvityksen mukaan noin viidesosassa paikallisista yrityksistä on paljastunut mahdollisesti sensitiivisen tiedon vaarantuneen henkilöstön tekoälyn käytön seurauksena.
- Syväväärennöksien eli ns. deepfake-tekniikan käytöstä osana kyberrikoksia on puhuttu kansainvälisessä uutisoinnissa.
  - Syväväärennösten tekeminen voi näyttäytyä rikollisille houkuttelevana tapana huijata organisaation työntekijöitä tai aiheuttaa mainehaittaa.
  - Kyberturvallisuuskeskukselle tehtyjen yksittäisten ilmoitusten valossa suomenkielisien syväväärennöksien käyttö ei kuitenkaan vaikuta olevan vielä kovinkaan yleistä.
- Europolin raportin mukaan tekoäly yleistyy rikollisten keinovalikoimassa. Europol nimesi raportissaan tekoälyn ja kielimallit yhdeksi tulevaisuuden pääuhista.[24]

5. Tietoliikenneinfran suojaamisen tärkeys korostuu

- Sekä maailmalla että kotimaassa on vuoden mittaan tapahtunut ikäviä tietoliikenneinfraan kohdistuneita vahinkoja ja luonnonilmiöitä, sekä ulkopuolisten tekijöiden aiheuttamia tahallisia häiriöitä.
- Kaikkien tietoliikenne- ja tietojärjestelmäinfran omistajien kannattaa huolehtia siitä, että viestintäverkon tai -palvelun komponentit on suojattu fyysisesti siten, etteivät asiattomat pääse niihin helposti käsiksi.
- Yleisen teletoiminnan osalta Liikenne- ja viestintävirasto Traficomin määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista asettaa vaatimukset laitetilojen ja siirtoteiden suojaamiselle yleisen viestintäverkon ja palvelujen komponenttien tärkeysluokkien perusteella. Tärkeysluokitus perustuu viestintäpalvelun tyyppiin sekä maantieteelliseen alueeseen tai käyttäjämäärään, johon viestintäverkon tai -palvelun komponentti vaikuttaa.
  - Fyysisen suojauksen lisäksi tärkeää on myös se, että itse laitetilojen rakenne täyttää määräyksen velvoitteet, ja että niissä on vaadittava ajantasainen kulunvalvonta, ja että niistä saadaan asianmukaiset hälytykset valvontahenkilöstölle.
- Pelkkä vahinkojen korjaaminen ei riitä. Häiriöiden ja niistä kerätyn informaation perusteella on tarpeen miettiä myös toimenpiteitä, joilla voidaan parantaa suojaustasoa.
- Suojaustason parantamiseksi Traficom sekä teleoperaattorit tekevät yhteistyötä, jotta esimerkiksi kotimaassa tapahtuneiden vahinkojen ja muiden häiriöiden määrää voitaisiin edelleen vähentää.

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 esittää uutta lakia ohjaamaan yhteiskunnan toimintakyvyn kannalta kriittisen infrastruktuurin suojaamista ja häiriönsietokyvyn parantamista [25, 26]
  - Hallitus antoi eduskunnalle ehdotuksen laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta (HE 205/2024 vp). Uudella lailla vahvistetaan yhteiskunnan kriisinkestävyyttä ja kansallista turvallisuutta hallitusohjelman mukaisesti.
  - Lailla tuodaan kansalliseen lainsäädäntöön kriittisten toimijoiden häiriönsietokyvystä annettu Euroopan parlamentin ja neuvoston direktiivi. Niin kutsutulla CER-direktiivillä (Critical Entities Resilience) parannetaan EU:n sisämarkkinoiden kriittisten palveluiden häiriönsietokykyä ja toimintavarmuutta. Tavoitteena on yhdenmukaistaa kriittisten toimijoiden tunnistaminen sekä häiriönsietokykyä koskevat menettelyt ja arviointiperusteet EU:ssa ja luoda selkeät menettelyt jäsenvaltioiden väliseen yhteistyöhön.
  - Lain ja direktiivin soveltamisala koskee yhtätoista sektoria, jotka ovat liikenne, energia, pankit, finanssimarkkinat, terveys, ruoka, vesi- ja jätevesihuolto, digitaalinen infrastruktuuri, julkishallinto ja avaruus.
  - Lakiehdotus määrittää viranomaistoiminnan järjestelyt, kaikkia toimijoita koskevat yhteiset vaatimukset, kriteerit ja keskeiset velvoitteet. Uusia tehtäviä ehdotetaan sektoriministeriöille, muille viranomaisille ja vuoden 2026 aikana kriittisiksi tunnistetuille yrityksille. Sektoriministeriöiden vastuulla olisi direktiivin mukaisten kriittisten toimijoiden tunnistaminen ja määrittäminen.
  - Kriittisiä toimijoita eli esimerkiksi elintärkeitä palveluja tuottavia yrityksiä valvoisivat ministeriöiden hallinnonaloilta nimetyt valvontaviranomaiset. Kriittisiksi tunnistetuille toimijoille tulee aikanaan uusia velvoitteita, miten suojata kriittistä infrastruktuuriaan. Velvoitteet liittyvät riskiarviointiin, häiriönsietokykyä koskevaan suunnitelmaan ja häiriönsietokyvyn varmistamiseen sekä poikkeamia koskeviin menettelyihin.

Oikeudelliset asiat

- Kyberturvallisuuslakia esitetään muutettavaksi [27, 28]
  - Kyberturvallisuuslakia on tarkoitus täydentää niin, että sen mukaisia velvoitteita kyberturvallisuutta koskevasta riskienhallinnasta ja merkittävistä poikkeamista ilmoittamisesta sovellettaisiin myös yhteisöihin, jotka määritettäisiin kriittisiksi toimijoiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla.
  - Kyberturvallisuuslain velvoitteet laajennettaisiin koskemaan kriittiseksi määritettäviä yrityksiä myös silloin, kun kriittinen toimija ei ennalta kuuluisi kyberturvallisuuslain soveltamisalaan. Näitä yrityksiä olisivat erityisesti kriittiseksi määritettävät pien- tai mikroyritykset kaikilla toimialoilla sekä kriittiseksi määritettävät julkisen liikenteen harjoittajat ja lääketukkukaupat.
  - Kriittiseksi määritetty yhteisö kuuluisi kyberturvallisuuslain velvoitteiden soveltamisalaan keskeisenä toimijana.
  - Esitykseen sisältyy lisäksi lainsäädäntöteknisiä ehdotuksia muun muassa valvovien viranomaisten toimivallasta ja yhteistyöstä sekä siirtymäajasta velvoitteiden soveltumiselle kriittiseksi määrittämisen jälkeen.
  - Kyberturvallisuuslakia koskevan hallituksen esityksen käsittely eduskunnassa on kesken.
  - Kyberturvallisuuslain muuttamista koskeva hallituksen esitys on tarkoitus käsitellä eduskunnassa samanaikaisesti hallituksen esityksen eduskunnalle laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja eräiksi muiksi laeiksi (HE 205/2024 vp) kanssa.

Oikeudelliset asiat

- Radiohäirintään tarkoitettujen laitteiden hallussapito halutaan säätää rangaistavaksi [29, 30]
  - Liikenne- ja viestintäministeriö on 15.1.2025 käynnistänyt säädöshankkeen radiohäirintään tarkoitettuja radiolaitteita koskevan lainsäädännön muuttamiseksi.
  - Tarkoituksena on muuttaa sähköisen viestinnän palveluista annetun lain sääntelyä, joka koskee radiotaajuuksilla käytävään viestintään kuten satelliittipaikannusjärjestelmään (Global Navigation Satellite System, GNSS) kohdistettavia häirintälaitteita. Tarkoituksena on valmistella hallituksen esitys, jolla kriminalisoitaisiin radiohäirintään tarkoitettujen radiolaitteiden eli nk. jammereiden yksityinen hallussapito. Tällä hetkellä jammereiden hallussapito on luvanvaraista.
  - Lakia valmistellaan liikenne- ja viestintäministeriössä yhteistyössä sidosryhmien kanssa. Valmistelun aikana järjestetään lausuntokierros.

Oikeudelliset asiat

- Liikenne- ja viestintävirasto Traficom on antanut 23.1.2025 määräyshankepäätöksen viestintäverkon kriittisistä osista [31]
  - Määräyshankkeessa ajantasaistetaan 20.5.2021 voimaan tullut määräys viestintäverkon kriittisistä osista. Hankkeessa tarkastellaan viestintäverkkojen kriittisten osien rajauksia viestintäteknologioiden kehittyminen ja erityisesti matkaviestinverkkojen 5G-verkkoteknologian kehittyminen, huomioiden sen keskeinen yhteiskunnallinen rooli.
  - Määräys tulee ohjaamaan teleyrityksiä ja määräyksen soveltamisalaan kuuluvia paikallisverkkotoimijoita nykyisten ja tulevien verkkosukupolvien suunnittelussa, verkkolaitteiden hankinnassa, verkkojen rakentamisessa, verkkojen ylläpidossa ja verkkojen hallinnoimisessa. Määräyksellä edistetään kansallista turvallisuutta ja viestintäverkkojen tietoturvaa. Määräys täsmentää niitä viestintäverkon osia, joihin sähköisen viestinnän palveluista annetun lain 244 a §:ssä mukaiset toimenpiteet (verkkolaitteen poistaminen verkosta) voisivat kohdistua.
  - Määräyksen valmistelemiseksi perustetaan työryhmä, johon kutsutaan keskeiset sidosryhmät, joita ovat erityisesti teleyritykset sekä kansalliseen turvallisuuteen tai maanpuolustukseen liittyviä viranomaistehtäviä hoitavat tahot. Valmisteltavasta määräyksestä järjestetään tavanomainen lausuntokierros. Lisäksi verkkoturvallisuuden neuvottelukuntaa kuullaan valmisteltavasta määräyksestä.
  - Alustavan aikataulun mukaan määräys on tarkoitus julkaista syksyllä 2025.

Oikeudelliset asiat

- EU:n radiolaitedirektiivin tietoturvavaatimuksia tarkentavat standardit julkaistiin 30.1.2025 [32, 33, 34]
  - Radiolaitedirektiivi (RED) asettaa tietoturvavaatimukset erilaisille langattomasti radiotaajuuksilla toimiville laitteille. Tietoturvavaatimuksia sovelletaan 1.8.2025 alkaen. Tietoturvavaatimuksia tarkentavat standardit (EU) 2025/138 julkaistiin EU:n virallisessa lehdessä 30.1.2025.
- EU:n kybersolidaarisuussäädös julkaistiin 15.1.2025 ja tuli voimaan 4.2.2025 [35, 36]
  - Kybersolidaarisuussäädöksellä (EU) 2025/38 pyritään vahvistamaan EU:n valmiuksia havaita merkittäviä ja laajamittaisia kyberturvallisuusuhkia ja -hyökkäyksiä sekä valmistautua ja reagoida niihin. Säädökseen sisältyy Euroopan kyberturvallisuuden hälytysjärjestelmä, joka koostuu eri puolilla EU:ta yhteen liitetyistä turvallisuusoperaatiokeskuksista, ja kattava kyberturvallisuuden hätämekanismi EU:n kyberuhkien sietokyvyn parantamiseksi.
- Finanssisektorin digitaalista häiriönsietokykyä koskevan DORA-asetuksen soveltaminen alkoi 17.1.2025 [37]
  - DORA-asetuksen (Digital Operational Resilience Act) tavoitteena on parantaa kuluttajien tietoturvaa ja palveluiden jatkuvuutta. Se tuo mukanaan merkittäviä uudistuksia finanssisektorin digitaaliseen toimintavarmuuteen ja kattaa lähes kaikki Finanssivalvonnan valvomat toimijat. Finanssivalvonta keskittyy asetuksen tullessa voimaan valvontatyössään valvottavien ICT- ja tietoturvariskien hallintakehikkoon, ICT-häiriöilmoitusprosessiin ja ICT-toimittajien riskienhallinnan valvontaan.

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) Kyberturvallisuuskeskuksen viikkokatsaus 06/2025: Sähköpostitunnuksia kalastellaan Dropboxia hyödyntäen - tietomurto tehdään yhä nopeammin https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-062025#82301-0
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) Tietoturva Nyt!: Verkon reunalaitteiden riskit ovat merkittävä uhka organisaatioille https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/verkon-reunalaitteiden-riskit-ovat-merkittava-uhka-organisaatioille
5) Kyberturvallisuuskeskuksen viikkokatsaus 06/2025: Sähköpostitunnuksia kalastellaan Dropboxia hyödyntäen - tietomurto tehdään yhä nopeammin https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-062025#82301-0
6) Kyberturvallisuuskeskuksen viikkokatsaus 03/2025: Varo väärennettyjä hakutuloksia https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-32025#81320-2
7) Haavoittuvuus 3/2025: Fortinetin FortiOS ja FortiProxy -tuotteissa kriittinen haavoittuvuus https://kyberturvallisuuskeskus.fi/fi/haavoittuvuus_3/2025
8) Tietoturva Nyt!: Internetin kauppapaikoilla leviää nyt haittaohjelma - toimi näin https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/internetin-kauppapaikoilla-leviaa-nyt-haittaohjelma-toimi-nain
9) BlinkenCity: From Art Project to Europe-wide Blackout Scenario https://positive.security/blog/blinkencity-38c3
10) Ivanti Connect Secure VPN Targeted in New Zero-Day Exploitation https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day
11) Haavoittuvuus 2/2025: Ivanti Connect Secure -haavoittuvuuden hyväksikäyttöä havaittu https://kyberturvallisuuskeskus.fi/fi/haavoittuvuus_2/2025

Lähdeluettelo

12) Tietoturva Nyt!: Verkon reunalaitteiden riskit ovat merkittävä uhka organisaatioille https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/verkon-reunalaitteiden-riskit-ovat-merkittava-uhka-organisaatioille

13) Tietoturva Nyt!: Internetin kauppapaikoilla leviää nyt haittaohjelma - toimi näin https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/internetin-kauppapaikoilla-leviaa-nyt-haittaohjelma-toimi-nain

14) Kyberturvallisuuskeskuksen viikkokatsaus 3/2025: Suomessa järjestetty Nato-huippukokous sujui rauhallisesti https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-32025#81305-0

15) Tietoturva 2025 -seminaari: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturva-2025-seminaari

16) Kyberturvallisuuskeskuksen haavoittuvuustiedotteet https://kyberturvallisuuskeskus.fi/fi/haavoittuvuudet?limit=20&offset=0&query=&sort=updated

17) Kyberturvallisuuskeskuksen viikkokatsaus 06/2025: Sähköpostitunnuksia kalastellaan Dropboxia hyödyntäen - tietomurto tehdään yhä nopeammin https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-062025#82301-0

18) Toimi näin Microsoft 365 -tilin tietomurron sattuessa https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/toimi-nain-microsoft-365-tilin-tietomurron-sattuessa

19) CVE Details: Vulnerabilities By Types/Categories https://www.cvedetails.com/vulnerabilities-by-types.php

20) ENISA: Another step forward towards responsible vulnerability disclosure in Europe https://www.enisa.europa.eu/news/another-step-forward-towards-responsible-vulnerability-disclosure-in-europe

21) Kyberkestävyyssäädös (Cyber Resilience Act, CRA) https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/kyberkestavyyssaados-cyber-resilience-act-cra

22) Microsoft Digital Defense Report 2024 https://www.microsoft.com/fi-fi/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024#digital-ecosystem

23) Cloudflare Application Security report: 2024 update https://blog.cloudflare.com/application-security-report-2024-update/

Lähdeluettelo

24) Internet Organised Crime Threat Assessment (IOCTA) 2024 https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

25) Hallitus esittää uutta lakia ohjaamaan yhteiskunnan toimintakyvyn kannalta kriittisen infrastruktuurin suojaamista ja häiriönsietokyvyn parantamista https://valtioneuvosto.fi/-/1410869/hallitus-esittaa-uutta-lakia-ohjaamaan-yhteiskunnan-toimintakyvyn-kannalta-kriittisen-infrastruktuurin-suojaamista-ja-hairionsietokyvyn-parantamista

26) Lainsäädäntöhanke: Kriittisen infrastruktuurin tunnistaminen ja kriisinkestävyyden parantaminen https://valtioneuvosto.fi/hanke?tunnus=SM047:00/2022

27) Lausuntopyyntö luonnoksesta hallituksen esitykseksi kyberturvallisuuslain muuttamisesta https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=1de8c184-65a1-4182-b7ad-f6432c9c305d

28) Hallituksen esitys Euroopan unionin kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi https://valtioneuvosto.fi/hanke?tunnus=LVM027:00/2023

29) Uuden lakihankkeen tavoitteena on säätää radiohäirintään tarkoitettujen laitteiden hallussapito rangaistavaksi https://valtioneuvosto.fi/-/1410829/uuden-lakihankkeen-tavoitteena-on-saataa-radiohairintaan-tarkoitettujen-laitteiden-hallussapito-rangaistavaksi

30) Hallituksen esitys laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta https://valtioneuvosto.fi/hanke?tunnus=LVM002:00/2025

31) Määräyshankepäätös: Määräys viestintäverkon kriittisistä osista https://traficom.fi/fi/ajankohtaista/maarayshankepaatos-maarays-viestintaverkon-kriittisista-osista-0

Lähdeluettelo

32) Ajankohtaista radiolaitteiden vaatimustenmukaisuudesta https://traficom.fi/fi/viestinta/radioluvat-ja-taajuudet/radiolaitteiden-vaatimustenmukaisuus/ajankohtaista

33) EUR-Lex: Commission Implementing Decision (EU) 2025/138 of 28 January 2025 amending Implementing Decision (EU) 2022/2191 as regards harmonised standards in support of the essential requirements of Directive 2014/53/EU of the European Parliament and of the Council that relate to cybersecurity, for the categories and classes of radio equipment specified in Delegated Regulation (EU) 2022/30 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202500138

34) European Commission: Radio equipment: Directive 2014/53/EU https://single-market-economy.ec.europa.eu/single-market/european-standards/harmonised-standards/radio-equipment_en

35) Euroopan komissio: EU:n kybersolidaarisuussäädös https://digital-strategy.ec.europa.eu/fi/policies/cyber-solidarity

36) EUR-Lex: Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) https://eur-lex.europa.eu/eli/reg/2025/38/oj/eng

37) Finanssivalvonta: Asetus finanssialan digitaalisesta häiriönsietokyvystä https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/valvottavatiedotteet/2024/asetus-finanssialan-digitaalisesta-hairionsietokyvysta/