TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Huhtikuu 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

Hyökkääjät käyttävät CVE –numeroituja haavoittuvuuksia nopeasti niiden julkaisun jälkeen. Uusista haavoittuvuuksista lähes 30%:a hyväksikäytetään jo ensimmäisen vuorokauden sisällä julkaisusta.[1]

Kyberturvallisuuteen osoitettiin Euroopan Komission Digitaalinen Eurooppa -rahoitusohjelman kautta 390 miljoonaa euroa vuosille 2025-2027.[2] Uutinen enteilee hyvää myös Suomessa toimiville organisaatioille sekä kyberturvallisuuden kokonaiskehitykselle.

Digiturvamessut houkutteli Jyväskylän paviljonkiin yli 1000 digi- ja kyberturvallisuudesta kiinnostunutta.[3]

Kybersää huhtikuu 2025

Tietomurrot ja -vuodot

- Huhtikuu oli tietomurtojen osalta alkuvuotta hiljaisempi.
- Hotelli- ja matkavarauspalveluiden murrettuja käyttäjätunnuksia erityisesti Booking.com-palvelussa käytettiin jälleen varauksen tehneiden asiakkaiden maksukorttitietojen kalasteluun.
- M365-tunnusten murrot jatkuivat ja erityisesti Dropbox-teemaiset AiTM-kalasteluviestit korostuivat.

Huijaukset ja kalastelut

- Aktiivista pankkitunnuskalastelua. SMS-huijausviestien teemoina on käytetty Tullia ja verottajaa, joiden nimissä on huijattu uhri klikkaamaan kalastelusivulle.
- Myös pysäköintivirhemaksulla pelottelemalla on ohjattu kalasteluun.
- Mobiilivarmenteen käyttäjiä on yritetty huijata hyväksymään tuntemattomia tunnistustapahtumia.

Haittaohjelmat ja haavoittuvuudet

- SAP NetWeaver -ohjelmistokomponentin kriittinen ja hyväksikäytetty haavoittuvuus (CVE-2025-31324) tulisi päivittää viipymättä.
- Ivanti Connect Secure -tuotteen kriittinen ja hyväksikäytetty haavoittuvuus (CVE-2025-22457). Vanhat versiot tulisi päivittää viipymättä.

Automaatio ja IoT

- Huhtikuu tarjosi hyvää kevätsäätä automaatio tai IoT –järjestelmien osalta, eikä tarkastelujaksolla tehty merkittäviä havaintoja.
- Yhdysvaltalaiset viranomaiset julkaisivat 6.5. ohjeen "Primary Mitigations to Reduce Unsophisticated Cyber Threats to Operational Technology".[14]

Verkkojen toimivuus

- Huhtikuussa yleisissä viestintäverkoissa havaittiin kuusi toimivuushäiriötä, joista yksi oli korkean vakavuusluokan häiriö (A).
- Alue- ja kuntavaaliviikolla venäjämielinen haktivistiryhmä kohdisti palvelunestohyökkäyksiä suomalaisille verkkosivuille, muun muassa puolueiden kotisivuille. Hyökkäyksillä ei ollut merkittäviä vaikutuksia vaalien sujumiseen.

Vakoilu

- Apple on lähettänyt varoituksia käyttäjilleen, joita on vakoiltu kaupallisilla vakoiluhaittaohjelmilla.
- Ranska yhdisti useat tutkimansa kyberhyökkäykset venäläiseen APT28-toimijaan.
- Puolassa ja Romaniassa paljastui valtionhallintoon ja yksityiseen sektoriin kohdistunutta vakoilua, jossa hyödynnettiin Microsoftin haavoittuvuutta.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Traficom julkaisi huhtikuussa uuden ohjeen tietojärjestelmien ja tietoturvallisuuden arviointi- ja hyväksyntäprosessista. Ohje on tarkoitettu viranomaisille ja yrityksille, jotka on käsittelevät kansallista tai kansainvälistä turvallisuusluokiteltua tietoa sähköisesti.[4]

NIS 2 -direktiivin velvoitteet ja kyberturvallisuuslaki astuivat voimaan 8.4.2025. Uusi laki luo struktuuria Suomen kyberturvallisuudelle ja asettaa samalla yhteiskunnan kriittisille toimijoille velvollisuuksia kyberturvallisuuden poikkeamiin liittyen.[15]

Kevään aikana on havaittu useita haavoittuvuuksia etenkin verkon reunalaitteissa. Haavoittuvuuksien hallinta on haastavaa, mikäli organisaatio ei tunne ympäristöään riittävän kattavasti. Järjestelmien kartoitus ja dokumentointi on syytä tehdä säännöllisesti.

Huhtikuun kyberturvallisuuden yleiskuva

Huhtikuu oli verrattain rauhallinen kyberturvallisuuden näkökulmasta:

- Kuukauden alkupuolelle ajoittuneet kunta- ja aluevaalit herätti Venäjä-mielisen NoName057(16)-haktivistiryhmän talvihorroksestaan, kun suomalaisia verkko-osoitteita nousi muutaman kuukauden tauon jälkeen jälleen ryhmän kohdelistoille. Palvelunestoyökkäyksen kohteena oli mm. puolueiden, joukkoliikenteen, sekä julkisen ja yksityisen sektorin verkkosivuja. Hyökkäysten vaikutukset jäivät kokonaisuudessaan kuitenkin vähäisiksi, eikä niillä ollut vaikutusta vaalien toteuttamiseen.[5]
- Pääsiäisen ajanjakso oli tänä vuonna erittäin hiljainen kyberturvallisuuteen liittyvien havaintojen osalta. Organisaatioiden on kuitenkin syytä huomioida, että pyhät tai arjesta poikkeavat merkittävät tapahtumat saattavat lisätä hyökkääjien aktiivisuutta.[6]

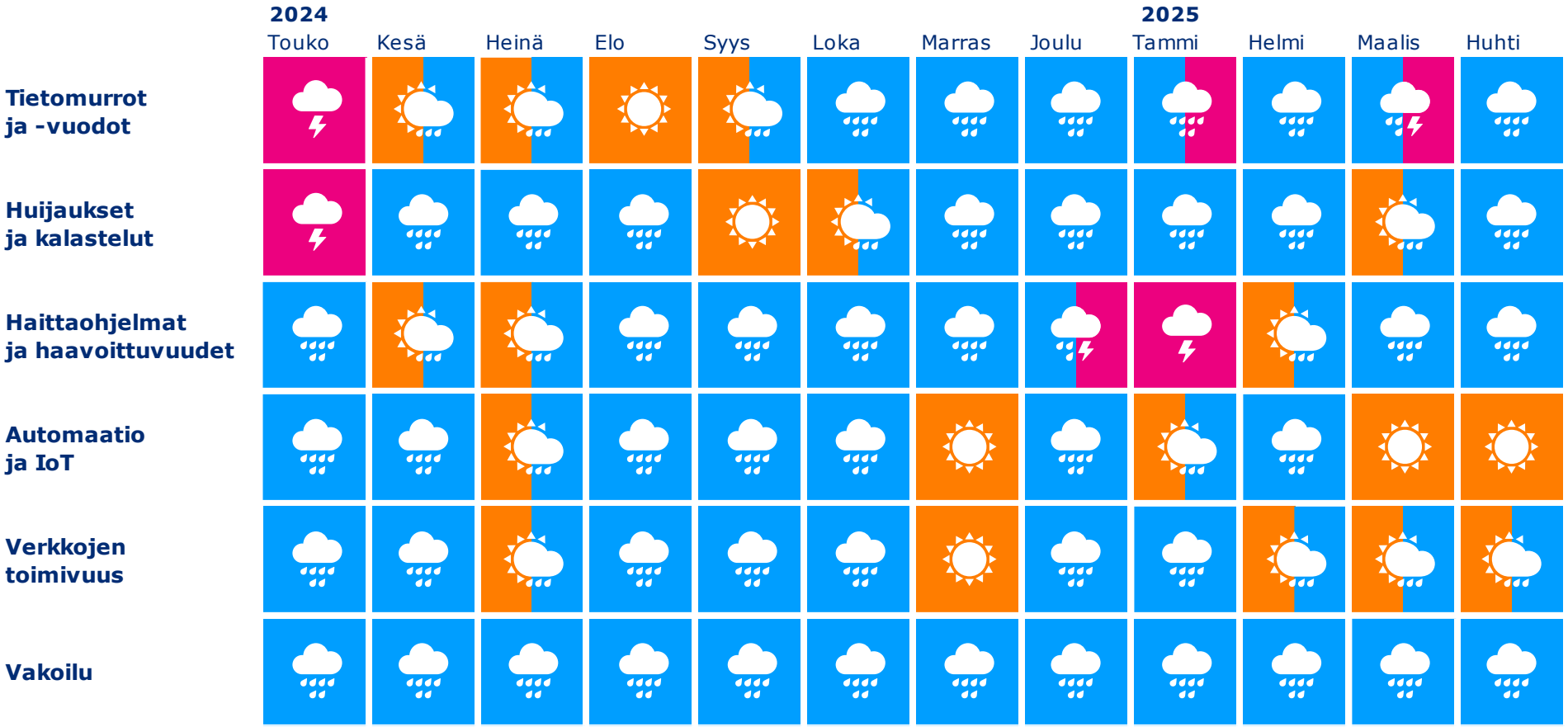
- Tietojenkalastelu korostui jälleen huhtikuun kybersäässä, jossa vallitsevia ilmiöitä olivat etenkin pankkien ja hotellivarauspalveluiden nimissä tehdyt huijaukset. Kalasteluviestit ja -sivustot olivat usein melko laadukkaita ja kalastelun kohteena oli joissain tapauksissa sähköiseen tunnistautumiseen käytettävä mobiilivarmenne.[7 & 8]
  - Hyökkääjät käyttävät yhteydenottoon usein tekstiviestejä tai WhatsApp-pikaviestisovellusta. Viestin lähettäjän nimitietoa on usein muokattu niin, että viesti vaikuttaa tuleen oikealta organisaatiolta.
  - Huijausten teemoissa on kausittaista vaihtelua ja lähestyvällä kesälomakaudella on todennäköisesti vaikutusta etenkin hotelli- ja varauspalveluihin liittyvän kalastelun hetkellisessä yleistymisessä. Osassa varauspalveluihin kytkeytyvistä huijausyrityksistä on ollut viitteitä palveluun kohdistuneista tietomurroista, joiden myötä hyökkääjät ovat pystyneet lähettämään viestejä varausjärjestelmän kautta.
- Verkon reunalaitteet ovat edelleen hyökkääjien kohteena:
  - Organisaatioiden käyttämien verkkojen reunalaitteisiin kohdistuvissa hyökkäyksissä on havaittu kasvua. Laitteiden nopeaa päivittämistä ei voi tarpeeksi korostaa, koska hyökkääjät etsivät aktiivisesti aiempien versioiden haavoittuvuuksia muun muassa julkaistujen päivitysten sisällöstä.
- Epäselvyys CVE-tietokannan rahoituksen jatkumisesta aiheutti huolta huhtikuussa. CVE-projekti sai lopulta rahoituksen tulevalle 11 kuukaudelle. Kaikki nykyiset haavoittuvuudenhallinnan työkalut käyttävät CVE-tunnisteita.[3]
  - EU:n kyberturvallisuusvirasto ENISA:n ylläpitämä European Vulnerability Database (EUVD) julkaistaan beta-versiona huhtikuun puolivälissä. Kyseinen haavoittuvuustietokanta tulee myöntämään erillisen tunnisteen haavoittuvuuksille, joten se ei ole CVE-tunnisteista riippuvainen, vaikkakin käyttää myös niitä toiminnassaan. Myös muut kansainväliset toimijat ovat kehitelleet tilanteeseen ratkaisuja pikaisella aikataululla.

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: Tekoälyn uhkat ja mahdollisuudet

Tekoäly ja sen eri sovellukset ovat alati kehittyviä teknologioita, jotka luovat monia mahdollisuuksia. Teknologioihin kuitenkin liittyy myös riskejä, minkä vuoksi tekoälyä integroitaessa on hyvä ymmärtää eri teknologioiden toimintalogiikkaa.

Selitettävä tekoäly – Explainable AI (XAI) :

- Selitettäviä tekoälymalleja kyberturvallisuuden ratkaisuissa on alettu tutkimaan viimeisten vuosien aikana. Useimmat tekoälyratkaisut ovat toistaiseksi olleet ns. mustan laatikon malleja, jotka eivät tarjoa selityksiä tai tulkittavuutta ratkaisuistaan. Selitettävät tekoälymallit antavat ihmiskäyttäjille tulkittavuutta ja avoimuutta monimutkaisiin kone- ja syväoppimismalleihin. Sillä tavoitellaan mm. korkeampaa luottamusta säilyttäen tarkkuus ja tehokkuus.[9]
  - Selitettäviä malleja on erilaisia. On malleja, jotka tarjoavat selityksiä tekoälymallin suorituksen aikana ja on sellaisia, jotka ajetaan mallin suorituksen jälkeen. Lähitulevaisuudessa ja pitkällä aikavälillä selitettävät tekoälymallit tulevat todennäköisesti lisääntymään myös kyberturvallisuuden alalla, ja ensimmäisiä konkreettisia ratkaisuja on jo ehdotettu ja testattu.[10]

Itsenäiset tekoälyagentit:

- Yksi merkittävimmistä trendeistä tekoälyn kentällä on siirtymä kehotteiden perusteella toimivista kielimalleista itsenäisiin tekoälyagentteihin. Tekoälyagentit ovat autonomisia tai semiautonomisia ohjelmistoja, jotka hyödyntävät tekoälyä havainnointiin, päätösten tekoon ja toimenpiteiden suorittamiseen. Suuret kielimallit ovat suorittaneet tähän asti tehtäviä käyttäjän kehotteesta, mutta ne eivät ole toimineet omasta aloitteestaan. Tekoälyagenteilla on oikeus toimia itsenäisesti.
  - Agentit toimivat omatoimisesti ja integroituvat eri järjestelmiin, kuten SaaS-palveluihin ja IoT-laitteisiin. Kehityksen seurauksena hyökkäyspinta-ala kasvaa ja järjestelmät muuttuvat monimutkaisemmiksi. Agentit voivat toimia myös hyökkäystyökaluina. Tutkijat ovat jo osoittaneet, että agentteja voidaan hyödyntää monimutkaisissa hyökkäyksissä.[11]
  - Kyberturvallisuuskeskus selvittää agenttien turvallista käyttöönottoa, uhkamallinnusta ja tietoturvatestaamista vuoden 2025 aikana. Tuloksia julkaistaan vuoden 2026 puolella.

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

- **Verkon reunalaitteet muodostavat merkittävän rajapinnan hyökkäyksille. Reunalaitteiden kirjo on laaja, ja niihin lukeutuvat muun muassa palomuurit ja VPN–laitteet. Organisaatioiden tulisi parhaansa mukaan pysyä selvillä käyttämänsä järjestelmäkokonaisuuden osista ja niiden päivitystarpeista. Hyökkääjät etsivät aktiivisesti haavoittuvuuksia esimerkiksi ohjelmistopäivitysten muistioista, mikä altistaa päivittämättömiä laitteita hyökkäyksille.**
- **Uhkien hallinnassa korostuvat sekä havainnointi että reagointikyky. Järjestelmäympäristön valvonta edistää hyökkäysten rajoittamista, mutta organisaatioilla tulee myös olla suunnitelma hyökkäyksestä ja sen vaikutuksista palautumiseen.**
- Monien merkittävien laitevalmistajien verkon reunalaitteissa, kuten VPN-yhdyskäytävissä, havaittu vakavia ja helposti hyödynnettäviä haavoittuvuuksia viimeisen vuoden aikana.
- Rikolliset pyrkivät hyväksikäyttämään haavoittuvuuksia jo ennen kuin niitä on ehditty korjata. **Haavoittuvuuden aktiivinen hyväksikäyttö saattaa usein tapahtua jo ensimmäisen vuorokauden sisällä siitä, kun haavoittuvuudesta on tullut julkinen.**[1]
  - Järjestelmien nopea päivittäminen on erityisen tärkeää ja valmius päivittämiseen on syytä ylläpitää jatkuvasti, myös yleisinä loma-aikoina.
- Haavoittuvuuksien hallinta on haastavaa, mikäli organisaatio ei tunne ympäristöään. Järjestelmien kartoitus ja dokumentointi on syytä tehdä säännöllisesti:
  - 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.

2. Kiristyshaittaohjelmat - Merkittävä uhka organisaatioille

- Viime vuosien 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. **Erityisesti verkon reunalaitteiden päivityksistä ja käyttäjätunnusten monivaiheisesta tunnistautumisesta on syytä pitää huolta**. 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.

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.
  - **Toimitusketjuihin liittyvä uhka ei kohdistu pelkästään komponentteihin, vaan saattaa myös konkretisoitua esimerkiksi ohjelmistojen ja ohjelmointikirjastojen kautta.**
  - Maailmalla uutisoidaan jatkuvasti toimitusketjuihin kohdistuvista kyberuhista sekä niissä havaituista heikkouksista.
- 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.
  - Toimintakulttuurilla ja prosesseilla on suuri merkitys uhkien havaitsemisessa, tunnistamisessa ja tiedon jakamisessa.
  - 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.

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. [12]

5. Tietoliikenneinfrastruktuurin suojaamisen tärkeys korostuu

- Sekä Suomessa että maailmalla on vuoden mittaan tapahtunut tietoliikenneinfrastruktuuriin kohdistuneita vahinkoja ja luonnonilmiöitä, sekä ulkopuolisten tekijöiden aiheuttamia tahallisia häiriöitä.
- Kaikkien tietoliikenne- ja tietojärjestelmäinfrastruktuurin omistajien kannattaa huolehtia siitä, että viestintäverkon tai -palvelun komponentit on suojattu fyysisesti siten, etteivät asiattomat pääse niihin helposti käsiksi.
- **Espanjassa ja Portugalissa 28.4 tapahtunut laaja sähkökatkos on osoitus kriittisen infrastruktuurin merkityksestä yhteiskunnan toimivuudelle.[13] Digitalisoituneissa maissa sähkö- ja tietoliikenneinfrastruktuuri ovat erittäin keskeisessä asemassa useimpien yhteiskunnan toimintojen jatkuvuuden kannalta.**
  - **Suomessa julkinen sektori on varautunut vastaaviin häiriötilanteisiin.**
  - **Yksityisen sektorin toimijoiden on syytä pohtia häiriötilanteisiin varautumista. Häiriönsietoa voidaan parantaa esimerkiksi kahdentamalla kriittisiä järjestelmiä ja yhteyksiä, sekä varmistamalla niiden sähkönsaanti lyhyen sähkökatkoksen varalta.**
- 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

Euroopan tietosuojaneuvostolta ohjeluonnos henkilötietojen käsittelystä lohkoketjuteknologioiden avulla.[16]

- Euroopan tietosuojaneuvosto hyväksyi ohjeluonnoksen henkilötietojen käsittelystä lohkoketjuteknologioiden avulla. Ohje on kommentoitavana julkisella kuulemiskierroksella 9.6.2025 saakka tietosuojaneuvoston verkkosivuilla.[17]
- Lohkoketjuteknologioiden käyttö lisääntyy, minkä vuoksi tietosuojaneuvosto pitää tärkeänä tukea näitä teknologioita käyttäviä organisaatioita tietosuojasäännösten noudattamisessa.
- Uudessa ohjeessa arvioidaan, miten erilaiset lohkoketjujärjestelmän rakentamisen tavat vaikuttavat henkilötietojen käsittelyyn.
- Tietosuojaneuvosto antaa ohjeessa esimerkkejä erilaisista tekniikoista henkilötietojen minimointia sekä tietojen käsittelyä ja säilyttämistä varten.

Oikeudelliset asiat

Euroopan komissio on julkaissut neljä täytäntöönpanoasetusta, jotka täsmentävät sähköistä tunnistamista ja luottamuspalveluita koskevaa Asetusta (EU) N:o 910/2014 (eIDAS-asetus) [18, 19, 20, 21]

- Asetukset koskevat digitaalisen identiteetin lompakon luetteloita, henkilöllisyyden linkittämistä, tietoturvaloukkauksia sekä luottavan osapuolen rekisteröintiä.
- Lisää asetuksia on valmistelussa ja niistä äänestetään viimeistään kesäkuussa.

Oikeudelliset asiat

LVM on käynnistänyt lakihankkeen, jolla on tarkoitus luoda lainsäädäntöpohja kaapelitietojen sijaintiselvityspyyntöihin vastaamiseksi tarkoitetun järjestelmän (aiemmin Sijaintitietopalvelu) uudelle toteutustavalle.[22]

- Liikenne- ja viestintävirasto on aikaisemmin valmistellut muun muassa datakaapeleiden sijaintiselvityspyyntöihin vastaamiseen ja valvontaan tarkoitettua järjestelmää (ns. Sijaintitietopalvelu).
- Sijaintitietopalvelun käyttöönottoon tähtäävä hanke keskeytettiin loppuvuodesta 2024 turvallisnäkökohtien vuoksi.
- Uudelleenarvion jälkeen toteutusmalliksi on valittu niin sanottu hybridimalli, jossa pienet toimijat voivat toimittaa verkkotietonsa keskitettyyn järjestelmään etukäteen, mutta suuret verkkotoimijat, joilla on parempi kyky reagoida sijaintiselvityspyyntöihin ja rakentaa rajapinta tähän tarkoitukseen, toimittavat tiedot vain selvityspyyntökohtaisesti.
- Järjestelmän kehittäminen ja käyttöönotto edellyttävät muutoksia *erittäin suuren kapasiteetin verkkojen käyttöönoton helpottamisesta annettuun lakiin*, jota koskeva hallituksen esitys on tarkoitus antaa eduskunnalle kevätistuntokauden 2025 aikana.
- Järjestelmän tarkoituksena on parantaa verkkoinfrastruktuurien sijaintitietojen hallinnointia Suomessa vähentäen maanalaiseen rakentamiseen liittyviä kaivuuvahinkoja.

Oikeudelliset asiat

Valtioneuvosto on julistanut haettaviksi verkkotoimiluvat yleiseen teletoimintaan 450 megahertsin taajuusalueelle.[23]

- Manner-Suomen ja Ahvenanmaan maakunnan toimiluvat haetaan erikseen.
- Hakuaika päättyy 23.5.2025 kello 12.
- Valtioneuvosto myöntää luvat teleoperaattoreille ajalle 22.6.2025–31.12.2033.
- Verkkotoimiluvan tavoitteena on muun muassa edistää sähköisten viestinnän palvelujen tarjontaa ja käyttöä sekä turvata radiotaajuuksien tehokas käyttö.

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) 159 CVEs Exploited in Q1 2025 — 28.3% Within 24 Hours of Disclosure - https://thehackernews.com/2025/04/159-cves-exploited-in-q1-2025-283.html
2) Digitaalinen Eurooppa -rahoitusohjelman työsuunnitelma vuosille 2025-2027 on julkaistu - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/digitaalinen-eurooppa-rahoitusohjelman-tyosuunnitelma-vuosille-2025-2027-julkaistu
3) Kyberturvallisuuskeskuksen viikkokatsaus – 16/2025 - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-162025
4) Uusittu ohje tietojärjestelmien tietoturvallisuuden arviointi- ja hyväksyntäprosesseista - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uusittu-ohje-tietojarjestelmien-tietoturvallisuuden-arviointi-ja
5) Kyberturvallisuuskeskuksen viikkokatsaus - 15/2025 - https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-152025#85209-2
6) Cyber Criminals Exploit Pope Francis Death to Launch Global Scams - https://blog.checkpoint.com/research/cyber-criminals-exploit-pope-francis-death-to-launch-global-scams/
7) Kyberturvallisuuskeskuksen viikkokatsaus - 14/2025 - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-142025?toggle=Mobiilivarmenne#84482-3
8) Kyberturvallisuuskeskuksen viikkokatsaus – 16/2025 - https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-162025#85345-1
9) Zhang, Z., Hamadi, H. A., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. IEEE access, 10, 93104-93139. https://doi.org/10.1109/ACCESS.2022.3204051
10) Gwassi, O. A. H., Uçan, O. N., & Navarro, E. A. (2024-09-11). Cyber-XAI-Block: An end-to-end cyber threat detection & fl-based risk assessment framework for iot enabled smart organization using xai and blockchain technologies. Multimedia tools and applications. https://doi.org/10.1007/s11042-024-20059-4
11) Cyberattacks by AI agents are coming - https://www.technologyreview.com/2025/04/04/1114228/cyberattacks-by-ai-agents-are-coming/
12) Internet Organised Crime Threat Assessment (IOCTA) 2024 https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024
13) Espanjassa ja Portugalissa massiivinen sähkökatko – Ukraina tarjoaa apuaan - https://yle.fi/a/74-20158515
14) Unsophisticated Cyber Actor(s) Targeting Operational Technology - https://www.cisa.gov/news-events/alerts/2025/05/06/unsophisticated-cyber-actors-targeting-operational-technology
15) NIS 2 - Euroopan unionin kyberturvallisuusdirektiivi - https://kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis-2-euroopan-unionin-kyberturvallisuusdirektiivi
16) Euroopan tietosuojaneuvostolta ohjeluonnos henkilötietojen käsittelystä lohkoketjuteknologioiden avulla - https://tietosuoja.fi/-/euroopan-tietosuojaneuvostolta-ohjeluonnos-henkilotietojen-kasittelysta-lohkoketjuteknologioiden-avulla

Lähdeluettelo

17) Guidelines 02/2025 on processing of personal data through blockchain technologies - https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-022025-processing-personal-data_en
18) Commission Implementing Regulation (EU) 2025/846 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards cross-border identity matching of natural persons - http://data.europa.eu/eli/reg_impl/2025/846/oj
19) Commission Implementing Regulation (EU) 2025/847 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reactions to security breaches of European Digital Identity Wallets - http://data.europa.eu/eli/reg_impl/2025/847/oj
20) Commission Implementing Regulation (EU) 2025/848 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the registration of wallet-relying parties - http://data.europa.eu/eli/reg_impl/2025/848/oj
21) Commission Implementing Regulation (EU) 2025/849 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the submission of information to the Commission and to the Cooperation Group for the list of certified European Digital Identity Wallets - http://data.europa.eu/eli/reg_impl/2025/849/oj
22) Uusi lakihanke: sijaintiselvityspyyntöjen vastausjärjestelmän valmistelu käynnistyy - https://lvm.fi/-/uusi-lakihanke-sijaintiselvityspyyntojen-vastausjarjestelman-valmistelu-kaynnistyy
23) Toimiluvat 450 megahertsin taajuusalueelle manner-Suomessa ja Ahvenanmaalla haettavissa - https://lvm.fi/-/toimiluvat-450-megahertsin-taajuusalueelle-manner-suomessa-ja-ahvenanmaalla-haettavissa