TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Lokakuu 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

50M

EU:n Digitaalinen Eurooppa –rahoitusohjelmanvuoden toinen hakukierros avautui 28.10.2025. Ohjelman kautta jaetaan rahoitusta kyberaiheisiin 50 miljoonaa euroa. Hakuaika kestää 31.03.2026 saakka. [1]

1,9 MRD

Englannissa uutisoitiin Jaguar Land Roveriin kohdistuneen kyberhyökkäyksen ennätyksellisen suurista vaikutuksista. Syyskuussa alkanut kyberhyökkäys pysäytti ajoneuvojen tuotannon yli kuukaudeksi. Kokonaistappioiden arvioidaan nousevan jopa 1,9 miljardiin puntaan. [2 & 3]

Kybersää Lokakuu 2025

Tietomurrot ja -vuodot

- M365-tilimurrot ovat jatkaneet kasvuaan. Tietomurtojen yrityksiä raportoitiin aiempaa vähemmän.
- Lokakuussa ilmoitettiin jo aiemmin tapahtuneista globaaleista tietovuodoista, joissa myös suomalaisia kohteita uhreina.
- Ruotsin kantaverkkoyhtiö Svenska kraftnät kohdistui tietomurto, jossa Everest-uhkatoimija on väittänyt vuotavansa haltuunsa saamaansa 280 GT dataa. Julkisuudessa vahvistettiin murron koskevan rajattua, ulkoista tiedostonsiirtoratkaisua. [4 & 5]

Huijaukset ja kalastelut

- Huijauspuheluissa on esiinnytty viranomaisena. Rikolliset ovat väittäneet soittavansa Kyberturvallisuuskeskuksesta, väittäen laitteiden olleen haittaohjelman saastuttamia ja urkkien pankkitunnuksia tai maksukorttien tietoja.
- Kansainvälisessä poliisioperaatiossa suljettiin rikollisten käyttämiä mobiilipalvelimia, pidätettiin epäiltyjä ja takavarikoitiin yli 1200 SIM-boksia sekä muuta rikoksella hankittua omaisuutta. Huijauksilla arvioitiin olleen ainakin 3200 uhria.

Haittaohjelmat ja haavoittuvuudet

- Maailmalla on raportoitu laajasti eri kiristyshaittaohjelmahyökkäyksistä. Suomeen hyökkäykset eivät ole vaikuttaneet suuresti vielä lokakuun aikana.
- Kalastelujen ja petosten määrän kasvaessa kohdennettua haittaohjelmien jakoa on havaittu sähköpostien liitetiedostoihin piilotettuna.
- CVE-2025-49844 Redis-ohjelmistossa on havaittu vakava haavoittuvuus. Suosittelemme haavoittuvien instanssien paikantamista ja päivittämistä välittömästi.

Automaatio ja IoT

- Dragosin vuosiraportti ja ENISAn Threat Landscape 2025 -raportti julkaistiin lokakuussa. [6 & 7]
- ENISAn raportissa todetaan, että mobiililaitteet ovat edelleen hyökkääjien eniten käyttämä rajapinta. Myös teollisuuteen ja kriittiseen infrastruktuuriin kohdistuvien OT-hyökkäysten määrä on kasvussa.

Verkkojen toimivuus

- Suomalaisia organisaatioita oli jälleen venäjämielisen toimijan palvelunestohyökkäysten kohteena. Hyökkäyksillä ei ollut merkittäviä vaikutuksia.
- Palvelunestohyökkäyksiin varautuessa on otettava huomioon suojattavien järjestelmien kokonaisuus ja keskinäisriippuvuudet. [8]

Vakoilu

- Kiinalainen uhkatoimija pyrki vakoilemaan diplomaattikohteita Euroopassa. Kampanjassa pyrittiin levittämään kohteelle PlugX-haittaohjelmaa mm. EU- ja NATO-teemaisilla viesteillä.
- Pohjois-Koreaan liitetty uhkatoimija on pyrkinyt vakoilemaan eurooppalaisia puolustusalan organisaatioita rekrytointiteemaisella yhteydenotolla alkavassa kampanjassaan.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Syyskuun lopulla tiedotimme Ciscon FTD ja ASA -tuotteiden kriittisistä haavoittuvuuksista, ja olimme lokakuussa yhteydessä haavoittuviksi tunnistettujen laitteiden omistajiin. Voit lukea kyseisistä haavoittuvuuksista ja päivitystarpeista verkkosivuillamme. [9]

Tietoomme on tullut tapauksia, joissa rikolliset olivat esiintyneet Kyberturvallisuuskeskuksen työntekijöinä. Julkaisimme aiheesta tiedotteen, jossa kerromme, miten voit tunnistaa tuleeko puhelu tai sähköpostiviesti aidolta virkahenkilöltä. Muista, että emme pyydä sinua koskaan esimerkiksi maksamaan laskua, asentamaan ohjelmistoa taikka luovuttamaan pankki- ja kirjautumistunnuksia. [10]

Microsoft lopetti Windows 10:n virallisen tuen 14. lokakuuta 2025. Tuen päättyminen tarkoittaa, että käyttöjärjestelmä ei enää saa tietoturvapäivityksiä tai virallista teknistä tukea. Käyttöjärjestelmä toimii edelleen, mutta sen käyttäminen lisää tietoturvariskejä, kun uusia haavoittuvuuksia ei enää korjata. [11]

Lokakuun kyberturvallisuuden yleiskuva

Lokakuu oli Kyberturvallisuuskeskuksen näkökulmasta melko vilkas.

Kuukauden merkittävimpiin kansainvälisiin tapauksiin lukeutui muun muassa Yhdysvaltalaiseen tietoturva- ja teknologiayritys F5:een kohdistunut tietomurto, jonka yhteydessä valtiolliseksi uhkatoimijaksi arvioitu taho oli saanut pääsyn F5:n sisäisiin järjestelmiin. Hyökkääjä oli kopioinut muun muassa BIG-IP-tuotteiden lähdekoodia sekä tietoja julkaisemattomista haavoittuvuuksista. [12]

- F5:n järjestelmiä on laajasti käytössä erilaisissa organisaatioissa ympäri maailman ja tapaus edellytti kiireellistä reagointia.
- Muita kansainvälisesti merkittäviä tapahtumia olivat Red Hat ohjelmistoyhtiöön kohdistunut tietomurto sekä Ciscon ASA ja FTD -tuotteiden kriittiset haavoittuvuudet. [13 & 14]

Suomessa Microsoft 365 -tilimurtoihin liittyviä ilmoituksia kirjattiin lokakuussa jälleen tavanomaista enemmän. Syyskuussa julkaisemamme vakava varoitus on edelleen voimassa. [15]

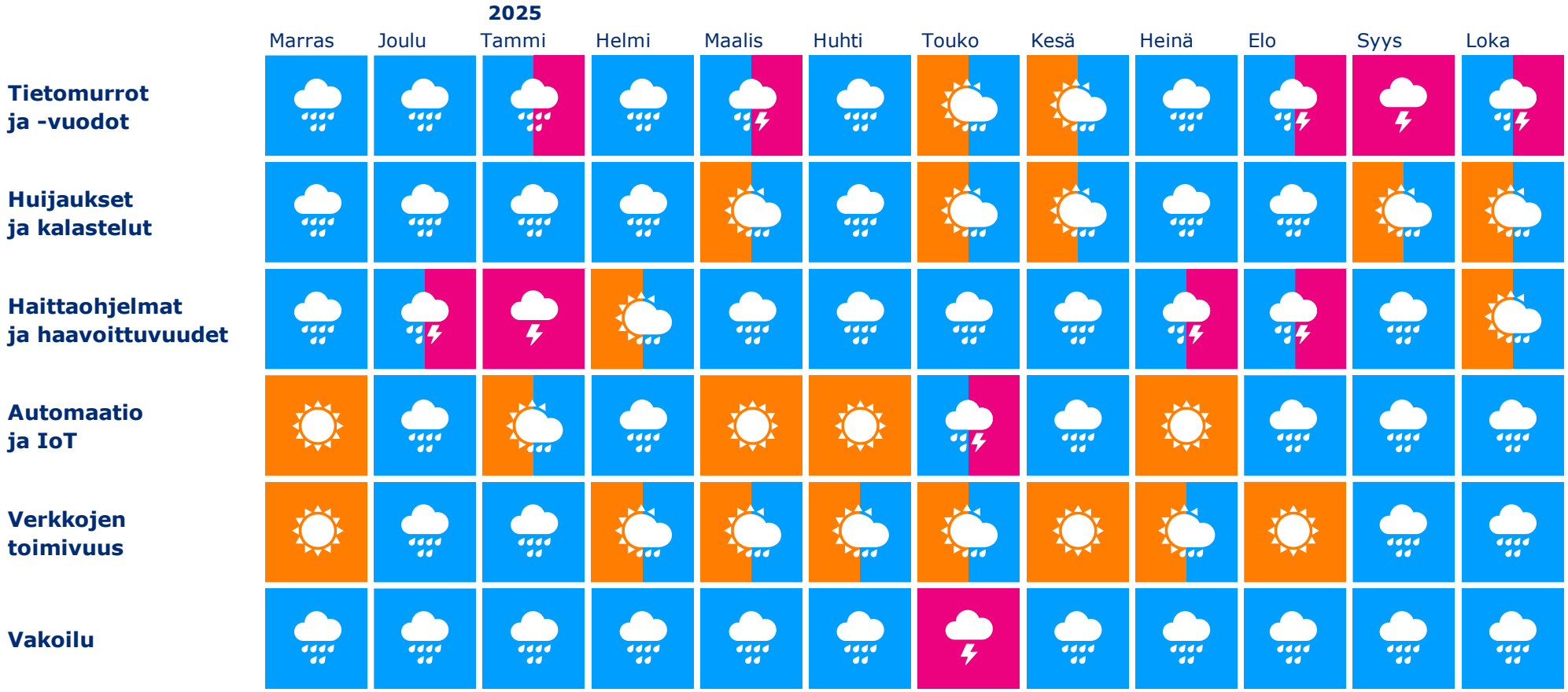
Kotimaassa turvallisuuden kannalta positiivisena uutisena oli Itä-Suomen Poliisin paljastama rikoskokonaisuus, jossa eläkeläisiltä huijattiin miljoonia euroja. [16]

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



Top 5 uhat lähitulevaisuudessa (6kk–2v)

1.

haavoittuvuuksia hyödynnetään yhä nopeammin

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

2.

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.

3.

Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa.

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

Symbolit

Uusi

Päivitetty

4.

Kiristyshaittaohjelmat -Merkittävä uhka organisaatioille

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

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, on havaittu vakavia ja helposti hyödynnettäviä haavoittuvuuksia viimeisen vuoden aikana.
  - **Reunalaitteet ovat viimeaikoina korostuneet valtiollisten toimijoiden vaikuttamisen kohteena.**
  - **Reunalaitteisiin kohdistuvia hyökkäyksiä toteutetaan usein nollapäivähaavoittuvuuksien kautta. Organisaatioiden verkkojen valvonta ja haavoittuvuuksien etsiminen ovat tärkeitä uhkilta välttymiseksi. Päivittämisen lisäksi on hyvä seurata valmistajan ohjeita tietomurtojen ja hyväksikäytön havaitsemiseksi.**
- 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.
  - Järjestelmien nopea päivittäminen on erityisen tärkeää ja valmius päivittämiseen on syytä ylläpitää jatkuvasti, myös yleisinä loma-aikoina.

2. 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.
  - Toimitusketjuihin liittyvä uhka ei kohdistu pelkästään komponentteihin, vaan saattaa myös konkretisoitua esimerkiksi ohjelmistojen ja ohjelmointikirjastojen kautta.
- 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.
- **Toimitusketjuhyökkäys voi vaikuttaa lamauttavasti organisaation toimintaan.** 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.
- **Hyökkäysten vaikutusten pienentämiseksi organisaatioiden kannattaa myös pohtia palveluntarjoajaan tai toimitusketjun osaan kohistuvan hyökkäysten mahdollisia vaikutuksia, sekä tapoja häiriötilanteiden hallintaan. Syys-lokakuussa Euroopan lentokenttiä häirinneen kyberhyökkäyksen kohteena oli boarding ja check-in järjestelmiä tarjoava yritys. Palveluiden lamaantuminen näkyi lentoyhtiöiden päässä, jotka joutuivat turvautumaan joissain tapauksissa kynään ja paperiin matkustajien kirjaamiseksi. Osin näiden varamenetelmien ansiosta lentoliikenne ei estynyt täysin, vaikka alkuvaiheessa merkittävä osa lennoista peruttiin.**

3. Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa

- Erilaiset tekoälysovellukset saattavat aiheuttaa uusia ja yllättäviä tietoturvauhkia organisaatioille. **Automaattisesti toimivat työkalut, kuten puhetta litteroivat tai muistiinpanoja tuottavat sovellukset ja avustajat,** saattavat esimerkiksi videoneuvottelun yhteydessä käsitellä dataa, jonka käyttöä kaikki osallistujat eivät ole hyväksyneet. **Integroiduilla tekoälysovelluksilla** saattaa myös olla laaja pääsy organisaation dataan. Riskit korostuvat, jos sovellus säilyttää tai käsittelee dataa organisaation ulkopuolisella palvelimella. [17]
- **Uhkatoimijat käyttävät yhä aktiivisemmin tekoälypalveluita haittaohjelmien ja hyökkäysten jalostamiseen**. Tekoälyä hyödynnetään esimerkiksi kalasteluviestien laatimiseen, haittaohjelmien kehittämiseen tai haitallisen koodin tulkittavuuden hankaloittamiseen (obfuscation). **Tekoäly näyttelee olennaista osaa myös Ukrainaan kohdistuvissa kyberoperaatioissa.** [18 & 19]
- 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. **Tekoälyn huoleton käyttö on yleinen riski. Arkaluontoista tietoa saattaa päätyä käyttäjien välityksellä erilaisiin tekoälypalveluihin.** [20]
  - 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.

4. Kiristyshaittaohjelmat - Merkittävä uhka organisaatioille

- Kiristyshaittaohjelmien muodostama uhka on säilynyt ennallaan, vaikka KTK:lle ilmoitetut tapausmäärät ovat olleet viime vuosina laskusuunnassa. 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.
- **Eurooppa on maantieteellisesti toisella sijalla verkkorikollisuuden kohdealueena.** [21] **Kiristystapaustoiminnan arviointiin pätee ns. Iceberg-viitekehys: tilastot eivät kerro koko totuutta. Toimintaa tapahtuu todennäköisesti enemmän kuin mitä sitä havaitaan ja raportoidaan.**
- Kiristyshaittaohjelmien määrä kasvaa jatkuvasti globaalisti, ja ilmiö ja siihen liittyvä palvelutuotanto on jatkuvassa kehityksessä.
  - Akira on viimeiset kaksi vuotta ollut Kyberturvallisuuskeskukselle eniten ilmoitettu kiristyshaittaohjelma. Sen lisäksi on raportoitu useita kiristyshaittaohjelmia, joita ei ole ennen havaittu Suomessa.
- Kiristysluontoisissa hyökkäyksissä salaavia haittaohjelmia on tavattu aiempaa vähemmän. Viimeaikoina kansainvälisesti kiristyshyökkäyksissä on korostunut tiedostojen salaamisen sijaan datan nopea varastaminen kohdejärjestelmästä, jolloin kiristäjä lupaa lunnaita vastaan hävittää varastetun aineiston, tai jättää sen julkaisematta. Tietoturvayhtiö Sophoksen tutkimuksen mukaan vuonna 2025 tiedostoja on salattu vain 50 prosentissa tapauksista.
- **Hyökkääjät eivät murtaudu sisään, vaan kirjautuvat sisään. Yli 97 % identiteettihyökkäyksistä on salasanahyökkäyksiä. Vuoden 2025 ensimmäisellä puoliskolla identiteettihyökkäykset lisääntyivät 32 %. 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 (info stealer) haittaohjelmia.** [22 & 23]
- 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.

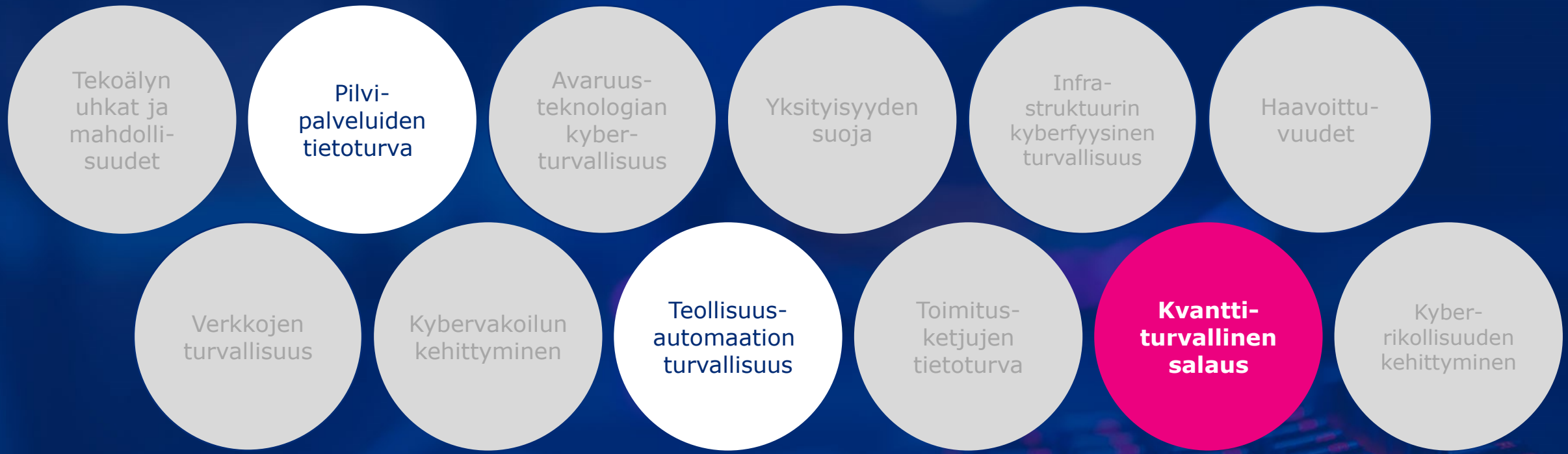
5. Tietoliikenneinfrastruktuurin suojaamisen tärkeys korostuu

- 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.
  - 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.
  - 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.

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: Kvanttiturvallinen salaus

Kvanttitietokoneiden kehittyminen uhkaa nykyisiä julkisen avaimen salausmenetelmiä. Kvanttitietokoneiden kehittyessä riittävän pitkälle, perinteisten salausmenetelmien matemaattinen tausta romahtaa. Tällöin puhutaan kryptografisesti merkittävistä kvanttitietokoneista, CRQC (Cryptographically Relevant Quantum Computer).

- Aika-arviot CRQC:n saavuttamiselle vaihtelevat, mutta viimeaikaiset kehitysaskeleet saattavat johtaa uhan konkretisoitumiseen jo kymmenen vuoden sisällä.

Kvanttiturvallisten salausmenetelmien (PQC, Post-Quantum Cryptography) kehitys ja standardointi ovat käynnissä. Yhdysvaltain standardointiviranomainen NIST on jo julkaissut kolme standardia sekä ilmoittanut myös kahdesta julkaisemattomasta, ja lisää on odotettavissa. Nämä ovat julkisen avaimen menetelmiä: KEM, Key Establishment Mechanism eli avaintenluontimenetelmiä sekä digitaalisia allekirjoitusalgoritmeja. NISTn prosessi PQC-algoritmien kehittämiseksi ja standardoimiseksi on avoin ja siinä on mukana kryptologeja ympäri maailmaa.

- Suomessa tullaan kansallisen kryptotyöryhmän päätöksellä hyväksymään NISTn standardoimat menetelmät kansallisissa salaustuotearvioinneissa.
- Symmetriset salausmenetelmät kuten AES eivät ole samalla tavoin uhattuna. Uusia algoritmeja ei näillä näkymin tarvita, vaan riittävä turvallisuus saavutetaan siirtymällä pidempien avainten käyttöön.
- Hybridimenetelmien käyttöä suositellaan. Näissä PQC-algoritmi yhdistetään klassiseen algoritmiin (kuten Diffie-Hellman-avaintenvaihtoon), jolloin saadaan suoja sitä vastaan, että käytetty PQC-algoritmi murtuisi jo klassisilla tietokoneilla. Hybridimenetelmien standardointi on vielä kesken.
- Itse asiassa uhka on jo päällä harvest-now-decrypt-later-hyökkäyksinä eli vastustaja voi jo nyt nauhoittaa salattua tietoliikennettä ja murtaa sen sitten kun CRQC on käytettävissä. Tämän takia siirtyminen PQC-algoritmien käyttöön nopealla aikataululla on tärkeää.
- Kaikkia organisaatioita kehotetaan aloittamaan PQC-siirtymä mitä pikimmiten jos se ei jo ole käynnissä.

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

EASA Part-IS delegoidun asetuksen (EU) 2022/1645 soveltaminen alkoi 16.10.2025. [24]

- Euroopan komission delegoidussa asetuksessa vahvistetaan ilmailun tietoturvaan liittyviä vaatimuksia, joilla suojataan lentoturvallisuutta kyberuhkilta.
- Part-IS tuli voimaan suunnitteluorganisaatioille (DOA), valmistusorganisaatioille (POA), lentoaseman ylläpitäjille sekä asematasohallintapalvelun tarjoajalle (Apron Management Service Provider).
- Muiden ilmailun toimijoiden osalta Part-IS tulee voimaan 22.2.2026 täytäntöönpanoasetuksella (EU) 2023/203.

Oikeudelliset asiat

Uudet ohjeet EU:n tietosuojalainsäädännön ja digi- ja datasäädösten keskinäisestä suhteesta. [25 - 27]

- Euroopan tietosuojasuojaneuvosto on julkaissut ohjeen EU:n digipalveluasetuksen (DSA) ja yleisen tietosuoja-asetuksen välisestä suhteesta.
  - Ohje auttaa ymmärtämään, miten tietosuoja-asetusta tulisi soveltaa yhdessä DSA:n velvoitteiden kanssa ja miten tietosuojaan liittyviä säännöksiä tulkitaan yhdenmukaisesti. Lisäksi ohje sisältää käytännön ohjeita viranomaisten yhteistyöstä.
  - Julkinen kuuleminen päättynyt 31.10.2025.
- Euroopan tietosuojaneuvoston ja Euroopan komission yhteinen ohjeluonnos EU:n digimarkkina-asetuksen (DMA) ja tietosuoja-asetuksen keskinäisestä suhteesta julkisessa kuulemisessa.
  - Ohje auttaa ymmärtämään, miten asetuksia sovelletaan rinnakkain ja yhdenmukaisesti. DMA:ssa säädetään velvoitteita EU-alueella toimiville suurimmille alustayrityksille, jotka ovat markkinoiden ns. portinvartijoita. Ohjeessa selvennetään, miten portinvartijayrityksen voivat toteuttaa DMA:n velvoitteita siten, että ne noudattavat samalla tietosuojalainsäädäntöä.
  - Sidosryhmät voivat antaa palautetta ohjeluonnoksesta 4.12.2025 saakka.

Oikeudelliset asiat

Aktialle seuraamusmaksu tietoturvapuutteista vahvan sähköisen tunnistamisen palvelussa. [28 & 29]

- Aktian vahvan sähköisen tunnistamisen palvelussa esiintyi teknisestä muutoksesta johtunut häiriö tammikuussa 2023. Noin tunnin kestäneen häiriön aikana osa henkilöistä, jotka kirjautuivat Aktian verkkopankkitunnuksilla vahvaa tunnistamista vaativiin palveluihin, oli nähnyt toisten henkilöiden tietoja. Myös asiointi toisen asiakkaan nimissä oli ollut mahdollista.
- Tietoturvaloukkaus koski viranomaisasioinnin palveluita, työttömyyskassoja, vakuutusyhtiöitä ja terveydenhuollon palveluntarjoajia. Vika ei kuitenkaan koskenut Aktian verkkopankkiin kirjautumista. Tietoturvaloukkauksen kohteeksi joutui noin 350 henkilöä. Häiriöstä johtuvaa tietojen väärinkäyttöä ei Aktian mukaan ole tiedossa.
- Tietosuojavaltuutetun toimiston selvityksessä havaittiin, että Aktian olisi tullut suunnitella ja toteuttaa tunnistuspalvelun tekninen muutos huolellisemmin ja testata palvelun toimintaa riittävästi muutoksen jälkeen.
- Tietosuojavaltuutetun toimiston seuraamuskollegio määräsi Aktialle 865 000 euron hallinnollisen seuraamusmaksun, sillä pankki ei ollut noudattanut tietosuojalainsäädännön vaatimuksia henkilötietojen turvallisesta käsittelystä. Seuraamusmaksun määrän arvioinnissa huomioitiin, että Aktialla oli ollut valmius reagoida häiriötilanteeseen nopeasti ja että se oli ryhtynyt viipymättä toimiin tilanteen korjaamiseksi, jolloin vahinkoja oli pystytty lieventämään. Apulaistietosuojavaltuutettu antoi pankille myös huomautuksen tietosuoja-asetuksen rikkomisesta.
- Päätökset eivät ole vielä lainvoimaisia ja niistä voi valittaa hallinto-oikeuteen.

Oikeudelliset asiat

Tietosuojavaltuutetun toimisto selvitti julkisen sektorin organisaatioiden menettelyä pilvipalvelujen käytössä. [30 - 33]

- Tietosuojavaltuutetun toimisto on arvioinut Valtion tieto- ja viestintätekniikkakeskus Valtorin, Digi- ja väestötietoviraston (DVV) ja Verohallinnon menettelyjä pilvipalvelujen käytössä helmi-huhtikuussa 2022. Selvitys oli osa laajempaa eurooppalaisten tietosuojaviranomaisten selvitystä, jossa tarkasteltiin noin sadan julkisen sektorin organisaation pilvipalvelujen käyttöä EU:ssa.
- Selvityksessä havaittiin, että henkilötiedoille ei ollut varmistettu riittävää tietosuojaa, kun niitä siirrettiin Valtorin tarjoaman pilvipalvelun kautta Yhdysvaltoihin aikana, jolloin EU:lla ja Yhdysvalloilla ei ollut voimassa olevaa tietosuojakehystä, jonka perusteella tietoja olisi voitu siirtää turvallisesti. Tämän takia organisaatioilla oli velvollisuus varmistaa erilaisin lisäsuojatoimin, että vaadittu tietosuojan taso säilyy, kun henkilötietoja siirrettiin Yhdysvaltoihin.
- Tietosuojavaltuutettu antoi Valtorille huomautuksen tietosuojapuutteista. Apulaistietosuojavaltuutettu antoi huomautuksen myös DVV:lle, sillä se oli laiminlyönyt velvollisuutensa varmistaa, että tiedonsiirroille taataan riittävä suoja. Verohallinnolle ei annettu huomautusta, sillä se oli selvityksen perusteella pyrkinyt huomioimaan tietosuojavaatimukset ottamalla käyttöön erilaisia täydentäviä suojatoimia.
- Päätökset eivät ole vielä lainvoimaisia ja niistä voi valittaa hallinto-oikeuteen.

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) Digitaalinen Eurooppa -ohjelma avasi uuden rahoitushaun: 50 miljoonaa euroa kyberturvallisuuteen https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/digitaalinen-eurooppa-ohjelma-avasi-uuden-rahoitushaun-50-miljoonaa-euroa
2) JLR hack is costliest cyber attack in UK history, say analysts https://www.bbc.com/news/articles/cy9pdld4y81o
3) JLR cyber-attack caused UK car production to hit 70-year low for September https://www.bbc.com/news/articles/cvgmp1prnv0o
4) Svenska kraftnät utreder ransomware https://www.expressen.se/nyheter/expressen-direkt/?post=979b170f-3d08-4c7f-9b15-1ef70bef34f4
5) Ransomware.live https://www.ransomware.live/id/U3ZlbnNrYSBLcmFmdG7DpHRAZXZlcmVzdA
6) Dragos Year in Review https://www.dragos.com/ot-cybersecurity-year-in-review
7) Enisa Threat Landscape 2025 https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf
8) Move Over, DDoS: It's the Era of Distributed Denial of Defense (DDoD) https://www.akamai.com/blog/security/move-over-ddos-era-distributed-denial-of-defense-ddod
9) Kriittisiä Cisco ASA- ja FTD-haavoittuvuuksia käytetään hyväksi hyökkäyksissä https://kyberturvallisuuskeskus.fi/fi/kriittisia-cisco-asa-ja-ftd-haavoittuvuuksia-kaytetaan-hyvaksi-hyokkayksissa
10) Rikolliset soittavat Traficomin Kyberturvallisuuskeskuksen nimissä huijauspuheluja https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/rikolliset-soittavat-traficomin-kyberturvallisuuskeskuksen-nimissa-huijauspuheluja
11) Windows 10:n tuki päättyi 14. lokakuuta https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-422025#90948-0
12) Yhdysvaltalainen tietoturva- ja teknologiayritys F5 tietomurron kohteena https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/yhdysvaltalainen-tietoturva-ja-teknologiayritys-f5-tietomurron-kohteena
13) Security update: Incident related to Red Hat Consulting GitLab instance https://www.redhat.com/en/blog/security-update-incident-related-red-hat-consulting-gitlab-instance
14) Kriittisiä Cisco ASA- ja FTD-haavoittuvuuksia käytetään hyväksi hyökkäyksissä https://kyberturvallisuuskeskus.fi/fi/kriittisia-cisco-asa-ja-ftd-haavoittuvuuksia-kaytetaan-hyvaksi-hyokkayksissa
15) Microsoft 365 -tilejä murretaan – varo tietojenkalastelua https://kyberturvallisuuskeskus.fi/fi/varoitus_1/2025
16) Tällaisia ovat salaiset soittokeskukset, joista suomalaisilta eläkeläisiltä huijattiin miljoonia euroja https://yle.fi/a/74-20186798?origin=ncscfi
17) Disrupting malicious uses of AI: an update https://cdn.openai.com/threat-intelligence-reports/7d662b68-952f-4dfd-a2f2-fe55b041cc4a/disrupting-malicious-uses-of-ai-october-2025.pdf
18) Russian hackers turn to AI as old tactics fail, Ukrainian CERT says https://therecord.media/russian-hackers-turn-to-ai-ukraine-cert
19) Employees regularly paste company secrets into ChatGPT https://www.theregister.com/2025/10/07/gen_ai_shadow_it_secrets/
20) Ole valppaana tekoälyn kanssa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ole-valppaana-tekoalyn-kanssa

Lähdeluettelo

17) Ole valppaana tekoälyn kanssa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ole-valppaana-tekoalyn-kanssa
18) Disrupting malicious uses of AI: an update https://cdn.openai.com/threat-intelligence-reports/7d662b68-952f-4dfd-a2f2-fe55b041cc4a/disrupting-malicious-uses-of-ai-october-2025.pdf
19) Russian hackers turn to AI as old tactics fail, Ukrainian CERT says https://therecord.media/russian-hackers-turn-to-ai-ukraine-cert
20) Employees regularly paste company secrets into ChatGPT https://www.theregister.com/2025/10/07/gen_ai_shadow_it_secrets/
21) CrowdStrike 2025 European Threat Landscape Report: Ransomware Hits Region at Record Pace https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-2025-european-threat-landscape-report-ransomware
22) Extortion and ransomware drive over half of cyberattacks https://blogs.microsoft.com/on-the-issues/2025/10/16/mddr-2025/
23) Ransomware Statistics and Ransomware Trends 2025 https://www.fortinet.com/resources/cyberglossary/ransomware-statistics
24) Komission delegoitu asetus (EU) 2022/1645 https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32022R1645
25) Euroopan tietosuojaneuvostolta ohje tietosuoja-asetuksen ja digipalveluasetuksen välisestä suhteesta https://tietosuoja.fi/-/euroopan-tietosuojaneuvostolta-ohje-tietosuoja-asetuksen-ja-digipalveluasetuksen-valisesta-suhteesta
26) Guidelines 3/2025 on the interplay between the DSA and the GDPR https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-32025-interplay-between-dsa-and-gdpr_en
27) Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/joint-guidelines-interplay-between-digital_en
28) Aktialle seuraamusmaksu tietoturvapuutteista vahvan sähköisen tunnistamisen palvelussa https://tietosuoja.fi/-/aktialle-seuraamusmaksu-tietoturvapuutteista-vahvan-sahkoisen-tunnistamisen-palvelussa
29) Tietoturvallisuuden laiminlyönti pankin tunnistamispalvelun muutosprosessin hallinnassa https://www.finlex.fi/fi/viranomaiset/tietosuojavaltuutettu/2025/2485
30) Tietosuojavaltuutetun toimisto: valtionhallinnon pilvipalveluiden on täytettävä tietosuojavaatimukset https://tietosuoja.fi/-/tietosuojavaltuutetun-toimisto-valtionhallinnon-pilvipalveluiden-on-taytettava-tietosuojavaatimukset
31) Pilvipalvelujen käyttö julkisella sektorilla ja palveluntarjoajan toiminta https://www.finlex.fi/fi/viranomaiset/tietosuojavaltuutettu/2025/2481
32) Pilvipalvelun käyttö julkisella sektorilla ja rekisterinpitäjän toiminta (TSV/164/2022) https://www.finlex.fi/fi/viranomaiset/tietosuojavaltuutettu/2025/2483
33) Pilvipalvelun käyttö julkisella sektorilla ja rekisterinpitäjän toiminta (TSV/24/2022) https://www.finlex.fi/fi/viranomaiset/tietosuojavaltuutettu/2025/2482