TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Lokakuu 2024

#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

Liikenne- ja viestintävirasto Traficom on jakanut tietoturvan kehittämisen tukea kuuden miljoonan euron verran. Tukea jaettiin 313 yhteiskunnan kannalta elintärkeälle yritykselle Suomessa. Myönnetyt tuet vaihtelevat 371 eurosta 100 000 euroon.[1]

Kyberturvallisuuskeskuksen tietoon on lokakuun loppuun mennessä tullut 16 kiristyshaittaohjelmatapausta Suomessa tänä vuonna. Vastaavan ajankohdan lukumäärä vuonna 2023 oli 25. Keskimäärin Kyberturvallisuuskeskus saa vuosittain ilmoituksia noin 40 kiristyshaittaohjelmatapauksesta.

Kybersää lokakuu 2024

Tietomurrot ja -vuodot

- FortiManagerin haavoittuvuus johti tietomurtoihin myös Suomessa.
- M365-tilejä murrettiin uudelleen aktivoituneella kalasteluteemalla, jossa uhrille lähetettiin salasanan vanhenemisviesti.
- Lokakuussa raportoitiin jopa kuukausia kestäneitä low&slow–tietomurron yrityksiä, joissa kirjautumisyrityksiä tehdään pienellä volyymillä, pitkällä aikavälillä.

Huijaukset ja kalastelut

- Lokakuun lopulla käynnistyi aggressiivinen SMS-kalastelu-kampanja eri toimijoiden nimissä. SMS-lähettäjänimenä näkyi sekä oikeita että vääriä muunnelmia Terveystalosta, Traficomista, Fortumista ja Mehiläisestä.
- Viranomaisten ja internet-palvelun-tarjoajien yhteistyöllä petoksellisia pankkitunnusten kalastelusivuja on saatu poistettua verkosta.

Haittaohjelmat ja haavoittuvuudet

- Fortinet on julkaissut korjauksia aktiivisen hyväksikäytön kohteena olevaan kriittiseen FortiManager-tuotteen haavoittuvuuteen.
- Kodeissa olevien laitteiden tietoturvasta tulee huolehtia. Haavoittuvia verkkolaitteita on mahdollista käyttää esimerkiksi palvelunestohyökkäysten tekemiseen.

Automaatio ja IoT

- Viime aikoina on havaittu useita kyberturvallisuushyökkäyksiä ja -ongelmia, joissa on hyödynnetty turvattomia kodin IoT-laitteita.
- NIST on julkaissut raportin IoT-laitteiden käyttöönoton rajoitteista.[2]
- Kattava raportti vastaa suurelta osin myös Kyberturvallisuus-keskuksen tekemiä havaintoja.

Verkkojen toimivuus

- Lokakuussa yleisissä viestintäverkoissa havaittiin seitsemän toimivuushäiriötä, joista yhtä lukuun ottamatta kaikki olivat lieviä.
- Palvelunestohyökkäyksiä ilmoitetaan edelleen alkuvuotta aktiivisemmin, mutta tilanne on rauhoittunut syyskuulta.

Vakoilu

- Venäjään liitetyt APT-ryhmät pyrkivät vakoilemaan valtionhallinnon ja puolustusalan kohteita Euroopassa ja Yhdysvalloissa sekä Ukrainassa.[3, 4, 5, 6]
- Kiinalaistoimija murtautui tele-operaattoreiden järjestelmiin Yhdysvalloissa saadakseen tietoa vaaleista. Kohteena olivat erityisesti telekuuntelujärjestelmät.[7, 8, 9]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Kyberturvallisuuskeskus julkaisi artikkelin verkkotunnusten voimassaolosta huolehtimisesta. Verkkotunnukset ovat merkittävää aineetonta omaisuutta, jonka päätyminen vääriin käsiin voi jopa vaarantaa tietoturvaa.[10]

Traficom päivitti kansallista kryptografista vahvuusvaatimusdokumenttia lisäämällä kvanttiturvallisia algoritmeja kansalliseen kriteeristöön. Kansalliseen käyttöön hyväksytään NISTin standardoimat avaintenmuodostusalgoritmi ML-KEM ja allekirjoitusalgoritmit ML-DSA ja SLH-DSA. Traficom suosittelee organisaatioita siirtymään mahdollisimman pian kvanttiturvallisten algoritmien käyttöön.[11]

Valtioneuvoston yleisistunto hyväksyi uudistetun kansallisen kyberturvallisuusstrategian. Strategiassa kyberturvallisuus määritellään kiinteäksi osaksi kokonaisturvallisuutta, jossa yhteiskunnan elintärkeistä toiminnoista huolehditaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä.[12]

Kyberturvallisuuskeskus suosittelee kansalaisia varautumaan useammalla vahvan sähköisen tunnistautumisen keinolla. Näin pääsy sähköistä tunnistautumista vaativiin palveluihin ei ole riippuvaista yhdestä toimijasta.

Lokakuun kyberturvallisuuden yleiskuva

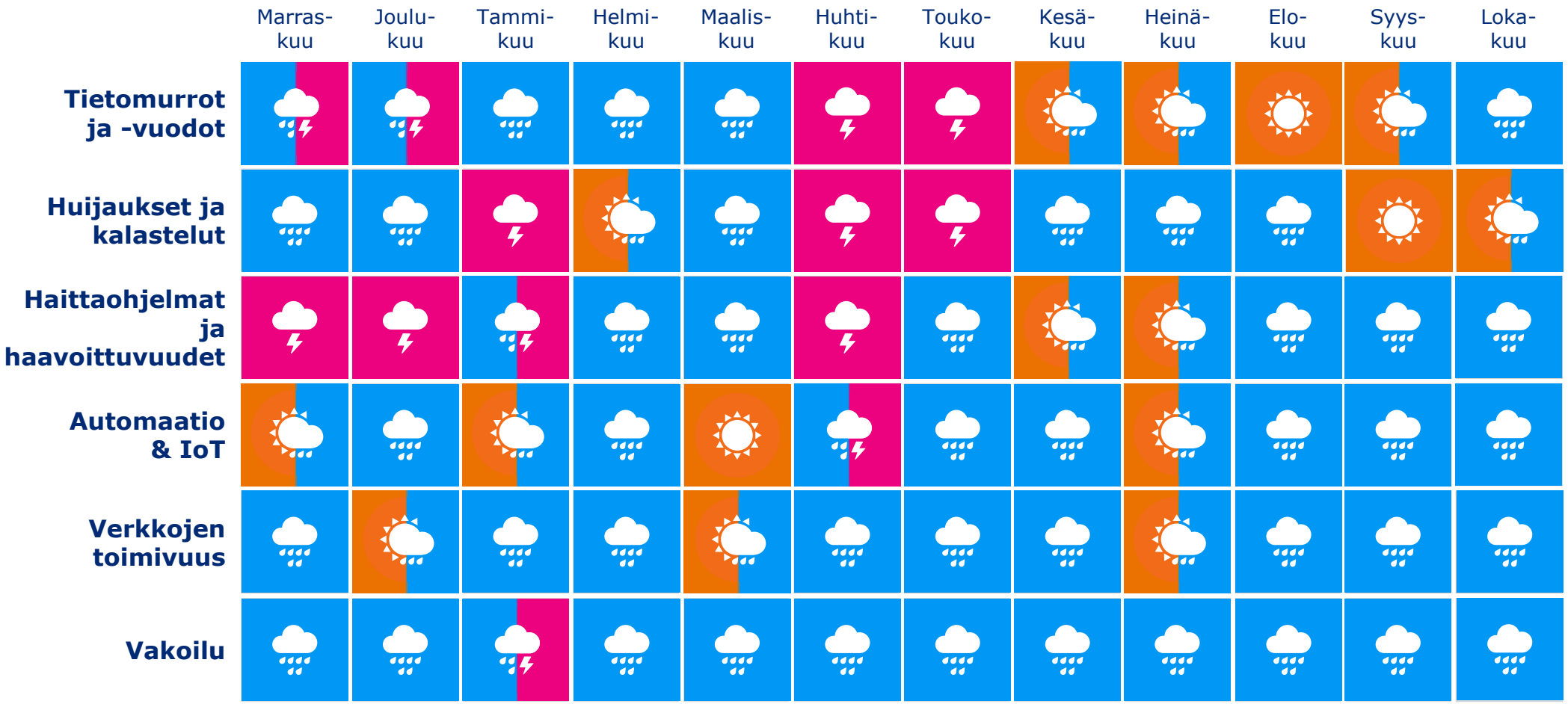
- Lokakuussa Kyberturvallisuuskeskukselle tehdyissä kyberpoikkeamatapauksissa havaittiin määrällistä kasvua rauhallisemman alkusyksyn jälkeen.
- Syyssäässä on esiintynyt ajoittaisia sadepilviä ja harmautta suomalaisiin organisaatioihin viime aikoina kohdistuneiden erilaisten sähköpostitse ja tekstiviestitse lähetettävien tietojenkalastelu- ja huijauskampanjoiden vuoksi. Etenkin M365-kampanjat ovat johtaneet osassa tapauksista tietomurtoihin.
  - Tekstiviestihuijauksia lähetetään sekä väärän että oikean näköisillä lähettäjänimillä. Kyberturvallisuuskeskus suosittelee kaikkia tekstiviestejä lähettäviä organisaatioita suojaamaan lähettäjätunnuksensa mahdollisimman pian.
  - Lokakuun alussa kymmenet tuhannet suomalaiset saivat poliisilta varoitusviestin, jossa kerrottiin, että viestin vastaanottaneella henkilöllä on kohonnut riski joutua rikollisten mielenkiinnon kohteeksi. Varoitusviestien taustalla on tietokanta, jonka poliisi on saanut haltuunsa rikollisilta. Listoilla on ollut suomalaisten nimiä, puhelinnumeroita ja joidenkin henkilöiden osalta myös näiden syntymäaika.
  - Kyberturvallisuuskeskus jakaa tietoa meneillään olevista huijauskampanjoista esimerkiksi Viikkokatsauksessa ja Tietoturva Nyt! -artikkeleissa.
- Palvelunestohyökkäykset jatkuivat edellisen kuukauden tapaan aktiivisina. Kohteina olivat edelleen etenkin finanssisektorilta eri pankit.

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

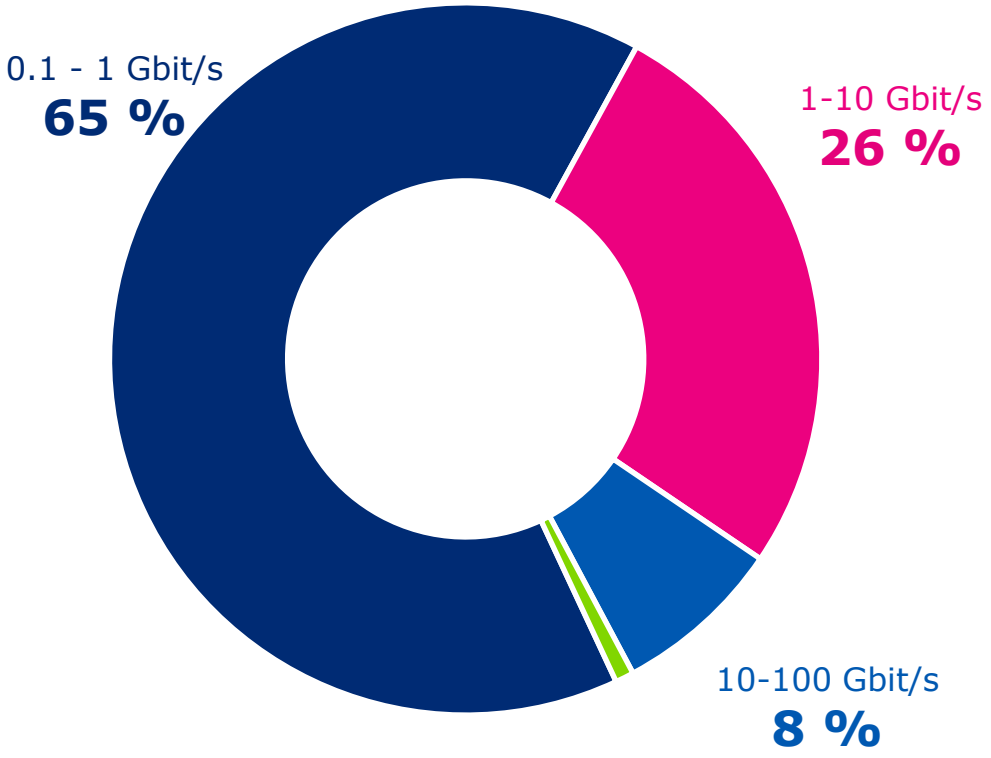
1 kk



3 kk

Palvelunestohyökkäysten tunnuslukuja
Q3/2024

- **198 Gbit/s** oli suurin Suomessa nähty palvelunestohyökkäys Q3/2024.
- Noin 80 % hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



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

Tarve kyberturvallisuuden osaajille

Tekoälyn riskienhallinta

Toimitusketjujen tietoturva

Sääntelyn tulevaisuus

Pilvipalvelujen tietoturva

Teollisuusautomaation suojaaminen

IoT

6G

Kuluttajien tietoturva

Haavoittuvuuksien nopeutuva hyväksikäyttö

Kvanttiturvallinen krypto

Osallistuminen digitaalisessa ympäristössä

Pitkän aikavälin kybersää: Teollisuusautomaation kyberturvallisuus

- Teollisuusautomaation ympäristöt eivät ole pysyneet kyberturvallisuuden kehityksen perässä verrattuna IT-maailmaan. Esimerkiksi vuonna 2022 julkaistun Huoltovarmuuskeskuksen toimialojen kyberkypsyysselvityksen mukaan OT-puolella (OT, *operational technology*) oli haasteita monella eri sektorilla.[13]
- Vaikutusyrityksien kohteena ovat erityisesti olleet teollisuustoimijoiden etäkäyttöjärjestelmät. Internetin kautta suoraan tai etätyöpöytäpalveluiden kautta ilman kirjautumista käytettävissä olevat automaatiojärjestelmät ja niiden hallintapaneelit ovat tarjonneet helppoja väärinkäyttötapoja. Tietomurtoyrityksiä on ollut kasvavissa määrin VPN-palveluihin teollisuusautomaatiokohteissa.
- Huomioitavaa on ollut, että useissa tapauksissa organisaatioiden toiminnan ovat vaarantaneet organisaation omat työntekijät. Varaanpaikan aiheuttavat myös toimittajaketjut ja yhteistyökumppanit, jotka eivät ole noudattaneet organisaation tietoturvapolitiikkaa tai -käytäntöjä.
- Laitehallinnan näkökulmasta riskin muodostavat puutteellisesti toteutettu organisaatioiden fyysinen laiteinventaario ja vajavainen näkyvyys omiin järjestelmiin. Nämä aiheuttavat organisaatiolle haavoittuvaisten ja unohdettujen laitteiden hyökkäyspinnan.
- Yleinen ongelma teollisuuden kyberturvallisuuden hallinnassa on päättää, mihin hallintakeinoihin kannattaa keskittyä erityisesti tuotantoympäristöissä. Kyberturvallisuuskeskus on koostanut ohjeita teollisuusautomaation tärkeimmistä tietoturvakontrolleista.[14]
- Kyberturvallisuuskeskus raportoi Internetiin näkyvistä suojaamattomista automaatiolaitteista laitteiden omistajille. Työ perustuu viraston lakisääteisiin tehtäviin, joihin kuuluu muun muassa tiedon kerääminen verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvista tietoturvaloukkauksista ja niiden uhkista. Vastuu automaatiolaitteiden kyberturvallisuudesta on kuitenkin laitteiden omistajilla.
  - Kyberturvallisuuskeskuksella on parhaillaan menossa teollisuusautomaatioympäristöihin suunnattu uhkanmetsästyksen pilottihanke, johon parhaillaan etsitään uusia organisaatioita. Asiasta voi olla yhteydessä Kyberturvallisuuskeskukseen.

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.

Symbolit

Uusi

Päivitetty

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.**[15, 16]
  - 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.
  - **Esimerkiksi Hyöky eli kansallinen hyökkäyspintakartoitus kyberturvallisuuden parantamiseksi on Kyberturvallisuuskeskuksen ilmainen palvelu, jonka avulla organisaatio saa täsmätietoa omasta julkiseen verkkoon näkyvästä hyökkäyspinnastaan. Palvelu on suunnattu kunnille ja julkisen hallinnon organisaatiolle sekä syksystä 2024 lähtien tietyille huoltovarmuuskriittisille organisaatioille.**[17]
  - 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.
  - Suomessa Akira-kiristyshaittaohjelmasta on raportoitu eniten havaintoja Kyberturvallisuuskeskukselle. Noin vuoden aikana lähes 20 kotimaista organisaatiota on joutunut Akiran uhriksi.[18]
- Varsinkin huoltovarmuuskriittisten organisaatioiden joutuessa kiristyshaittaohjelman uhriksi yhteiskunnan elintärkeät toiminnot voivat vaarantua. Organisaatioiden kannattaa ottaa kiristyshaittaohjelmat huomioon varautumisessa ja harjoitustoiminnassa.
  - Esimerkiksi Britanniassa kiristyshaittaohjelma vaikutti alkukesästä usean Lontoon sairaalan sekä perusterveydenhuollon yksiköiden toimintaan. Kiristyshaittaohjelman aiheuttamat häiriöt saivat aikaan leikkausten ja verensiirtojen perumisia suurissa sairaaloissa, sekä päivystyspotilaiden ohjaamista muihin sairaaloihin. Hyökkäys vaikutti myös potilaiden testitulosten saatavuuteen.[19, 20, 21]
  - 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 kannattaa säilyttää poissa verkosta.
- 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, ovat 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 tai 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 mahdolliseen käyttöön liittyen, 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.[22]

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

- **NIS2-direktiiviä täydentävä täytäntöönpanosäädös julkaistu**[23]
  - NIS2-direktiivi julkaistiin joulukuussa 2022, määräaika direktiivin saattamiseksi osallista kansallista lainsäädäntöä oli 17.10.2024.
  - Komissio on 17.10.2024 hyväksynyt täytäntöönpanosäädöksen, jolla vahvistetaan tekniset ja menetelmiin liittyvät vaatimukset koskien digitaalista infraa, eli DNS-palveluntarjoajia, aluetunnusrekistereitä, pilvipalvelujen tarjoajia, datakeskuspalvelujen tarjoajia, sisällönjakeluverkkojen tarjoajia, hallintapalvelun tarjoajia, tietoturvapalveluntarjoajia, verkossa toimivien markkinapaikkojen tarjoajia, verkossa toimivien hakukoneiden tarjoajia, verkkoyhteisöalustojen tarjoajia ja luottamuspalvelun tarjoajia.
  - Tavoitteena on mm. tarkentaa kyberturvallisuusriskien hallintatoimenpiteiden sekä merkittävän poikkeaman määritelmää.
  - Kyberturvallisuuskeskus on koostanut verkkosivuilleen NIS2-direktiivistä laajasti tietoa ja ohjeita.[24]

Oikeudelliset asiat

- **EU:n tekoälyasetuksen toimeenpanon lainsäädäntö lausuntokierrokselle**
- Työ- ja elinkeinoministeriö pyytää lausuntoja luonnoksesta hallituksen esitykseksi EU:n tekoälyasetuksen kansallista toimeenpanoa koskevaksi lainsäädännöksi. Lausuntoja voi antaa 4.12.2024 asti.[25, 26]
  - Tekoälyasetus tuli voimaan 1.8.2024 ja sen soveltaminen alkaa vaiheittain. Asetus on suoraan sovellettava EU:n jäsenvaltioissa, mutta se vaatii myös täydentävää kansallista lainsäädäntöä.
  - Tekoälyasetuksen tavoitteena on varmistaa, että markkinoille tulevat tai käyttöön otettavat tekoälyjärjestelmät eivät vaaranna ihmisten turvallisuutta, terveyttä tai perusoikeuksia. Sääntely keskittyy erityisesti haitallisiin tekoälyn käyttötapauksiin.
  - Ehdotetussa laissa nimettäisiin riippumattomat kansalliset toimivaltaiset viranomaiset. Liikenne- ja viestintävirastolle ehdotettaisiin tekoälyjärjestelmien markkinavalvontaan liittyviä valvontatehtäviä. Liikenne- ja viestintävirasto toimisi myös keskitettynä yhteyspisteenä ja sen yhteyteen perustettaisiin seuraamusmaksulautakunta.
  - Laissa säädettäisiin myös viranomaisten toimivallasta määrätä seuraamuksia sekä seuraamusmaksulautakunnasta, jolla olisi toimivalta määrätä seuraamusmaksu vakavimmista asetuksen säännösten rikkomisesta.

Oikeudelliset asiat

- **Korkeimman hallinto-oikeuden ennakkopäätös (KHO:2024:115) 1.11.2024**[27]
  - Helsingin hallinto-oikeuden tuomio 18.12.2023 nro 7408/2023, josta ulkoministeriö on valittanut.
  - Tapauksessa oli kyse suomalaisiin diplomaatteihin kohdistetusta verkkovakoilusta vakoiluhaittaohjelmalla, joka mahdollisti laajasti puhelimessa olevan tiedon ja ominaisuuksien hyväksikäytön.
  - Asiassa oli ratkaistavana, oliko rekisterinpitäjä ulkoministeriö ilmoittanut verkkovakoilusta aiheutuneesta henkilötietojen tietoturvaloukkauksesta tietosuojavaltuutetulle ja rekisteröidyille yleisessä tietosuoja-asetuksessa säädettyjen aikarajojen mukaisesti.
  - Tietosuoja-asetuksessa tarkoitettuina rekisteröityinä pidettiin tapauksessa henkilöitä, joiden tietoja oli sisältynyt puhelimeen, johon vakoiluhaittaohjelma oli tuotu. Näille henkilöille tietoturvaloukkauksesta ei ilmoitettu henkilökohtaisesti, vaan ulkoministeriö oli tiedottanut tilanteesta kotisivullaan.
  - KHO katsoi, että tässä m turvallisuuteen ja ulkopolitiikkaan kytkeytyvässä asiassa sovelletaan tietosuojalain 2 §:n 1 momentin perusteella GDPR:ää. Unionin oikeudessa on kuitenkin nimenomaisesti säädetty kansalliseen turvallisuuteen ja yhteiseen ulko- ja turvallisuuspolitiikkaan liittyvistä toimista GDPR:n ulkopuolelle. Tapaukseen sovellettiin näin ollen kansallista lainsäädäntöä.
  - Huomioiden salassapitosäädöksillä suojatut Suomen kansainvälisiin suhteisiin ja valtion turvallisuuteen liittyvät intressit, ulkoministeriön voidaan katsoa ilmoittaneen tietoturvaloukkauksesta ilman aiheetonta viivytystä tietosuoja-asetuksen mukaisesti. KHO kuitenkin totesi, että ilmoitus tietoturvaloukkauksesta tietosuojaviranomaiselle oli viivästynyt.

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) Tietoturvan kehittämisen tukea 313 yhteiskunnan kannalta elintärkeälle yritykselle https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvan-kehittamisen-tukea-313-yhteiskunnan-kannalta-elintarkealle-yritykselle
2) IoT Assignment Completed! Report on Barriers to U.S. IoT Adoption https://www.nist.gov/blogs/cybersecurity-insights/iot-assignment-completed-report-barriers-us-iot-adoption
3) Amazon identified internet domains abused by APT29 https://aws.amazon.com/blogs/security/amazon-identified-internet-domains-abused-by-apt29/
4) Midnight Blizzard conducts large-scale spear-phishing campaign using RDP files https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/
5) Protecting Democratic Institutions from Cyber Threats https://blogs.microsoft.com/on-the-issues/2024/10/03/protecting-democratic-institutions-from-cyber-threats/
6) Justice Department Disrupts Russian Intelligence Spear-Phishing Efforts - https://www.justice.gov/opa/pr/justice-department-disrupts-russian-intelligence-spear-phishing-efforts
7) Chinese hackers access US telecom firms, worrying national security officials https://www.cnn.com/2024/10/05/politics/chinese-hackers-us-telecoms/index.html
8) U.S. Wiretap Systems Targeted in China-Linked Hack https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b?mod=hp_lead_pos1
9) Joint Statement by FBI and CISA on PRC Activity Targeting Telecommunications https://www.cisa.gov/news-events/news/joint-statement-fbi-and-cisa-prc-activity-targeting-telecommunications
10) Älä ota kesädomainia! – verkkotunnukset ovat arvokasta omaisuutta https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/ala-ota-kesadomainia-verkkotunnukset-ovat-arvokasta-omaisuutta

Lähdeluettelo

11) Kvanttiturvallisia algoritmeja lisätty kansalliseen kriteeristöön https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kvanttiturvallisia-algoritmeja-lisatty-kansalliseen-kriteeristoon

12) Suomen kyberturvallisuusstrategia 2024–2035 http://urn.fi/URN:ISBN:978-952-383-376-0

13) Toimialojen kyberkypsyyden selvitys 2022 https://www.huoltovarmuuskeskus.fi/julkaisu/toimialojen-kyberkypsyyden-selvitys-2022

14) Teollisuusautomaation tärkeimmät kyberturvallisuuskontrollit https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/teollisuusautomaation-tarkeimmat-kyberturvallisuuskontrollit

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

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

17) Hyöky https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/hyoky

18) Suomalaiset organisaatiot Akira-kiristyshaittaohjelmien kohteena https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suomalaiset-organisaatiot-akira-kiristyshaittaohjelmien-kohteena

19) Kyberhyökkäys Lontoon sairaaloihin – Leikkauksia perutaan, potilaita siirretään https://www.hs.fi/maailma/art-2000010476767.html

20) Critical incident over London hospitals' cyberattack https://www.bbc.com/news/articles/c288n8rkpvno

21) Services disrupted as London hospitals hit by cyberattack https://www.theguardian.com/society/article/2024/jun/04/cyber-attack-london-hospitals

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

23) NIS2: Commission implementing regulation on critical entities and networks https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks

Lähdeluettelo

24) NIS2 - Euroopan unionin kyberturvallisuusdirektiivi https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi

25) Lausuntopyyntö: luonnos hallituksen esitykseksi tekoälyasetuksen toimeenpanoa koskevaksi lainsäädännöksi https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=0e252297-c14b-4b6b-a0da-0a35756c9a90

26) Hallituksen esitys laiksi eräiden tekoälyjärjestelmien valvonnasta ja siihen liittyvien lakien muuttamisesta https://valtioneuvosto.fi/hanke?tunnus=TEM050:00/2024

27) KHO:2024:115 https://www.kho.fi/fi/index/paatokset/ennakkopaatokset/1730265221609.html