TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Heinäkuu 2023

#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

Kyberturvallisuuskeskus kartoitti erään haavoittuvuuden tilannetta Suomessa ottamalla yhteyttä yli 140 organisaatioon. Toistaiseksi yksikään organisaatio Suomessa ei ole ilmoittanut haavoittuvuuden hyväksikäytöstä.[1]

Jaoimme kahdeksan vinkkiä tietoturvalliseen kesään, koska kyberrikolliset eivät lomaile.[2]

Kybersää heinäkuu 2023

Tietomurrot ja -vuodot

- Heinäkuussa ilmoitusmäärät laskivat alkuvuoden tasolle.
- Lasku oli tasaista niin SOME-tilimurtojen kuin yrityssähköposteihin kohdistuneiden murtojen osalta.

Huijaukset ja kalastelut

- Huijausviestit kiertävät sähköpostisuodattimia piilottamalla kalastelusivulinkit QR-koodin taakse.
- Pankkitunnuksia kalasteltiin pitkin kesää pelottelemalla uhreja pankkien tai suomi.fi-viranomaispalvelun nimissä.

Haittaohjelmat ja haavoittuvuudet

- Heinäkuun aikana on julkaistu useita kriittisiä haavoittuvuuksia.
- Kyberturvallisuuskeskus on tehnyt heinäkuussa kriittisten ohjelmistohaavoittuvuuksien kartoitustyötä. Yksikään organisaatio Suomessa ei ole toistaiseksi ilmoittanut todetusta hyväksikäytöistä.

Automaatio ja IoT

- Yhdysvallat ottaa käyttöön uuden vapaaehtoisen älylaitteiden kyberturvallisuuden sertifiointi- ja merkintäohjelman "U.S. Cyber Trust Mark" vuonna 2024.[3]
- Laitteiden päivitystarvetta on seurattava myös lomien aikana hyödyntäen riskiperustaista haavoittuvuuksien hallintaa.

Verkkojen toimivuus

- Heinäkuussa yleisissä viestintäpalveluissa oli kuusi merkittävää toimivuushäiriötä.
- Presidentti Bidenin vierailu ei aiheuttanut toimivuushäiriöitä verkkosivuille.

Vakoilu

- Kiinaan yhdistetty Storm-0558-toimija tunkeutui länsimaissa valtionhallinnon organisaatioiden sähköpostitileille saatuaan käyttöönsä salausavaimen, jolla se pystyi luomaan väärennettyjä Microsoft-tilien kirjautumistietoja. Hyökkäyksessä hyödynnettiin lisäksi näiden tietojen vahvistamisessa ollutta puutetta.[4, 5]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Julkaisimme uuden ohjeen, jossa kerromme neuvoja puhelimen tietoturvalliseen käyttöön.[2]

Jaoimme vinkkimme tietoturvalliseen kesään.[2]

Ohjeistimme Tietoturva Nyt! –artikkelissamme, miten eSIM-huijaukselta voi välttyä, ja miten sen voi tunnistaa.[6]

Heinäkuun kyberturvallisuuden yleiskuva

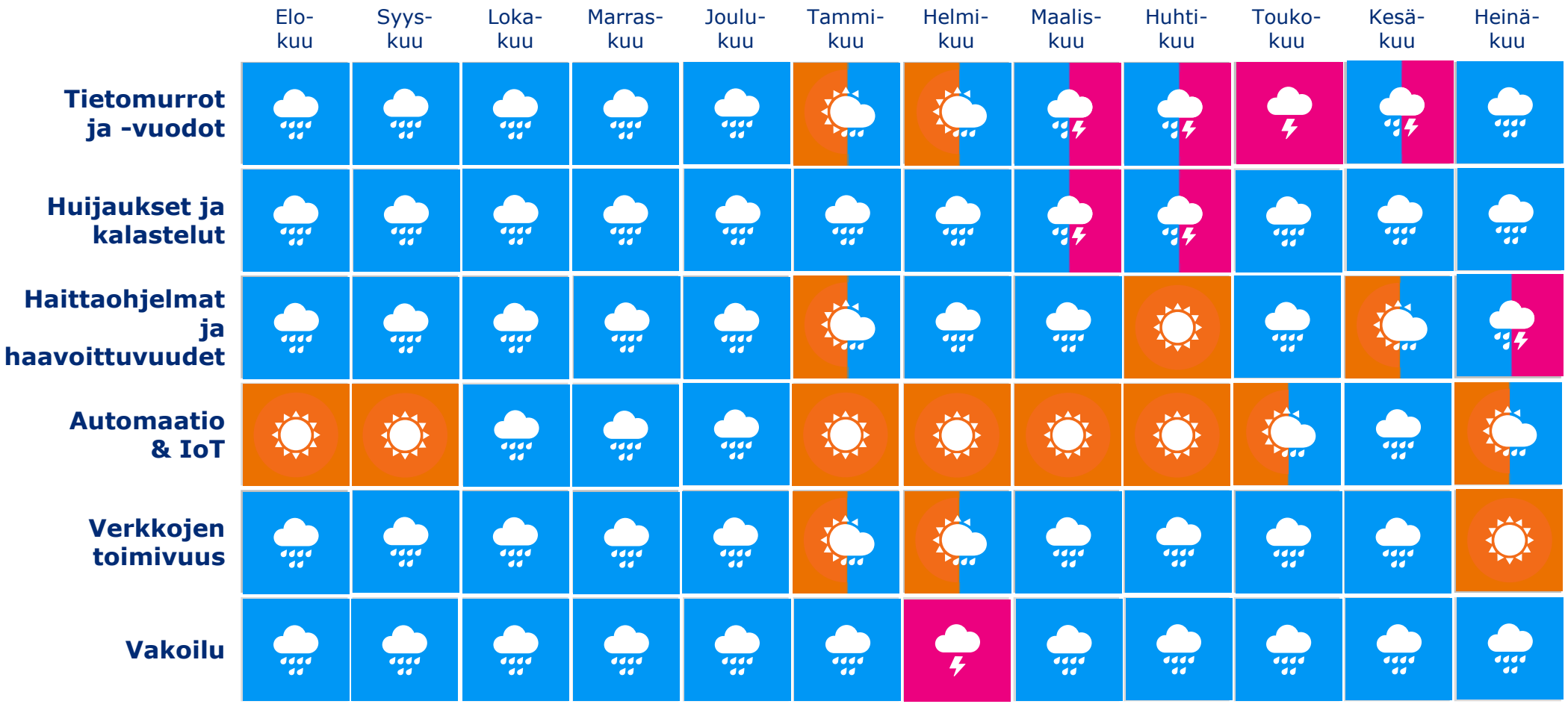
- Heinäkuun aikana julkaistiin useita päivityksiä kriittisiin ja Suomessakin laajasti käytössä oleviin tuotteisiin. Kyberturvallisuuskeskus kartoitti Suomessa tilannetta heti haavoittuvuuden tultua julki ja otti yhteyttä yli sataan organisaatioon haavoittuvuuksiin liittyen.
  - Toistaiseksi yksikään organisaatio Suomessa ei ole ilmoittanut näiden haavoittuvuuksien hyväksikäytöstä.
- Laitteiden ja järjestelmien päivityksistä onkin suositeltavaa pitää huolta myös loma-aikoina.

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

Tarve kyber-turvallisuuden osaajille

Pula puolijohteista

Tekoälyn käyttö kyberrikolli-suudessa

Suurvalta-kilpailun vaikutukset sääntelyyn

Älylaitteiden elinkaari ja kierrätys

Kyber-vakoilun ja rikollisuuden rajojen hämärtymi-nen

IoT

6G

Kiristyshaitta-ohjelmien käyttö murroksessa

Teknologia osana suurvalta-kilpailua

Sääntelyn ulottuminen uusille toimialoille

Osallistu-minen digitaalisessa ympäristössä

Pitkän aikavälin kybersää:
Osallistuminen digitaalisessa ympäristössä

- Valtioneuvoston kanslian ja Jyväskylän yliopiston Digiosallisuus Suomessa –hanke määrittelee digiosallistumisen osallistumiseksi yhteiskunnan toimintaan digitaalisten välineiden ja palvelujen kautta.[7]
  - Hanke nimeää digiosallisuuden osa-alueiksi infrastruktuurin ja teknologiset välineet; saavutettavuuden; turvallisuuden ja luotettavuuden; taidot, osaamisen ja digituen; käytettävyyden sekä käyttämisen ja hyödyt. Nämä osa-alueet voidaan nähdä digiosallisuutta edistävinä tai sitä estävinä tekijöinä.[8]
- Digitaalinen ympäristö tuo uusia mahdollisuuksia yhteiskunnan toimintaan osallistumiseen, esimerkiksi tarjoamalla alustoja yhteiskunnalliseen keskusteluun, sekä mahdollistamalla kansalaisaloitteiden ja adressien kaltaisten kannanottojen helpomman ja nopeamman toteuttamisen.
- Digitaalisen osallistumisen haasteena on esimerkiksi resurssien, kuten laitteiden, ja osaamisen, sekä palvelujen saavutettavuuden aiheuttama eriarvoisuus.
- Haasteena on, miten yhteiskunnassa voidaan taata tasavertaiset mahdollisuudet osallistua digitaalisessa ympäristössä.

Top 5 uhat lähitulevaisuudessa (6kk–2v)

1.

Suomeen kohdistunut kyberympäristön uhkataso on pysynyt kohonneena.

Kohdistettujen hyökkäysten määrä on noussut. Kohonneen uhkatason vuoksi organisaatioiden varautumisen merkitys korostuu.

2.

Politiikan ja talouden ilmiöt heijastuvat myös kyber-turvallisuuteen.

Ilmiöt voivat näkyä digitaalisessa toimintaympäristössä nopeasti ja aiheuttaa vaikeasti ennakoitavia tapahtumia kyberturvallisuudessa.

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.

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.

5.

Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille!

Uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisää entisestään tarvetta erilaisille osaajille. Myös riskienhallinnan ja jatkuvuuden näkökulmasta riittävän osaamisen varmistaminen kaikkina vuodenaikoina on organisaatioille tärkeää.

1. Suomeen kohdistunut kyberympäristön uhkataso on edelleen kohonneella tasolla

Kyberhyökkäykset lisääntyivät maailmanlaajuisesti vuoden 2022 aikana, ja Suomessa havaitut ilmiöt noudattelevat kansainvälisiä trendejä.

- Merkittävä uhka organisaatioille ovat kiristyshaittaohjelmat, joiden määrä kasvaa jatkuvasti. Viimeisen vuoden aikana usea organisaatio Suomessa on joutunut kiristyshaittaohjelman uhriksi.
- Varsinkin huoltovarmuuskriittisten organisaatioiden joutuessa kiristyshaittaohjelman uhriksi yhteiskunnan elintärkeät toiminnot voivat vaarantua.
- Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista.
- Erityisesti kohdistettujen kyberhyökkäysten määrä, joissa kohdeorganisaatio on tarkkaan valittu, on kasvanut.
- Tutustu Kyberturvallisuuskeskuksen huhtikuiseen tiedotteeseen kohonneesta kyberuhkatasosta, ja katso Kyberturvallisuuskeskuksen ja Suojelupoliisin keväällä järjestämän ajankohtaiskatsauksen tallenne.[9, 10]

2. Politiikan ja talouden ilmiöt heijastuvat myös kyberturvallisuuteen

Muutokset kansainvälisessä turvallisuustilanteessa on huomioitava organisaatioiden jatkuvuuden- ja riskienhallinnassa. Riskienhallinnan ja jatkuvuussuunnittelun tulee reagoida turvallisuusympäristön muutoksiin.

- Venäjän hyökkäys Ukrainaan heijastuu myös kyberturvallisuuteen. Esimerkiksi sodan aiheuttamat muutokset talouteen, energian hinnan voimakas heilahtelu ja informaatioympäristön herkkyys näkyvät vaikeasti ennakoitavina kehityskulkuina, jotka ulottuvat myös digitaaliseen maailmaan.
- Valtioiden ja organisaatioiden päätökset altistavat entistä helpommin vaikuttamiselle, kuten mielenilmauksena tehdyille palvelunestohyökkäyksille.
  - Palvelunestohyökkäysten määrä lisääntyi niin Suomessa kuin Euroopassakin vuonna 2022. Myös niiden käyttötapa poliittisena mielenilmauksena korostui.
- Kuluneena vuonna on nähty entistä enemmän haktivismia, jonka tavoitteena on ottaa kantaa yhteiskunnallisiin asioihin.
- Organisaatioiden on tärkeää tunnistaa oman toimintaympäristönsä riskitekijät. Niillä voi olla isoja vaikutuksia organisaatioiden päivittäiseen toimintaan. Organisaatioiden tulee huomioida omassa riskienhallinnassaan ja jatkuvuussuunnittelussaan toimintaympäristön muutokset ja sen aiheuttamat uhkat kriittisille prosesseille.

3. 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.[11]

- Tekoälyä voidaan hyödyntää esimerkiksi työn automatisointiin, kyberhyökkääjien työkalujen tehostamiseen, sekä täysin uusien hyökkäyskyvykkyyksien luomiseen.[12]
- Organisaatioiden olisikin hyvä tunnistaa tekoälyn tuomia haasteita, ja varautua niihin esimerkiksi kouluttamalla henkilöstöään. Olennaista on sisäistää, että tekoäly ja siihen liittyvät ilmiöt kehittyvät nopeasti, mihin on hyvä varautua myös organisaatioissa.
- Organisaatioiden on hyvä ottaa huomioon erityisesti tietosuoja- ja salassapitonäkökulmat tekoälyn mahdolliseen käyttöön liittyen, ja pohtia näihin liittyviä linjauksia organisaation sisällä.
- Euroopan komissio ehdotti vuonna 2021 tekoälysäädöstä, jossa tekoälyjärjestelmiä säädeltäisiin niiden aiheuttaman riskin perusteella. Tämä tarkoittaa, että tekoälyjärjestelmien sääntelyn määrä riippuisi niiden mukanaan tuomien riskien tasosta.[13]
  - Euroopan parlamentti hyväksyi neuvottelukantansa säädökseen kesäkuussa 2023, ja seuraavaksi vuorossa ovat neuvottelut parlamentin ja jäsenmaita edustavan Euroopan unionin neuvoston välillä. Tavoitteena on, että neuvottelut valmistuisivat vuoden 2023 loppuun mennessä. Toteutuessaan kyseessä olisi maailman ensimmäinen tekoälylaki.[13]

4. 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.

- Organisaatioiden on keskeistä ymmärtää omat alihankkijaketjunsa. On tärkeä selvittää kolmannen osapuolen tietoturvan taso ja ulottaa tietoturvallisuuden hallinta myös palveluihin. 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 alihankinnanketju, koska myös alihankkija voi hankkia tuotteen/palvelun seuraavalta ketjussa olevalta palveluntarjoajalta.
- On hyvä ymmärtää, että käytettävien palvelujen kautta voidaan murtautua organisaation, jos kyberturvallisuutta ei ole huomioitu.
- Kyberturvallisuuskeskuksessa on ollut alkuvuoden aikana käynnissä Huoltovarmuuskeskuksen rahoittama Ketjutonttu-projekti, jonka tarkoituksena on auttaa suomalaisia yrityksiä ja niiden toimittajia hallitsemaan toimitusketjuihin liittyviä kyberriskejä.

5. Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille!

Uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisää entisestään tarvetta erilaisille osaajille. Myös riskienhallinnan ja jatkuvuuden näkökulmasta riittävän osaamisen varmistaminen kaikkina vuodenaikoina on organisaatioille tärkeää.

- Osaamisen saaminen riittävälle tasolle kestää vielä pitkään. Organisaatioiden kyberturvallisuus vaarantuu, mikäli osaavaa henkilöstöä ei ole tarpeeksi saatavilla, niin lyhyellä kuin pitkälläkin aikavälillä. Myös loma-aikoina tulee turvata organisaatioiden riittävä kyvykkyys tietoturvalliseen toimintaan.
  - Uhkatoimijat hyödyntävät yhä enemmän päivittämättömistä järjestelmistä löytyviä haavoittuvuuksia.[14] Tämän vuoksi esimerkiksi kriittiset päivitykset sekä muut korjaavat toimenpiteet olisi hyvä pystyä toteuttamaan nopeasti, jolloin osaavan henkilöstön oleminen saatavilla korostuu.
- Osaajapula ei ole kiinni määrästä vaan laadusta! Osaaminen ei saisi henkilöityä liikaa, jotta jatkuvuus voidaan turvata kaikissa tilanteissa. Organisaation tietoturvan hallinta tulee osallistaa ja kouluttaa osaksi kaikkien työntekijöiden päivittäistä toimintaa.
- Johdon tulee ymmärtää ja varmistaa riittävä osaaminen organisaatiossa kyberturvallisuusosaajien kysynnän kasvaessa.
- Viime vuoden lopussa opetus- ja kulttuuriministeriö myönsi noin 3,4 miljoonaa euroa kyberturvallisuuskoulutuksen kehittämiseen. Rahoitus suunnattiin Jyväskylän yliopistolle ja Jyväskylän ammattikorkeakoululle, ja niiden koordinoimalle yhteistyöhankkeelle.[15]

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

- Liikenne- ja viestintävirasto Traficom pyytää lausuntoa luonnoksesta määräykseksi 28 K/2023 koskien viestintäverkkojen ja -palveluiden yhteentoimivuutta.[16]
  - Määräyksen tavoitteena on, että tilaajat voivat luottaa päätelaitteeseensa saapuvien viestien oikeellisuuteen, ja ettei tilaajaa yritetä erehdyttää luulemaan, että väärennetty viesti olisi tullut luotetulta lähettäjältä.
  - Koska A-numeron väärentäminen suomalaiseksi puhelinnumeroksi ja SMS Sender ID -tunnuksien väärinkäyttö ovat keskeisessä osassa huijauksien toteuttamisessa, määräykseen lisättävän kiellon ja siihen liittyvien estotoimenpiteiden tarkoituksena on vaikeuttaa huijauksia ja vähentää rikollisille menetettävän rahan määrää.
  - Vastausaika päättyy: 31.8.2023

- Sähköisen tunnistuspalvelun arviointiohje 211/2023 on julkaistu.[17]
  - Sähköisen tunnistuspalvelun arviointiohje sekä auditointi- ja raportointimalli on julkaistu 13.7.2023.
  - Ohje on tarkoitettu vahvan sähköisen tunnistuspalvelun tarjoajille ja arviointielimille, joilta tunnistuspalvelut hankkivat arviointeja. Ohjeen tavoitteena on selkeyttää sähköisen tunnistuspalvelun vaatimustenmukaisuuden arviointia ja arvioinnista lopputuloksena laadittavaa tarkastuskertomusta.

Oikeudelliset asiat

- Tiedonsiirto Yhdysvaltoihin helpottuu – Euroopan komissio hyväksyi päätöksen Yhdysvaltojen tietosuojan riittävästä tasosta.[18, 19]
  - Euroopan komission päätös Yhdysvaltojen tietosuojan tason riittävyydestä astui voimaan 10. heinäkuuta.
  - Komissio katsoo, että Yhdysvallat varmistaa riittävän suojan henkilötiedoille, jotka siirretään EU:sta yhdysvaltalaisille yrityksille riittävyyspäätöksen nojalla.
  - Riittävyyspäätöksen nojalla henkilötietoja voidaan siirtää sertifioiduille yhdysvaltalaisille yrityksille, jotka ovat sitoutuneet tietosuojakehyksessä sovittuihin suojatoimiin.
  - Tietosuojakehys takaa EU-alueen rekisteröidyille oikeuksia, kuten mahdollisuuden käyttää tarkastusoikeutta siirrettyihin henkilötietoihinsa sekä poistaa tai oikaista väärät tai lainvastaisesti käsitellyt tietonsa. Lisäksi tietosuojakehys tarjoaa EU-kansalaisille uusia oikeussuojamekanismeja.
  - EU:n ja Yhdysvaltojen välisellä tietosuojakehyksellä korvataan EU-tuomioistuimen kesällä 2020 Schrems II -tuomiossa mitätöimä Privacy Shield -järjestely.

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 - 30/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-302023
2) Kyberturvallisuuskeskuksen viikkokatsaus - 29/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-292023
3) The White House: Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/
4) Enhanced Monitoring to Detect APT Activity Targeting Outlook Online https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-193a
5) Mitigation for China-based threat actor activity https://blogs.microsoft.com/on-the-issues/2023/07/11/mitigation-china-based-threat-actor/
6) Elektroninen SIM tarjoaa uuden hyökkäysvektorin rikollisille https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/elektroninen-sim-tarjoaa-uuden-hyokkaysvektorin-rikollisille

Lähdeluettelo

7) Digiosallisuus Suomessa: Digiosallisuus Suomessa -hankkeen loppuraportti https://julkaisut.valtioneuvosto.fi/handle/10024/163789
8) Digiosallisuuden käsite ja keskeiset osa-alueet : Digiosallisuus Suomessa -hankkeen väliraportti https://julkaisut.valtioneuvosto.fi/handle/10024/163036
9) Kyberturvallisuuden uhkataso pysynyt kohonneena - kohdistettujen hyökkäysten määrä noussut https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuden-uhkataso-pysynyt-kohonneenakohdistettujen-hyokkaysten-maara
10) Kyberturvallisuuden ajankohtaiskatsaus 21.04.2023 klo 12, tallenne https://youtu.be/UEFvTVLH5Rc
11) NCSC-UK: ChatGPT and large language models: what's the risk? https://www.ncsc.gov.uk/blog-post/chatgptand-large-language-models-whats-the-risk
12) Tekoälyn mahdollistamat kyberhyökkäykset https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/tekoalynmahdollistamat-kyberhyokkaykset
13) EU:n tekoälysäädös on ensimmäinen laatuaan https://www.europarl.europa.eu/news/fi/headlines/society/20230601STO93804/eu-n-tekoalysaados-on-ensimmainen-laatuaan

Lähdeluettelo

14) FBI, CISA, and NSA reveal top exploited vulnerabilities of 2022 https://www.bleepingcomputer.com/news/security/fbi-cisa-and-nsa-reveal-top-exploited-vulnerabilities-of-2022/
15) OKM: Kyberturvallisuusalan koulutusta kehitetään korkeakoulujen yhteistyönä – myös informaatiopsykologista tutkimusta vahvistetaan https://okm.fi/-/kyberturvallisuusalan-koulutusta-kehitetaan-korkeakoulujenyhteistyona-myos-informaatiopsykologista-tutkimusta-vahvistetaan
16) Määräys 28 K/2023 viestintäverkkojen ja -palveluiden yhteentoimivuudesta https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=fdea1eac-e2e5-4ef2-8c1f-17d993e20e2c
17) Sähköisen tunnistuspalvelun arviointiohje 211/2023 O https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/O211_Sahkoisen_tunnistuspalvelun_arviointiohje_2023.pdf
18) Tiedonsiirto Yhdysvaltoihin helpottuu – Euroopan komissio hyväksyi päätöksen Yhdysvaltojen tietosuojan riittävästä tasosta https://tietosuoja.fi/-/tiedonsiirto-yhdysvaltoihin-helpottuu-euroopan-komissio-hyvaksyi-paatoksen-yhdysvaltojen-tietosuojan-riittavasta-tasosta
19) Adequacy decision for the EU-US Data Privacy Framework https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en