TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Lokakuu 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

Haavoittuvuus Cisco IOS XE -ohjelmiston web-käyttöliittymässä oli maailmanlaajuisen tietomurtokampanjan kohteena. Lokakuussa Ciscon verkkolaitteisiin kohdistunut hyökkäysaalto johti lopulta kymmenien tuhansien laitteiden tietomurtoon, joista kymmeniä oli Suomessa.

Lokakuussa järjestimme kaksi seminaaria: Tietoturva 2023 – seminaarin sekä Ketjutonttu-kampanjan tuloskatsauswebinaarin.

Kybersää lokakuu 2023

Tietomurrot ja -vuodot

- Julkaisimme lokakuussa keltaisen varoituksen liittyen erittäin aktiiviseen ja laajalle levinneeseen M365-kalasteluun ja tietomurtoihin liittyen.[1]
- Lokakuussa saimme muutamia ilmoituksia, joissa Teams-kokouskutsun mukana oli lähetetty haittaohjelmaa ZIP-tiedostona.

Huijaukset ja kalastelut

- Pankkitunnuksia yritettiin huijata veronpalautusteemalla.
- Turvapostiksi väärennetty tunnuskalastelu yltyi niin suureksi, että siitä julkaistiin keltainen varoitus.
- Lokakuun lopuksi laajalla tekstiviestikampanjalla yritettiin huijata marraskuun vuokrarahoja.[2]

Haittaohjelmat ja haavoittuvuudet

- Lokakuussa julkaistiin lukuisia kriittisiä haavoittuvuuksia, joista monia oli myös käytetty jo hyväksi.
- Modeemi tai reititin on portti kotiverkkoomme ja sen turvaaminen on tärkeää, kun rikolliset etsivät käsin tai automatisoidusti verkosta haavoittuvuuksia.

Automaatio ja IoT

- Tietoturva tai päivitysten saatavuus eivät näytä olevan olennaisessa roolissa Black Friday -tarjouksissa.
- Yhdysvaltain viranomaiset julkaisivat ohjeet avoimen lähdekoodin käytöstä OT-ympäristöissä.[3]
- APT-ryhmä on kehittänyt kykyjään kriittisen infrastruktuurin automaatiojärjestelmiin vaikuttamiseksi.[4]

Verkkojen toimivuus

- Lokakuussa yleisissä viestintäpalveluissa oli 16 merkittävää toimivuushäiriötä.
- Haktivistiryhmä NoName057(16) on kohdistanut palvelunestohyökkäyksiä kymmeniin organisaatioihin Suomessa syksyn aikana.
- Sovellustason palvelunestohyökkäykset ovat aiheuttaneet vaikutuksia osaan organisaatioista.

Vakoilu

- Kybervakoilussa hyödynnetään aktiivisesti erilaisia haavoittuvuuksia.
- Lokakuussa raportoitiin esimerkiksi WinRAR-pakkaustyökalun, Atlassian Confluencen, Roundcube-sähköpostipalvelimien ja Jetbrains TeamCityn haavoittuvuuksien hyödyntämisestä vakoilutarkoituksessa.[5, 6, 7]

Varoitus 1/2023 ”Tietomurtoaalto leviää organisaatiosta toiseen” oli aktiivinen lokakuussa

- Julkaisimme 20.10.2023 vakavan varoituksen Microsoft 365 -tilien tietomurtoaallosta, jossa Microsoft 365 -ympäristön salasanoja kalasteltiin väärennetyillä sähköpostiviesteillä.[1]
- Tietojenkalastelussa käytetty turvapostiteema lisäsi väärennettyjen viestien uskottavuutta, ja uhreja oli poikkeuksellisen paljon.
- Varoitus poistettiin 8.11.2023, koska kampanja on hiipunut, ja ilmoitusmäärät M365-tilimurroista kääntyivät merkittävästi laskuun.[8]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Tietoturva 2023 -seminaari pidettiin torstaina 12.10.2023. Seminaarin tallenne ja esitysmateriaalit ovat verkkosivuillamme.[9]

Traficomin ja Huoltovarmuuskeskuksen tuore selvitys kartoitti ohjelmistokehityksen nykytilaa ja kehittämistarpeita.[10]

Julkaisimme uuden ohjeen kotiverkon ja reitittimien suojaamiseen.[11]

Ketjutonttu-kampanjan 5.10.2023 pidetyn tuloskatsauswebinaarin tallenne sekä loppuraportti ovat verkkosivuillamme.[12]

Julkaisimme uuden ohjeen erillistyöasemien tietoturvallisuuden varmistamisesta.[13]

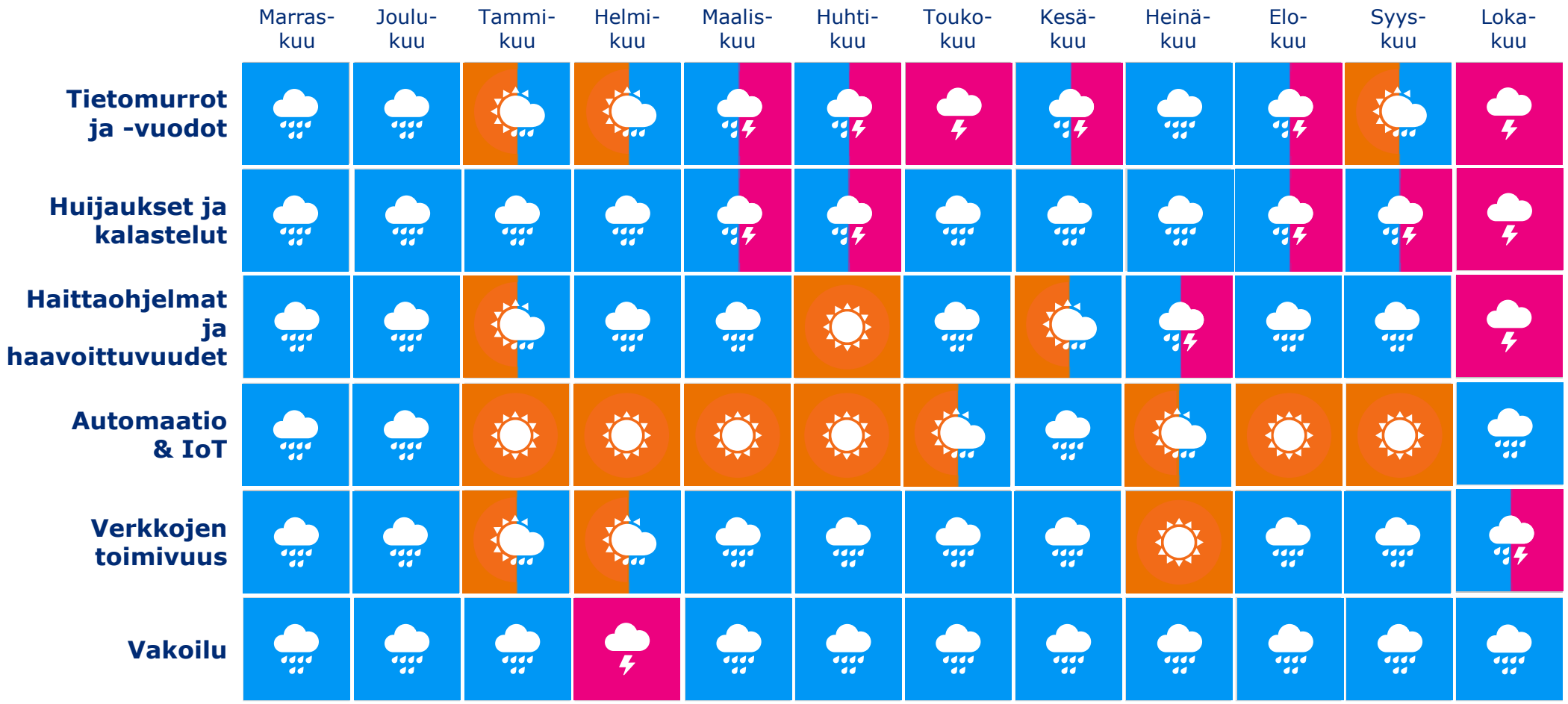
Lokakuun kyberturvallisuuden yleiskuva

- Lokakuussa julkaistiin useita kriittisiä haavoittuvuuksia.
  - Järjestelmät ja laitteet on hyvä päivittää aina mahdollisimman pikaisesti!
- Julkaisimme 20.10.2023 vakavan varoituksen Microsoft 365 -tilien tietomurtoaallosta, jossa Microsoft 365 -ympäristön salasanoja on kalasteltu väärennetyillä sähköpostiviesteillä. Tietojenkalastelussa hyödynnettiin turvapostiteemaa, joka lisäsi väärennettyjen viestien uskottavuutta. Kampanjan uhreja oli poikkeuksellisen paljon.
  - Varoitus poistettiin epäaktiivisena 8.11.2023.
- Lokakuun alussa voimaan astunut Traficomin määräys velvoittaa teleoperaattorit torjumaan ulkomailta tulevia suomalaisiksi naamioituja puheluita myös mobiilinumeroiden osalta. Ilmoitusten määrä väärennetyistä numeroista tulleiden valepuheluista onkin laskenut lokakuussa.

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



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:
Suurvaltakilpailun vaikutukset sääntelyyn

Teknologinen kehitys on johtanut siihen, että sääntelystä ja kansainvälisistä standardeista on tullut yhä tärkeämpiä tekijöitä myös suurvaltapolitiikassa. Valtion kyvykkyys vaikuttaa sääntelyyn voidaankin nähdä myös kilpailuvalttina esimerkiksi sen tuoman etulyöntiaseman myötä.[14]

- Sääntely ja standardointi voivat nykyään toimia myös osana ulko- ja turvallisuuspoliittista keinovalikoimaa.[14]
- Viimeisen vuosikymmenen aikana erityisesti Kiina on noussut länsimaiden rinnalle kansainväliseen standardointiin liittyvässä aktiivisuudessa, mikä on puolestaan johtanut Yhdysvaltojen yhä vahvempaan panostukseen.[14]
  - Yhdysvalloissa standardointia pidetään demokratian edistämisen välineenä, kun taas Kiinassa standardointiin panostaminen nähdään strategisena keinona oman innovatiivisen johtajan aseman saavuttamisessa.[14]
- Euroopan unionin ja Yhdysvaltojen yhteistyötä standardoinnin kentällä on vaikeuttanut toisistaan eroavat standardisoimisjärjestelmät. Euroopan unioni on kuitenkin halukas lisäämään yhteistyötä Yhdysvaltojen kanssa erityisesti kyberturvallisuuteen, tekoälyyn sekä 5G- ja 6G-teknologioihin liittyvässä sääntelyssä.[14]

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.

Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

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

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.

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.
- Kyberturvallisuuskeskus ja Suojelupoliisi järjestivät keväällä kyberturvallisuuden ajankohtaiskatsauksen.[15]
- 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.

2. Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

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

- 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.[16]
  - Järjestelmien nopea päivittäminen onkin erityisen tärkeää, ja valmius päivittämiseen pitäisi olla jatkuvasti, myös yleisinä loma-aikoina.
- Valitettavasti pelkkä järjestelmien päivittäminen ei riitä niiden turvaamiseksi, vaan järjestelmissä tulisi aina tehdä tutkintaa haavoittuvuuden tultua julki. Näin voidaan varmistua, ettei haavoittuvuutta ole jo ehditty hyväksikäyttää, eikä järjestelmään ole luotu takaovia, eli piilotettuja sisäänpääsyreittejä.[16]
- Haavoittuvuuksien hallintaa on haastavaa tehdä, mikäli organisaatio ei tunne ympäristöään. Järjestelmien kartoitus ja dokumentointi on syytä tehdä viimeistään nyt.
- Haavoittuvia palveluita on ollut myös näkyvissä julkisesti verkkoon. Organisaatioiden olisikin hyvä myös tarkastella omia palveluitaan ja varmistaa, että mahdollisuuksien mukaan palveluita ei olisi näkyvissä julkisesti verkkoon.[17]

2. Case: Tietomurtojen aalto haavoittuvissa Ciscon verkkolaitteissa

Lokakuun loppupuolella kerroimme viikkokatsauksessamme kriittisestä haavoittuvuudesta Cisco IOS XE –ohjelmistossa. Haavoittuvuus on mahdollistanut kansainvälisen tietomurtojen aallon. Haavoittuvuutta on mahdollista hyödyntää, jos haavoittuvan laitteen käyttöliittymä (Web GUI) on avoin julkiseen Internetiin. Ciscon Talos-tiimin mukaan murretuilla laitteilla tunnistettiin takaovena toimiva haittaohjelma sekä ylimääräisiä käyttäjiä. Tapaukseen ei ole liitetty tunnettua kyberuhkatoimijaa, mutta Taloksen mukaan laitteissa havaittujen haittaohjelmien taustalla on sama toimija.

Kansainvälisesti on tunnistettu kymmeniä tuhansia haavoittuvuudelle alttiita laitteita, joista moniin oli asennettu takaovena toimiva haittaohjelma. Ciscon haavoittuvuutta korjaavia päivityksiä alettiin julkaista 22.10. alkaen. Haavoittuvuuden hyödyntämistä voi rajoittaa sallimalla Cisco IOS XE web-käyttöliittymäkomponenttiin pääsyn vain luotetuista verkoista tai poistamalla sen näkyvyyden julkiseen Internetiin.[17]

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.

- 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 oli alkuvuoden aikana käynnissä Huoltovarmuuskeskuksen rahoittama Ketjutonttu-projekti, jonka tarkoituksena oli auttaa suomalaisia yrityksiä ja niiden toimittajia hallitsemaan toimitusketjuihin liittyviä kyberriskejä. Ketjutonttu-kampanjan tuloskatsauswebinaarin tallenne sekä loppuraportti löytyvät verkkosivuiltamme.[12]

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.[18]

- Tekoälyä voidaan hyödyntää esimerkiksi työn automatisointiin, kyberhyökkääjien työkalujen tehostamiseen, sekä täysin uusien hyökkäyskyvykkyyksien luomiseen.[19]
- 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.[20]
  - 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.[20]

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.[21] Tämän vuoksi esimerkiksi kriittiset päivitykset sekä muut korjaavat toimenpiteet olisi hyvä pystyä toteuttamaan nopeasti, jolloin osaavan henkilöstön oleminen saatavilla korostuu.
- Myös uusi ja nopeasti muuttuva sääntely asettaa omat haasteensa organisaatioille, joiden tulisi pystyä nopeasti mukauttamaan toimintaansa sääntelyn tuomiin uusiin vaatimuksiin. Organisaatioissa tarvitaankin myös osaamista ja ymmärrystä sääntelystä, sekä valmiutta ymmärtää, minkälaisia vaatimuksia uusi sääntely tuo kyseiselle organisaatiolle. Näin organisaation toimintaa voidaan mukauttaa sääntelyn tuomien vaatimusten mukaan.

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 Traficomin määräys lopettaa suomalaisiksi naamioidut valepuhelut lähes kokonaan.[22]
  - Lokakuun alussa voimaan tulleella Traficomin määräyksellä 28 teleoperaattorit velvoitetaan torjumaan yhä paremmin ulkomailta tulevia, mutta suomalaisiksi naamioituja puheluita, myös mobiilinumeroiden osalta. Soittojen suodatus on nyt käytössä kaikilla suomalaisilla, ulkomailta liikennettä vastaanottavilla teleoperaattoreilla.
  - Lisäksi Traficom ja teleoperaattorit ovat yhdessä valmistelleet määräystä tekstiviestihuijausten torjumiseksi. Määräyksen myötä organisaatiot voivat suojata oman lähettäjätunnuksensa. Näin viestin vastaanottaja voi varmistua viestin olevan aito. Organisaatiot voivat hakea lähettäjätunnuksensa suojausta 9.11.2023 alkaen.[23]
  - Huijaussoittoja ja -tekstiviestejä koskevaa ongelmaa on taklattu viranomaisten ja teleoperaattorien tiiviillä yhteistyöllä.

Oikeudelliset asiat

- EU:n digipalvelusäädöksen toimeenpano etenee – hallitus esittää lakia verkon välityspalvelujen valvonnasta.[24]
  - Valtioneuvosto antoi eduskunnalle 12.10.2023 hallituksen esityksen, jolla toimeenpannaan kansallisesti EU:n digipalvelusäädös. Digipalvelusäädöksen tarkoituksena on parantaa internetissä toimivien välityspalvelujen avoimuutta ja turvallisuutta käyttäjille. Säädös koskee muun muassa internetyhteyden tarjoajia, pilvipalveluita ja verkkoalustoja, kuten sosiaalisen median palveluita, verkon markkinapaikkoja sekä internetin hakukoneita.
  - Digipalvelusäädöksen myötä verkkoalustoilta vaaditaan aiempaa enemmän läpinäkyvyyttä esimerkiksi sisällön suosittelussa ja moderoinnissa. Verkkoalustojen käyttäjillä on jatkossa oikeus saada tietoa näkemistään mainoksista.
  - Liikenne- ja viestintävirasto Traficomia ehdotetaan digitaalisten palvelujen koordinaattoriviranomaiseksi ja digipalvelusäädöksen pääasialliseksi valvontaviranomaiseksi. Muut säädöstä valvovat viranomaiset olisivat kuluttaja-asiamies ja tietosuojavaltuutettu. Erittäin suuria verkkoalustoja valvoo kuitenkin EU:n komissio.
  - Kansallisille valvoville viranomaisille säädettäisiin myös toimivaltuudet, kuten oikeus tehdä tarkastuksia ja saada valvontaan tarvittavia tietoja. Digipalvelusäädöksen rikkomisesta voitaisiin määrätä lisäksi seuraamusmaksuja. Valvonnassa pääpaino olisi kuitenkin ohjauksessa ja neuvonnassa. Esityksessä ehdotetaan uutta menettelyä myös suurten, yli 100 000 euron seuraamusmaksujen määräämiseen Traficomissa. Jatkossa päätöksen tekisi yksittäisen virkahenkilön sijaan Traficomiin perustettava toimielin eli seuraamuskollegio.
  - Ehdotetun lain ja siihen liittyvien eräiden muiden lakien on tarkoitus tulla voimaan 17.2.2024.

Oikeudelliset asiat

- EU:n datanhallinta-asetuksen täytäntöönpanon johdosta muutoksia sähköisen viestinnän palveluista annettuun lakiin.[25, 26]
  - Hallitus esittää muutoksia sähköisen viestinnän palveluista annettuun lakiin ja antoi tätä koskevan esityksen eduskunnalle 9.10.2023. Lain muutokset ovat osa datanhallinta-asetuksen kansallista täytäntöönpanoa. Asetuksella luodaan datan hallinnalle eurooppalaiseen arvopohjaan pohjautuva kehys, joka lisää datan saatavuutta ja yhtenäistää sen jakamista EU:n alueella.
  - Keskeistä asetuksessa on luoda pelisäännöt datatalouden uusille toimijoille: datan välityspalveluille ja tunnustetuille data-altruismipohjaisille organisaatioille. Data-altruismilla tarkoitetaan datan vastikkeetonta lahjoittamista yleishyödylliseen käyttöön, minkä käytännön toteuttamisessa tunnustetut data-altruismiorganisaatiot auttaisivat. Tavoitteena on kehittää edelleen digitaalisia sisämarkkinoita sekä ihmiskeskeistä, luotettavaa ja turvallista datataloutta.
  - Hallituksen esityksessä ehdotetaan, että datan välityspalveluihin ja tunnustettuihin data-altruismipohjaisiin organisaatioihin liittyvät viranomaistehtävät annetaan Suomessa Liikenne- ja viestintävirasto Traficomille. Jatkossa Liikenne- ja viestintävirasto rekisteröi ja valvoo datan välityspalveluita ja tunnustettuja data-altruismipohjaisia organisaatioita. Liikenne- ja viestintävirastolle säädettäviin uusiin viranomaistehtäviin sisältyy myös mahdollisuus määrätä seuraamusmaksu datan välityspalveluille. Lisäksi virasto osallistuu Euroopan datainnovaatiolautakunnan työhön.
  - EU:n datanhallinta-asetuksen soveltaminen jäsenmaissa alkoi 24.9.2023. Suomessa asetuksen täytäntöön panevan lainsäädännön on tarkoitus tulla voimaan vuoden 2024 alusta.

Oikeudelliset asiat

- Valtionhallinnon pilvipalvelulinjaukset on päivitetty.[27]
  - Pilvipalvelulinjauksien tavoitteena on tukea valtionhallinnon sekä soveltuvin osin hyvinvointialueiden ja kuntien päätöksentekoa pilvipalvelujen käytössä. Pilvipalveluja hyödyntämällä voidaan edistää julkisen hallinnon digitalisaatiota ja julkisen hallinnon tuottavuutta.
  - Linjauksien tarkoituksena on antaa ohjeita pilvipalvelujen turvallisesta käytöstä ja tukea riskienhallinnan päätöksentekoa sekä tarjota suuntaviivoja pilvipalvelujen toteuttamiseen. Linjauksien tarkoituksena on lisäksi selkeyttää henkilötiedon ja salassa pidettävän tiedon käsittelyyn liittyviä periaatteita.
  - Päivitetyt linjaukset koskevat muun muassa kilpailutuksia ja hankintoja valtionhallinnon yhteisillä hankintasopimuksilla, pilvipalvelujen hankintaa, käyttöönottoa ja hyödyntämistä sekä tiedon käsittelyä julkisessa pilvipalvelussa.

Oikeudelliset asiat

- EU:n lentoturvallisuusvirasto EASA (The European Union Aviation Safety Agency) on koonnut yhteen lentoturvallisuutta koskevat kyberturvallisuuden vaatimukset.[28]
  - EASA julkaisi lokakuussa ”Easy Access Rules for Information Security” –dokumentin, johon on koottu helppolukuiseen muotoon lentoturvallisuutta koskevat kyberturvallisuuden EU-lainsäädännön vaatimukset sekä ohjeet niiden täyttämiseksi.
  - Dokumentti on vapaasti luettavissa ja ladattavissa EASA:n internetsivuilta.

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)

Yhteiskunnan kannalta kriittisten organisaatioiden ilmoituslomake: https://eservices.traficom.fi/dataservices/forms/NISlomake.aspx

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) Varoitus 1/2023 https://www.kyberturvallisuuskeskus.fi/fi/tietomurtoaalto-leviaa-organisaatiosta-toiseen-katkaise-tietojenkalastelu
2) Kyberturvallisuuskeskuksen viikkokatsaus - 44/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-442023
3) CISA, FBI, NSA, and Treasury Release Guidance on OSS in IT/ICS Environments https://www.cisa.gov/news-events/alerts/2023/10/10/cisa-fbi-nsa-and-treasury-release-guidance-oss-itics-environments
4) Mandiant Intelligence Chief Raises Alarm Over China's 'Volt Typhoon' Hackers in US Critical Infrastructure https://www.securityweek.com/mandiant-intelligence-chief-raises-alarm-over-chinas-volt-typhoon-hackers-in-us-critical-infrastructure/
5) Multiple North Korean threat actors exploiting the TeamCity CVE-2023-42793 vulnerability https://www.microsoft.com/en-us/security/blog/2023/10/18/multiple-north-korean-threat-actors-exploiting-the-teamcity-cve-2023-42793-vulnerability/
6) Government-backed actors exploiting WinRAR vulnerability https://blog.google/threat-analysis-group/government-backed-actors-exploiting-winrar-vulnerability/
7) Winter Vivern exploits zero-day vulnerability in Roundcube Webmail servers https://www.welivesecurity.com/en/eset-research/winter-vivern-exploits-zero-day-vulnerability-roundcube-webmail-servers/

Lähdeluettelo

8) Microsoft 365 -tietomurtoaallosta kertova varoitus on poistettu https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/microsoft-365-tietomurtoaallosta-kertova-varoitus-poistettu
9) Tietoturva 2023 -seminaari https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturva-2023-seminaari
10) Miten ohjelmistokehityksen turvallisuutta voidaan kehittää? Tuore selvitys kartoitti ohjelmistokehityksen nykytilaa ja kehittämistarpeita https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/miten-ohjelmistokehityksen-turvallisuutta-voidaan-kehittaa-tuore-selvitys-kartoitti
11) Kyberturvallisuuskeskuksen viikkokatsaus - 42/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-422023
12) Tonttu-projektit - uusien menetelmien toteutettavuustestaus https://www.kyberturvallisuuskeskus.fi/fi/tonttu
13) Ohje erillistyöasemien tietoturvallisuuden varmistamisesta https://www.kyberturvallisuuskeskus.fi/fi/saadokset/ohje-erillistyoasemien-tietoturvallisuuden-varmistamisesta
14) Kiina ja Yhdysvallat – haaste yrityksille : Suurvaltakilpailun vaikutukset suomalaisyrityksille https://julkaisut.valtioneuvosto.fi/handle/10024/163272
15) Kyberturvallisuuden ajankohtaiskatsaus 21.04.2023 klo 12, tallenne https://youtu.be/UEFvTVLH5Rc

Lähdeluettelo

16) Kyberturvallisuuskeskuksen viikkokatsaus - 33/2023
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-332023
17) Kyberturvallisuuskeskuksen viikkokatsaus - 43/2023
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-432023
18) NCSC-UK: ChatGPT and large language models: what's the risk? https://www.ncsc.gov.uk/blog-post/chatgptand-large-language-models-whats-the-ris k
19) Tekoälyn mahdollistamat kyberhyökkäykset
https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/tekoalynmahdollistamat-kyberhyokkaykset
20) EU:n tekoälysäädös on ensimmäinen laatuaan
https://www.europarl.europa.eu/news/fi/headlines/society/20230601STO93804/eu-n-tekoalysaados-on-ensimmainen-laatuaan
21) 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/
22) Traficomin määräys lopettaa suomalaisiksi naamioidut valepuhelut lähes kokonaan
https://traficom.fi/fi/ajankohtaista/traficomin-maarays-lopettaa-suomalaisiksi-naamioidut-valepuhelut-lahes-kokonaan

Lähdeluettelo

23) Traficomin määräys kampittaa rikollisten mahdollisuuksia tekstiviestihuijauksiin – organisaatiot voivat hakea lähettäjätunnuksensa suojausta 9.11.2023 alkaen https://www.traficom.fi/fi/ajankohtaista/traficomin-maarays-kampittaa-rikollisten-mahdollisuuksia-tekstiviestihuijauksiin
24) Digipalvelusäädöksen toimeenpano etenee – hallitus esittää lakia verkon välityspalvelujen valvonnasta https://lvm.fi/-/digipalvelusaadoksen-toimeenpano-etenee-hallitus-esittaa-lakia-verkon-valityspalvelujen-valvonnasta
25) Datanhallinta-asetuksen täytäntöönpano – muutoksia sähköisen viestinnän palveluista annettuun lakiin https://lvm.fi/-/datanhallinta-asetuksen-taytantoonpano-muutoksia-sahkoisen-viestinnan-palveluista-annettuun-lakiin
26) EU:n datanhallinta-asetuksen soveltaminen alkoi – Traficomin uudet tehtävät käynnistyvät, kun laki tulee voimaan https://traficom.fi/fi/ajankohtaista/eun-datanhallinta-asetuksen-soveltaminen-alkoi-traficomin-uudet-tehtavat-kaynnistyvat
27) Valtionhallinnon pilvipalvelulinjaukset https://julkaisut.valtioneuvosto.fi/handle/10024/165214
28) EASA published first Easy Access Rules for Information Security https://www.easa.europa.eu/en/newsroom-and-events/news/easa-published-first-easy-access-rules-information-security