TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Tammikuu 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

>1000

Kyberala murroksessa -seminaari keräsi yli 1000 osallistujaa.

13

Kyberturvallisuuskeskus vastaanotti 13 ilmoitusta Akira-kiristyshaittaohjelmatapauksista kotimaisilta organisaatioilta vuonna 2023.

1,5 MILJ.

Rahoitustukihaku modernien tietoturvaratkaisujen ja -innovaatioiden käyttöönottoon pk-yrityksissä on auki 1.3.2024 asti. Haettavana on yhteensä 1,5 miljoonaa euroa.

Kybersää tammikuu 2024

Tietomurrot ja -vuodot

- M365-tilimurrot lisääntyivät alkuvuonna. Murtoihin johtivat esim. turvapostiteemaiset kalasteluviestit.
- Saimme useita ilmoituksia VPN-palveluihin kohdistuneista kirjautumisyrityksistä, osa yrityksistä johti Akira-kiristyshaittaohjelmatartuntaan.

Huijaukset ja kalastelut

- Sähköpostitilien murrot etenivät organisaatiosta toiseen turvapostiteemaisten kalasteluviestien avulla.
- Poliisin nimiin väärennetyissä tekstiviesteissä uhkailtiin ylinopeussakoilla.
- OmaVeron nimiin kirjaillut huijausviestit jatkuivat erittäin runsaina myös tammikuussa.

Haittaohjelmat ja haavoittuvuudet

- Ivantin tuotteissa kriittisiä hyväksikäytettyjä haavoittuvuuksia.
- Cisco Anyconnect -haavoittuvuutta on käytetty Akira-kiristyshaittaohjelman sisääntuloväylänä.
- Tammikuun aikana julkaistiin viisi ja helmikuun alussa kaksi tiedotetta kriittisistä haavoittuvuuksista.

Automaatio ja IoT

- Kyberala murroksessa -seminaarissa avattiin kybersääntelyn nykytilaa.[1]
- IoT-laitteita saastuttavat haittaohjelmat pysyvät vuodesta toiseen kyberrikollisten suosiossa. Rikolliset luovat uusia bottiverkkoja uusin ominaisuuksin erityisesti Mirain lähdekoodin pohjalta.[2]

Verkkojen toimivuus

- Tammikuussa yleisissä viestintäpalveluissa oli 3 toimivuushäiriötä.
- Haktivistien palvelunestohyökkäykset jatkuvat.
- Organisaatiot varautuvat, suojautuvat ja torjuvat palvelunestohyökkäyksiä hyvällä rutiinilla.

Vakoilu

- Microsoft kertoi pilvipalveluihinsa kohdistuneesta Midnight Blizzardin toteuttamasta hyökkäyksestä.[3]
- Hyökkäyksen kohteena oli myös muita Microsoftin asiakasorganisaatioita.
- Hyökkääjän tavoitteena oli hakea tietoa mm. päättäjien ja kyberturvallisuusasiantuntijoiden sähköposteista.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Kyberala murroksessa -seminaari pidettiin 23.1.2024. Tilaisuuden tallenne julkaistaan mahdollisimman pian Traficomin YouTube-kanavalla. Esitysaineistoja on julkaistu seminaarin ohjelmasivulla.[1]

Rahoitustukihaku modernien tietoturvaratkaisujen ja -innovaatioiden käyttöönottoon pk-yrityksissä on auki 1.3.2024 asti. Haettavana on yhteensä 1,5 miljoonaa euroa. Rahoitustukea voidaan myöntää enintään 60 000 euroa per projekti.[4]

Julkaisimme Tietoturva Nyt! -artikkelin *Vaalit turvataan viranomaisten yhteistyöllä*. Kyberturvallisuuskeskus on mukana tukemassa oikeusministeriötä ja muita vaaliviranomaisia valmistautumisessa ja varautumisessa kansallisiin vaaleihin.[5]

Älylaitteiden heikko tietoturva sääntelyllä kuriin 1.8.2024 alkaen, kun aletaan soveltaa pakollisia tietoturvavaatimuksia langattomille laitteille.[6]

Tammikuun kyberturvallisuuden yleiskuva

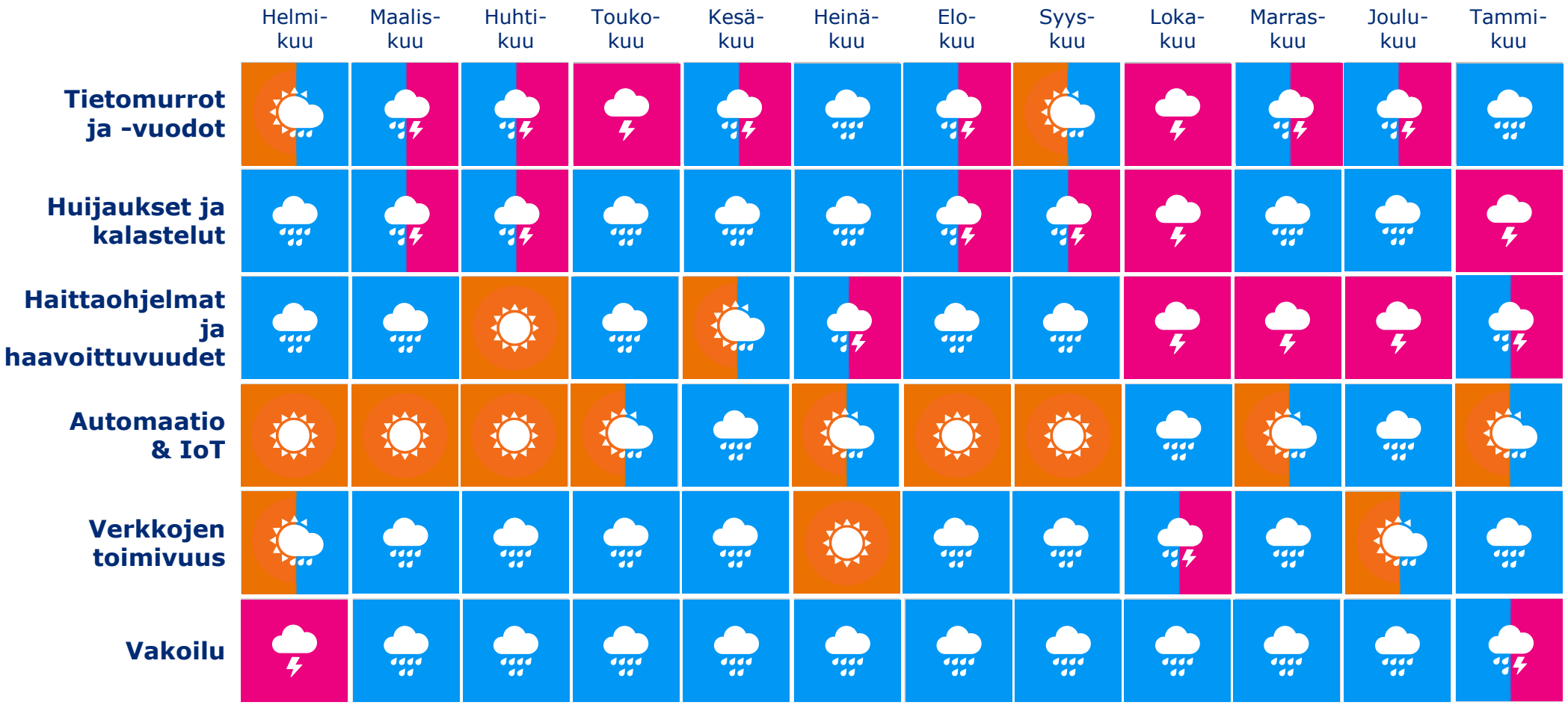
- Palvelunestohyökkäykset jatkuvat myös vuonna 2024. Kymmeniä kotimaisia organisaatioita on listattu venäläismielisten haktivistiryhmien palvelunestohyökkäysten kohteiksi alkuvuodesta 2024.
  - Kokonaan uusia kohteita listoilla on alkuvuonna ollut esimerkiksi kunta- ja koulutussektorilta.
  - Viime vuonna etenkin finanssi-, logistiikka- ja liikenne- ja valtionhallinnon toimijat olivat suosittuja kohteita.
- Alkuvuodesta on julkaistu useita kriittisiä haavoittuvuuksia.
  - Esimerkiksi Suomessakin laajassa käytössä olevia Ivantin tuotteita koskevia kriittisiä haavoittuvuuksia on julkaistu alkuvuodesta.
- Organisaatioiden tekemä aktiivinen tiedonjako lisää muiden organisaatioiden kykyä suojautua digitaalisilta uhkilta. Organisaation kohtaama kyberuhka saattaa kohdata toista organisaatiota seuraavana päivänä. Avoin ja ajankohtainen tiedonjako vähentää uhkien vaikutuksia ja kustannuksia. Toisilta oppiminen on myös kustannustehokasta, kun muiden ei tarvitse keksiä uudelleen toisaalla jo käytössä olevaa ratkaisua.

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

Tekoälyn riskienhallinta

Toimitus-ketjujen tietoturva

Sääntelyn tulevaisuus

Pilvi-palvelujen tietoturva

Teollisuus-automaation suojaaminen

IoT

6G

Kuluttajien tietoturva

Haavoittu-vuuksien nopeutuva hyväksikäyttö

Kvantti-turvallinen krypto/salaus menetelmät

Osallistu-minen digitaalisessa ympäristössä

Pitkän aikavälin kybersää:
Osallistuminen digitaalisessa ympäristössä

Digitaalinen ympäristö tuo poliittiseen osallistumiseen paitsi uusia mahdollisuuksia, myös haasteita.

- Vaalit on Suomessa aina järjestetty luotettavasti ja suomalainen vaalijärjestelmä on vakaa ja turvallinen.[5]
  - Äänestyslipuilla toteutettavaan vaalitapaan on erittäin vaikea vaikuttaa tietojärjestelmiin hyökkäämällä. Myöskään käsin tehtävän ääntenlaskennan luotettavuuteen ei voida vaikuttaa kyberhyökkäyksillä.
  - Esimerkiksi palvelunestohyökkäyksiä voidaan hyödyntää aiheuttamaan katkoksia tulosten hakemiseen vaalitietojärjestelmästä. Varsinaiseen vaalitulokseen ja sen luotettavuuteen ei kuitenkaan voida vaikuttaa palvelunestohyökkäyksillä. Palvelunestohyökkäyksiin onkin myös vaalien yhteydessä varauduttu.
- Vaaleihin tai laajemminkin yhteiskunnallisiin puheenaiheisiin voidaan pyrkiä vaikuttamaan disinformaatiolla sekä syvävääreennöksillä eli deepfakeilla.[5]
  - Kyberturvallisuuskeskukselle tehtyjen yksittäisten ilmoitusten valossa suomenkielisien syvävääreennöksien käyttö ei kuitenkaan vaikuta olevan vielä kovinkaan yleistä. Tämä voi muuttua tulevaisuudessa teknologian kehittyessä.[7]

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

Vuoden 2023 aikana nähtiin paitsi haktivistien tekemiä palvelunestohyökkäyksiä, myös kyberrikollisten kiristyshaittaohjelmia.

- Merkittävä uhka organisaatioille ovat kiristyshaittaohjelmat, joiden määrä kasvaa jatkuvasti. Viimeisen vuoden aikana usea organisaatio Suomessa on joutunut kiristyshaittaohjelman uhriksi.
  - Kyberturvallisuuskeskus vastaanotti 13 ilmoitusta Akira-kiristyshaittaohjelmatapauksista kotimaisilta organisaatioilta vuonna 2023. Joulukuussa 2023 Kyberturvallisuuskeskukselle ilmoitetuista kiristyshaittaohjelmatapauksista kuusi seitsemästä koski Akira-perheen haittaohjelmia.[8]
- Varsinkin huoltovarmuuskriittisten organisaatioiden joutuessa kiristyshaittaohjelman uhriksi yhteiskunnan elintärkeät toiminnot voivat vaarantua.
- Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista. Esimerkiksi päivitysten asentamisen pitäisi hoitua organisaatioissa aina pikimmiten, myös loma-aikoina.
- Valtioiden ja organisaatioiden päätökset altistavat entistä helpommin vaikuttamiselle, kuten mielenilmauksena tehdyille palvelunestohyökkäyksille.
  - Haktivistit tekivät ahkerasti palvelunestohyökkäyksiä myös vuonna 2023. Viime vuonna etenkin finanssi-, logistiikka- ja liikenne- ja valtionhallinnon toimijat olivat suosittuja kohteita. Myös alkuvuodesta on nähty kotimaisiin organisaatioihin kohdistuvia venäläismielisten haktivistiryhmien palvelunestohyökkäyksiä. Kokonaan uusia kohteita listoilla on ollut esimerkiksi kunta- ja koulutussektorilta.[9]

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.
  - 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.
- 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.
- Esimerkiksi vuoden 2023 lopulla tiedossamme olevissa kiristyshaittaohjelmatapauksissa korostui pääsy uhrin verkkoon huonosti suojatun Ciscon ASA- tai FTD-laitteissa olevan VPN-yhdyspisteen kautta.[8]

2. Case: Ivantin tuotteissa kaksi erittäin kriittistä haavoittuvuutta

Tammikuun puolivälin tienoilla Ivanti julkaisi kaksi kriittistä haavoittuvuutta, jotka koskivat sen kahta eri tuotetta. Kotimaiset organisaatiot käyttävät esimerkiksi Ivantin VPN-ratkaisua Connect Secure (entinen Pulse Secure). Kyberturvallisuuskeskuksen tekemien kartoitusten mukaan haavoittuvia palvelimia oli Suomessa useita satoja. Tämän vuoksi useiden kotimaisten organisaatioiden on syytä reagoida näihin julkistettuihin haavoittuvuuksiin välittömästi. Kyseiset haavoittuvuudet koskevat organisaatioita ja palveluntarjoajia, joilla kyseistä tuotetta on käytössä tai ylläpidossa. Haavoittuvuuksien hyväksikäytöstä on havaintoja viime vuoden joulukuun alkupuolelta asti.

Haavoittuvuuksien hyväksikäytön rajoittaminen tai lopulta edes päivittäminen ei kuitenkaan ratkaise tilannetta, jossa rikolliset ovat jo päässet sisään järjestelmään näiden haavoittuvuuksien avulla. Organisaatioiden tulisi olettaa, että mikäli tuotteet ovat heillä käytössä, niitä on voitu hyväksikäyttää ja siksi omista järjestelmistä tulisi etsiä mahdollisia tietomurron tunnusmerkkejä.[10]

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.

- Organisaatioissa pitäisi aina olla tietoisuus, miten asiat on sovittu palveluntarjoajien kanssa.
- Kyberturvallisuuskeskukselle ilmoitetuissa tapauksissa vaikuttaa usein siltä, että alihankintaketjuihin liittyvät vastuut ovat organisaatioille usein epäselviä. Vastuut olisikin hyvä määritellä aina siten, että poikkeamatilanteessa olisi selvää, mitä vastuunjaoista on sovittu.
- 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 alihankintaketju, koska myös alihankkija voi hankkia tuotteen/palvelun seuraavalta ketjussa olevalta palveluntarjoajalta.

4. Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa

Lyhyellä aikavälillä tekoälyn haasteisiin on liitetty skenaarioita esimerkiksi tekoälyn kyvystä kirjoittaa haittaohjelmia tai laatia paremmin kohdistettuja ja kielellisesti laadukkaampia tietojenkalasteluviestejä eri kielillä. Ainakin toistaiseksi tekoälyn kyvykkyyttä luoda aidosti toimivia haittaohjelmia on kuitenkin pidetty rajallisena.[11]

- Organisaatioiden on hyvä ottaa huomioon erityisesti tietosuoja- ja salassapitonäkökulmat tekoälyn mahdolliseen käyttöön liittyen, ja pohtia näihin liittyviä linjauksia organisaation sisällä.
- Euroopan komission tekoälysäädösehdotuksessa tekoälyjärjestelmiä säädeltäisiin niiden aiheuttaman riskin perusteella. Tämä tarkoittaa, että tekoälyjärjestelmien sääntelyn määrä riippuisi niiden mukanaan tuomien riskien tasosta.[12]
  - Euroopan parlamentti hyväksyi neuvottelukantansa säädökseen kesäkuussa 2023, ja seuraavaksi vuorossa ovat neuvottelut parlamentin ja jäsenmaita edustavan Euroopan unionin neuvoston välillä. Toteutuessaan kyseessä olisi maailman ensimmäinen tekoälylaki.[12]
- Syväväärennöksien eli ns. deepfake-tekniikan käytöstä osana kyberrikoksia on puhuttu kansainvälisessä uutisoinnissa.[7]
  - 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.

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. 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.
  - Esimerkiksi NIS2-sääntely tuo tullessaan uusia vaatimuksia ja velvoitteita myös uusille toimialoille.

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

Digitoimijoille uusia velvollisuuksia:[13]

- EU:n digipalvelusäädöksen soveltaminen alkaa 17.2.2024.
- Sääntely koskee internetin verkkoalustoja ja erilaisia digipalveluita.
- Tavoitteena on laittoman sisällön vähentäminen ja palveluiden avoimuuden lisääminen.
- Sääntelyn noudattamista valvoo pääasiassa Liikenne- ja viestintävirasto Traficom, mutta tietyiltä osin myös kuluttaja-asiamies ja tietosuojavaltuutettu.

Oikeudelliset asiat

Lakiluonnos yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta lausuntokierroksella 4.3.2024 asti.[14]

- Sisäministeriö pyytää lausuntoja luonnoksesta hallituksen esitykseksi eduskunnalle kriittisen infrastruktuurin direktiivin (CER-direktiivi) täytäntöönpanemiseksi.
- Sääntelyn tarkoituksena on parantaa yhteiskunnan kriittisen infrastruktuurin ja kriittisten palveluiden varautumista ja resilienssiä.
- Sääntely linkittyy myös valmisteilla olevaan lakiin kyberturvallisuuden riskienhallinnasta (NIS2-direktiivin täytäntöönpano).

Oikeudelliset asiat

Euroopan tietosuojaneuvosto on julkaissut verkkosivujen auditointityökalun.[15]

- Työkalun avulla tietosuojan valvontaviranomaiset, verkkosivukehittäjät ja organisaatiot voivat arvioida, ovatko verkkosivustot tietosuojalainsäädännön mukaisia.
- Uusi työkalu mahdollistaa tarkastusten tekemisen ja arvioinnin suoraan työkalussa vierailemalla kyseisellä verkkosivustolla. Työkalun avulla voi myös luoda raportteja.
- Työkalu on EUPL 1.2 -lisenssin mukainen maksuton avoimen lähdekoodin ohjelmisto.

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) Kyberala murroksessa -seminaari 23.1.2024 https://tietoturvamerkki.fi/fi/kyberala-murroksessa-seminaari-2312024
2) You Had Me at Hi — Mirai-Based NoaBot Makes an Appearance https://www.akamai.com/blog/security-research/mirai-based-noabot-crypto-mining
3) Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/
4) Kyberturvallisuuskeskuksen viikkokatsaus - 01/2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-012024
5) Vaalit turvataan viranomaisten yhteistyöllä https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vaalit-turvataan-viranomaisten-yhteistyolla
6) Älylaitteiden heikko tietoturva sääntelyllä kuriin https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/alylaitteiden-heikko-tietoturva-saantelylla-kuriin
7) Kyberturvallisuuskeskuksen viikkokatsaus - 03/2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-032024

Lähdeluettelo

8) Suomalaiset organisaatiot Akira-kiristyshaittaohjelmien kohteena https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suomalaiset-organisaatiot-akira-kiristyshaittaohjelmien-kohteena
9) Palvelunestohyökkäykset jatkuvat myös vuonna 2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaykset-jatkuvat-myos-vuonna-2024
10) Kyberturvallisuuskeskuksen viikkokatsaus - 02/2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-022024
11) NCSC-UK: ChatGPT and large language models: what's the risk? https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk
12) EU:n tekoälysäädös on ensimmäinen laatuaan https://www.europarl.europa.eu/news/fi/headlines/society/20230601STO93804/eu-n-tekoalysaados-onensimmainen-laatuaan

Lähdeluettelo

13) Digitoimijoille uusia velvollisuuksia – tavoitteena turvallisemmat ja avoimemmat verkkopalvelut https://www.traficom.fi/fi/ajankohtaista/digitoimijoille-uusia-velvollisuuksia-tavoitteena-turvallisemmat-ja-avoimemmat

14) Luonnos hallituksen esitykseksi laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja eräiksi muiksi laeiksi https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=67962948-2e20-43d7-a9e5-e43c99b60a8c

15) Euroopan tietosuojaneuvosto on julkaissut verkkosivujen auditointityökalun https://tietosuoja.fi/-/euroopan-tietosuojaneuvosto-on-julkaissut-verkkosivujen-auditointityokalun