TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Huhtikuu 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

Autoreporter-järjestelmän kautta välitettiin vuoden 2023 viimeisen kolmen kuukauden aikana yhteensä 2 073 Mirai-havaintoa. Näin ollen Mirai on tällä hetkellä Suomessa viiden yleisimmän tunnistettavaa verkkoliikennettä aiheuttavan haittaohjelman joukossa.[1]

Varoitettuun Palo Alto –haavoittuvuuteen liittyen KTK sai noin 15 ilmoitusta tietomurrosta tai sen epäilystä. Tilanne oli lopulta rauhallisempi kuin ennakoitiin, ja Varoitus poistettiin 7.5.2024.[2, 3]

Kybersää huhtikuu 2024

Tietomurrot ja -vuodot

- Palo Alton kriittinen haavoittuvuus (CVE-2024-3400) johti useisiin tietomurtoihin ja tietomurron yrityksiin. Saimme n.15 ilmoitusta, joiden perusteella vakavilta vahingoilta kuitenkin vältyttiin.
- Huhtikuussa M365-käyttäjätilejä murrettiin DropBox-teemaisilla kalasteluviesteillä. Osassa murroista käytettiin AiTM-tekniikkaa.

Automaatio ja IoT

- Kuluttajatuotteissa on ollut merkittäviä kyberturvallisuus-ongelmia. Osassa niistä viestintä on herättänyt tyytymättömyyttä kuluttajissa. Huono kriisiviestintä on yritykselle merkittävä maine- ja liiketoimintariski.[4, 5]
- Kriisiviestinnän suunnittelu ja harjoittelu on jatkuvuudenhallinnan ydintä.

Huijaukset ja kalastelut

- Android-puhelimiin levitetään haittaohjelmaa huijausviesteillä perintäyhtiön nimissä. Kredinorin lähettämiltä näyttävät tekstiviestit ja puhelinsoitot ohjaavat asentamaan puhelimeen "virustorjuntaohjelmiston", joka onkin pankkitietoja varastava haittaohjelma.
- Huijaussivustoja on väärennetty myös .fi-päätteisiin verkko-osoitteisiin mm. PRH:n nimissä.

Verkkojen toimivuus

- Huhtikuussa yleisissä viestintäpalveluissa oli 9 toimivuushäiriötä.
- Haktivistien palvelunestohyökkäykset eivät kohdistuneet huhtikuun aikana Suomeen.
- Muilla palvelunestohyökkäyksillä ei raportoitu olleen merkittäviä vaikutuksia.

Haittaohjelmat ja haavoittuvuudet

- Varoitus 1/2024: Organisaatioissa laajasti käytetyn Palo Alto GlobalProtect-tuotteen haavoittuvuutta (CVE-2024-3400) käytettiin aktiivisesti hyväksi.
- Kyberturvallisuuskeskukselle tehtyjen ilmoitusmäärien vähennettyä päätettiin poistaa Varoitus 7.5.2024.

Vakoilu

- Sandwormiin liitetyt havainnot nousivat esiin useissa julkaisuissa.
- Toimijan takaovena käyttämää haittaohjelmaa havaittiin mm. Ukrainassa ja Virossa.[6, 7, 8]
- Ukrainassa toimijan raportoitiin valmistelleen hyökkäyksiä paikallista energia-, vesi- ja lämmöntuotantoa vastaan.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

M365-tietomurroissa hyödynnetään yhä useammin AiTM-tietojenkalastelutekniikkaa. Julkaisimme ohjeen, jossa kerrotaan AiTM-kalastelun kulusta, sen tunnistamisesta sekä suojautumiskeinoista.[9]

Rikolliset ovat pyytäneet lunnaita murrettujen käyttäjätilien palauttamisesta. Lunnaita ei koskaan tule maksaa, sillä se tukee rikollisuuden ja kiristystoiminnan jatkumista.

Lue uudesta blogistamme vinkit yhteiseen taisteluun Mirain ja monen muunkin haittaohjelman toimintaedellytysten poistamiseksi.[1]

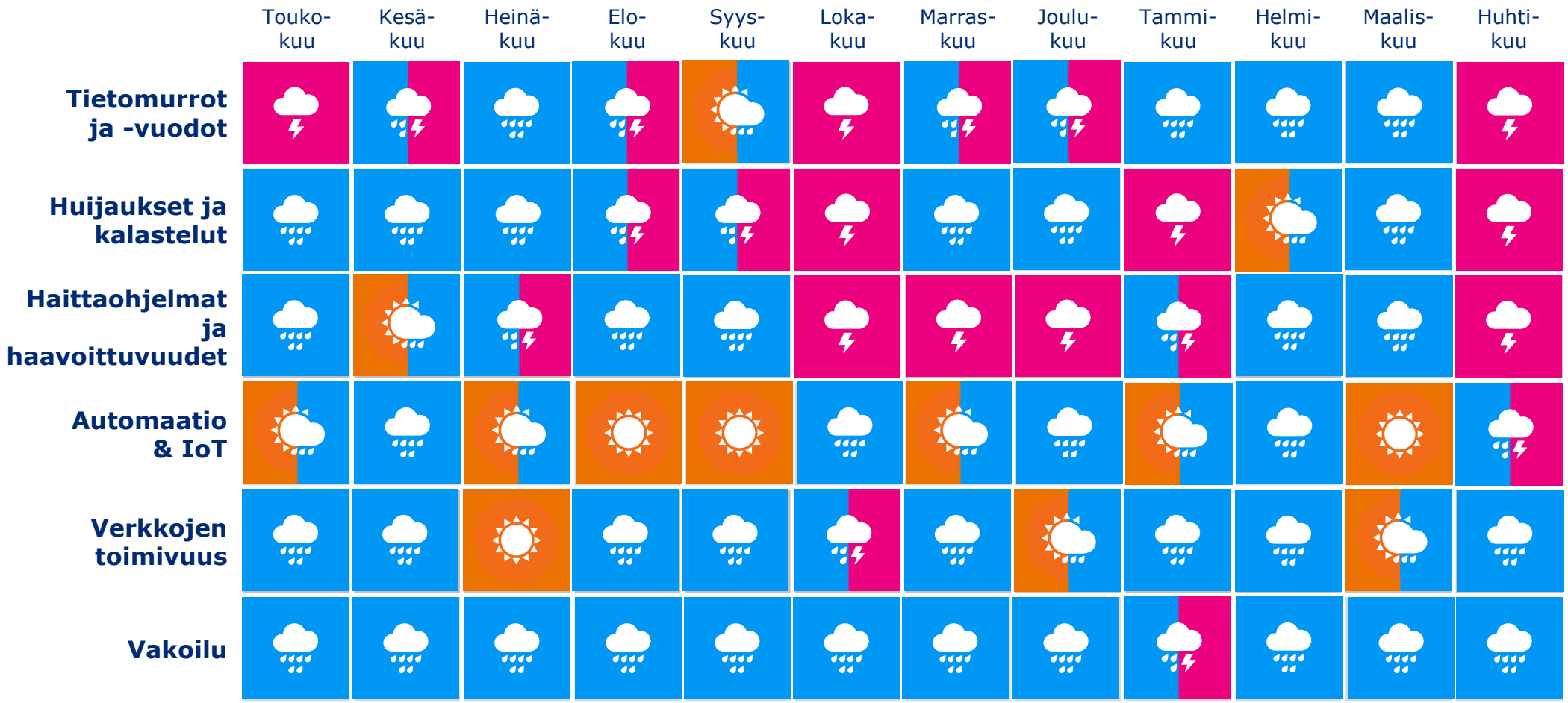
Huhtikuun kyberturvallisuuden yleiskuva

- Julkaisimme 18.4.2024 Varoituksen 1/2024 Palo Alto GlobalProtect-tuotteisiin kohdistuneisiin tietomurtoihin liittyen.[2]
  - Palo Alto GlobalProtect Gateway ja sen hallintaan käytetty GlobalProtect Portal ovat tuotteita, joita organisaatiot käyttävät esimerkiksi turvallisiin VPN-etätyöratkaisuihin.
  - Tilanne oli lopulta rauhallisempi kuin ennakoitiin, ja Varoitus poistettiin 7.5.2024.[3]
- Fitsec on julkaissut keinon Akira-haittaohjelman tekemän salauksen purkamiseen ja tarjoaa apuaan Akira:n uhreille sivuillaan.[10]

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

Tekoäly

Toimitus-ketjujen tietoturva

Sääntelyn tulevaisuus

Pilvi-palvelujen tietoturva

Teollisuus-automaation suojaaminen

IoT

6G

Kuluttajien tietoturva

Haavoittu-vuuksien nopeutuva hyväksikäyttö

Kvantti-turvallinen krypto

Osallistu-minen digitaalisessa ympäristössä

Pitkän aikavälin kybersää:
Tekoäly tulevaisuuden tietoturvaratkaisuissa

Kyberturvallisuusalalla on jo pitkään käytetty tekoälyteknologioita esimerkiksi roskapostin suodattamiseen, haittaohjelmien tunnistamiseen ja tunkeutumisen estämiseen. Tekoälybuumin myötä kiinnostus tekoälyyn ja erityisesti laajojen kielimallien tuomiin mahdollisuuksiin kyberturvallisuusratkaisuissa ovat nousseet pinnalle. Traficom ja Huoltovarmuuskeskus julkaisivat selvityksen tekoälypohjaisista kyberturvallisuusratkaisuista maaliskuussa.[11]

- Tekoälypohjaisille ratkaisuille on tarvetta, sillä tekoäly voi tulevaisuudessa tarjota hyökkääjille ennennäkemätöntä kykyä nopeuttaa ja automatisoida toimintaansa. Hyökkääjien ottaessa käyttöön yhä kehittyneempiä työkaluja, myös puolustajien on otettava täysi hyöty irti teknologisesta kehityksestä. Traficom ja Huoltovarmuuskeskus julkaisivat selvityksen tekoälyn mahdollistamista kyberhyökkäyksistä vuonna 2022.[12]
- Uusimmassa maaliskuussa julkaistussa selvityksessä näkökulma on vaihdettu tekoälyn mahdollistamista hyökkäyksistä tekoälyn hyödyntämiseen kyberturvallisuuden edistämisessä.
  - Selvitys osoittaa, että tekoälyn onnistunut soveltaminen kyberturvallisuudessa vaatii sekä tekoälyn että kyberturvallisuuden syvällistä ymmärrystä ja osaamista.
- Organisaatioiden tulisi arvioida huolellisesti tekoälyyn pohjautuvien ratkaisujen soveltumista kriittisiin käyttötapauksiin.
- Datan ymmärtäminen, sen saatavuus ja laatu ovat avainasemassa tekoälyratkaisujen toimivuudelle. Tekoälypohjaisten kyberturvallisuusratkaisuja tulee myös testata todellisissa ympäristöissä ennen laajamittaisen käyttöönoton harkitsemista.
- Tekoäly on edistynyt uhkien havaitsemisessa ja päätelaitteiden suojauksessa, mutta sen soveltaminen esimerkiksi uhkatiedusteluun ja haavoittuvuuksien hallintaan on vielä kehitysvaiheessa.
- Uusien tekoälyteknologioiden, kuten suurten kielimallien, yleistyminen tarjoaa merkittäviä mahdollisuuksia kyberturvallisuussovellusten kehittämiselle. Näitä teknologioita voidaan hyödyntää muun muassa turvallisuuskoulutuksessa, analytiikassa ja uhkatiedustelussa. Kielimallit mahdollistavat erityisesti suurten datamäärien tehokkaan käsittelyn ja asiayhteyksien tunnistamisen.

[11]

Ennuste suurten kielimallien käytöstä kyberturvallisuudessa

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.

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.

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.
  - **Alkuvuonna 2024 Akira-kiristyshaittaohjelmatapauksista saatujen ilmoitusten määrä on laskenut vuoden 2023 joulukuulta, jolloin Kyberturvallisuuskeskukselle ilmoitettiin kuusi Akira-perheen haittaohjelmaa.**
- 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 haktivistien mielenilmauksena tekemille palvelunestohyökkäyksille.

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.
- **Monien merkittävien laitevalmistajien verkon reunalaitteissa, kuten VPN-yhdyskäytävissä, havaittu vakavia ja helposti hyödynnettäviä haavoittuvuuksia viimeisen puolen vuoden aikana.**
  - **Osa haavoittuvuuksista on ollut nollapäivähaavoittuvuuksia eli niitä on hyväksikäytetty ennen kuin korjaava päivitys on ollut saatavilla.**

2. Case: Tietomurtoja Palo Alto GlobalProtect-tuotteisiin

Kyberturvallisuuskeskus julkaisi 18.4.2024 Varoituksen 1/2024 Palo Alton GlobalProtect-tuotteisiin liittyen. Palo Alton tuotteet ovat suosittuja myös Suomessa, ja useita satoja verkon reunalla sijaitsevia laitteita on alttiina perjantaina 12.4.2024 julkaistulle haavoittuvuudelle. Haavoittuvuuden hyväksikäyttöön liittyvät esimerkkikoodit ovat jaossa internetissä, joten ne ovat myös hyökkääjien saatavilla.[2]

Palo Alto GlobalProtect Gateway ja sen hallintaan käytetty GlobalProtect Portal ovat tuotteita, joita organisaatiot käyttävät esimerkiksi turvallisiin VPN-etätyöratkaisuihin. Kriittiset haavoittuvuudet näissä tuotteissa voivat tarjota avaimet käteen hyökkääjälle, koska tämänkaltaisten tuotteiden tarkoitus on mahdollistaa sisäänpääsy organisaation verkkoon.

Tuotteita käyttävien organisaatioiden tulee reagoida kriittisiin haavoittuvuuksiin ja niiden korjaustoimenpiteisiin entistäkin nopeammin. Haavoittuvuuksien hyväksikäyttö on Palo Altonkin tapauksessa alkanut jo ennen korjaavien toimenpiteiden tai päivitysten julkaisua. Varoitettuun Palo Alto –haavoittuvuuteen liittyen KTK sai noin 15 ilmoitusta tietomurrosta tai sen epäilystä. Varoitus poistettiin 7.5.2024.[3]

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.
- **Maaliskuussa 2024 Linuxiin useimmiten kuuluvassa XZ Utils -ohjelmistossa raportoitiin toimitusketjuhaavoittuvuus. XZ Utilsin edistynyt haavoittuvuus on takaportti, joka olisi tarpeeksi levitessään mahdollistanut laajojakin kyberhyökkäyksiä lähes mihin tahansa Linuxia ajaviin järjestelmiin. Sen kautta hyökkääjä olisi pystynyt käyttämään saastunutta järjestelmää omiin tarkoitusperiinsä periaatteessa täysin vapaasti.**[13]

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.[14]**
- **Euroopan parlamentti on hyväksynyt maailman ensimmäiset tekoälysäädökset alkuvuonna 2024.[15]**
- 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.

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.
  - **Euroopan kyberkestävyyssäädöksen (CRA) tavoitteena on vahvistaa yhteiset kyberturvallisuusvaatimukset internetiin kytkettäville, digitaalisen elementin sisältäville tuotteille.**

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

- Euroopan parlamentti hyväksyi uudet kyberkestävyysstandardit digitaalisten tuotteiden suojaamiseksi kyberuhkilta EU:ssa.[16]
  - Parlamentti hyväksyi 12.3.2024 kyberkestävyyssäädöksen, jolla pyritään varmistamaan, että digitaalisia elementtejä sisältäviä tuotteita on turvallista käyttää, ne ovat kestäviä kyberuhkia vastaan ja tarjoavat riittävästi informaatiota turvallisuusominaisuuksista.
  - EU:n neuvoston on vielä virallisesti hyväksyttävä säädös.
- EU:n kyberturvallisuusvirasto ja Euroopan komission yhteinen tutkimuskeskus julkaisivat 4.4.2024 listan standardeista edistämään kyberkestävyyssäädöksen (CRA) turvallisuusvaatimusten noudattamista.[17]
  - Julkaisussa on pyritty tunnistamaan relevanteimmat olemassa olevat kyberturvallisuusstandardit jokaiselle CRA:n vaatimukselle, analysoimaan standardien kattavuus ja tuomaan esiin mahdolliset puutteet suhteessa CRA:n vaatimuksiin.

Oikeudelliset asiat

- eIDAS-asetuksen muutos julkaistiin EU:n virallisessa lehdessä.[18]
- Asetuksessa säädetään henkilöiden tunnistamisesta valtioiden rajat ylittävässä asioinnissa sekä sähköisen asioinnin luottamuspalveluista. Uudistetun asetuksen keskeinen velvoite on, että jäsenvaltioiden tulee tarjota asetuksen vaatimukset täyttävä digitaalisen identiteetin lompakko viimeistään vuonna 2026.
  - eIDAS-asetuksen muutos julkaistiin EU:n virallisessa lehdessä 30.4.2024 ja asetus tulee voimaan 20.5.2024.
  - Komission on viimeistään 21.11.2024 annettava lompakkoon liittyvät täytäntöönpanosäädökset.
- Valtiovarainministeriö on 26.4.2024 asettanut hankkeen ohjaamaan kansallisen digitaalisen identiteetin lompakon toteuttamista.[19]

Oikeudelliset asiat

- Liikenne- ja viestintävirasto Traficomin luonnos suositukseksi NIS2-direktiivin kyberturvallisuuden riskienhallinnan toimenpiteistä lausuntokierroksella 31.5.2024 saakka.[20, 21]
  - Traficomin Kyberturvallisuuskeskus pyytää lausuntoja suositusluonnoksesta valvoville viranomaisille NIS2-direktiivin mukaisten kyberturvallisuuden riskienhallinnan toimenpiteiden valvomiseksi.
  - Suositusluonnos on tarkoitettu valvoville viranomaisille, mutta se tukee myös toimijoiden omaa kyberturvallisuuden riskienhallinnan suunnittelua.
  - Suositusluonnokseen on koottu tietoa ja käytännön esimerkkejä siitä, millaisia toimenpiteitä laissa säädettäviin vaatimuksiin voi kuulua. Suositusluonnoksessa esitellään perustason tietoturvakäytännöt, jotka kuvaavat millaisilla toimilla organisaatio voi suojautua yleisimmiltä verkkouhkilta.
  - Suosituksen valmistelu perustuu liikenne- ja viestintäministeriön luonnokseen laiksi kyberturvallisuuden riskienhallinnasta ja julkisen hallinnon tiedonhallinnasta annettuun lakiin luonnosteltuihin muutoksiin. Lopullinen suositus muotoutuu lakien valmistuttua.

Oikeudelliset asiat

- Liikenne- ja viestintävirasto Traficom on 28.3.2024 antanut suosituksen kohdennetun viranomaistiedotteen välittämisestä.[22]
  - Suositus käsittelee kohdennetun viranomaistiedotteen välittämistä. Kohdennetulla viranomaistiedotteella tarkoitetaan tekstiviestillä (SMS) päätelaitteisiin kertaluonteisesti välitettävää tiedotetta.
  - Toimivaltainen ministeriö päättää kohdennetun viranomaistiedotteen antamisesta oman ohjeistuksensa mukaisesti ja kohdennetun viranomaistiedotteen antamiseen käytetään Hätäkeskuslaitoksen lomaketta.
  - Suositus koskee matkaviestinverkkoja tarjoavia teleyrityksiä.

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) Miraissa on tulevaisuus https://traficom.fi/fi/ajankohtaista/blogit/miraissa-tulevaisuus
2) Tietomurtoja Palo Alto GlobalProtect-tuotteisiin – vaatii välittömiä toimia https://www.kyberturvallisuuskeskus.fi/fi/tietomurtoja-palo-alto-globalprotect-tuotteisiin-vaatii-valittomia-toimia
3) Palo Alto GlobalProtect -tuotteita koskenut Varoitus on poistettu https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palo-alto-globalprotect-tuotteita-koskenut-varoitus-poistettu
4) Moni kesämökki kylmenee nyt: Ilmalämpöpumpun omistajat ihmeissään https://www.is.fi/digitoday/art-2000010376407.html
5) Thousands of LG TVs are vulnerable to takeover—here's how to ensure yours isn't one https://arstechnica.com/security/2024/04/patches-released-for-as-many-as-91000-hackable-lg-tvs-exposed-to-the-internet/

Lähdeluettelo

6) WithSecure uncovers Kapeka, a new malware with links to Russian nation-state threat group Sandworm https://www.withsecure.com/en/whats-new/pressroom/withsecure-uncovers-kapeka-a-new-malware-with-links-to-russian-nation-state-threat-group-sandworm
7) Плани UAC-0133 (Sandworm) щодо кібердиверсії на майже 20 об'єктах критичної інфраструктури України https://cert.gov.ua/article/6278706
8) Unearthing APT44: Russia’s Notorious Cyber Sabotage Unit Sandworm https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm
9) M365-tietomurroissa hyödynnetään yhä useammin AiTM-tietojenkalastelutekniikkaa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/m365-tietomurroissa-hyodynnetaan-yha-useammin-aitm
10) Akirahelp https://akirahelp.com/
11) Tekoäly on yhä keskeisempi tekijä tulevaisuuden tietoturvaratkaisuissa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tekoaly-yha-keskeisempi-tekija-tulevaisuuden-tietoturvaratkaisuissa
12) Tekoäly tulee muuttamaan myös kyberhyökkäyksiä https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tekoaly-tulee-muuttamaan-myos-kyberhyokkayksia

Lähdeluettelo

13) Kyberturvallisuuskeskuksen viikkokatsaus - 14/2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-142024
14) Fifth of CISOs Admit Staff Leaked Data Via GenAI https://www.infosecurity-magazine.com/news/fifth-cisos-staff-leaked-data-genai/
15) Parlamentti hyväksyi maailman ensimmäiset tekoälysäännöt https://www.europarl.europa.eu/news/fi/press-room/20240308IPR19015/parlamentti-hyvaksyi-maailman-ensimmaiset-tekoalysaannot
16) Cyber Resilience Act: MEPs adopt plans to boost security of digital products https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products
17) Cyber Resilience Act Requirements Standards Mapping - Joint Research Centre & ENISA Joint Analysis https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping
18) Euroopan parlamentin ja neuvoston asetus (EU) 2024/1183, annettu 11 päivänä huhtikuuta 2024, asetuksen (EU) N:o 910/2014 muuttamisesta eurooppalaisen digitaalisen identiteetin kehyksen vahvistamisen osalta https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=OJ:L_202401183
19) Digitaalisen identiteetin lompakko tulee vuonna 2026 https://vm.fi/-/digitaalisen-identiteetin-lompakko-tulee-vuonna-2026

Lähdeluettelo

20) Lausuntopyyntö suositusluonnoksesta NIS2-direktiivin kyberturvallisuuden riskienhallinnan toimenpiteistä https://www.traficom.fi/fi/ajankohtaista/lausuntopyynto-suositusluonnoksesta-nis2-direktiivin-kyberturvallisuuden-0

21) Liikenne- ja viestintävirasto Traficomin lausuntopyyntö suositusluonnoksesta NIS-valvoville viranomaisille https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=ebc51269-712e-4115-b137-b0b2a710dac4

22) Suositus kohdennetun viranomaistiedotteen välittämisestä https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Suositus_kohdennetun_viranomaistiedotteen_v%C3%A4litt%C3%A4misest%C3%A4.pdf