TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Heinäkuu 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

CrowdStriken yksittäinen päivitys aiheutti merkittäviä käyttökatkoja ympäri maailmaa, mutta Suomessa kriittiset vaikutukset jäivät vähäisiksi.

JetBrains TeamCity -tuotteen haavoittuvuutta hyväksikäytettiin 22 minuuttia haavoittuvuuden hyväksikäyttömenetelmän julkaisun jälkeen. Tieto käy ilmi Cloudflaren tuottamasta raportista.[1]

Tietomurrosta aiheutuvat kustannukset ovat matalammat viranomaisten osallistuessa tietomurron selvittämiseen. Viranomaisten ollessa mukana tietomurron selvityksessä kustannus oli keskimäärin 4 miljoonaa euroa, kun ilman viranomaisten apua tietomurrosta kertyi yrityksille kustannuksia noin 5 miljoonaa euroa.[2]

Kybersää heinäkuu 2024

Tietomurrot ja -vuodot

- M365-tilimurrot synkistivät aurinkoista kesäsäätä. Heinäkuussa murtojen määrä kasvoi edellisiin kuukausiin nähden. Tunnusten havittelussa käytettiin erityisesti AiTM-tekniikkaa.
- Kokonaisuutena tietomurto-ilmoitusten määrä on kesän aikana puolittunut alkuvuoteen nähden.

Huijaukset ja kalastelut

- Huijari väittää soittavansa pankista ja pelottelee uhreja epäilyttävillä tilisiirroilla ulkomaille. Huijari pyytää pankkitunnuksia "palautustiliä" varten.
- Tekstiviesteissä pelotellaan taas "ulosottoon siirtyvällä sakolla" viranomaiselta muistuttavilla TRAF COMin ja TRAFCORNin nimillä.

Haittaohjelmat ja haavoittuvuudet

- CrowdStriken 19.7. häiriö sai opportunistit liikkeelle: CrowdStriken nimissä kalastellaan tietoja ja levitetään haittaohjelmia, joiden väitettiin korjaavan päivityksen aiheuttamat ongelmat.
- Cisco Secure Email Gatewaysta (entinen IronPort) löytyi kriittinen haavoittuvuus.

Automaatio ja IoT

- Langattomien murtosuojaus- ja kameravalvontajärjestelmien häiritseminen on teknisesti helppoa. Yhdysvalloissa poliisit ovat varoittaneet ilmiön olevan kasvussa. Osasyy kasvulle lienee valvontakameroiden yleistyminen kodeissa.[3]

Verkkojen toimivuus

- Heinäkuussa yleisissä viestintäverkoissa 9 toimivuushäiriötä.
- Palvelunestohyökkäyksiä raportoitiin myös kesäaikana, mutta palveluvaikutukset ovat olleet olemattomia.
- Kaikki palvelunestohyökkäykset eivät ole yhdistettävissä haktivistitoimijoihin.

Vakoilu

- Pohjois-Koreaan liitetty kyberuhkatoimija APT45 (Andariel) on hyökännyt kiristyshaitta-ohjelmilla yhdysvaltalaisia terveydenhuollon tarjoajia vastaan ansaitakseen rahaa valtiolle.
- APT45:n vakoilun kohteena on ollut mm. puolustusteollisuus, ilmailuala ja ydinvoimaan liittyvät organisaatiot.[4, 5, 6, 7]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Julkaisimme ohjeen Sometilit kuntoon, vinkit turvalliseen somettamiseen. Ohje sopii niin yksityishenkilöille kuin yrityksenkin somea päivittäville.[8]

Osa kiristyshaittaohjelmista on pyrkinyt etsimään ja tuhoamaan myös kohteensa varmuuskopiot. Tärkeimpien varmuuskopioiden osalta on suositeltavaa seurata 3-2-1-sääntöä: säilytä vähintään **kolmea** varmuuskopiota **kahdessa** eri paikassa ja pidä **yksi** näistä kopioista kokonaan poissa verkosta.

Digitaalinen Eurooppa -ohjelman rahoitushakemuskoulutus järjestetään 27.8.2024. Hakemuskoulutuksessa esitellään Digitaalinen Eurooppa -ohjelman kyberturvallisuustyöohjelman rahoitushakuja, sekä käydään läpi kokeneiden asiantuntijoiden johdolla konkreettisia neuvoja ja vinkkejä korkeatasoisten Digitaalinen Eurooppa -ohjelmaan lähetettävien hakemusten laatimiseksi.[9]

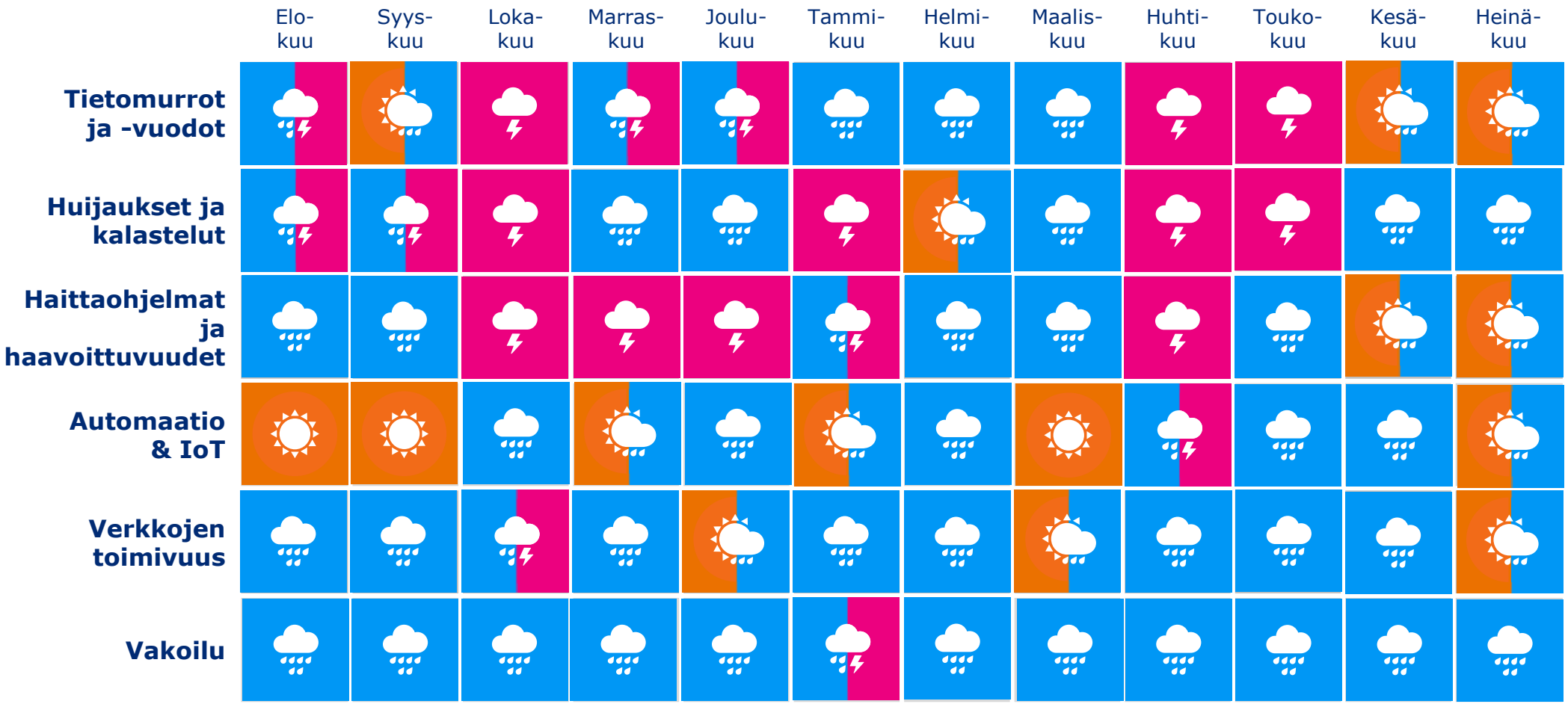
Heinäkuun kyberturvallisuuden yleiskuva

- Heinäkuu oli hyvin rauhallinen ja kesälomakausi näkyi myös yleiskuvassa.
- CrowdStrike-tietoturvatuotteen päivitys sai aikaan häiriön, jonka vuoksi kyseistä tuotetta käyttävät Windows-laitteet eivät käynnistyneet. Häiriö aiheutti käyttökatkoja useissa palveluissa maailmanlaajuisesti vaikuttaen muun muassa maksuliikenteeseen, lentoliikenteeseen, junaliikenteeseen, terveydenhuoltoon ja mediataloihin. Myös Suomessa oli organisaatioita, joihin tilanne vaikutti joko suoraan tai välillisesti toimitusketjun kautta.
- Heinäkuun aikana saimme useita ilmoituksia erilaisista organisaatioihin kohdistuvista Microsoft 365 -käyttäjätilien kalasteluista. Osa kalasteluista oli johtanut sähköpostitilin tietomurtoon.
- Erilaisia huijausviestejä lähetettiin myös heinäkuun aikana. Rikolliset elävät myös ajassa ja kuun lopulla veronpalautusteemaiset huijausviestit alkoivat yleistymään, koska veronpalautukset tulevat elokuusta eteenpäin monelle ajankohtaiseksi.
- Palvelunestohyökkäyksiä kohdistui eri organisaatioihin, erityisesti valtionhallintoon, heinäkuun aikana.

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
- Tekoälyn riskienhallinta
- 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: Tarve kyberturvallisuuden osaajille kattaa koko yhteiskunnan

Kyberturvallisuusosaaminen kuuluu kansalaistaitoihin ja jokainen voi omalla toiminnallaan myötävaikuttaa yhä turvallisemman kybertoimintaympäristön syntyyn. Tämän lisäksi kyberturvallisuusala tarvitsee erilaisia osaajia, jotta organisaatiot voivat tunnistaa uhkat ja reagoida haitalliseen toimintaan sekä ilmoittaa havaituista häiriöistä.

- Kyberturvallisuusala työllistää yhä enemmän monipuolisia ammattilaisia. Tarve osaajille on silti suuri.
- Viranomaiset ja yritykset tarvitsevat erittäin monipuolista osaamista niin työntekijöiden kuin alihankkijoidensa piirissä hallitakseen kyberturvallisuutta koskevia riskejä. Kansallisella tasolla on varmistettava, että yrityksillä on sekä huippuosaajia että muuta osaavaa henkilöstöä riittävästi saatavilla.
- Merkittävämmässä roolissa ovat tulevaisuudessa ne yritykset, joiden varsinainen liiketoiminta on kyberturvallisuusalan ulkopuolella, mutta joiden toimintaan kyberturvallisuus ja siihen liittyvät häiriöt vaikuttavat merkittävästi.
- Kyberturvallisuusalan kattojärjestö FISC:in mukaan vuonna 2025 tarve olisi 15 000:lle alan osaajalle Suomessa. Liikenne- ja viestintäministeriön kyberosaamistarvetta mittaavan kyselyn mukaan 73 prosenttia viranomaisista sekä elinkeinoelämän ja kolmannen sektorin toimijoista kokee merkittävää osaamispulaa.

Top 5 uhat lähitulevaisuudessa (6kk–2v)

1.

Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

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

2.

Kiristyshaittaohjelmat - Merkittävä uhka organisaatioille

Viimeisen vuoden aikana usea organisaatio Suomessa on joutunut kiristyshaittaohjelman uhriksi, ja niiden määrä kasvaa jatkuvasti myös globaalisti.

3.

Toimitus- ja palveluketjujen tietoturva ja jatkuvuus ovat yhä kriittisempiä.

Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä. Valtaosa organisaatioista on enemmän tai vähemmän riippuvaisia ulkoistetuista digitaalisista palveluista.

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.

Tietoliikenneinfran suojaamisen tärkeys korostuu

Tietoliikenne- ja tietojärjestelmäinfran suojaaminen maailmalla ja kotimaassa on tärkeää, sekä siihen kohdistuvien vahinkojen ja luonnonilmiöiden että ulkopuolisten aiheuttamien tahallisten häiriöiden takia.

1. Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

- Haavoittuvuuden korjaavan päivityksen asentamisen lisäksi on usein tarpeen tutkia, onko haavoittuvuutta hyödynnetty jo ennen päivityksen asentamista, tai onko järjestelmään luotu takaovia, eli piilotettuja sisäänpääsyreittejä.
- Rikolliset pyrkivät hyväksikäyttämään haavoittuvuuksia jo ennen kuin niitä on ehditty korjata. Haavoittuvuuden aktiivista hyväksikäyttöä aletaan yrittää viimeistään siinä vaiheessa, kun haavoittuvuudesta on tullut julkinen. Rikolliset etsivätkin ahkerasti verkosta päivittämättömiä järjestelmiä kohteikseen.
  - Järjestelmien nopea päivittäminen onkin erityisen tärkeää, ja valmius päivittämiseen pitäisi olla jatkuvasti, myös yleisinä loma-aikoina.
  - **Cloudflare kertoi raportissaan JetBrains TeamCity -tuotteeseen liittyvää haavoittuvuutta hyväksikäytetyn jopa 22 minuuttia haavoittuvuuden hyväksikäyttömenetelmän julkaisun jälkeen.**[1]
- 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. Kiristyshaittaohjelmat - Merkittävä uhka organisaatioille

- Viimeisen vuoden aikana usea organisaatio Suomessa on joutunut kiristyshaittaohjelman uhriksi, ja niiden määrä kasvaa jatkuvasti myös globaalisti.
  - Suomessa Akira-kiristyshaittaohjelmasta on raportoitu eniten havaintoja Kyberturvallisuuskeskukselle. Noin vuoden aikana lähes 20 kotimaista organisaatiota on joutunut Akiran uhriksi.[10]
- Varsinkin huoltovarmuuskriittisten organisaatioiden joutuessa kiristyshaittaohjelman uhriksi yhteiskunnan elintärkeät toiminnot voivat vaarantua. Organisaatioiden kannattaa ottaa kiristyshaittaohjelmat huomioon varautumisessa ja harjoitustoiminnassa.
  - Esimerkiksi Britanniassa kiristyshaittaohjelma vaikutti alkukesästä usean Lontoon sairaalan sekä perusterveydenhuollon yksiköiden toimintaan. Kiristyshaittaohjelman aiheuttamat häiriöt saivat aikaan leikkausten ja verensiirtojen perumisia suurissa sairaaloissa, sekä päivystyspotilaiden ohjaamista muihin sairaaloihin. Hyökkäys vaikutti myös potilaiden testitulosten saatavuuteen.[11, 12, 13]
- Kiristyshaittaohjelma tartutetaan usein kalasteluviestin, vuotaneiden käyttäjätunnusten tai päivittämättömien haavoittuvuuksien kautta. Tiedostojen salaus ja muut hyökkääjän tekemät toimenpiteet saatetaan toteuttaa viipymättä sisäänpääsyn jälkeen, joten ennaltaehkäisy, havainnointi ja nopea reagointi ovat avainasemassa.
- Osa kiristyshaittaohjelmista pyrkii etsimään ja tuhoamaan myös kohteensa varmuuskopiot, joten ainakin yksi varmuuskopio kannattaa säilyttää poissa verkosta.
- Viime vuosina on yleistynyt ns. Double extortion, jossa salaamisen lisäksi rikolliset myös varastavat tiedot ja kiristävät organisaatiota tietovuodolla. Kiristyshaittaohjelmatoimijoiden vaatimia lunnaita ei tule maksaa. Palautumisesta ei ole takeita, ja lunnaat maksamalla rahoittaa rikollista toimintaa.
- Kiristyshaittaohjelmia myydään yhä enenevissä määrin myös palveluna (RaaS). Tämän vuoksi hyökkääjän ei enää tarvitse olla teknisesti taitava toteuttaakseen hyökkäyksiä, ja RaaS-palvelua hyödyntäviä rikollisia voi olla enemmän. Europolin arvion mukaan tulevaisuudessa nähdään yhä enemmän rikollisia, jotka tarjoavat muille RaaS-palveluita. Kuinka kauan nämä ryhmät ovat aktiivisia, ovat kiinni siitä, miten tyytyväisä palveluita ostaneet ovat.[14]

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.
- **CrowdStrike-tietoturvatuotteen päivitys sai 19.7.2024 aikaan häiriön, jonka vuoksi kyseistä tuotetta käyttävät Windows-laitteet eivät käynnistyneet.**[15]
  - **Häiriö aiheutti käyttökatkoja useissa palveluissa maailmanlaajuisesti, vaikuttaen muun muassa maksuliikenteeseen, lentoliikenteeseen, junaliikenteeseen, terveydenhuoltoon ja mediataloihin. Myös Suomessa oli organisaatioita, joihin tilanne vaikutti joko suoraan tai välillisesti toimitusketjun kautta.**

3. Case: Toimitusketjuhyökkäyksen seurauksena usean viranomaisen rekisteritietoihin päästiin käsiksi.

- Liikenne- ja viestintävirasto Traficomin ajoneuvorekisterin asiakasorganisaatio ilmoitti palveluunsa kohdistuneesta väärinkäytöstä. Väärinkäytön johdosta ajoneuvojen omistajien ja haltijoiden henkilötunnuksia päätyi toukokuussa 2024 asiakkaan järjestelmästä kolmannen osapuolen haltuun.[16]
- Samaan aikaan Verohallinto kertoi, että positiivisesta luottotietorekisteristä oli kysytty luottotietorekisteriotteita väärin perustein. Luotonantajan käyttämään ohjelmistoon oli tehty tietomurto, jonka seurauksena positiivisesta luottotietorekisteristä oli kysytty luottotietorekisteriotteita ilman perustetta.[17]
- Positiiviseen luottotietorekisteriin tai ajoneuvorekisteriin ei ole kohdistunut tietomurtoa. Sen sijaan epäillään, että kyseessä on ollut toimitusketjuhyökkäys, ja näitä rekistereitä hyödyntävän sopimuskumppanin asiakastileihin on kohdistunut tietomurtoja. Näiden murtojen kautta on tehty perusteettomia kyselyitä kymmenien tuhansien ihmisten henkilötiedoista.[18]
- Toimitusketjuhyökkäyksessä organisaation tietojärjestelmiin murtaudutaan sen käyttämien verkostojen, palveluiden, tuotteiden tai avoimen lähdekoodin projektien kautta. Hyökkäyksessä hyväksikäytetään organisaatioiden luottamusta toimittajiinsa. Hyökkäyksen reittinä voivat olla yhteistyökumppanit, palveluntarjoajat, ohjelmistot tai laitteet. Hyökkääjä tunkeutuu toimittajan järjestelmiin ja saastuttaa toimitusketjussa käytetyn osan omalla haittakoodillaan, jonka jälkeen se leviää normaalia tuotteen jakelukanavaa pitkin yhteistyö- ja asiakasorganisaatioihin.

4. Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa

- Lyhyellä aikavälillä tekoälyn haasteisiin on liitetty skenaarioita esimerkiksi tekoälyn kyvystä kirjoittaa haittaohjelmia tai laatia paremmin kohdistettuja ja kielellisesti laadukkaampia tietojenkalasteluviestejä eri kielillä. Ainakin toistaiseksi tekoälyn kyvykkyyttä luoda aidosti toimivia haittaohjelmia on kuitenkin pidetty rajallisena.
- Organisaatioiden on hyvä ottaa huomioon erityisesti tietosuoja- ja salassapitonäkökulmat tekoälyn mahdolliseen käyttöön liittyen, ja pohtia näihin liittyviä linjauksia organisaation sisällä.
  - Tekoälyn käyttöön tulisi laatia organisaation sisäinen käyttöpolitiikka ja ohjeistus henkilöstölle siitä, miten tekoälyä voi sallitulla tavalla hyödyntää työssä.
  - Iso-Britanniassa laaditun selvityksen mukaan noin viidesosassa paikallisista yrityksistä on paljastunut mahdollisesti sensitiivisen tiedon vaarantuneen henkilöstön tekoälyn käytön seurauksena.
- Syväväärennöksien eli ns. deepfake-tekniikan käytöstä osana kyberrikoksia on puhuttu kansainvälisessä uutisoinnissa.
  - Syväväärennösten tekeminen voi näyttäytyä rikollisille houkuttelevana tapana huijata organisaation työntekijöitä tai aiheuttaa mainehaittaa.
  - Kyberturvallisuuskeskukselle tehtyjen yksittäisten ilmoitusten valossa suomenkielisien syväväärennöksien käyttö ei kuitenkaan vaikuta olevan vielä kovinkaan yleistä.
- **Europolin raportin mukaan tekoäly yleistyy rikollisten keinovalikoimassa. Europol nimesi raportissaan tekoälyn ja kielimallit yhdeksi tulevaisuuden pääuhista.**[14]

5. Tietoliikenneinfran suojaamisen tärkeys korostuu

- Sekä maailmalla että kotimaassa on vuoden mittaan tapahtunut ikäviä tietoliikenneinfraan kohdistuneita vahinkoja ja luonnonilmiöitä, sekä ulkopuolisten tekijöiden aiheuttamia tahallisia häiriöitä.
- Kaikkien tietoliikenne- ja tietojärjestelmäinfran omistajien kannattaa huolehtia siitä, että viestintäverkon tai –palvelun komponentit on suojattu fyysisesti siten, etteivät asiattomat pääse niihin helposti käsiksi.
- Yleisen teletoiminnan osalta Liikenne- ja viestintävirasto Traficomin määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista asettaa vaatimukset laitetilojen ja siirtoteiden suojaamiselle yleisen viestintäverkon ja palvelujen komponenttien tärkeysluokkien perusteella. Tärkeysluokitus perustuu viestintäpalvelun tyyppiin sekä maantieteelliseen alueeseen tai käyttäjämäärään, johon viestintäverkon tai -palvelun komponentti vaikuttaa.
- Fyysisen suojauksen lisäksi tärkeää on myös se, että itse laitetilojen rakenne täyttää määräyksen velvoitteet, ja että niissä on vaadittava ajantasainen kulunvalvonta, ja että niistä saadaan asianmukaiset hälytykset valvontahenkilöstölle.
- Pelkkä vahinkojen korjaaminen ei riitä. Häiriöiden ja niistä kerätyn informaation perusteella on tarpeen miettiä myös toimenpiteitä, joilla voidaan parantaa suojaustasoa.
- Suojaustason parantamiseksi Traficom sekä teleoperaattorit tekevät yhteistyötä, jotta esimerkiksi kotimaassa tapahtuneiden vahinkojen ja muiden häiriöiden määrää voitaisiin edelleen vähentää.

Tietoturva-alan kehitys, sääntely ja standardit

Tietoturva-alan kehitys -osiossa kerromme keskeisistä uudistuksista esimerkiksi alaa koskevan lainsäädännön tai asetusten päivityksiin liittyen. Kerromme kaikille tärkeää kyberturvallisuustietoa ja Kyberturvallisuuskeskuksen ajankohtaisista asioista.

Oikeudelliset asiat

Euroopan tietosuojaneuvosto on 16.7.2024 antanut lausunnon tietosuojaviranomaisten roolista tekoälyasetuksen valvonnassa.[19, 20]

- EU-maiden on nimitettävä tekoälyasetusta valvovat kansalliset viranomaiset 2.8.2025 mennessä.
- Tätä varten lausunnossa suositellaan, että EU-maiden tietosuojaviranomaiset toimisivat erityisesti tiettyjen suuririskisten tekoälyjärjestelmien valvontaviranomaisina eli niin sanottuina markkinavalvontaviranomaisina.
- EU-maita suositellaan nimittämään tietosuojaviranomaiset valvomaan suuririskisiä tekoälyjärjestelmiä, joita käytetään muun muassa lainvalvonnassa, rajavalvonnassa, muuttoliikkeen hallinnassa ja turvapaikka-asioissa.
  - Näitä ovat esimerkiksi biometriseen tunnistamiseen ja luokitteluun sekä tunteiden tunnistamiseen perustuvat tekoälyjärjestelmät.
  - Lisäksi EU-maiden tulisi harkita, että tietosuojaviranomaiset nimitettäisiin valvomaan muitakin suuririskisiä tekoälyjärjestelmiä, joissa henkilötietojen käsittely vaikuttaa ihmisten oikeuksiin.

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) Kyberturvallisuuskeskuksen viikkokatsaus - 29/2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-292024
2) Näin paljon tietomurto voi maksaa https://www.talouselama.fi/uutiset/nain-paljon-tietomurto-voi-maksaa/a3425fb3-018c-4b81-bdca-3bf97a7958b9
3) Burglars are jamming Wi-Fi security cameras — here's what you can do https://www.pcworld.com/article/2405434/burglars-are-jamming-wi-fi-security-cameras.html
4) North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers https://www.justice.gov/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals
5) North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs https://media.defense.gov/2024/Jul/25/2003510137/-1/-1/0/Joint-CSA-North-Korea-Cyber-Espionage-Advance-Military-Nuclear-Programs.PDF
6) Onyx Sleet uses array of malware to gather intelligence for North Korea https://www.microsoft.com/en-us/security/blog/2024/07/25/onyx-sleet-uses-array-of-malware-to-gather-intelligence-for-north-korea/
7) APT45: North Korea's Digital Military Machine https://cloud.google.com/blog/topics/threat-intelligence/apt45-north-korea-digital-military-machine

Lähdeluettelo

8) Sometilit kuntoon, vinkit turvalliseen somettamiseen https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/sometilit-kuntoon-vinkit-turvalliseen-somettamiseen
9) Digitaalinen Eurooppa -ohjelman hakemuskoulutus 27.8.2024 https://www.kyberturvallisuuskeskus.fi/fi/digitaalinen-eurooppa-ohjelman-hakemuskoulutus-2782024
10) Suomalaiset organisaatiot Akira-kiristyshaittaohjelmien kohteena https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suomalaiset-organisaatiot-akira-kiristyshaittaohjelmien-kohteena
11) Kyberhyökkäys Lontoon sairaaloihin – Leikkauksia perutaan, potilaita siirretään https://www.hs.fi/maailma/art-2000010476767.html
12) Critical incident over London hospitals' cyber-attack https://www.bbc.com/news/articles/c288n8rkpvno
13) Services disrupted as London hospitals hit by cyber-attack https://www.theguardian.com/society/article/2024/jun/04/cyber-attack-london-hospitals
14) Internet Organised Crime Threat Assessment (IOCTA) 2024 https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024
15) Kyberturvallisuuskeskuksen viikkokatsaus - 30/2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-302024

Lähdeluettelo

16) Traficomin ajoneuvorekisterin tietoja käytetty väärin https://traficom.fi/fi/ajankohtaista/traficomin-ajoneuvorekisterin-tietoja-kaytetty-vaarin
17) Positiivisesta luottotietorekisteristä kysytty luottotietorekisteriotteita väärin perustein https://www.vero.fi/positiivinenluottotietorekisteri/tietoa-rekisterista/uutishuone/Uutiset/positiivisesta-luottotietorekisterista-kysytty-luottotietorekisteriotteita-vaarin-perustein
18) Miten toukokuussa paljastunut massiivinen tietovuoto tapahtui? Asiakirjat paljastavat, että keskiöön joutui pikkukaupungin autokorjaamo https://www.hs.fi/suomi/art-2000010499479.html
19) EDPB adopts statement on DPAs role in AI Act framework, EU-U.S. Data Privacy Framework FAQ and new European Data Protection Seal https://www.edpb.europa.eu/news/news/2024/edpb-adopts-statement-dpas-role-ai-act-framework-eu-us-data-privacy-framework-faq_en
20) Euroopan tietosuojaneuvostolta lausunto tietosuojaviranomaisten roolista tekoälyasetuksen valvonnassa https://tietosuoja.fi/-/euroopan-tietosuojaneuvostolta-lausunto-tietosuojaviranomaisten-roolista-tekoalyasetuksen-valvonnassa