TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Tammikuu 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

Vuosi 2023 aloitetaan ensimmäisellä päivittyneellä Kybersäällä. Uutta on niin sisällössä kuin päivittyneessä ulkoasussa.

CrowdStrike-tietoturvayhtiön raportin mukaan ensimmäisestä järjestelmään sisälle pääsystä hyökkääjällä kesti keskimäärin 1 tunti ja 38 minuuttia suorittaa tunkeutuminen syvemmälle kohteeseen.

Palvelunestohyökkäysten osalta tammikuu oli hiljainen. Ilmoitusten määrä väheni peräti 71% joulukuun huippulukemista.

Kybersää tammikuu 2023

Tietomurrot ja -vuodot

- Microsoft Office 365 -kalasteluaallon seurauksena yksittäisiä tilejä on onnistuttu murtamaan. **Monivaiheinen tunnistautuminen** on myös pelastanut murrolta![1]
- Sosiaalisen median tileihin kohdistuu edelleen aktiivisia murtokampanjoita.[2]

Huijaukset ja kalastelut

- ”Hei äiti”-tekstiviestihuijauksilla pyritään voittamaan kohteen luottamus. Tutustu ohjeisiimme tilien suojaamiseksi![1]
- ”Oletko tällä videolla?” Facebookissa leviävä Messenger-huijaus varastaa tilinhaltijan tunnukset.[2]

Haittaohjelmat ja haavoittuvuudet

- Alkuvuosi on ollut hiljainen haittaohjelmailmoituksien osalta.
- Vuonna 2021 julkaistussa haavoittuvuustiedotteessa mainittu VMWare ESXi -ohjelmisto on syytä päivittää tai huolehtia siitä, ettei haavoittuva palvelu ole saavutettavissa internetistä.[3]

Automaatio ja IoT

- EU on puuttunut älylaitteiden tietoturvaan. Uudet vaatimustenvastaiset älytuotteet voidaan poistaa EU-markkinoilta 1.8.2024 lähtien.[7]
- Suomessa myydyissä verkkokameroissa on havaittu tietoturvapuutteita. Muistutamme tietoturvallisen käytön ja asetusten tärkeydestä.[4]

Verkkojen toimivuus

- Tammikuussa yleisissä viestintäpalveluissa oli viisi merkittävää toimivuushäiriötä.
- Ilmoitettujen palvelunestohyökkäysten määrä laski loppuvuodesta, mutta osalla hyökkäyksistä oli vaikutuksia palveluihin.[2]

Vakoilu

- Sosiaalista mediaa hyödynnetään kohdistetun tietojenkalastelun valmistelussa.
- Yhdistyneen kuningaskunnan tietoturvaviranomaisen mukaan kohteena ovat olleet esimerkiksi tiedemaailma, valtiolliset organisaatiot, kansalaisjärjestöt, ajatushautomot sekä poliitikot, toimittajat ja aktivistit.[4]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

VMWare ESXi –ohjelmiston haavoittuvuus on syytä päivittää heti, tai huolehtia ettei haavoittuva palvelu ole saavutettavissa internetistä. Kampanjan laajuuden vuoksi päivittämättömien palvelinten voi olettaa olevan murrettu.(3)

Salasanojen hallintasovellus auttaa salasanojen säilyttämisessä ja käytössä eri nettipalveluissa. Hallintasovelluksen avulla vahvan salasanan luominen eri tileille suojaa paremmin tietovuodoissa paljastuneiden salasanojen rikollista käyttöä vastaan.(5)

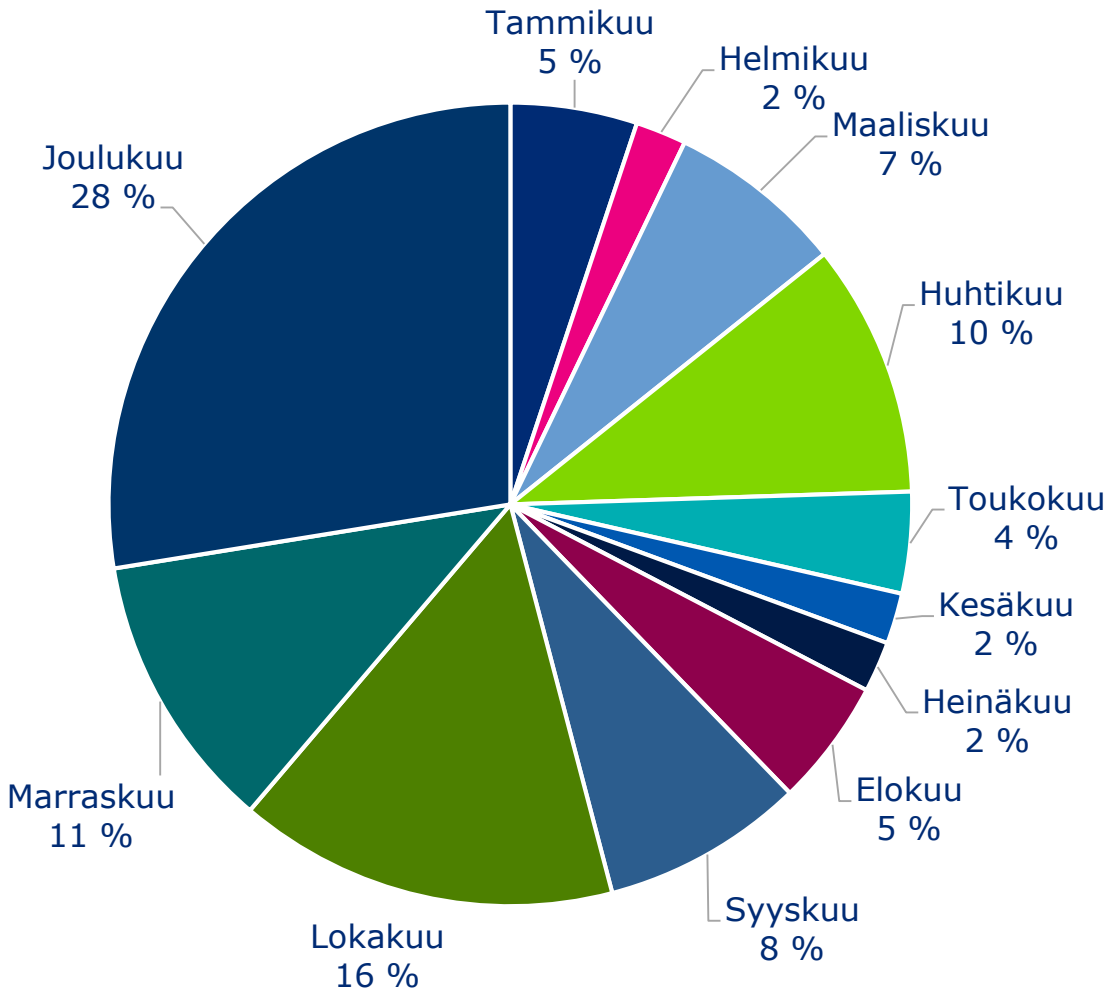
Liikenne- ja viestintävirasto Traficom on myöntänyt tietoturvan kehittämisen tukea ensimmäisille yrityksille. Tuen tavoitteena on nostaa yritysten tietoturvallisuuden tasoa ja sitä kautta parantaa koko yhteiskunnan kykyä suojautua kyberturvallisuusuhkia vastaan.(6)

Kyberturvallisuuskeskuksen havaintojen mukaan nykylaitteiden tietoturva on oletuksena usein heikko. 1.8.2024 alkaen tietoturvavaatimusten vastaiset laitteet voidaan poistaa myynnistä EU:n radiolaitedirektiivin nojalla. Tulevaa sääntelyä silmällä pitäen valmistajien, maahantuojien ja myyjien pitää varmistaa tuotteiden tietoturvataso heti.(7)

Tammikuun kyber-turvallisuuden yleiskuva

- Tammikuu oli tietoturvapoikkeamien osalta edellisvuotta hiljaisempi, eikä laajavaikutteisia merkittäviä yksittäisiä tietoturvapoikkeamia ilmennyt.
- Tammikuuta sävyttivät kuitenkin haktivistiryhmien kuten Killnetin innoittamat palvelunestohyökkäykset.
- Palvelunestohyökkäyksiä kohdistui Euroopan ja Yhdysvaltojen lisäksi myös Suomeen esimerkiksi Helsingin ja Uudenmaan sairaanhoitopiirin verkkosivuille. Silti ilmoitettujen tapausten määrä laski 71% vuoden 2022 joulukuusta.

Palvelunestohyökkäykset Suomessa vuonna 2022

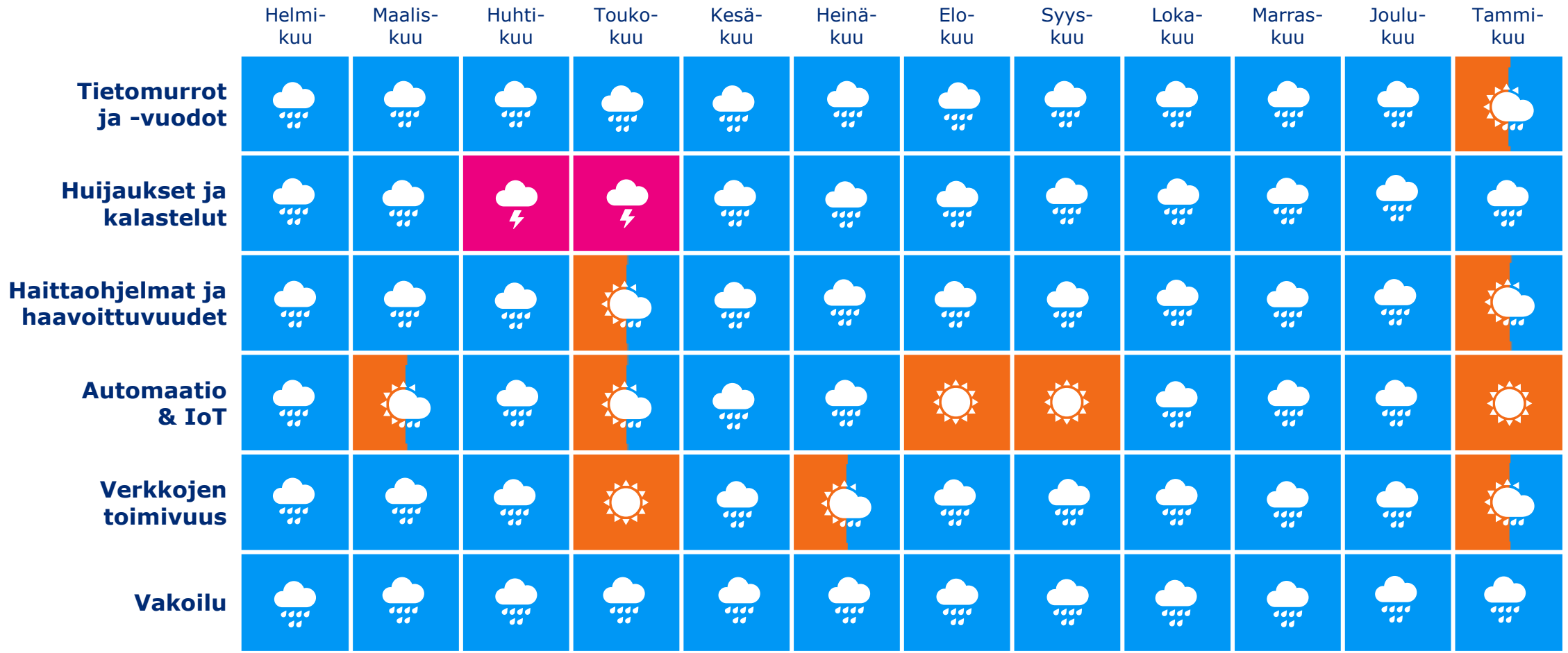


Ilmiöiden ja toimialojen trendit

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

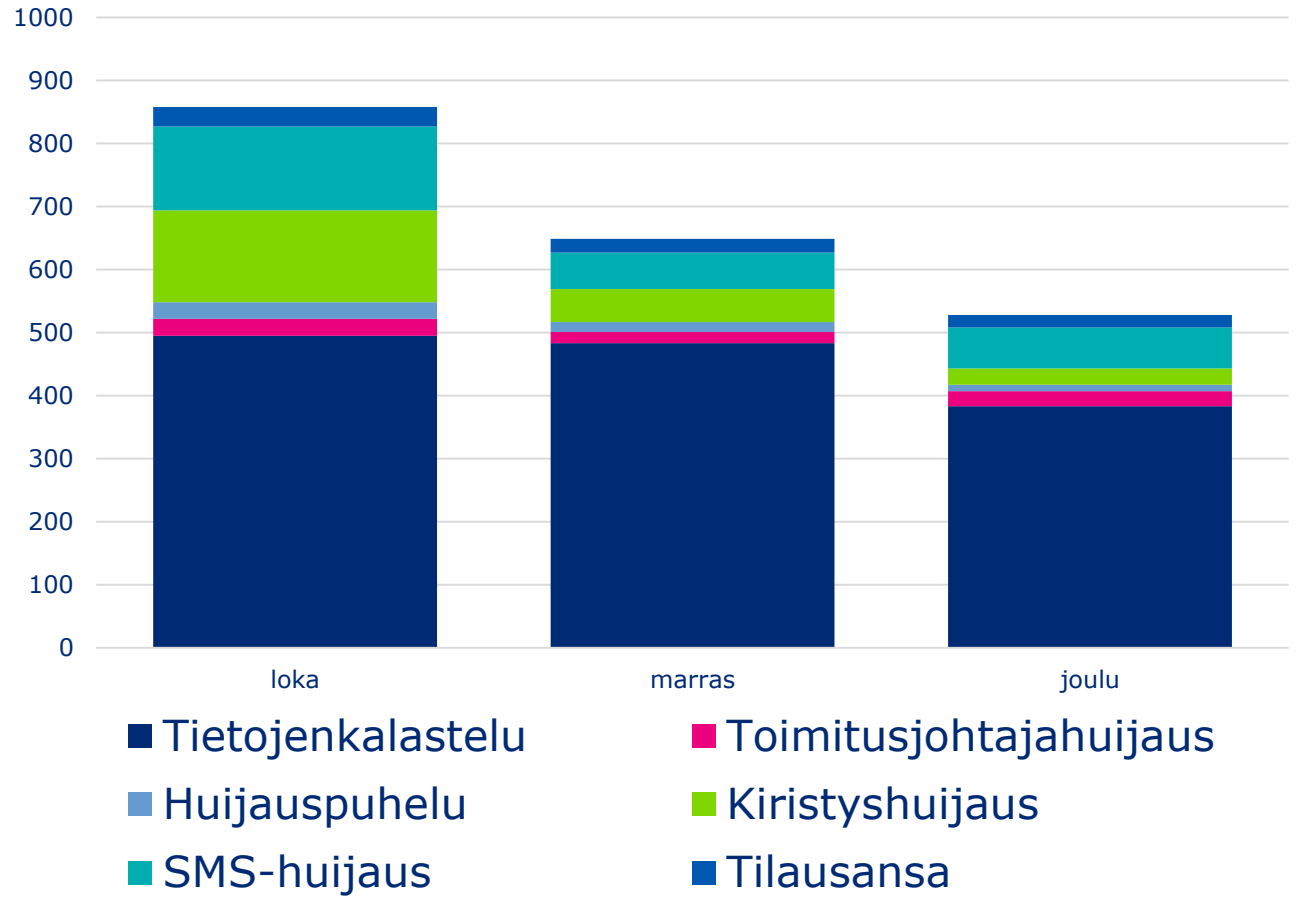


Käsiteltyjä huijaustapauksia
Q4/2022

3 kk

Vuoden 2022 viimeisen neljänneksen ilmiöitä ovat:

- Vuoden vaihdetta kohden huijausten kokonaismäärä näytti rauhoittuvan. Silti kalasteluhuijarit ovat edelleen hyvin kiinnostuneita erityisesti pankkitunnuksista.
- Suurin osa tekstiviestihuijauksista kalastelee pankkitunnuksia.
- Poliisiaiheisia kiristyshuijauksia saadaan edelleen samaan tapaan kuin muuallakin Euroopassa.

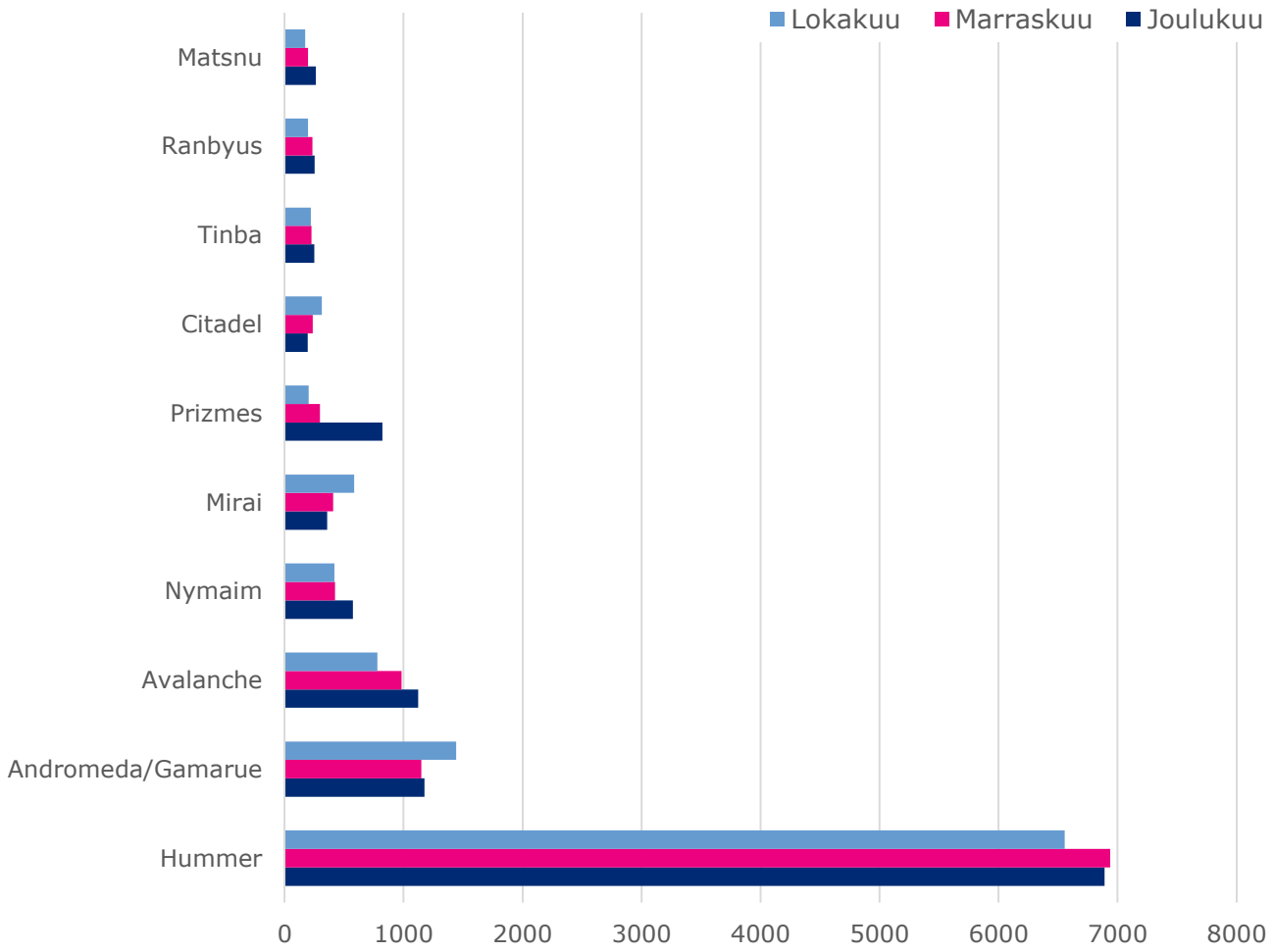


3 kk

Autoreporterin haittaohjelmahavainnot

Torjumme haittaohjelmia yhteistyössä teleyritysten kanssa **Autoreporter-järjestelmän** avulla. Järjestelmä saa tietoja Suomesta lähtöisin olevasta haittaohjelmaliikenteestä lähes kaikkialta maailmasta. Tiedot välitetään liittymiä ylläpitäville teleyrityksille, jotka ilmoittavat havainnoista asiakkailleen.

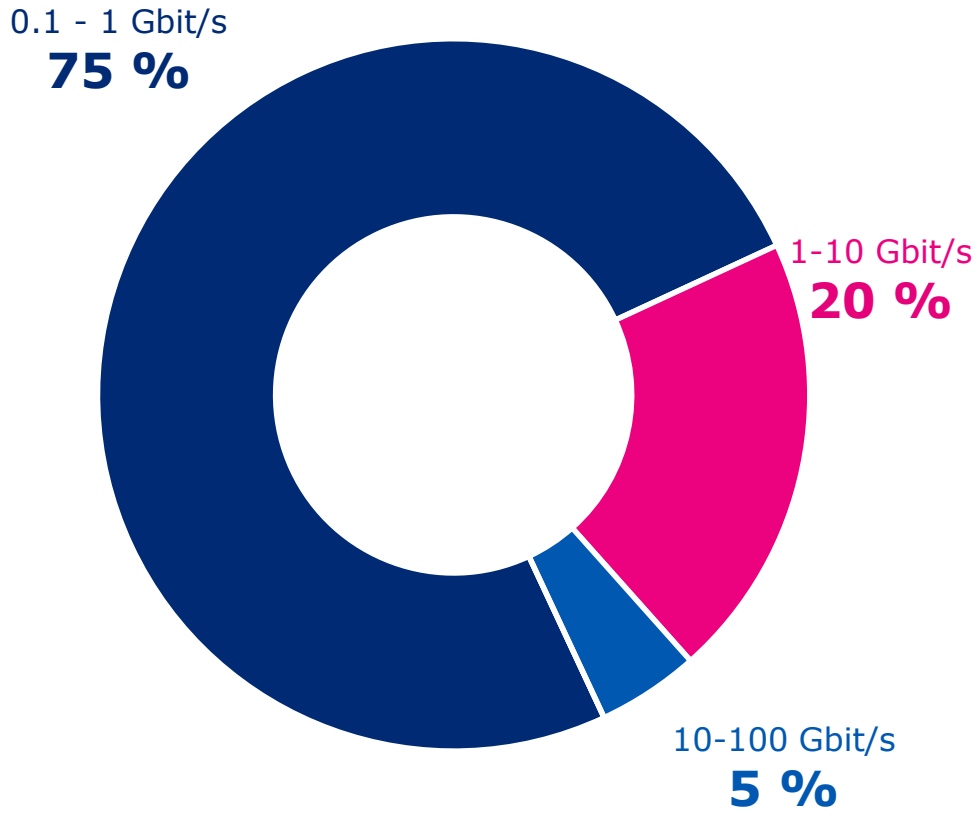
Tilastossa kerromme **10 yleisintä ja nimettyä** haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla. Autoreporterin tietoihin voi perehtyä tarkemmin Kyber-turvallisuuskeskuksen verkkosivuilla.



3 kk

Palvelunestohyökkäysten tunnuslukuja
Q4/2022

- **52 Gbit/s** oli suurin Suomessa nähty palvelunestohyökkäys Q4/2022.
- Noin 73% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



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

Pitkän aikavälin kybersää:
Tekoälyn läpimurto kyberrikollisuudessa lähenee

Teknologian kehittyessä myös sen lainvastainen hyödyntäminen lisääntyy. Toistaiseksi tekoälyn hyödyntäminen on ollut osa edistyneimpien uhkatoimijoiden keinovalikoimaa, mutta avoimesti saatavilla olevat kehittyneemmät palvelut mahdollistavat tekoälyn hyödyntämisen myös matalamman tason rikollisille.

- Todennäköisesti kalasteluviestit, romanssihuijaukset ja toimitusjohtajahuijausten kaltaiset kampanjat muuttuvat sisällöllisesti laadukkaammiksi ja vaikeammin tunnistettaviksi.
- Kyberhyökkäykseen kuuluvat aikaisen vaiheen toimet ovat tekoälyn hyödyntämisessä lähitulevaisuudessa yhä houkuttelevimpia, sillä ne kohdistuvat useammin ihmisiin kuin koneisiin.
- Organisaation onkin keskityttävä ensisijaisesti kouluttamaan henkilöstöään tunnistamaan tiedusteluun, ensimmäiseen pääsyyn ja tunnuksien saamiseen kohdistuvia hyökkäysyrityksiä.
- Kyberturvallisuuskeskus on julkaissut Tekoälyn mahdollistamat kyberhyökkäykset –raportin(16) joulukuussa 2022. Raportissa on ennakoitu viiden vuoden aikajanalla tekoälyn mahdollistamia todennäköisiä hyökkäysmenetelmiä.

Top 5 uhat lähitulevaisuudessa
(6kk–2v)

1.

Talouden ja politiikan ilmiöt heijastuvat myös kyber-turvallisuuteen.

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

2.

Suomeen kohdistunut kyberympäristön uhkataso on edelleen kohonneella tasolla.

Kohonneen uhkatason vuoksi organisaatioiden varautumisen merkitys korostuu.

3.

Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista.

Esimerkiksi käyttäjäoikeuksien hallinta, ohjelmistojen ajantasaisuuden ylläpito ja hyvä tietoturvakulttuuri ovat kyberturvallisuuden kivijalkaa.

Symbolit

Uusi

Päivitetty

4.

Toimitus- ja palveluketjujen tietoturva ja jatkuvuus ovat yhä kriittisempiä.

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

5.

Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille!

Tarve kyberturvallisuuden osaajille monipuolistuu. Uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisää entisestään tarvetta osaajille.

1. Talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen

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

- Venäjän hyökkäys Ukrainaan heijastuu myös kyberturvallisuuteen. Esimerkiksi sodan aiheuttamat muutokset talouteen, energian hinnan nopea nousu ja informaatioympäristön herkkyys näkyvät vaikeasti ennakoitavina kehityskulkuina, jotka ulottuvat myös digitaaliseen maailmaan.
- Valtioiden ja organisaatioiden päätökset altistavat entistä helpommin vaikuttamiselle, kuten mielenilmauksena tehdyille palvelunestohyökkäyksille.
- Energiamarkkinoiden häiriöt voivat vaikuttaa myös kyberturvallisuuteen. Kriittiseen infrastruktuuriin vaikuttaminen voi näkyä myös kyberympäristön häiriöinä Euroopassa.
- Organisaatioiden on tärkeää tunnistaa oman toimintaympäristönsä riskitekijät. Niillä voi olla isoja vaikutuksia organisaatioiden päivittäiseen toimintaan. Organisaatioiden tulee huomioida omassa riskienhallinnassaan ja jatkuvuussuunnittelussaan toimintaympäristön muutokset ja sen aiheuttamat uhkat kriittisille prosesseille.

1. Case: Palvelunestohyökkäykset lisääntyivät merkittävästi vuonna 2022

Palvelunestohyökkäysten määrä lisääntyi niin Suomessa kuin Euroopassakin vuonna 2022. Myös niiden käyttötapa poliittisena mielenilmauksena korostui.

Palvelunestohyökkäyksiä tekevien tahojen motiivit ja kyvyt vaihtelevat runsaasti. Suurimmassa osassa palvelunestohyökkäyksiä vaikutukset ovat olleet pieniä, ja hyökkäyksiä käytetäänkin paljolti mielenilmauksena esimerkiksi valtion tai muun tahon päätösten vuoksi. Palvelunestohyökkäysten taustalla on yhä useammin erilaisia haktivistiryhmiä, jotka toimivat ilman selkeää keskitettyä ohjausta.

Palvelunestohyökkäysten lisääntynyt trendi tulee todennäköisesti jatkumaan, eikä ilmiötä lieventäviä tekijöitä ole nähtävissä. Organisaatioiden riskienhallinta, varautuminen ja harjoittelu ovat avainasemassa uhkiin varautumisessa. Kyberturvallisuuskeskus tarjoaa varautumiseen useita ohjeita.(8)

2. Suomeen kohdistunut kyberympäristön uhkataso on edelleen kohonneella tasolla.

Kyberhyökkäykset ovat lisääntyneet 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.
- Erityisesti huoltovarmuuskriittisten organisaation joutuessa kiristyshaittaohjelman uhriksi yhteiskunnan elintärkeät toiminnot voivat vaarantua.
- Suojelupoliisi on todennut kansallisen turvallisuuden katsauksessaan kriittiseen infrastruktuuriin kohdistuvan tiedustelun ja vaikuttamisen uhkan pysyvän kohonneena lähitulevaisuudessa.(10)
- Vaikka tavanomaisten kyberhyökkäysten määrä on kokonaisuudessaan kasvanut, myös mm. kohdennetut tietojenkalasteluviestit ja murtautumisyritykset ovat lisääntyneet.
- Tutustu Kyberturvallisuuskeskuksen tiedotteeseen kohonneesta kyberuhkatasosta.(9)

3. Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista.

Organisaation kyberturvallisuuden kivijalka rakennetaan arkisilla kyberturvallisuuden toiminnoilla. Suurin osa tietoturvapoikkeamista olisi vältettävissä tavanomaisilla keinoilla, kuten ohjelmistopäivityksillä, hyvillä salasanakäytänteillä ja tietoturvakulttuurilla.

- Käyttöoikeuksien kontrollointi on organisaatioissa tärkeää. Erilaisia hyökkäyskeinoja voidaan hyödyntää tunnusten haltuun saamiseksi.
- Haavoittuvuuksien hyväksikäyttö on nopeaa. Verkkoon saatetaan jättää auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu.
- Tietojen kalastelu on edelleen helppo ja yleinen tapa rikolliselle pyrkiä organisaatioon sisälle. Tietoisuuden lisääminen organisaatiossa auttaa tunnistamaan epäilyttävän toiminnan.
- Suurin osa loppuvuonna 2022 tapahtuneista tietoturvapoikkeamista olisi ollut estettävissä hyvin arkisella kyberturvallisuuden hallinnan ylläpidolla.

- Kyberturvallisuuskeskus tarjoaa organisaatioille runsaasti käytännön ohjeita kyberturvallisuuden parantamiseksi.(11)

4. Toimitus- ja palveluketjujen tietoturva ja jatkuvuus on yhä kriittisempää.

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

- Organisaatioiden on keskeistä ymmärtää omat alihankkijaketjunsa. On tärkeä selvittää kolmannen osapuolen tietoturvan taso ja ulottaa tietoturvallisuuden hallinta myös palveluihin. Esimerkiksi:
  - Konsultit ja heidän oman organisaation 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.
- Organisaation tulisi kartoittaa, mistä osista sen eri palvelut muodostuvat, jotta ison kokonaisuuden voi hahmottaa. Esimerkiksi pilvipohjaista palvelua hankkiessa tällaisen tekeminen on oleellista.
- On hyvä ymmärtää, että käytettävien palvelujen kautta voidaan murtautua organisaation, jos kyberturvallisuutta ei ole huomioitu.

5. Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille!

Uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisää entisestään tarvetta erilaisille osaajille.

- Yritykset eivät etsi pelkkiä koodareita. Tulevaisuudessa laaja-alaisemmalle digitalisaation, kyberturvallisuuden ja datan osaamiselle on entistä enemmän kysyntää.
- Osaamisen saaminen riittävälle tasolle kestää vielä pitkään. Organisaatioiden kyberturvallisuus vaarantuu, mikäli osaavaa henkilöstöä ei ole tarpeeksi saatavilla.
- Arviomme mukaan lyhyen aikavälillä tarvitaan erityisesti teknisiä osaajia, jotka osallistuvat tietoturvatutkintaan sekä ennaltaehkäisevään työhön.
- Pitkällä aikavälillä osaajatarve monipuolistuu ja esimerkiksi hallinnollisia osaajia tarvitaan lisää.
- Osaajapula ei ole kiinni määrästä vaan laadusta! Osaaminen ei saisi henkilöityä liikaa, jotta jatkuvuus voidaan turvata kaikissa tilanteissa. Organisaation tietoturvan hallinta tulee osallistaa ja kouluttaa osaksi kaikkien työntekijöiden päivittäistä toimintaa.
- Johdon tulee ymmärtää ja varmistaa riittävä osaaminen organisaatiossa kyberturvallisuusosaajien kysynnän kasvaessa. On tärkeää miettiä, millaista asiantuntemusta tarvitaan nyt ja tulevaisuudessa, sekä miten se hankitaan.

Tietoturva-alan kehitys, sääntely ja standardit

Osiossa kerromme keskeisistä uudistuksista esimerkiksi alaa koskevan lainsäädännön tai asetusten päivityksiin liittyen. Kerromme organisaatioille tärkeää kyberturvallisuustietoa ja Kyberturvallisuuskeskuksen ajankohtaisia asioita.

Oikeudelliset asiat

Kyberturvallisuusdirektiivin (NIS2) kansallinen toimeenpanohanke käynnistynyt

- EU:n kyberturvallisuusdirektiivi (nk. NIS2-direktiivi) julkaistiin 27.12.2022. Uusi direktiivi korvaa aiemman verkko- ja tietoturvadirektiivin (NIS-direktiivi).
- Liikenne- ja viestintäministeriö on 2.1.2023 käynnistänyt kansallisen toimeenpanohankkeen NIS2-direktiivin velvoitteiden saattamiseksi osaksi kansallista lainsäädäntöä. Määräaika kansalliselle toimeenpanolle on 21 kk direktiivin julkaisusta.(13)
- NIS2-direktiivi koskettaa laajasti yhteiskunnan kriittisillä toimialoilla toimivia yrityksiä mm. kyberturvallisuutta koskevien riskienhallintatoimenpiteiden ja merkittäviä poikkeamia koskevan ilmoitusvelvollisuuden osalta.
- Direktiivi myös jatkaa jäsenvaltioiden olemassa olevia yhteistyömekanismeja ja tiivistää eri viranomaisten välistä yhteistyötä.

Oikeudelliset asiat

Avaruussektorin maa-asema- ja tutkatoiminnan turvallisuutta edistetään - toiminta jatkossa luvanvaraista(13)

- Laki maa-asemista ja eräistä tutkista tuli voimaan 1.2.2023 alkaen.
- Toimivaltaisena lupa- ja valvontaviranomaisena toimii Liikenne- ja viestintävirasto Traficom.
- Lain tarkoittamaa säänneltyä maa-asematoimintaa on tiedon ja signaalien vastaanottaminen avaruudesta eri järjestelmistä ja lähettäminen avaruuteen.
- Tutkatoiminnan osalta toimiluvanvaraiseksi tulee radiosignaalien ja laserpulssien lähettäminen yläilmakehään tai avaruuteen ja näistä heijastuneiden tutkakaikujen vastaanottaminen.

Oikeudelliset asiat

Galileon PRS-palvelun käyttöönottoa koskevia lainmuutoksia voimaan 1.1.2023

- Sähköisen viestinnän palveluista annettuun lakiin on tehty muutoksia, jotta Galileo-satelliittipaikannusjärjestelmän julkisesti säännelty satelliittipalvelu (PRS-palvelu) on mahdollista ottaa Suomessa kansallisesti käyttöön vuoden 2025 aikana.(14)
- Lakiin lisättiin säännökset julkisesti säännellyn satelliittipalvelun vastuuviranomaisesta, palvelun tarjoamisesta, palveluntarjoajan henkilöstöstä, alihankkijasta, palvelun käyttämisestä, teknologian valmistamisesta, vientivalvonnasta sekä Liikenne- ja viestintäviraston tarkastusoikeudesta.
- Liikenne- ja viestintävirasto Traficom hallinnoi eurooppalaisen Galileo-satelliittipaikannusjärjestelmän PRS-palvelua Suomessa.
- Palvelu on tarkoitettu viranomaisille, kuten esimerkiksi pelastus- ja turvallisuusviranomaisille sekä huoltovarmuuskriittisille yrityksille.

Oikeudelliset asiat

Irlannin tietosuojaviranomainen määräsi seuraamusmaksuja Facebookille ja Instagramille Euroopan tietosuojaneuvoston ratkaisun perusteella

- Euroopan tietosuojaneuvoston antamien sitovien päätösten perusteella Irlannin tietosuojaviranomainen on antanut 31.12.2022 ratkaisut, joissa Facebook ja Instagram määrättiin maksamaan 390 miljoonan euron seuraamusmaksut.(15)
- Facebook ja Instagram ovat käsitelleet henkilötietoja käyttäytymiseen perustuvaa mainontaa varten ilman lainmukaista oikeusperustetta.
- Käyttöehtojen hyväksyminen ei ollut riittävä oikeusperuste käsittelylle, sillä käyttäytymiseen perustuvan mainonnan ei katsottu kuuluvan Facebookin ja Instagramin ydintoimintoihin.
- Euroopan tietosuojaneuvoston mukaan kyseisillä päätöksillä voi olla merkittävä vaikutus myös muihin alustoihin, joiden liiketoimintamallin keskiössä on käyttäytymiseen perustuva mainonta.

Epäiletkö tietoturvaloukkausta?

Jos teihin on kohdistunut tai epäilette teihin kohdistuneen tietoturvaloukkauksen, olkaa yhteydessä meihin.

- Sähköinen lomake: https://www.kyberturvallisuuskeskus.fi/fi/ilmoita
- Sähköposti: cert@traficom.fi
- Puhelin: 0295 345 630 (arkisin klo 9-15)

Muissa asioissa voitte olla meihin yhteydessä osoitteessa kyberturvallisuuskeskus@traficom.fi

Kyberturvallisuuskeskuksen eri toimintojen ja hankkeiden yhteystiedot löydät keskitetysti täältä: https://www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot

Lähdeluettelo

1) Viikkokatsaus 03/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-32023

2) Viikkokatsaus 04/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-42023

3) Haavoittuvuustiedote Wmware-tuotteissa https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuuksia-vmwaren-tuotteissa-paivita-heti

4) Viikkokatsaus 05/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-52023

5) Neuvoja salasanan hallintaohjelmiston käyttöönottoon https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon

6) Tietoturvan kehittämisen tukea myönnetty ensimmäisille yrityksille vauhdittamaan tietoturvaa parantavien toimenpiteiden toimeenpanoa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvan-kehittamisen-tukea-myonnetty-ensimmaisille-yrityksille-vauhdittamaan

7) Älylaitteiden heikko tietoturva sääntelyllä kuriin https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/alylaitteiden-heikko-tietoturva-saantelylla-kuriin

Lähdeluettelo

8) Toimintaohje palvelunestohyökkäyksiin https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Palvelunestohy%C3%B6kk%C3%A4ysToimintaohje.pdf

9) Tiedote kohonneesta kyberympäristön uhkatasosta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt

10) Suojelupoliisin kansallisen turvallisuuden katsaus https://supo.fi/kansallisen-turvallisuuden-katsaus

11) Kyberturvallisuuskeskuksen ohjeet ja oppaat organisaatioille https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille

12) Kyberturvallisuusdirektiivi vahvistaa koko EU:n kyberturvallisuustasoa – kansallinen toimeenpanohanke käynnistyi https://www.lvm.fi/-/kyberturvallisuusdirektiivi-vahvistaa-koko-eu-n-kyberturvallisuustasoa-kansallinen-toimeenpanohanke-kaynnistyi-1903681

13) Avaruussektorin maa-asema- ja tutkatoiminnan turvallisuutta edistetään - toiminta jatkossa luvanvaraista https://traficom.fi/fi/ajankohtaista/avaruussektorin-maa-asema-ja-tutkatoiminnan-turvallisuutta-edistetaan-toiminta

Lähdeluettelo

14) HE 170/2022 vp https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_170+2022.aspx

15) Tietosuojavaltuutetun toimisto: Euroopan tietosuojaneuvosto julkaisi Facebookia ja Instagramia koskevat kiistanratkaisupäätökset https://tietosuoja.fi/-/euroopan-tietosuojaneuvosto-julkaisi-facebookia-ja-instagram-koskevat-kiistanratkaisupaatokset-merkittava-vaikutus-henkilotietojen-kayttoon-kayttaytymiseen-perustuvassa-mainonnassa-

16) Tekoälyn mahdollistamat kyberhyökkäykset https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/tekoalyn-mahdollistamat-kyberhyokkaykset