TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Elokuu 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

1.9.

Traficomin määräys teletoiminnan tietoturvasta tuli voimaan 1.9.2024. Päivityksellä parannetaan viestintäverkkojen tietoturvaa asettamalla uusia velvoitteita mm. haitallisen liikenteen suodatukseen, reitityksen suojaamiseen, asiakkaan tunnistamiseen ja uuden sukupolven verkkojen turvallisuuteen.[1]

1 kk

Kyberturvallisuusdirektiivin eli NIS2-direktiivin soveltamisalaan kuuluviin toimijoihin kohdistuvia velvoitteita on sovellettava kansallisesti viimeistään kuukauden päästä, 18.10.2024 alkaen.

1 v

Vuosi laitteiden kyberturvallisuusvaatimuksiin: Kaikkien EU-markkinoille saatettavien IoT-laitteiden täytyy olla radiolaitedirektiivin delegoidun tietoturvasäädöksen mukaisia 1.8.2025 alkaen. IoT-laitteella tarkoitetaan tässä yhteydessä säädöksen soveltamisalaan lukeutuvia radiolaitteita. Viranomainen voi poistaa vaatimustenvastaiset tuotteet markkinoilta.[2]

Kybersää elokuu 2024

Tietomurrot ja -vuodot

- Tietomurroissa kesä jatkui rauhallisena, eikä tavanomaista syksyistä kasvua ilmoitusmäärissä ole nähty.

Huijaukset ja kalastelut

- Veronpalautukset olivat elokuun suosituin huijausten aihe. Kymmenillä erilaisilla tekstiviestihuijauksilla yritettiin varastaa verkkopankkitunnuksia.
- Pankkitunnuksia kalasteltiin muillakin verukkeilla, kuten sähköyhtiön, teleoperaattorin, Kanta-palvelun, viranomaisten ja tietysti myös pankkien nimissä.

Haittaohjelmat ja haavoittuvuudet

- SonicWall SSL VPN -haavoittuvuutta hyväksikäytetään aktiivisesti.
- Havaintoja on tehty tavanomaista enemmän Quad7- ja Mirai-bottiverkoista.
- Laitteiden päivitys ja vanhojen uusiminen korostuvat edelleen tietoturvauhkilta suojautumisessa.

Automaatio ja IoT

- IoT-järjestelmien hallinta siirtyy yhä enemmän pilveen. Julkisuudessa tuotiin esiin, ettei hajautetun sähköntuotannon ja sähkön varastoinnin pilvipohjaisten etähallintajärjestelmien kyber-turvallisuus ole aina riittävän hyvä.[3, 4, 5]
- Palveluiden loppukäyttäjien kannalta tilanne on hankala, ellei turvallisia vaihtoehtoja ole tarjolla.

Verkkojen toimivuus

- Elokuussa yleisissä viestintäverkoissa havaittiin 10 toimivuushäiriötä.
- Viime aikoina on raportoitu paljon lyhytkestoisia palvelunesto-hyökkäyksiä suomalaisten organisaatioiden palveluihin. Vaikutukset ovat kuitenkin olleet vähäisiä.

Vakoilu

- APT29:n kerrottiin päässeen käsiksi joihinkin Iso-Britannian valtionhallinnon sähköposteihin Microsoftiin kohdistuneen tietomurron seurauksena.[6]
- Sama toimija hyödynsi kaupallisten vakoiluohjelmien käyttämiä menetelmiä Mongoliassa. Kohteisiin murtautumisessa hyödynnettiin murrettua valtionhallinnon verkkosivua.[7]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Uhka-analyysi ja uhkamallinnus ovat keskeisiä työkaluja kyberturvallisuusriskien hallinnassa. Uhka-analyysin teko ja uhkamallinnuksen käyttöönotto ja ajan tasalla pitäminen tarjoavat järjestelmällisen menetelmän kyberturvallisuusriskien tunnistamiseen ja varautumiseen. Julkaisimme aiheesta artikkelin.[8]

Kotiverkon ja reitittimen tietoturva -ohjeemme on edelleen ajankohtainen.[9] Viime aikoina olemme havainneet tavallista enemmän kahden kotireitittimiä haltuunsa ottavan bottiverkon toimintaa Suomessa. Bottiverkkoja hyödynnetään sekä osana hajautettuja palvelunestohyökkäyksiä että haitallisen verkkoliikenteen välityspisteenä kyberhyökkäyksissä.[10]

Microsoft aloittaa vaiheittain pakotetun monivaiheisen tunnistautumisen käyttöönottamisen Azure-, Intune- ja Entra ID -pääkäyttäjäportaaleissa. Osana MFA:n käyttöön pakottamista Microsoft suosittelee luomaan nk. Break glass -tunnukset. Lisätietoja tenanttikohtaisista aikatauluista löytyy yllämainittujen palveluiden Message Centereistä.[11]

Elokuun kyberturvallisuuden yleiskuva

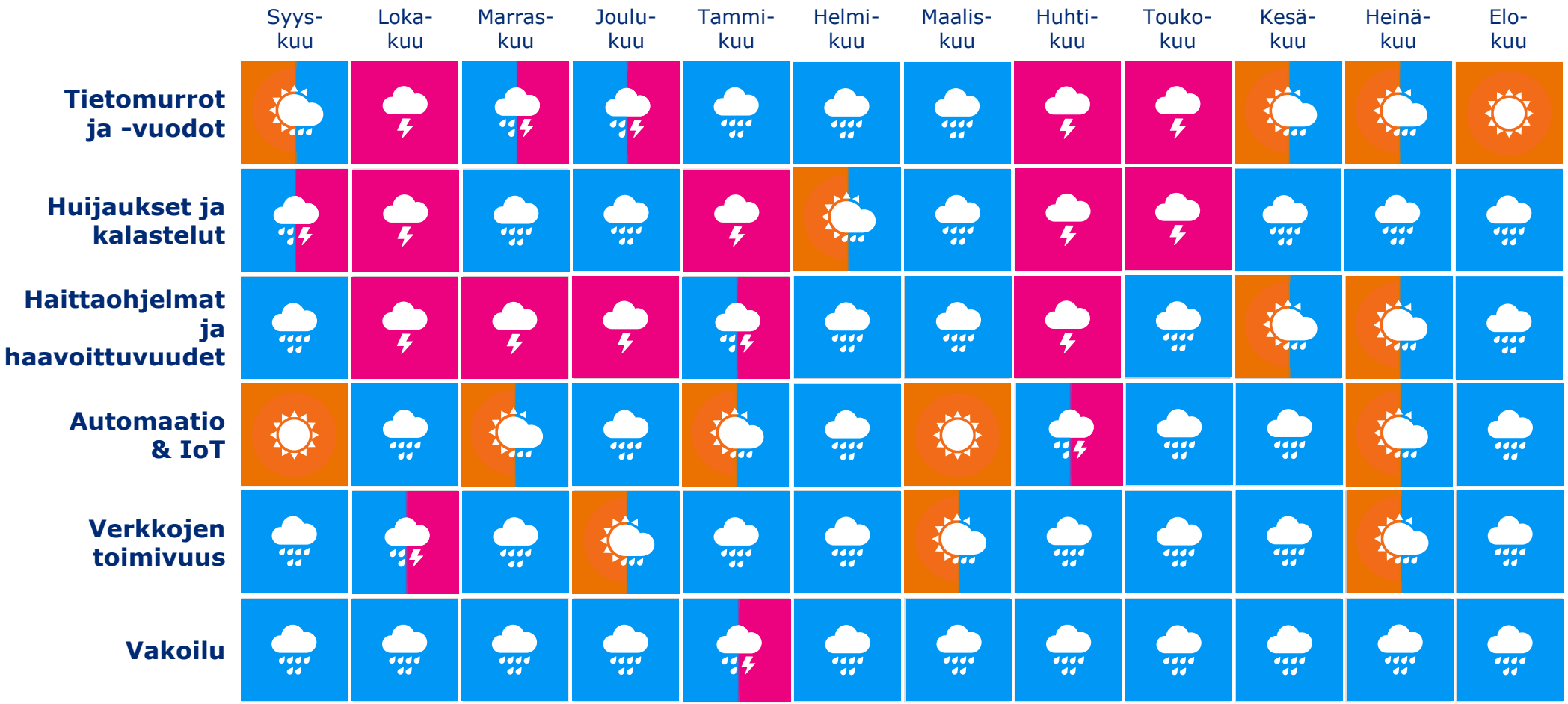
- Elokuu oli vastaanottamiemme tietoturvapoikkeamailmoitusten osalta poikkeuksellisen rauhallinen.
- Ilmoitetuissa tapauksissa korostuivat erilaiset kansalaisiin kohdistuvat kalastelu- ja huijauskampanjat. Etenkin suomi.fi-teemaiset kalasteluviestit kiusasivat elokuun puolivälissä. Myös veronpalautus-teema jatkuu.
- Varautumisen sekä jatkuvuussuunnittelun merkitykset korostuvat etenkin kiristyshaittaohjelmatapauksissa kaiken kokoisissa organisaatioissa ja yrityksissä.
  - Tietomurto voi aiheuttaa hyvin vakavia taloudellisia seurauksia. Kiristyshaittaohjelmahyökkäyksen vaikutukset voivat pahimmillaan lamauttaa organisaation toiminnan viikoiksi tai jopa lopullisesti.
  - Myös ilmoittamalla nopeasti poikkeamista on mahdollista saada paremmin ja tehokkaampaa apua poikkeaman selvittämiseen. Kyberturvallisuuskeskus voi parhaimmassa tapauksessa pystyä tarjoamaan työkaluja kiristyshaittaohjelman salauksen purkamiseen.
  - Julkaisimme elokuussa artikkelin kiristyshaittaohjelmien toiminnasta ja niiltä suojautumisesta.[12]

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 kyberturvallisuuden osaajille

Tekoälyn riskienhallinta

Toimitusketjujen tietoturva

Sääntelyn tulevaisuus

Pilvipalvelujen tietoturva

Teollisuusautomaation suojaaminen

IoT

6G

Kuluttajien tietoturva

Haavoittuvuuksien nopeutuva hyväksikäyttö

Kvanttiturvallinen krypto

Osallistuminen digitaalisessa ympäristössä

Pitkän aikavälin kybersää:
Pilvipalvelujen tietoturva

Viimeisen vuosikymmenen aikana pilvipalvelut ovat vakiintuneet osaksi organisaatioiden arkipäiväistä tietojenkäsittelyä. Niiden nopeus, kustannustehokkuus ja joustavuus houkuttelevat jatkuvasti uusia käyttäjiä. Samalla pilvipalveluihin liittyviä riskejä havaitaan edelleen.

- Organisaatioiden voi olla vaikea hahmottaa pilvipalveluratkaisujen kokonaisuus osana omaa tietojärjestelmäarkkitehtuuria. Lisäksi hybridiympäristöt aiheuttavat helposti monimutkaisten ympäristöjen konfigurointivirheitä ja puutteita uhkien valvonnassa. Useiden käyttäjien ja laitteiden käyttöoikeuksien hallinta eri pilvipalveluissa vaikeuttaa arkaluontoisten tietojen pääsynhallintaa.
- Pilvipalveluihin kohdistuvat kyberhyökkäykset ovat olleet myös viime aikoina paljon esillä. Organisaatioiden siirtyessä pilviympäristöihin siirtyvät sinne myös kyberuhkatoimijoiden tekemät kyberhyökkäykset. Kuten perinteisissä tietoverkoissa, jos hyökkääjä onnistuu tunkeutumaan pilven reunalle, voi hyökkääjä levittäytyä muihinkin verkon osiin. Tietoturvapoikkeamien selvittäminen ja tutkinnan toteuttaminen pilviympäristössä voi olla haastavaa, ellei näitä huomioida palveluja hankittaessa ja käyttöönotossa.
- Pilvipohjainen suojaus, tehokas käyttöoikeuksien hallinta ja säännöllinen koulutus auttavat vahvistamaan tietoturvaa. Monivaiheisen tunnistautumisen avulla voidaan pienentää tunnusten luvattoman käytön riskiä ja Zero Trust -suojausmallilla rajoittaa pääsynhallintaa. Lisäksi säännölliset päivitykset, tietojen salaus ja valvonta hyökkäysten havaitsemiseksi ovat olennaisia suojaustoimia.

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

- EU:n tekoälysäädös astui voimaan 1.8.2024[13]
  - Tekoälysäädöksen tarkoituksena on varmistaa, että EU:ssa kehitetty ja käytetty tekoäly on luotettavaa ja että sillä suojataan ihmisten perusoikeuksia. Asetuksen tavoitteena on luoda yhdenmukaistetut tekoälyn sisämarkkinat EU:hun, kannustaa tämän teknologian käyttöönottoon ja luoda innovointia ja investointeja tukeva ympäristö.
  - Jäsenvaltioiden on 2.8.2025 mennessä nimettävä kansalliset toimivaltaiset viranomaiset, jotka valvovat tekoälyjärjestelmiä koskevien sääntöjen soveltamista ja toteuttavat markkinavalvontatoimia. Euroopan komission tekoälytoimisto on tekoälysäädöksen keskeinen täytäntöönpanoelin EU:n tasolla sekä yleiskäyttöisiä tekoälymalleja koskevien sääntöjen valvontaviranomainen.
  - Yrityksille, jotka eivät noudata sääntöjä, määrätään sakko. Sakot voivat olla enintään 7 prosenttia maailmanlaajuisesta vuotuisesta liikevaihdosta kiellettyjen tekoälysovellusten rikkomisista, enintään 3 prosenttia muiden velvoitteiden rikkomisesta ja enintään 1,5 prosenttia virheellisten tietojen toimittamisesta.
  - Suurinta osaa tekoälysäädöksen säännöistä aletaan soveltaa 2.8.2026. Sellaisia tekoälyjärjestelmiä koskevia kieltoja, joiden katsotaan aiheuttavan riskin, jota ei voida hyväksyä, sovelletaan kuitenkin jo kuuden kuukauden kuluttua, kun taas niin sanottuja yleiskäyttöisiä tekoälymalleja koskevia sääntöjä sovelletaan 12 kuukauden kuluttua.

Oikeudelliset asiat

- Digitaalinen identiteettilompakko: eIDAS-asetusta täydentävät täytäntöönpanosäädökset ovat valmisteilla[14, 15]
  - Uudistetun eIDAS-asetuksen keskeinen velvoite on, että kaikkien EU-jäsenvaltioiden pitää tarjota asetuksen vaatimukset täyttävä digitaalinen identiteettilompakko viimeistään kahden vuoden päästä teknisten täytäntöönpanosäädösten valmistumisesta.
  - Asetusta täydentäviä teknisiä täytäntöönpanosäädöksiä valmistellaan parhaillaan. Euroopan komissio julkaisi 9.9.2024 asti kommentoitavaksi täytäntöönpanosäädösten luonnokset, jotka koskevat eurooppalaisen digitaalisen identiteetin lompakon sertifiointia, tuettavia protokollia ja rajapintoja, henkilön tunnistetietoja ja sähköisiä attribuuttitodistuksia sekä eheyttä ja ydintoimintoja.
  - Valtiovarainministeriö vastaa kommentointipyyntöön olemassa olevan Suomen kannan mukaisesti. Suomen kanta löytyy valtioneuvoston U-kirjelmästä 41/2021 vp.

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) Uudistettu teletoiminnan tietoturvamääräys voimaan 1.9.2024 https://www.traficom.fi/fi/ajankohtaista/uudistettu-teletoiminnan-tietoturvamaarays-voimaan-192024

2) Komission delegoitu asetus (EU) 2022/30 https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32022R0030&from=EN

3) 512-bit RSA key in home energy system gives control of “virtual power plant” https://arstechnica.com/security/2024/08/home-energy-system-gives-researcher-control-of-virtual-power-plant/

4) 60 Hurts per Second – How We Got Access to Enough Solar Power to Run the United States https://www.bitdefender.com/blog/labs/60-hurts-per-second-how-we-got-access-to-enough-solar-power-to-run-the-united-states/

5) The gigantic and unregulated power plants in the cloud https://berthub.eu/articles/posts/the-gigantic-unregulated-power-plants-in-the-cloud/

6) Exclusive: Russian spies hacked UK government data and emails earlier this year https://therecord.media/russia-hack-uk-government-home-office-microsoft

7) State-backed attackers and commercial surveillance vendors repeatedly use the same exploits https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repeatedly-use-the-same-exploits/

Lähdeluettelo

8) Uhka-analyysi ja uhkamallinnus varautumisen työkaluina kyberturvallisuusriskien hallinnassa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uhka-analyysi-ja-uhkamallinnus-varautumisen-tyokaluina-kyberturvallisuusriskien

9) Kotiverkon ja reitittimen tietoturva https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/kotiverkon-ja-reitittimen-tietoturva

10) Kyberturvallisuuskeskuksen viikkokatsaus – 36/2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-362024

11) Kyberturvallisuuskeskuksen viikkokatsaus - 35/2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-352024#74271-1

12) Mikä ihmeen kiristyshaittaohjelma? https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/mika-ihmeen-kiristyshaittaohjelma

13) European Artificial Intelligence Act comes into force https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4123

14) Osallistu ja vaikuta! eIDAS-asetusta täydentäviä täytäntöönpanosäädöksiä voi nyt kommentoida https://dvv.fi/-/osallistu-ja-vaikuta-eidas-asetusta-taydentavia-taytantoonpanosaadoksia-voi-nyt-kommentoida

15) Valtioneuvoston U-kirjelmä U 41/2021 vp https://www.eduskunta.fi/FI/vaski/Kirjelma/Sivut/U_41+2021.aspx