TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Marraskuu 2024

#kybersää

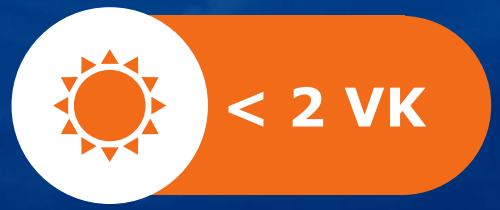
Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä.

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

Microsoft 365 -tunnusten kalastelu oli marraskuussa erityisen aktiivista. Tunnuksia kalasteltiin etenkin Dropbox-teemaisilla huijausviesteillä.



Merenalaisen C-Lion1-tietoliikennekaapelin korjaaminen vei alle kaksi viikkoa. Maalla tapahtuvat pystytään toteamaan ja korjaamaan jopa tunneissa.

Kybersää marraskuu 2024

Tietomurrot ja -vuodot

- M365-tilejä murrettiin aktiivisesti AiTM-kalastelusivuille johtavilla Dropbox-teemaisilla kalasteluviesteillä.
- Muutamia ilmoituksia tehtiin verkkopalveluista, jotka paljastivat tarpeettoman laajasti ja avoimesti tietoa kaikkien saataville.

Huijaukset ja kalastelut

- S-pankki, OP, OmaKanta ja Danske Bank ovat olleet huijareiden suosiossa marraskuussa.
- Merkittävä osuus pankkitunnuskalasteluun johtavasta huijausliikenteestä lähetetään edelleen tekstiviestitse.

Haittaohjelmat ja haavoittuvuudet

- Julkiverkkoon avoimena näkyviä palveluita ja hallintapaneeleita on ilmoitettu palveluiden omistajille.
- Fortinetin vanhojen FortiEMS-versioiden sekä FortiManager-haavoittuvuuden hyväksikäyttöyrityksiä.

Automaatio ja IoT

- Black Friday muistutti ostosten tietoturvan ja päivitysten jatkuvuuden tärkeydestä. [1]
- Uusi versio ja suomennos teollisuuden automaatiojärjestelmien kyberturvallisuusstandardista IEC 62443-2-1 on valmistunut. [2]
- SANS on julkaissut raportin OT/ICS:n kyberturvallisuuden nykytilasta. [3]

Verkkojen toimivuus

- Marraskuussa yleisissä viestintäverkoissa havaittiin kuusi toimivuushäiriötä.
- Katkenneet tietoliikennekaapelit saatiin korjattua ripeästi. Katkoksista huolimatta verkot toimivat.
- Palvelunestohyökkäysten osalta tilanne on rauhoittunut loppuvuotta kohden.

Vakoilu

- Kybervakoilussa hyödynnetään säännöllisesti nollapäivähaavoittuvuuksia.
- Marraskuussa raportoitiin maailmalla esimerkiksi Fortinetin VPN-ohjelmiston haavoittuvuudesta, jota kiinalaistoimija oli hyödyntänyt.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

AiTM-tekniikkaa (adversary-in-the-middle) hyödyntäviä tietomurtoja on mahdollista havaita ja estää ottamalla käyttöön salasanaton todentaminen sekä tiukentamalla ehdollisia sääntöjä M365-palveluihin liittyen. [4, 5]

Julkaisimme vinkkejä verkkokaupan ylläpitäjille digitaalisen skimmauksen havaitsemiseen, ennaltaehkäisyyn ja toimenpiteisiin skimmaus-havainnon jälkeen. Digitaalinen skimmaus tarkoittaa verkkokaupan asiakkaiden maksukorttitietojen varastamista. [6]

Naton Cyber Coalition -kyberharjoitus järjestettiin marras-joulukuun taitteessa. Harjoittelu on osa sekä kansallisten viranomaisten että kansainvälisten kumppaneiden kanssa tehtävää jatkuvaa varautumista koko yhteiskuntaa koskeviin poikkeamiin. [7]

Koko väestölle suunnattu Häiriö- ja kriisitilanteisiin varautuminen -opas julkaistiin Suomi.fi-verkkosivuilla. Opas sisältää osuuden kyberhyökkäyksiin ja -häiriöihin varautumisesta. Sisäministeriö toteutti oppaan DVV:n ja laajan yhteistyöverkoston kanssa. [8]

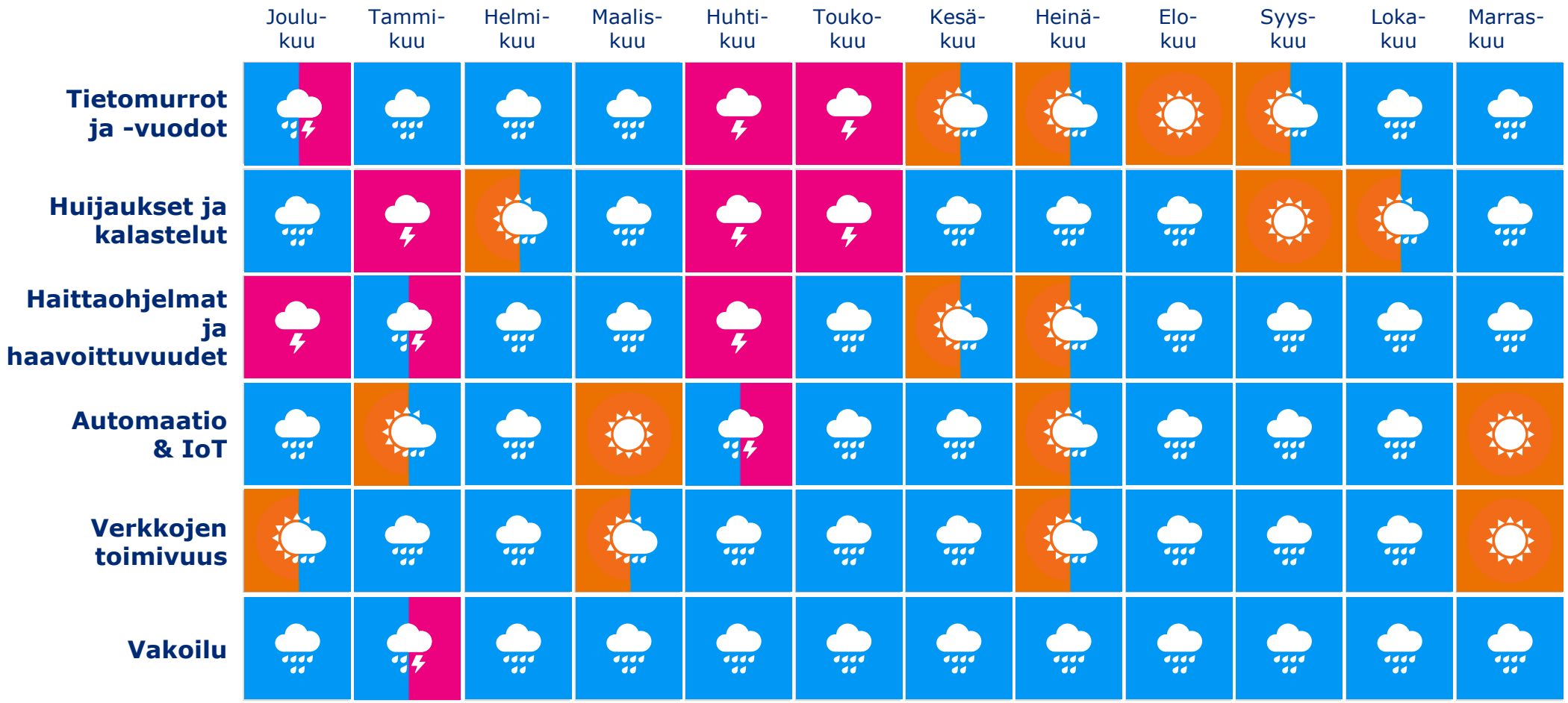
Marraskuun kyberturvallisuuden yleiskuva

- Marraskuu osoitti varautumisen tärkeyden, kun Suomea kohtasi kaksi hyvin erilaista digitalisoituneen yhteiskunnan poikkeamaa. Viikon 47 alussa uutisoitiin Suomen ja Saksan välisen merenalaisen tietoliikennekaapelin (C-Lion1) katkeamisesta, ja myöhemmin samalla viikolla Suomeen saapui etelästä voimakas Jari-myrsky. [9]
  - Traficom järjesti tiistaina 19.11. yhdessä muiden viranomaisten ja C-Lion1-kaapelin omistajan Cinian kanssa tiedotustilaisuuden merikaapelin katkeamisesta. Kaapelin katkeamisella ole ollut näkyviä vaikutuksia Suomen tietotoliikenneyhteyksiin maailmalle, eikä yhteiskunnan huoltovarmuus vaarantunut. Keskusrikospoliisi tutkii kaapelin katkeamista.
  - Marraskuussa Jari-myrskyn aikana Suomessa oli kymmeniä tuhansia sähköttömiä kotitalouksia. Pitkäkestoiset sähkökatkot voivat aiheuttaa ongelmia esimerkiksi mobiiliyhteyksiin.
  - Kaikkiaan suomalaisen yhteiskunnan kriisinkestävyys on hyvällä tasolla. Tästä huolimatta häiriöillä voi olla verrattaen lyhytkestoisia paikallisia vaikutuksia tietoliikenneyhteyksiin.
- Vuoden harmaimmaksi luonnehdittua kuukautta ovat sävyttäneet lisäksi eri pankkien nimissä tehdyt huijaus- ja kalastelukampanjat. Merkittävä osuus pankkitunnuskalasteluun johtavasta huijausliikenteestä lähetetään edelleen tekstiviestitse.
  - Kyberturvallisuuskeskukselle tulleissa ilmoituksissa näkyivät myös Dropbox-teemaiset M365-kalastelut, joista osa on johtanut tietomurtoihin.
  - Olemme vastaanottaneet säännöllisesti ilmoituksia hotelli- ja matkanvarauspalveluita koskevista tietoturvapoikkeamista, jotka ovat johtaneet myös rahallisiin menetyksiin. Esimerkiksi Suomessa on liikkeellä Booking.com-teeman ympärillä useita erilaisia huijaustapoja. Julkaisimme aihetta käsittelevän Tietoturva Nyt! -artikkelin marraskuun alkupuolella. [10]
- Palvelunestohyökkäysten osalta tilanne on rauhoittunut loppuvuodesta ja ilmoituksia hyökkäysten aiheuttamista häiriöistä on vastaanotettu syksyä vähemmän.

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 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: IoT-laitteiden tietoturvan parantaminen

- Verkkoon yhdistettäviä älylaitteita (esineiden internet eli Internet of Things, IoT) on tullut vuosien saatossa markkinoille kiihtyvällä tahdilla, ja ne ovat jalkautuneet digitalisoituneessa yhteiskunnassa lähes kaikkialle.
  - Vaikka turvallisen laitteen valmistaminen on valmistajan vastuulla, saatavilla on valtavasti laitteita, joiden suojaamiseen ei ole kiinnitetty riittävästi huomiota.
- Kehityskulkuna on havaittu, että kyberhyökkäyksissä hyödynnetään yhä useammin haavoittuvia laitteita ja ohjelmistoja, mikä voi aiheuttaa merkittäviä kustannuksia yhteiskunnassa.
  - Esimerkiksi Mirai-haittaohjelma on yksi viime vuosikymmenten merkittävimmistä kyberturvallisuuteen vaikuttaneista ja yhä vaikuttavista ilmiöistä, jonka myötä mm. haavoittuvia kotireitittimiä on valjastettu osaksi rikollisten bottiverkkoa. Näitä suojaamattomia laitteiden muodostamia bottiverkkoja voidaan käyttää myös osana rikollista verkkotoimintaa tai valtiollisten toimijoiden vakoilu- ja vaikuttamisoperaatioita.
  - Kuluttajien on mahdollista parantaa monien laitteiden suojausta omilla toimenpiteillä, mutta laitteiden laajan kirjon vuoksi osaaminen suojausten tekemiseksi voi olla puutteellista tai aikaa niiden perehtymiseen ei ole. Ohjeita laitteiden suojaamiseen on julkaistu verkkosivuillamme. [11]
- Marraskuussa julkaistu EU:n kyberkestävyyssäädös (Cyber Resilience Act, CRA) määrittelee EU:ssa vähimmäisvaatimukset internetiin kytkettävien digitaalisten tuotteiden ja ohjelmistojen kyberturvallisuudelle. Säädöksen arvioidaan parantavan yhteiskunnan kokonaisturvallisuutta, kun käytössä ja markkinoilla on aikaisempaa tietoturvallisempia laitteita.
  - Säädöksen soveltamisala on laaja. Se koskee IoT-laitteita, kuten valvontakameroita, jääkaappeja, älykelloja, puhelimia ja leluja. Se kattaa myös ohjelmistot, kuten sovellukset ja pelit, sekä teollisuuden tuotteet, kuten käyttöjärjestelmät ja etähallintajärjestelmät.

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 kyberkestävyyssäädös (CRA) julkaistu ja kansallinen toimeenpanohanke käynnissä

- EU:n kyberkestävyyssäädös (2024/2847) julkaistiin 20.11.2024, säädöksen tavoitteena on parantaa EU:n markkinoille saatettujen tuotteiden tietoturvaa.
- Kyberkestävyyssäädös koskee digitaalisen elementin sisältäviä laitteita tai ohjelmistoja, jotka ovat suoraan tai epäsuorasti liitettävissä toiseen laitteeseen tai verkkoon. Asetuksen mukaisten turvallisuusvaatimusten täyttyminen on jatkossa markkinoille pääsyn edellytys EU:ssa.
- Organisaatiot voivat hakeutua CRA:n vaatimustenmukaisuuden arviointeja tekeväksi ilmoitetuksi laitokseksi 11.6.2026 alkaen.
- Velvoite raportoida tuotteissa havaituista haavoittuvuuksista astuu voimaan 11.9.2026.
- Markkinoille saatettavien uusien tuotteiden on noudatettava kyberturvallisuusvaatimuksia 11.12.2027 alkaen.
- Kyberkestävyyssäädöksen toimeenpano edellyttää täydentävää kansallista sääntelyä, asiaa koskeva hanke on vireillä liikenne- ja viestintäministeriössä. [12]

Oikeudelliset asiat

ENISA:n tekninen ohjeistus NIS2-täytäntöönpanoasetuksen soveltamisesta lausuttavana

- Euroopan unionin kyberturvallisuusvirasto ENISA pyytää kommentteja Euroopan komission täytäntöönpanoasetuksen (EU) 2024/2690 mukaisia kyberturvallisuuden riskienhallintatoimenpiteitä koskevaan tekniseen ohjeistukseen.
- Ohjeistuksen tarkoituksena on tukea täytäntöönpanoasetuksen kohteena olevia NIS2-sääntelyn alaisia toimijoita toteuttamaan asetuksen mukaisia riskienhallintatoimenpiteitä. Ohjeistus tarjoaa mm. käytännön esimerkkejä ja viittauksia standardeihin ja jäsenmaiden viitekehyksiin.
- Ohjeistus on avoimella lausuntokierroksella 9. tammikuuta 2025 saakka. Lausuntokierros on suunnattu erityisesti elinkeinoelämälle ja komission täytäntöönpanoasetuksen soveltamisalaan kuuluville toimijoille.
- Lisätietoja ENISA:n verkkosivuilla. [13]

Oikeudelliset asiat

Eurooppalaisen digitaalisen identiteetin lompakon valmistelu etenee

- Ensimmäiset eIDAS-täytäntöönpanoasetukset on hyväksytty 21.11.2024 ja ne julkaistaan EU:n virallisessa lehdessä 24.12.2024. Tällöin alkaa kulua kahden vuoden määräaika eurooppalaisen digitaalisen identiteetin lompakon tarjoamiseksi EU:n jäsenmaissa.
  - Suomessa lompakon teknisestä toteutuksesta vastaa Digi- ja väestötietovirasto. [14]
- Eurooppalaisella digitaalisen identiteetin lompakolla tarkoitetaan puhelimessa toimivaa sovellusta, joka muistuttaa toiminnaltaan tavallisia lompakoita erityisesti erilaisten tietojen säilyttämisen näkökulmasta.
- Digitaalisen identiteetin lompakossa voi säilyttää erilaisia henkilötietoja sähköisessä muodossa. Käyttäjä itse päättää, mitä tietoja hän haluaa lompakkoon viedä.
- Jatkossa digitaalisen identiteetin lompakolla voi myös tunnistautua ja tehdä sähköisiä allekirjoituksia. Digitaalisten lompakoiden käyttäminen tulee olemaan EU-kansalaisille sekä maksutonta että täysin vapaaehtoista.

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) Varo tätä virhettä Black Friday -ostoksilla https://www.is.fi/digitoday/tietoturva/art-2000010857831.html

2) Standardi IEC 62443-2-1 pian suomenkielisenä https://sesko.fi/standardi-iec-62443-2-1-pian-suomenkielisena/

3) SANS 2024 State of ICS/OT Cybersecurity https://sansorg.egnyte.com/dl/encCm80cl8

4) Passwordless authentication options for Microsoft Entra ID https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless

5) M365-tietomurroissa hyödynnetään yhä useammin AiTM-tietojenkalastelutekniikkaa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/m365-tietomurroissa-hyodynnetaan-yha-useammin-aitm

6) Digitaalinen skimmaus - vinkkejä verkkokaupan suojaamiseen https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/digitaalinen-skimmaus-vinkkeja-verkkokaupan-suojaamiseen

7) Traficomin Kyberturvallisuuskeskus osallistui Puolustusvoimien järjestämään Naton Cyber Coalition -harjoitukseen https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficomin-kyberturvallisuuskeskus-osallistui-puolustusvoimien-jarjestamaan-naton

8) Sisäministeriö on julkaissut Häiriö- ja kriisitilanteisiin varautumisen oppaan https://traficom.fi/fi/ajankohtaista/sisaministerio-julkaissut-hairio-ja-kriisitilanteisiin-varautumisen-oppaan

9) Kyberturvallisuuskeskuksen viikkokatsaus - 47/2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-472024

10) Hotelli- ja matkanvarauspalveluiden tietomurtoja käytetään asiakkaiden huijaamiseen https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/hotelli-ja-matkanvarauspalveluiden-tietomurtoja-kaytetaan-asiakkaiden-huijaamiseen

Lähdeluettelo

11) Ohjeet ja oppaat yksityishenkilöille https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-yksityishenkiloille

12) Hallituksen esitys kyberkestävyyssäädöksen täytäntöönpanemiseksi https://valtioneuvosto.fi/hanke?tunnus=LVM014:00/2024

13) Asking for your feedback: ENISA technical guidance for the cybersecurity measures of the NIS2 Implementing Act https://www.enisa.europa.eu/news/asking-for-your-feedback-enisa-technical-guidance-for-the-cybersecurity-measures-of-the-nis2-implementing-act

14) Digitaalisen identiteetin lompakko tulee vuonna 2026 https://vm.fi/-/digitaalisen-identiteetin-lompakko-tulee-vuonna-2026