TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Toukokuu 2023

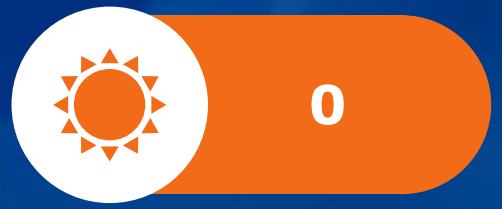
#kybersää

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



Merkittävien valtiovierailujen aikana ei ilmoitettu tapahtuneeksi palvelunestohyökkäyksiä.

Ilmoitusmäärät sosiaalisen median tilien murroista kasvoivat räjähdysmäisesti, noin 300 prosenttia, alkuvuoden keskiarvoon nähden.

On ennustettu, että vallitseva puolijohdepula kestäisi vielä ainakin vuoteen 2024 asti.

Kybersää toukokuu 2023

Tietomurrot ja -vuodot

- Ilmoitusmäärät sosiaalisen median tilien murroista nousivat lähes 300 prosenttia alkuvuoden keskiarvoon nähden.
- Myös ilmoitukset M365-tietomurroista jatkoivat nousua alkukuusta. Toukokuun lopulla havaittiin kuitenkin pientä taitetta parempaan.

Huijaukset ja kalastelut

- Sitkeät huijarit lähettävät tekstiviestejä ja soittavat perään.
- Puhelinhuijauksia soitetaan yhä useammin väärennetyillä puhelinnumeroilla. Määräys 28 velvoittaa teleoperaattorit estämään numeroiden väärentämisen 2.10. alkaen.

Haittaohjelmat ja haavoittuvuudet

- MoveIT-tiedostonsiirto-ohjelmistossa havaittiin nollapäivähaavoittuvuus. Hyväksikäyttöä on havaittu Suomessa ja maailmalla.
- Barracuda ESG -laitteessa ollut nollapäivähaavoittuvuus.
- Zyxelin palomuuri- ja VPN-tuotteissa haavoittuvuuksia. Hyväksikäyttöä on havaittu Suomessa ja maailmalla.[1]

Automaatio ja IoT

- Julkaisimme Tietoturva Nyt! – artikkelin otsikolla ”Teollisuuden järjestelmätoimittajaan kohdistunut tietomurto edellyttää myös sen asiakkailta ripeitä toimenpiteitä”.[2]

Verkkojen toimivuus

- Toukokuussa yleisissä viestintäpalveluissa oli neljä merkittävää toimivuushäiriötä.
- Satamatoimijat joutuivat palvelunestohyökkäysten kohteeksi.
- Viime aikoina erityisesti sovellustason hyökkäykset ovat aiheuttaneet vaikutuksia esimerkiksi verkkosivujen toimintaan.

Vakoilu

- Yhdysvaltojen viranomaiset julkaisivat raportin Turla-kyberuhkatoimijan käyttämästä haittaohjelmasta nimeltä “Snake”.
- Raportissa ohjeistetaan, kuinka haittaohjelma voidaan havaita saastuneista järjestelmistä.[3][4]
- Lisäksi viranomaiset suorittivat haittaohjelman poisto-operaation osasta saastuneita järjestelmiä.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Kesällä 2023 voimaan astuvat vahvan sähköisen tunnistuksen uudet vaatimukset tekevät sähköisestä asioinnista entistä turvallisempaa. Uusilla vaatimuksilla halutaan varmistaa, että käyttäjä pystyy entistä helpommin tarkistamaan, mihin palveluun hän on kirjautumassa.[5]

Julkaisimme artikkelin, jossa organisaatioita muistutetaan varautumaan myös toimittajiin kohdistuviin tietoturvapoikkeamiin. Kehotammekin erityisesti kaikkia teollisuusympäristöjen omistajia varautumaan mahdollisuuteen, että oman tuotannon kannalta kriittiseen toimittajaan kohdistuu tietomurto tai –vuoto.[2]

Kybermittarin uusi versio sekä uudet tukimateriaalit ovat saatavilla verkkosivuillamme. Uudessa versiossa on kehitetty ominaisuuksia, jotka helpottavat työkalun käyttöä, havaintojen raportointia päätöksenteon tueksi sekä arvioinnin toistettavuutta. Ilmoittaudu kesän ja syksyn esittely- ja koulutustapahtumiin![6]

Toukokuun kyberturvallisuuden yleiskuva

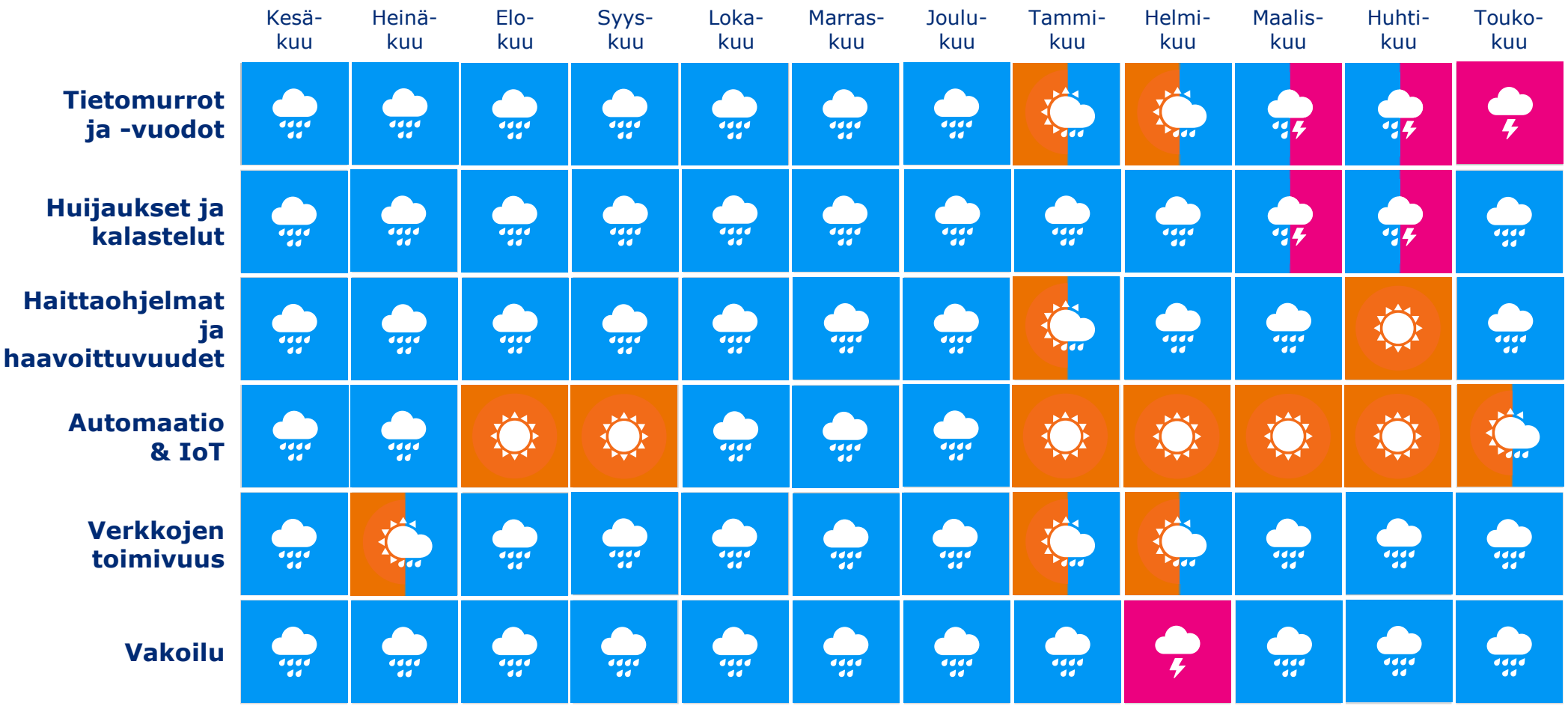
- Erityisesti ilmoitukset sosiaalisen median tilimurroista lisääntyivät huomattavasti toukokuussa.
- Viime kuun lopulla alettiin nähdä myös kaksoishuijauksia, joissa ihminen saa useamman huijausyhteydenoton tekstiviestillä tai puhelimitse. Huijarit uskottelevat kohteen tilin olevan vaarassa, ja kehottavat siirtämään rahat turvatilille.
- Ilmoitukset M365-kalasteluista lisääntyivät toukokuussa, mutta kuun loppua kohden havaittiin jo pientä käännettä parempaan.
  - Kyberturvallisuuskeskuksen tietojen mukaan noin 60 organisaatiossa vähintään yksi M365-sähköpostitili on murrettu huhtikuun jälkeen.

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 kyber-turvallisuuden osaajille

Pula puolijohteista

Tekoälyn käyttö kyberrikolli-suudessa

Suurvalta-kilpailun vaikutukset sääntelyyn

Älylaitteiden elinkaari ja kierrätys

Kyber-vakoilun ja rikollisuuden rajojen hämärtymi-nen

IoT

6G

Kiristyshaitta-ohjelmien käyttö murroksessa

Teknologia osana suurvalta-kilpailua

Sääntelyn ulottuminen uusille toimialoille

Osallistu-minen digitaalisessa ympäristössä

Pitkän aikavälin kybersää:
Pula puolijohteista

- Puolijohdepulalla tarkoitetaan puutetta komponenteista, joita tarvitaan laajasti tietotekniikassa ja teknologiassa. Puolijohteista on ollut pulaa maailmanlaajuisesti vuoden 2020 loppupuolelta alkaen.
- Puolijohteita tarvitaan eri teknologisten laitteiden valmistukseen aina matkapuhelimista autoihin saakka.
  - Teknologiaan vahvasti nojaavalle yhteiskunnalle puolijohdepula voi olla kriittistä. Ilman puolijohteita laitteiden hinnat nousevat ja valmistus viivästyy, eikä uusia laitteita saada markkinoille niin nopeasti, kuin kysyntää ja tarvetta olisi. Tämä näkyy eri teknologisten laitteiden saatavuudessa, sekä puolijohteita tarvitsevien toimialojen ahdinkona.[7]
- EU pyrkii turvaamaan puolijohteiden saatavuutta tukemalla puolijohdetuotantoa Euroopassa. EU:n sirusäädöksen tavoitteena on kerätä rahoitusta alan tutkimukseen, kehitykseen sekä innovaatioihin. Nykyisellään EU:ssa valmistetaan vain noin 10 prosenttia koko maailman tuotannosta.[7][8]
- Puolijohteisiin liittyy monimutkaisia ja maailmanlaajuisia toimitusketjuja, jotka ovat herkkiä erilaisille poikkeustiloille. Esimerkiksi koronaviruspandemia, sään ääri-ilmiöt puolijohteiden tuotantoalueilla, sekä Ukrainan sota ovat vaikuttaneet myös puolijohteiden saatavuuteen.
- Puolijohteiden tuotanto hyvin keskittynyttä. Valtaosa puolijohteiden tuotannosta sijaitsee Aasiassa ja Yhdysvalloissa.
- Puolijohteiden kysynnän odotetaan yhä kasvavan tulevaisuudessa.[9]
- On ennustettu, että puolijohdepula kestäisi vielä ainakin vuoteen 2024 asti.

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

- Nato-jäsenyyteen liittyvä tietoturvallisuussopimus eduskunnan lähetekeskustelussa
  - Eduskunta käsitteli 23.5.2023 täysistunnon lähetekeskustelussa tietoturvallisuussopimusta, johon Suomen edellytetään Pohjois-Atlantin liiton (Nato) uutena jäsenmaana sitoutuvan. Sopimus sisältää sovellettavat määräykset turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta ja turvaamisesta. Monenvälinen sopimus korvaa aiemmat Suomen kahdenväliset tietoturvallisuusjärjestelyt Pohjois-Atlantin liiton kanssa, joihin Suomi oli sitoutunut liittyessään Naton rauhankumppanuusohjelmaan vuonna 1994.[10][11]
  - Tietoturvallisuussopimuksessa määritellään Naton ja sen jäsenvaltioiden turvallisuusluokiteltu tieto, johon sopimusta sovelletaan. Sopimuksen keskeinen lähtökohta on, että osapuolet säilyttävät tiedon turvallisuusluokituksen ja pyrkivät kaikin keinoin turvaamaan tietoa. Tietoa ei luovuteta kolmansille osapuolille ilman tiedon luovuttajan suostumusta. Sopimuksen mukaan luottamuksellista (CONFIDENTIAL) ja sitä ylempiin turvallisuusluokkiin kuuluvaa tietoa käsittelevillä henkilöillä tulee myös olla asianmukainen turvallisuusselvitys.
  - Asia lähetettiin ulkoasiainvaliokuntaan, jolle hallintovaliokunnan ja puolustusvaliokunnan on annettava lausunto.
  - Suomi on sitoutunut liittymään Naton tietoturvallisuussopimukseen 12 kuukauden kuluessa siitä, kun Suomi on tallettanut Pohjois-Atlantin sopimusta koskevan liittymiskirjansa. Suomen liittymiskirja talletettiin 4.4.2023.

Oikeudelliset asiat

- Sähköisen tunnistuspalvelun arviointiohje O211 lausuttavana Lausuntopalvelussa.[12]
  - Liikenne- ja viestintävirasto on valmistellut ohjetta koskien sähköisen tunnistuspalvelun vaatimustenmukaisuuden arviointia ja arvioinnista laadittavaa tarkastuskertomusta.
  - Ohje on tarkoitettu vahvan sähköisen tunnistuspalvelun tarjoajille ja arviointielimille, joilta tunnistuspalvelut hankkivat arviointeja. Ohjeen tarkoitus on selkeyttää, mitä seikkoja palveluun liittyvien auditointien täytyy kattaa, jotta auditoinnit kattavat kaikki vaaditut osa-alueet. Ohjeen tarkoituksena on myös selkeyttää tarkastuskertomuksen vähimmäissisältöä ja esittämistapaa.
  - Mukaan on otettu mm. etäensitunnistamisessa videoyhteydellä huomioitavia asioita sekä huomioitu tulevaisuudessa mahdollisesti yleistyvät lompakkosovellukset.
  - Määräaika lausunnoille on 20.6.2023.

Oikeudelliset asiat

- Irlannin tietosuojaviranomainen määräsi Metalle 1,2 miljardin euron seuraamusmaksun lainvastaisista henkilötietojen siirroista Yhdysvaltoihin Facebook-palvelussa.[13]
  - Seuraamusmaksu määrättiin Euroopan tietosuojaneuvoston sitovan kiistanratkaisupäätöksen perusteella. Kyseessä on tähän mennessä suurin tietosuoja-asetuksen perusteella määrätty sakko. Lisäksi Meta määrättiin keskeyttämään eurooppalaisten käyttäjien henkilötietojen siirtäminen Yhdysvaltoihin ja saattamaan tiedonsiirrot tietosuoja-asetuksen mukaisiksi.
  - Päätöksessä katsottiin, että tiedonsiirrot vakiolausekkeiden perusteella olivat tietosuoja-asetuksen vastaisia, sillä Yhdysvaltojen lainsäädännössä ei taata EU:n vaatimuksia vastaavaa tietosuojan tasoa. Myöskään vakiolausekkeita täydentävillä suojatoimilla ei ollut mahdollista puuttua riskeihin, joita yksilöiden oikeuksiin ja vapauksiin kohdistuu Yhdysvaltojen lainsäädännön vuoksi.
  - Meta on ilmoittanut valittavansa päätöksestä.

Oikeudelliset asiat

- Tietosuojavaltuutetun toimisto: Ilmatieteen laitokselle huomautus henkilötietojen siirroista yhdysvaltalaisyritys Googlelle.[14][15]
  - Apulaistietosuojavaltuutettu antoi Ilmatieteen laitokselle huomautuksen henkilötietojen siirtämisestä Yhdysvaltoihin verkkosivujen seurantateknologioiden (Google reCAPTCHA ja Google Analytics) kautta ilman pätevää siirtoperustetta.
  - Ilmatieteen laitos ilmoitti ryhtyneensä toimenpiteisiin reCAPTCHA- ja Google Analytics -palveluiden poistamiseksi verkkosivuiltaan. Apulaistietosuojavaltuutettu määräsi Ilmatieteen laitoksen poistamaan henkilötiedot, jotka oli siirretty Yhdysvaltoihin ilman asianmukaista siirtoperustetta.
  - Päätös ei ole vielä lainvoimainen.

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 1/3

1) Haavoittuvuus 6/2023: Kriittisiä haavoittuvuuksia Zyxelin palomuurituotteissa - Hyväksikäytöstä viitteitä https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_6/2023
2) Teollisuuden järjestelmätoimittajaan kohdistunut tietomurto edellyttää myös sen asiakkailta ripeitä toimenpiteitä https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/teollisuuden-jarjestelmatoimittajaan-kohdistunut-tietomurto-edellyttaa-myos-sen
3) Hunting Russian Intelligence "Snake" Malware https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a
4) Justice Department Announces Court-Authorized Disruption of Snake Malware Network Controlled by Russia's Federal Security Service https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled
5) Kyberturvallisuuskeskuksen viikkokatsaus 19/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-192023
6) Kybermittarista apua kyberturvallisuusriskien hahmottamiseen https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybermittarista-apua-kyberturvallisuusriskien-hahmottamiseen

Lähdeluettelo 2/3

7) Sirusäädös – EU:n suunnitelma puolijohdepulan ratkaisemiseksi https://www.europarl.europa.eu/news/fi/headlines/society/20230210STO74502/sirusaados-eu-n-suunnitelma-puolijohdepulan-ratkaisemiseksi
8) EU:n sirusäädös https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_fi
9) European Chips Survey https://digital-strategy.ec.europa.eu/en/library/european-chips-survey
10) HE 4/2023 https://finlex.fi/fi/esitykset/he/2023/20230004
11) Nato-jäsenyyteen liittyvä tietoturvallisuussopimus eduskunnan lähetekeskustelussa https://www.eduskunta.fi/FI/tiedotteet/Sivut/Nato_tietoturvallisuussopimus_eduskunta_23052023.aspx
12) Lausuntopalvelu: Sähköisen tunnistuspalvelun arviointiohje O211 https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=59f052f8-6c60-4b1c-a2f6-19ade714b84b&proposalLanguage=da4408c3-39e4-4f5a-84db-84481bafc744
13) Metalle 1,2 miljardin euron seuraamusmaksu lainvastaisista henkilötietojen siirroista Yhdysvaltoihin Euroopan tietosuojaneuvoston päätöksen seurauksena https://tietosuoja.fi/-/metalle-1-2-miljardin-euron-seuraamusmaksu-lainvastaisista-henkilotietojen-siirroista-yhdysvaltoihin-euroopan-tietosuojaneuvoston-paatoksen-seurauksena

Lähdeluettelo 3/3

14) Ilmatieteen laitokselle huomautus henkilötietojen siirroista yhdysvaltalaisyritys Googlelle https://tietosuoja.fi/-/ilmatieteen-laitokselle-huomautus-henkilotietojen-siirroista-yhdysvaltalaisyritys-googlelle

15) Oikaisu Ilmatieteen laitokselle annettuun päätökseen: huomautus vaikutustenarvioinnin tekemättä jättämisestä poistettiin https://tietosuoja.fi/-/oikaisu-ilmatieteen-laitokselle-annettuun-paatokseen-huomautus-vaikutustenarvioinnin-tekematta-jattamisesta-poistettiin