TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Huhtikuu 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

Suomessa ilmoitettiin seitsemän palvelunestohyökkäystä tapahtuneeksi sinä päivänä, kun Suomi liittyi Natoon.

Vastaamo-tietomurtoon liittyvän lausuman on huhtikuun lopulla antanut jo 8600 uhria. Tietomurron uhreilla on toukokuun loppuun asti aikaa tehdä rikosilmoitus ja täyttää lausumalomake.

Huhtikuussa järjestettiin kaksi Tietoturvamerkki-tapahtumaa, yksi Tampereella ja toinen Jyväskylässä.

Kybersää huhtikuu 2023

Tietomurrot ja -vuodot

- Huhtikuu oli tietomurtojen ja -vuotojen osalta maaliskuun kaltainen.
- Suurimpina kansallisina ilmiöinä jatkavat yrityssähköpostitilien (M365) ja sosiaalisen median tilien murrot.

Huijaukset ja kalastelut

- Väärennetyillä numeroilla soitetut huijauspuhelut ovat aiheuttaneet paljon harmia numeroiden oikeille haltijoille. Sekä yritysten että yksityisten henkilöiden puhelinnumeroita on käytetty huijauksiin.
- Pankki- ja maksukorttitietoja on taas kalasteltu ärhäkästi pankkien lisäksi myös veronpalautusten ja OmaPostin nimissä.

Haittaohjelmat ja haavoittuvuudet

- Muistutimme jälleen päivitysten tärkeydestä ja kehotimme päivittämään kriittiset haavoittuvuudet Applen laitteissa.
- Huhtikuun aikana tehtiin tähän ilmiöön liittyen hieman vähemmän ilmoituksia kuin maaliskuun aikana.

Automaatio ja IoT

- Saamme silloin tällöin ilmoituksia organisaatioiden henkilöstölle markkinoiduista, usein pilvipohjaisista palveluista tai laitteista, jotka olisivat helposti käyttöönotettavissa ilman organisaation oman tietohallinnon tukea.[1]
- Digitaalisten palveluiden ja laitteiden käyttöönoton tulee kuitenkin aina tapahtua hallitusti.

Verkkojen toimivuus

- Huhtikuussa yleisissä viestintäpalveluissa oli seitsemän merkittävää toimivuushäiriötä.
- Kolme häiriöistä johtui sähkönsaantiin liittyvistä ongelmista.
- Suomi liittyi 4.4.2023 NATO:n jäseneksi palvelunestohyökkäysten saattelemana. Päivän ilmoituslukumäärä oli 7 kappaletta.

Vakoilu

- Puolan viranomaiset julkaisivat raportin laajasta vakoilukampanjasta. Raportissa kampanjaan linkitetään kyberuhkatoimija APT29.[1]
- Raportti kuvaa kampanjaa, jonka tavoitteena oli kerätä tietoja mm. NATO- ja EU-maiden diplomaattisista yksiköistä kohdistetun tietojenkalastelun avulla.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Kyberturvallisuuskeskus kartoittaa ohjelmistoturvallisuuden tilaa Suomessa. Nykytilanteen kartoittamisen lisäksi toivomme tietoa kipukohteista ja hyvistä käytännöistä, joilla voisimme tukea yrityksiä ja muita organisaatioita. Vastaa kyselyyn![2]

Huhtikuun lopulla USA:ssa järjestetyssä RSA-tietoturvakonferenssissa Kyberturvallisuuskeskus, KRP ja Elisa pitivät yhteisesityksen Traficomin ja suomalaisten teleoperaattoreiden yhteistyöstä puhelinnumeroiden väärentämistä vastaan.[3]

Haavoittuvuuksien ilmoittamista helpottavaa käytäntöä ei vielä täysin hyödynnetä Suomessa, selviää Kyberturvallisuuskeskukselle tehdystä opinnäytetyöstä. Kyseinen käytäntö perustuu RFC 9116:een, joka esittää, että organisaatioiden yhteystiedot löytyisivät aina samasta paikasta.[4]

Huhtikuun kyberturvallisuuden yleiskuva

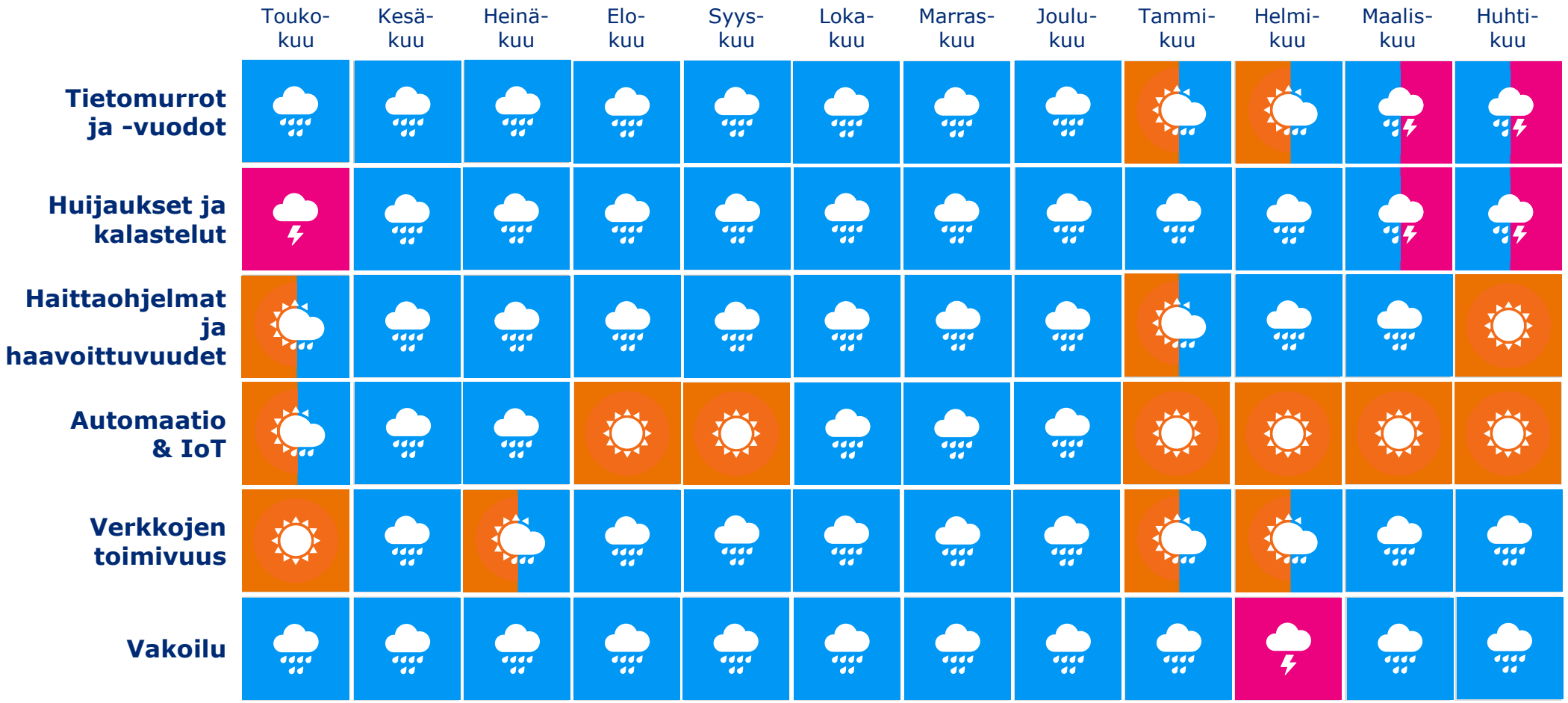
- Yrityssähköpostitileihin kohdistuvat kalastelut ja niiden seurauksena tapahtuvat tilimurrot vaihtavat viikoittain teemaa. Viimeisen kuukauden aikana on havaittu ainakin eri turvapostien, Adoben ja Microsoft OneDriven näköisiä kalasteluja. Monivaiheinen tunnistautuminen olisi suojannut tilimurroilta lähes jokaisessa meille tulleessa ilmoituksessa.
- Huhtikuussa Traficom piti yhdessä Suojelupoliisin kanssa ajankohtaiskatsauksen kyberturvallisuuden uhkatasosta, joka on pysynyt kohonneena. Suomalaisiin organisaatioihin suuntautuukin nyt jatkuvasti kasvavaa kiinnostusta. Erityisesti kohdistettujen hyökkäysten määrä on noussut.[5]
- Jälleen kesän ja lomien lähestyessä erilaiset laskutushuijaukset yleistyvät. Kyberturvallisuuskeskus on saanut viime aikoina useita ilmoituksia laskutushuijausten yrityksistä eri puolilta Suomea. Kaikkien organisaatioiden tulisikin kouluttaa henkilöstöä, kausi- ja kesätyöntekijöitä unohtamatta, yrityksen laskutuskäytäntöihin toimitusjohtaja- ja laskutushuijausten ehkäisemiseksi.[1]

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: IoT

- Internet of Things (IoT) viittaa verkkoon kytkettäviin älylaitteisiin, kuten kodinkoneisiin ja älyrannekkeisiin. Kuluttajille myytävän IoT:n kyberturvallisuusvaatimukset kiristyvät, ja kaupan hyllyllä olevien tuotteiden turvallisuuspotentiaali kasvaa.
- Datan määrä lisääntyy hurjasti, ja sitä hyödynnetään entistä enemmän mm. ennakoinnissa. IoT-tuotteet ovat datan tuotannossa merkittävässä roolissa. IoT käsitteenä siirtyy taka-alalle, kun se yhdistyy muihin uusiin teknologiakonsepteihin, kuten tekoälyyn, älykaupunkeihin ja 5G:hen.
- Yhteiskunnan digitalisoituminen jatkuu. Olemme entistä enemmän riippuvaisia IoT:n toiminnasta. Kuluttajien IoT-tuotteet kiinnostavat rikollisia muutenkin kuin potentiaalisina DDoS-botteina. Käyttäjät usein olettavat markkinoilla olevien tuotteiden olevan turvallisia käyttää.
- EU pyrkii omalta osaltaan lieventämään turvattomien IoT-laitteiden aiheuttamia ongelmia pakottavalla sääntelyllä. Jo voimassa olevaa radiolaitedirektiivin delegoitua asetusta tietoturvasta (3.3 d, e, f) aletaan soveltaa, ja tekeillä oleva kyberkestävyyssäädös lisää elinkaarivelvoitteet sääntelyn piiriin.
- Säädökset siirtävät tulevaisuudessa vastuuta tuotteiden tietoturvasta oleellisesti käyttäjältä valmistajalle, maahantuojille ja jälleenmyyjille. Vastuiden siirtymisen myötä merkitystään kasvattavat myös tuotteiden tietoturvallinen kehitys (Security by Design) ja yritysten tarve IoT-ratkaisuiden parempaan toimitusketjujen hallintaan.

Top 5 uhat lähitulevaisuudessa (6kk–2v)

1.

Suomeen kohdistunut kyberympäristön uhkataso on pysynyt kohonneena.

Kohdistettujen hyökkäysten määrä on noussut. Kohonneen uhkatason vuoksi organisaatioiden varautumisen merkitys korostuu.

2.

Talouden ja politiikan ilmiöt heijastuvat myös kyber-turvallisuuteen.

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

3.

Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa.

Organisaatioiden olisi hyvä tunnistaa tekoälyn tuomia haasteita, ja varautua niihin esimerkiksi kouluttamalla henkilöstöään.

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. Suomeen kohdistunut kyberympäristön uhkataso on edelleen kohonneella tasolla

Kyberhyökkäykset lisääntyivät 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.
- Varsinkin huoltovarmuuskriittisten organisaatioiden joutuessa kiristyshaittaohjelman uhriksi yhteiskunnan elintärkeät toiminnot voivat vaarantua.
- Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista.
- Erityisesti kohdistettujen kyberhyökkäysten määrä, joissa kohdeorganisaatio on tarkkaan valittu, on kasvanut.
- Tutustu Kyberturvallisuuskeskuksen tiedotteeseen kohonneesta kyberuhkatasosta, ja katso Kyberturvallisuuskeskuksen ja Suojelupoliisin ajankohtaiskatsauksen tallenne.[5][6]

2. 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.
  - Palvelunestohyökkäysten määrä lisääntyi niin Suomessa kuin Euroopassakin vuonna 2022. Myös niiden käyttötapa poliittisena mielenilmauksena korostui.
- Kuluneena vuonna on nähty entistä enemmän haktivismia, jonka tavoitteena on ottaa kantaa yhteiskunnallisiin asioihin.
- 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.

3. 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.[7]

- Tekoälyä voidaan hyödyntää esimerkiksi työn automatisointiin, kyberhyökkääjien työkalujen tehostamiseen, sekä täysin uusien hyökkäyskyvykkyyksien luomiseen.[8]
- Myös syväväärennösvideot eli deep fake -videot ovat puhututtaneet viime aikoina julkisuudessa. Syväväärennösvideoilla tarkoitetaan väärennettyjä tai tekaistuja videoita, joiden luomiseen on hyödynnetty tekoälyä. Tekoäly voikin haastaa luottamuksen käsitettä, kun esimerkiksi tuttuun kuvaan tai ääneen ei voikaan välttämättä enää luottaa henkilöllisyyden todentamisessa.[8]
- Organisaatioiden olisikin hyvä tunnistaa tekoälyn tuomia haasteita, ja varautua niihin esimerkiksi kouluttamalla henkilöstöään. Olennaista on sisäistää, että tekoäly ja siihen liittyvät ilmiöt kehittyvät nopeasti, mihin on hyvä varautua myös organisaatioissa.
- Organisaatioiden on hyvä ottaa huomioon erityisesti tietosuoja- ja salassapitonäkökulmat tekoälyn mahdolliseen käyttöön liittyen, ja pohtia näihin liittyviä linjauksia organisaation sisällä.

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 organisaatioidensa 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.
- On hyvä ymmärtää, että käytettävien palvelujen kautta voidaan murtautua organisaation, jos kyberturvallisuutta ei ole huomioitu.
- Kyberturvallisuuskeskus on käynnistänyt kevään aikana Huoltovarmuuskeskuksen rahoittaman Ketjutonttu-projektin, jonka tarkoituksena on auttaa suomalaisia yrityksiä ja niiden toimittajia hallitsemaan toimitusketjuihin liittyviä kyberriskejä. Ketjutonttu on yhä auki uusille osallistujille![9]

5. Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille!

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

- Osaamisen saaminen riittävälle tasolle kestää vielä pitkään. Organisaatioiden kyberturvallisuus vaarantuu, mikäli osaavaa henkilöstöä ei ole tarpeeksi saatavilla.
- 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.
- Viime vuoden lopussa opetus- ja kulttuuriministeriö myönsi noin 3,4 miljoonaa euroa kyberturvallisuuskoulutuksen kehittämiseen. Rahoitus suunnattiin Jyväskylän yliopistolle ja Jyväskylän ammattikorkeakoululle, ja niiden koordinoimalle yhteistyöhankkeelle.[10]
- Alkuvuonna 2023 Aalto-yliopiston tutkijaryhmä julkaisi osana laajempaa hanketta tutkimusraporttinsa kyberkansalaistaidoista ja niiden kehittämisestä EU:ssa. Hankkeen tavoitteena on tuottaa eurooppalainen malli kyberturvallisuuden perustaitojen opettamiseen.[11]

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 komissio ehdottaa uutta kybersolidaarisuussäädöstä kyberuhkien ja –poikkeamien torjuntaan.[12]
  - Tavoitteena on vahvistaa EU:n yhteistä kyberhäiriöiden havainnointia, tilannekuvaa sekä kyvykkyyttä vastata vakaviin kyberhäiriöihin.
    - Komissio ehdottaa EU:n laajuista European Cyber Shield SOC-verkoston perustamista, mikä koostuisi kansallisista sekä rajat ylittävistä SOC:eista.
  - Lisäksi tavoitteena on vahvistaa kriittisten toimijoiden valmiuksia koko EU:ssa, ja vahvistaa solidaarisuutta kehittämällä yhteisiä toimintavalmiuksia merkittävien tai laajamittaisten kyberturvallisuuspoikkeamien varalle.
    - EU ehdottaa myös eurooppalaisen kyberturvallisuusreservin perustamista jäsenvaltioiden tukemiseksi merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin varautumisessa, niihin vastaamisessa ja niistä toipumisessa.
    - Reservi koostuisi luotettavista yksityisen sektorin palveluntarjoajista.
  - Ehdotus kyberturvallisuuspoikkeamien arviointimekanismin perustamisesta.
    - Merkittävien tai laajamittaisten poikkeamien tarkastelu ja arviointi Euroopan unionin kyberturvallisuusvirasto ENISA:n tehtäväksi.

Oikeudelliset asiat

- Vastaamon tietomurtoon liittyvät esitutkinta- ja oikeusprosessit etenevät.
  - Syksyllä 2020 paljastuneen Vastaamon tietomurron uhriluku (noin 33 000) on rikoshistorian suurin. Teosta epäilty vangittiin helmikuussa 2023.
    - Uhrien poikkeuksellisen suuren lukumäärän takia kuulemiset toteutetaan sähköisellä lausumalomakkeella poliisin sähköisessä asiointipalvelussa.
    - Tietomurron uhreilla on **toukokuun loppuun** asti aikaa tehdä rikosilmoitus ja täyttää lausumalomake. Vasta lausumalomakkeen lähettäminen antaa oikeuden päästä rikosprosessiin mukaan.
    - Huhtikuun lopulla uhreista noin 24 000 oli tehnyt rikosilmoituksen ja 8600 antanut lausuman.[13]
    - Keskusrikospoliisi jatkaa tietomurron sekä siihen liittyvien rikosten tutkintaa, ja tavoitteena on nostaa syyte viimeistään lokakuussa.
  - Helsingin käräjäoikeus tuomitsi huhtikuussa Vastaamon entisen toimitusjohtajan kolmen kuukauden ehdolliseen vankeusrangaistukseen tietosuojarikoksesta. Tuomio ei ole vielä lainvoimainen, ja sekä puolustus että syyttäjä harkitsevat valittamista.

Oikeudelliset asiat

- Traficom on päivittänyt suosituksen kyberturvallisuuden edistämisestä raideliikenteessä.
  - Suositusteksti ja sen liitteet löytyvät suomeksi, ruotsiksi ja englanniksi verkkosivuiltamme.[14]
  - Suosituksessa muun muassa kaikkia raideliikennetoimijoita suositetaan arvioimaan ja mittaamaan oman organisaationsa kyberturvallisuuden tasoa.
  - Toimijoita suositetaan hyödyntämään ISO27001 tietoturvallisuuden hallintajärjestelmää sekä rautatieliikenteen kyberturvallisuuden teknistä eritelmää tai IEC 62443 -standardisarjaa.
  - Muu vaihtoehtoinen kyberturvallisuuden viitekehys voi olla esimerkiksi Kyberturvallisuuskeskuksen Kybermittari, jossa kaikkia toimijoita suositetaan ylittämään Kybermittarin tasoa 1 ja kriittisten palveluiden tarjoajia (NIS-toimijat) ylittämään Kybermittarin tavoitetasoa 2.

Oikeudelliset asiat

- Euroopan komissio antoi ilmailun tietoturvahallinnan vaatimuksia vahvistavan delegoidun asetuksen (EU) 2022/1645[15] sekä täytäntöönpanoasetuksen (EU) 2023/203.[16]
  - Asetukset sisältävät vaatimuksia sekä ilmailuviranomaisille että ilmailuorganisaatioille.
  - Asetukset tulevat sovellettavaksi 10/2025 ja 02/2026. Työ niiden täytäntöönpanemiseksi on käynnissä.
  - Hyväksyttävät asetusten vaatimusten täyttämisen menetelmät (AMC-materiaali) sekä ohjemateriaali (GM) olivat jäsenvaltioiden kommentoitavana maalis-huhtikuussa ja lopulliset versiot julkaistaan näillä näkymin syksyyn mennessä.
  - Euroopan unionin lentoturvallisuusvirasto EASA:n ja jäsenvaltioiden yhteistyö täytäntöönpanon valmistelussa on käynnissä Part-IS Implementation Task Force -ryhmässä, johon Suomikin osallistuu.
  - Ryhmässä haetaan hyviä, yhdenmukaisia käytäntöjä ja käydään läpi täytäntöönpanon haasteellisia kohtia.
  - Lisätietoa ilmailun kyberturvallisuuden kokonaisuudesta löytyy Traficomin verkkosivuilta.[17]

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) Kyberturvallisuuskeskuksen viikkokatsaus - 16/2023
   https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-162023
2) Selvitämme ohjelmistoturvallisuuden tilaa - vastaa kyselyyn
   https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/selvitamme-ohjelmistoturvallisuuden-tilaa-vastaa-kyselyyn
3) Kyberturvallisuuskeskuksen viikkokatsaus - 18/2023
   https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-182023
4) Haavoittuvuuksien ilmoittamista helpottavaa käytäntöä ei vielä täysin hyödynnetä Suomessa
   https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuuksien-ilmoittamista-helpottavaa-kaytantoa-ei-viela-taysin-hyodynneta
5) Kyberturvallisuuden uhkataso pysynyt kohonneena - kohdistettujen hyökkäysten määrä noussut
   https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuden-uhkataso-pysynyt-kohonneena-kohdistettujen-hyokkaysten-maara
6) Kyberturvallisuuden ajankohtaiskatsaus 21.04.2023 klo 12, tallenne https://youtu.be/UEFvTVLH5Rc

Lähdeluettelo

7) NCSC-UK: ChatGPT and large language models: what's the risk? https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk
8) Tekoälyn mahdollistamat kyberhyökkäykset https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/tekoalyn-mahdollistamat-kyberhyokkaykset
9) Tonttu-projektit - uusien menetelmien toteutettavuustestaus https://www.kyberturvallisuuskeskus.fi/fi/tonttu
10) OKM: Kyberturvallisuusalan koulutusta kehitetään korkeakoulujen yhteistyönä – myös informaatiopsykologista tutkimusta vahvistetaan https://okm.fi/-/kyberturvallisuusalan-koulutusta-kehitetaan-korkeakoulujen-yhteistyona-myos-informaatiopsykologista-tutkimusta-vahvistetaan
11) Tutkimusraportti: Kyberkansalaistaidot ja niiden kehittäminen Euroopan Unionissa https://cyber-citizen.eu/aineisto/aineisto-2/
12) Cyber: towards stronger EU capabilities for effective operational cooperation, solidarity and resilience https://digital-strategy.ec.europa.eu/en/news/cyber-towards-stronger-eu-capabilities-effective-operational-cooperation-solidarity-and-resilience

Lähdeluettelo

13) Vastaamon tietomurron uhreilla on toukokuun loppuun asti aikaa tehdä rikosilmoitus ja antaa lausunto – nyt ilmoituksia on tehty noin 24 000 https://yle.fi/a/74-20028919
14) Suositus kyberturvallisuuden edistämisestä raideliikenteessä https://www.traficom.fi/fi/saadokset/suositus-kyberturvallisuuden-edistamisesta-raideliikenteessa
15) (EU) 2022/1645 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1645
16) (EU) 2023/203 https://eur-lex.europa.eu/eli/reg_impl/2023/203
17) Ilmailun kyberturvallisuus osana ilmailujärjestelmän kokonaisturvallisuutta https://www.traficom.fi/fi/liikenne/ilmailu/ilmailun-kyberturvallisuus