TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Tietoturvan vuosi 2023

Sisällys

Traficomin julkaisuja 10/2024
ISSN 2669-8757 (verkkojulkaisu)
ISBN 978-952-311-909-3

Johdanto

Vuoden 2024 lähdettyä rivakasti vauhtiin, on hyvä pysähtyä hetkeksi ja palata edelliseen vuoteen. Mitä kaikkea kyberturvallisuuden rintamalla tapahtuikaan? Paljonkin. Uhkien puolella näimme kiristyshaittaohjelmien, huijausviestien levittämistä ja palvelunesto-hyökkäyksiä. Rikolliset olivat opportunistisia ja keksivät koko ajan uudenlaisia keinoja yrittää tunkeutua organisaatioiden tietojärjestelmiin tai huijata ihmisiltä näiden rahoja tai henkilötietoja. Lisäksi kybervakoiluyritykset organisaatioita kohtaan jatkuivat aktiivisena. Tässä rikollisessa busineksessa härskiydellä ja moraalittomuudella ei ole rajoja.

Seuraamme Traficomissa jatkuvasti digitaalisen yhteiskunnan ja kyberturvallisuuden ilmiöitä. Autamme yrityksiä, viranomaisia ja kansalaisia varautumaan ja tunnistamaan tämän hetken ja tulevaisuuden kyberuhkia. Työmme antaa eväitä myös teknologiseen kehitykseen vaikuttamiseksi sekä kehityksen luomien haasteiden minimoimiseksi.

Julkisuudessa ja julkisessa keskustelussa erilaiset uhkat saavat paljon näkyvyyttä. Vähemmälle huomille jää usein se työ, jota yhteiskunnan eri sektoreilla tehdään jatkuvasti kyberturvallisuuden kehittämiseksi. Yhteistyötä, tietojenvaihtoa, menetelmiä ja torjunnassa käytettyjä teknologioita kehitetään jatkuvasti.

Kyberturvallisuus ja arjen tietoturva on pieniä ja suuria tekoja. Kaikki lähtee siitä, että on huolellinen ja valppaana. Pitää käytössä olevat laitteiden ja palveluiden ohjelmistopäivitykset ja tietoturvan kunnossa. Lisäksi auttaa kaveria esimerkiksi uusien älylaitteiden käyttöönotossa.

Organisaatioille tietoturvan ja siitä huolehtimisen tulee olla kaiken liike- ja operatiivisen toiminnan perusta. Hyvä tietoturva ja siitä huolehtiminen on keskeinen osa moderniin digitaaliseen yhteiskuntaan kuuluvaa organisaation yhteiskuntavastuuta.

Huono tietoturva vaarantaa yrityksen liiketoiminnan ja voi pahimmassa tapauksessa merkitä liiketoiminnan loppua. Oikoteitä hyvään tietoturvaan ei ole. Mutkien vetäminen suoraksi ei kannata.

Tietoturvasta huolehtiminen on vastuuta omasta organisaatiosta, sen työntekijöistä, asiakkaista ja loppupeleissä myös koko suomalaisen yhteiskunnan kyberturvallisuudesta.

Kyberturvallista Suomea ei tehdä yksin, vaan se vaatii koko yhteiskunnan eri sektorit läpileikkaavaa yhteistyötä. Haluankin kiittää kaikkia, jotka tekevät päivittäin työtä kyberturvallisuuden edistämiseksi Suomessa.

Jarkko Saarimäki
Pääjohtaja

> ”Hyvä tietoturva ja siitä huolehtiminen on keskeinen osa moderniin digitaaliseen yhteiskuntaan kuuluvaa organisaation yhteiskuntavastuuta.

Ps. Olethan tutustunut Kyberturvallisuuskeskuksen tuottamiin **viikkokatsauksiin** ja **Kybersäähän**? Näistä molemmista saa tärkeää ja ajantasaista tietoa siitä, mitä kyberturvallisuuden puolella tapahtuu. Lisätietoja kyberturvallisuuskeskus.fi

Kyberturvallisuutta kehitetään pitkäjänteisesti ja strategisesti Suomessa

Yhteiskunnan digitalisoituessa toimialat ja yhteiskunnan eri sektorit ovat entistä riippuvaisempia toisistaan. Tänä päivänä harva häiriötilanne koskettaa vain yhtä toimi- tai hallinnonalaa. Moderneihin uhkiin varautuminen ja vastaaminen edellyttävät sitä, että yhteistyö yhteiskunnan eri sektorien välillä on tiivistä ja tieto kulkee häiriöttömästi ja nopeasti. Johtamisen, tilannekuvan ja viestinnän välisten yhteyksien tulee olla kunnossa. Päätöksiä on tehtävä oikein tiedoin ja oikean tilannekuvan perusteella. Tämän päivän ja tulevaisuuden kriisit edellyttävät myös sitä, että viestintään panostetaan entistä enemmän.

Kyberturvallisuus on keskeinen osa Suomen ja suomalaisen yhteiskunnan kokonaisturvallisuutta. Samalla tavoin kuin muukin turvallisuus myös kyberturvallisuus vaatii panostuksia ja jatkuvaa kehittämistä olemassa oleviin ja tuleviin uhkiin vastaamiseksi. Erityisesti nykyisin, kun maailman turvallisuuspoliittiseen tilanteeseen kohdistuu muutoksia.

Kyberturvallisuutta ei tehdä yksin ja sen varmistaminen vaatii yritysten ja viranomaisten saumatonta, luottamukseen perustuvaa yhteistyötä. Suomessa tälle yhteistyölle on pitkät perinteet ja yhteistyötä on tehty kattavasti ja laaja-alaisesti kyberturvallisuuden edistämiseksi yhteiskunnan eri sektoreiden välillä.

Suomessa kyberturvallisuutta, varautumista ja viranomaisten yhteistyötä koskevaa lainsäädäntöä, menetelmiä ja standardeja kehitetään jatkuvasti sekä kotimaassa että EU-tasolla. Kyberturvallisuutta koskeva koulutus ja tutkimus vahvistuvat Suomessa jatkuvasti.

Vuonna 2023 kyberturvallisuuden uhkataso pysyi kohonneena. Traficom ja Suojelupoliisi tiedottivat uhkatason tilanteesta huhtikuussa 2023. Edellisen kerran kohonneesta uhkatasosta viestittiin syksyllä 2022. Muutoksen syynä on, että kyberhyökkäykset ovat muuttuneet aiempaa vakavammiksi ja kohdennetuimmaksi.

Entistä useammin nähdään, että hyökkääjä yrittää päästä sisään johonkin tiettyyn organisaatioon. Lisäksi palvelunestohyökkäykset, erilaiset huijaukset, haittaohjelmat ja kiristyshyökkäykset organisaatioiden ICT-ympäristöihin sekä tietojenkalastelu vaikuttavat suomalaisten ja Suomessa toimivien organisaatioiden arkeen. **Kyberturvallisuuskeskuksen arvion mukaan uhkataso säilyy kohonneena myös vuonna 2024.**

Kyberturvallisuuden uhkataso pysynyt kohonneena – kohdistettujen hyökkäysten määrä noussut | Traficom

Kyberturvallisuus edellyttää jatkuvaa kehitystyötä

Suomessa kyberturvallisuudessa viranomaisten tehtävät ja roolit ovat selvät. Valtioneuvostotasolla sekä operatiivisella tasolla yhteistyö toimii. Operatiivista yhteistyötä tehdään päivittäin ja viranomaisilla on hyvin organisoidut koordinaatioryhmät ja -toimintamallit.

Pääministeri Orpon hallitusohjelmassa kyberturvallisuus ja sen kehittäminen huomioidaan monin tavoin. Kyberturvallisuus näkyy hallitusohjelmassa aiempaa vahvemmin. Hallituskauden aikana tullaan uudistamaan Suomen kyberturvallisuusstrategia. Strategian esivalmistelu käynnistyi vuoden 2023 aikana. Osana hallituskausien ylittävää kyberturvallisuuden kehittämisohjelmaa (valtioneuvoston periaatepäätös 2021, Kyberturvallisuuden kehittämisohjelma – Valto) valmisteltiin virkatyönä poikkihallinnollinen kyberturvallisuutta koskeva "Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa". Merkittävä osa selvityksen ehdotuksista, kuten kyberturvallisuuden koulutuksen lisääminen, kriittisten järjestelmien tunnistaminen ja niiden turvallisuuden varmistaminen huomioidaan hallitusohjelmassa, kuten laajemminkin myös vuoden 2021 kyberturvallisuuden kehittämisohjelma.

Hallituskauden aikana uudistetaan kokonais- ja kyberturvallisuuden johtamisrakenne pääministerin johdolla. Uudistuksessa varmistetaan viranomaisten vastuunjaon ja toimivaltuuksien selkeys ja tiedonvaihdon tehokkuus sekä toteutetaan näiden edellyttämät lainsäädäntömuutokset. Lisäksi kyberturvallisuutta vahvistetaan tiiviissä yhteistyössä yritysten, elinkeinoelämän ja kolmannen sektorin kanssa huomioiden sen, että iso osa kriittisestä infrastruktuurista on yksityisessä omistuksessa.

Lähitulevaisuuden kyberturvallisuuden keskeiset kehittämistarpeet liittyvät lainsäädäntöön. Toiminta- ja turvallisuusympäristön sekä teknologioiden muuttuessa nopeasti, on tärkeää, että myös lainsäädäntö on ajan tasalla ja pysyy kehityksessä mukana. Tämän päivän ja tulevaisuuden kyberuhkin varautumisessa ja vastaamisessa on tärkeää, että käytössä ovat hyvin suojatut järjestelmät ja toimivaltaiset viranomaiset voivat vaihtaa tietoja entistä tehokkaammin ja nopeammin. Kybertilanteet poikkeavat fyysisen maailman tapahtumista siinä, että tilanteiden hallinnassa nopeus ratkaisee, kyse on minuuteista ja sekunneista.

Lainsäädännön kehittämisen lisäksi uskottavan kansallisen kyberturvallisuuden ja laajemmin ulko- ja turvallisuuspoliittisen vaikuttamisen edistämiseksi tulee kehittää tavoitteellista attribuutioviitekehystä. Valtiollisesta vihamielisestä kybertoiminnasta puhuttaessa attribuutiolla tarkoitetaan yhtäältä vastuullisen valtiotahon tunnistamista koskevaa analyysi- ja päätöksentekoprosessia ja toisaalta sen pohjalta vastatoimena tehtyä julkista syyksilukemista. Valtiollisen vihamielisen kybertoiminnan vastaisessa toiminnassa keskeinen kysymys on, kuka on viime kädessä vihamielisestä kybertoiminnasta vastuussa oleva valtiontaho. Tämän vuoksi attribuutioprosessi edellyttää teknisten tietojen lisäksi laaja-alaista tietoa sekä strategista ja ulko- ja turvallisuuspoliittista arviota vihamielisen kybertoiminnan takana olevan valtiotahon ja sen motiivin selvittämiseksi ja eri reagointivaihtoehtojen punnitsemiseksi.

- Valtioneuvoston periaatepäätös 2021, Kyberturvallisuuden kehittämisohjelma Valto | Valtioneuvosto
- Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa | Valtioneuvosto

Yrityksillä on tärkeä vastuu kyberturvallisuuden ylläpitämisessä ja kehittämisessä

Kyberturvallisuuden ja -suojauksen kokonaisuus koostuu useista toimijoista. Tässä yrityksillä on tärkeä vastuu. Ne vastaavat yhteiskunnan toiminnan kannalta useiden keskeisten kriittisten palveluiden tuottamisesta. Ilman yksityisen sektorin palveluntarjoajia ei käytännössä olisi sähköistä viestintää – ainakaan kaikille kansalaisille tarjolla.

Esimerkiksi teleyritykset vastaavat kaikkien meidän käyttämien matkaviestinyhteyksien toimivuudesta ja tarjoavat verkkojensa kautta pääsyn vaikkapa internetiin. Ilman teleyrityksiä ei myöskään olisi antenni- tai kaapeli-TV-jakelua ja -palveluja. Teleyritykset ja pankit tarjoavat meille mobiilivarmenteet ja verkkopankkitunnukset, joilla voimme kirjautua sähköisiin asiointipalveluihin ja hoitaa nykyään useita viranomaisasioinnin tarpeita.

Suomessa toimialojen kyberturvallisuudesta vastaavat toimijat itse yhdessä toimialojen viranomaisten kanssa. Toimintaympäristön muuttuessa tarvitaan entistä enemmän julkisen ja yksityisten sektorin välistä yhteistyötä. Tällaisella yhteistyöllä kyberturvallisuudessa on Suomessa jo pitkät perinteet yhteiskunnan eri sektorien välillä ja sisällä. Tätä maailmallakin kiinnostusta herättänyttä yhteistyötä on rakennettu ja kehitetty pitkäjänteisesti kokonaisturvallisuuden periaatteiden ja konseptin mukaisesti. Vuosien aikana yhteistyötä on tiivistetty ja sille on luotu toimintamallit. Lisäksi yhteisestä harjoittelutoiminnasta saatuja oppeja viedään jatkuvasti käytäntöön eri sektoreilla.

Kybersuojauksen kokonaisuus syntyy huolella oman tehtävänsä hoitavista toimijoista, yhteistyöstä ja jatkuvasta tiedonvaihdosta.

> ” Yhteistyöllä kyberturvallisuudessa on Suomessa jo pitkät perinteet yhteiskunnan eri sektorien välillä ja sisällä.

Tietoturvan vuosi 2023

Uhkataso pysyi kohonneena

Vuonna 2022 nostettu kyberuhkataso pysyi vuoden 2023 aikana kohonneena. Suomeen kohdistettiin aktiivisesti erilaisia kyberhyökkäyksiä, muun muassa huijauksia, tietojenkalastelukampanjoita ja kiristyshaittaohjelmatapauksia. Kyberturvallisuuskeskukselle raportoidut poikkeamatapaukset kasvoivat noin 44 % verrattuna edellisvuoteen. Poikkeamatapauksissa kasvua oli esimerkiksi huijauksissa, tietomurron yrityksissä ja huijausviesteissä. Kyberturvallisuuskeskus julkaisi yhden varoituksen M365-sähköpostitilimurroista vuonna 2023.

Vuoden 2022 tavoin hyökkäykset olivat aiempia vuosia kohdennetumpia ja räätälöidympiä. Erilaisten kyberuhkatoimijoiden kyvykkyydet ovat kehittyneet mm. helposti saatavilla olevien palveluiden ja automatisoinnin myötä. Eri tavoin motivoituneet uhkatoimijat hyödyntävät samoja haittaohjelmia ja kriittisiä haavoittuvuuksia. Muun muassa tämän vuoksi on yhä hankalampi erottaa toimijoita toiminnan taustalta.

Venäjän hyökkäyksen jatkuminen Ukrainassa on näkynyt kybertoimintaympäristössä esimerkiksi Venäjä-mielisten haktivistien Venäjä-vastaisiksi koettuja toimia vastaan kohdistuneina palvelunestohyökkäyksinä Euroopassa. Suomessa palvelunestohyökkäyksiä havaittiin etenkin alkusyksystä lähtien. Hyökkäysten motiiveiksi ilmoitettiin julkisuudessa esimerkiksi poliittiset syyt. Vastaava toiminta oli yleistä myös muualla Euroopassa. Suomalaisiin organisaatioihin kohdistetuilla palvelunestohyökkäyksillä ei ollut merkittäviä vaikutuksia. Erityisesti kotimainen, matalan kynnyksen yhteistyö viranomaisten ja yrityskentän välillä korostuu vaikutusten rajoittamisessa.

Useassa poikkeamatapauksessa korostui organisaation aktiiviset toimenpiteet, joilla hyökkäystapausten vaikutukset saatiin rajattua. Analyysin perusteella vuoden 2023 poikkeamahavainnot korostivat esimerkiksi monivaiheisen tunnistautumisen käyttöönoton merkitystä organisaatioissa.

Keski-Uudenmaan koulutuskuntayhtymä Keuda sai Vuoden 2023 Tietoturvan suunnannäyttäjä -tunnustuksen avoimesta viestinnästään ja toiminnastaan jouduttuaan kiristyshaittaohjelmahyökkäyksen uhriksi. Avoin ja nopea viestintä kiristyshaittaohjelmahyökkäyksissä auttaa organisaatiota tapauksen selvittämisessä ja palautumisessa sekä tukee myös muita toimijoita kyberuhkiin varautumisessa.

Tietoturvan suunnannäyttäjä | Kyberturvallisuuskeskus

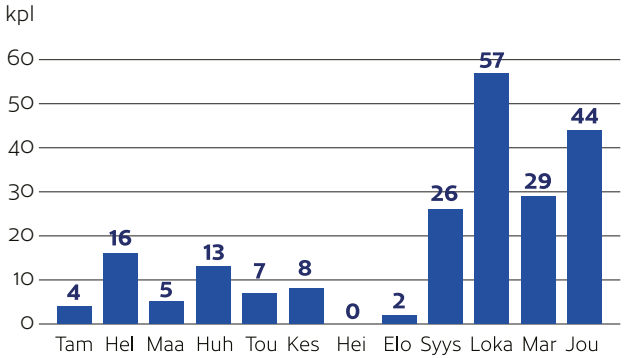
Palvelunestohyökkäykset

Palvelunestohyökkäyksissä verkkosivuille tai -palveluihin ohjataan suuria määriä liikennettä. Tämä näkyy käyttäjälle siten, että verkkosivuille ei pääse tai niiden käyttäminen on erittäin hidasta. Palvelunestohyökkäykset ovat helposti toteutettava ja näyttävä hyökkäystekniikka. Ne saavatkin usein huomiota myös mediassa. Yleisimmin palvelunestohyökkäyksistä ei aiheudu käyttäjille näkyviä vaikutuksia ja pahimmillaankin ne johtavat lähinnä julkisten verkkopalveluiden lyhyisiin käyttökatkoksiin.

Nykyisin palvelunestohyökkäykset ovat erityisen yleisiä haktivismin muotona. Haktivismi on kyberrikollisuutta, jossa rahallisen hyötymisen sijaan motiivit ovat poliittisia. Palvelunestohyökkäyksillä osoitetaan tyytymättömyyttä kohteen poliittiseen päätökseen tai muuhun toimintaan, ja pyritään vaikuttamaan informaatioympäristöön tapauksen ympärillä. Lisäksi lyhyetkin käyttökatkokset voivat kasvattaa epäluottamusta kohteena olevan tahon asiakkaissa ja sidosryhmissä. Haktivismi on lisääntynyt erityisesti Venäjän aloitettua hyökkäyssodan aktiivivaiheen Ukrainassa vuonna 2022. Niin Venäjä-mieliset kuin Ukrainaa tukevat haktivistiryhmät ovat käyttäneet palvelunestohyökkäyksiä informaatiovaikuttamisen keinona.

Kotimaassa palvelunestohyökkäyksiä raportoitiin etenkin keväällä NATO-liittymispäivänä 4.4. ja koko syksyn ajan. Etenkin venäjämielinen haktivistiryhmä NoName057(16) kohdisti palvelunestohyökkäyksiä eri sektoreiden kotimaisia organisaatioita kohti vuonna 2023. NoNamen tapana on juhlistaa palvelunestohyökkäysten toteutumista Telegram-kanavallaan, vaikka hyökkäyksellä ei olisi ollut minkäänlaisia vaikutuksia kohdesivun toimintaan. Osa julkis- ja valtionhallinnon verkkosivujen toimintaan vaikuttaneista palvelunestohyökkäyksistä päätyi myös kotimaiseen mediaan. Organisaatiot kertoivat julkisesti olevansa palvelunestohyökkäysten kohteena, mikäli verkkosivut ovat tämän vuoksi alhaalla. Vuonna 2024 palvelunestohyökkäyksistä ei enää ajatella aiheutuvan mainehaittaa organisaatiolle. Mikä tahansa organisaatio voi joutua palvelunestohyökkäyksen kohteeksi ja organisaatioiden tuleekin varautua myös sovellustason palvelunestohyökkäyksiin.

Kyberturvallisuuskeskuksen käsittelemät ilmoitukset palvelunestohyökkäyksistä 2023



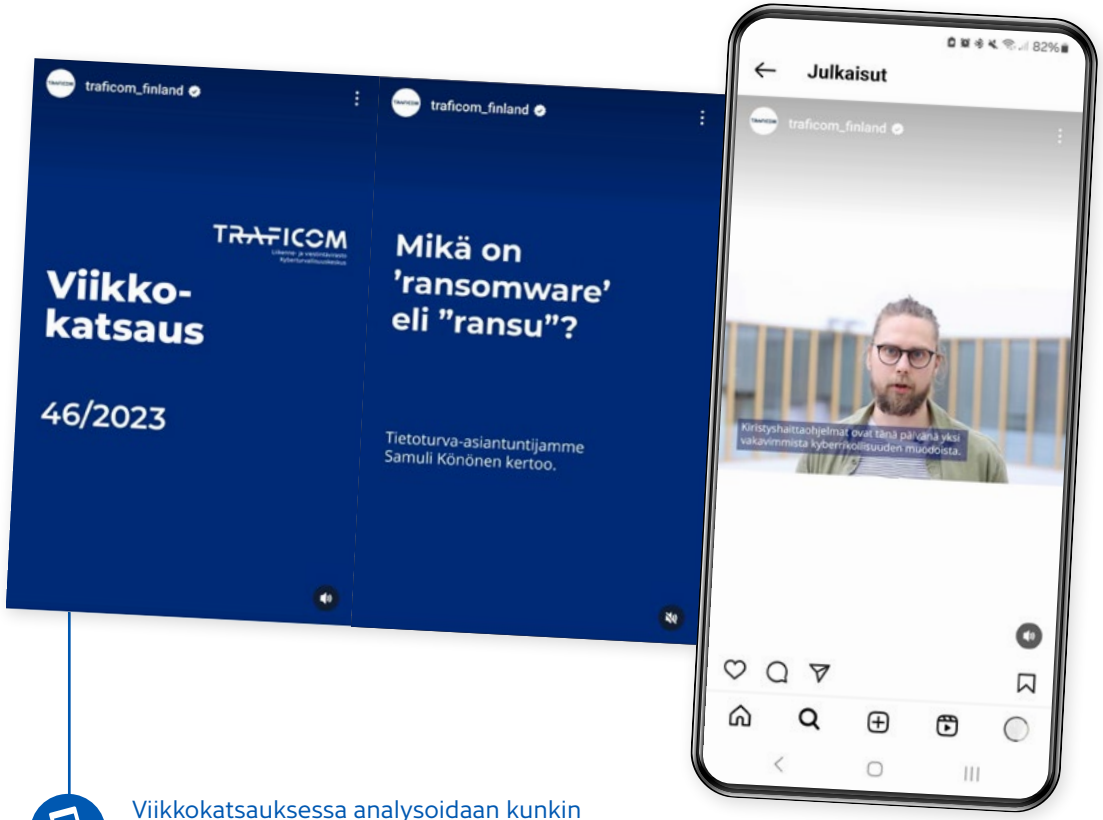
> Nykyisin palvelunestohyökkäykset ovat erityisen yleisiä haktivismin muotona.

Kiristyshaittaohjelmat

Kiristyshaittaohjelmatapaukset lisääntyivät Suomessa selvästi loppuvuonna, jolloin tapauksia raportoitiin enemmän kuin muilla kvartaaleilla. Tapaukset ovat koskettaneet useita aloja, mutta organisaatioiden toimilla on kyetty rajoittamaan niiden vaikutuksia. Esimerkiksi ajantasaiset varmuuskopiot ovat pelastaneet monen organisaation tilanteen.

Yleisesti kiristyshaittaohjelmatoimijoiden osalta vuonna 2023 havaittiin niiden kehittymistä yhä vaikuttavammiksi ja ammattimaisemmiksi. Maailmalla on raportoitu vakavia kiristyshaittaohjelmatapauksia esimerkiksi valtionhallinnoissa, oikeustoimissa ja terveydenhuoltoalalla. Näissä tapauksissa on esimerkiksi vuotanut sensitiivisiä henkilötietoja ja tapauksista palautuminen on voinut kestää viikoista kuukausiin. Suomessa yleisin kiristyshaittaohjelma vuonna 2023 oli Akira, johon liittyviä tapauksia raportoitiin etenkin loppuvuodesta.

Kiristyshaittaohjelmatapauksista koituu organisaatioille yleensä merkittävästi vaivaa ja kustannuksia. Kiristyshaittaohjelmahyökkäyksiin on usein vaikea reagoida hyökkäyksen alkamisen jälkeen. Hyvä varautuminen antaa paljon paremmat lähtökohdat toimia, kun poikkeamatilanne tapahtuu.



Viikkokatsauksessa analysoidaan kunkin viikon merkittävimmät kansalliset ja kansainväliset kybertapahtumat.

Lue lisää tilannekuvatuotteista sivulta 16.

Tietojenkalastelu ja verkkohuijaukset

Tietojenkalastelusta ja verkkohuijauksista lukumääräisesti eniten ilmoituksia tehtiin pankkitunnusten kalastelusta. Verkkopankkitunnuksia yritettiin huijata pankkien, verottajan, poliisin, Kelan ja muiden viranomaisten ja yritysten nimissä hyvin laajalla kirjolla. Seuraavaksi vilkkain huijauskohde oli Microsoft M365 -tunnusten kalastelu, josta Kyberturvallisuuskeskus julkaisi vakavan varoituksen viikolla 42. Kalastelluilla tunnuksilla tehtiin satoja sähköpostitilien tietomurtoja, joiden määrä alkoi onneksi vähentyä varoituksen julkaisemisen jälkeen.

Julkisuudessa raportoitiin maailmalta runsaasti erilaisten tekoälypohjaisten ratkaisujen käsittämistä ongelmista tieto- ja kyberturvallisuusongelmista, esimerkiksi vaalien turvallisuuteen liittyen. Vuonna 2023 tekoälyyn perustuvat suomenkieliset kyberpoikkeamahavainnot olivat Suomessa vielä harvinaisia. Kyberturvallisuuskeskuksen tietoon tuli yksi laadukkaasti toteutettu tekoälypohjainen syvävääreennös- eli deepfake-tapaus, jossa on kloonattu organisaation toimitusjohtajan ääntä ja pyydetty tekemään iso rahasiirto, mutta tässäkään ei Suomen kieltä käytetty.

Julkaisimme kesällä 2023 somessa tietoturvakampanjan, jonka tavoitteena oli lisätä tietoisuutta huijauksista ja tietojenkalastelusta kevyellä tavalla.

Lue lisää Kyberturvallisuuskeskuksen kampanjoista s. 19

Huijaussoittojen estämistä on taklattu viranomaisten ja teleyritysten tiiviillä yhteistyöllä jo useamman vuoden ajan. Lokakuun alussa 2023 voimaan tulleella Traficomin määräyksellä teleoperaattorit velvoitettiin torjumaan yhä paremmin ulkomailta tulevia, mutta suomalaisiksi naamioituja puheluita, myös mobiilinumeroiden osalta. Soittojen suodatus on nyt käytössä kaikilla suomalaisilla, ulkomailta liikennettä vastaanottavilla teleyrityksillä. Virastossa on valmisteilla määräys, jonka avulla torjutaan tulevaisuudessa myös tekstiviestihuijauksia.

Suomessa tehty työ huijaussoittojen estämiseksi on herättänyt myös poikkeuksellisen aktiivista kansainvälistä kiinnostusta, koska käyttöönotettu malli oli kansainvälisestikin vertailtuna hyvin edistynyt. Suomen viranomaiset ja teleyritykset esittelivät käyttöönotettua ratkaisumallia muun muassa Yhdysvalloissa keväällä 2023.

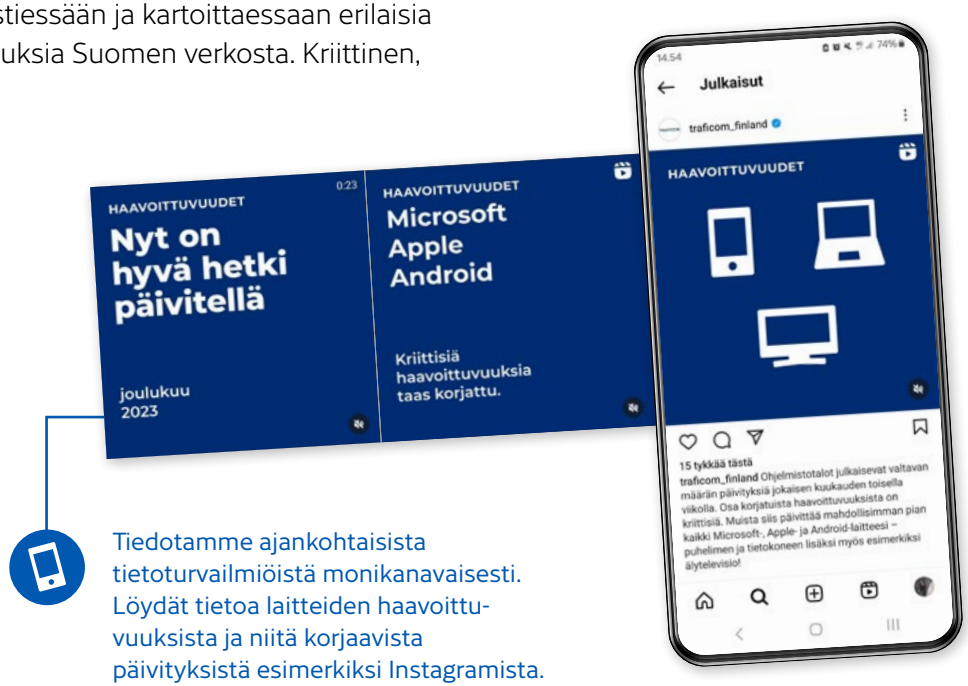
Väärennettyjen soittonumeroiden estäminen | Youtube

Haavoittuvuudet

Vuosi 2023 oli jälleen vilkas haavoittuvuuksien osalta. Maailmassa julkaistiin yli 20 000 uniikkia CVE-haavoittuvuustunnisteen omaavaa haavoittuvuutta. Osa haavoittuvuuksista on kriittisempiä kuin toiset. Näistä etenkin etänä hyväksikäytön mahdollistavat haavoittuvuudet korostuvat Kyberturvallisuuskeskuksen arjessa. Kriittinen haavoittuvuus voi mahdollistaa hyökkääjälle tietomurron lisäksi mahdollisuuden jopa kiristyshaittaohjelman asentamiseen. Kyberturvallisuuskeskus julkaisee vuosittain noin 30–40 haavoittuvuustiedotetta kriittisimmistä haavoittuvuuksista, jotka koskevat kotimaan käyttäjiä.

Kyberturvallisuuskeskus seuraa päivittäin haavoittuvuuksiin liittyvää uutisointia ja keskustelua. Vakavimmissa tapauksissa Kyberturvallisuuskeskus kartoittaa kotimaisia käyttäjiä ja kontaktoi suoraan organisaatiot, mikäli on epäilys tai havainto haavoittuvasta laitteesta. Verkon yli haavoittuvat laitteet ovat hyökkääjille kuin helppo kohde. Vuonna 2023 esimerkiksi Cisco-verkkolaitevalmistajan haavoittuvuutta käytettiin Suomessa kiristyshaittaohjelmatapauksien alkusysäyksenä useammassa tapauksessa. Tunnetun tietoturvayrityksen mukaan erityisesti kriittiset haavoittuvuudet ovat tärkeitä kirityshaittaohjelmatoimijoille. Esimerkiksi Lockbit-toimijaryhmä hyväksikäytti Citrix Bleed -haavoittuvuutta vuoden 2023 vakavia maailmanlaajuisia vaikutuksia aiheuttaneissa hyökkäyksissään.

Haavoittuvuuksien hyväksikäyttö on vuosi vuodelta nopeampaa. Kriittisen haavoittuvuuden julkaisun jälkeen hyökkääjien liikkeitä saatetaan havaita maailmalla jo lähipäivien aikana. Onneksi tiedonvaihto on kybermaailmassa aktiivista ja tieto hyväksikäytetyistä haavoittuvuuksista leviää. Kyberturvallisuuskeskus priorisoi jo maailmalla hyväksikäytettyjä haavoittuvuuksia viestiessään ja kartoittaessaan erilaisia haavoittuvuuksia Suomen verkosta. Kriittinen, jo hyväksikäytetty etänä suoritettavia komentoja hyökkääjälle mahdollistava haavoittuvuus suositussa verkkopalvelussa- tai laitteessa on usein kriittisin esimerkki vuositasolla. Tämänkaltaisia haavoittuvuuksia Suomessakin suosituissa ratkaisuissa on onneksi vuositasolla vain muutamia, jotka vaativat aktiivisempia toimia ja työtunteja niin viranomaisilta kuin yksityissektorinkin toimijoilta.



Tiedotamme ajankohtaisista tietoturvailmiöistä monikanavaisesti. Löydät tietoa laitteiden haavoittuvuuksista ja niitä korjaavista päivityksistä esimerkiksi Instagramista.

Kybervakoilu

Vuonna 2023 kybervakoiluyritykset jatkuivat aktiivisena edellisvuoden tapaan. Suomalaisten organisaatioiden käyttämiä palveluita, niiden erilaisia haavoittuvuuksia tai heikosti suojattuja käyttäjätunnuksia pyrittiin löytämään jatkuvasti.

Kohdistettuja haitallisia sähköpostiviestejä ja mobiililaitteisiin kohdistettuja haittaohjelmia hyödynnettiin osana kybervakoilua. Lisäksi laajasti käytettyihin pilvipalveluihin kohdistui kybervakoilua. Osa toiminnasta viittaa julkisten, kaupallisten, viranomais- tai muiden lähteiden pohjalta valtiollisten toimijoiden toimintaan.

Kansainvälisenä ilmiönä verkkolaitteiden ja sähköpostijärjestelmien haavoittuvuuksia hyödynnettiin yhä laajemmin osana kybervakoilua. Haavoittuvia koti- ja pienyritysreitittimiä sekä verkkolevypalvelimia hyödynnettiin laajasti osana valtiollisten toimijoiden toimintaympäristöä, joiden tavoitteena oli päästä lähemmäs haluttua kohdetta ja häivyttää liikenteen alkuperäinen lähde.

Venäjän hyökkäys Ukrainaan näkyi yhä kybervakoilussa ja -vaikuttamisessa. Ukrainassa havaittiin vuoden aikana esimerkiksi useita kriittisiä järjestelmiä häiritseviä hyökkäyksiä, tietoja kalastelevia sähköpostikampanjoita sekä haittaohjelmien levityskampanjoita.

Kybervakoilu voi kasvaa suoraan tai välillisesti Suomen NATO-jäsenyyden myötä. Muualla Euroopassa kybervakoilua on kohdistunut esimerkiksi sotaan liittyviin toimijoihin, logistiikkaan sekä teollisuuden ja teknologia-alan tuotekehitykseen.

Viestintäverkot toimivat vakaasti Suomessa vuonna 2023

Vuonna 2023 viestintäverkkojen toiminta oli Suomessa vakaata. Palvelukatkoksia tapahtui edellisvuotta selvästi enemmän, mutta vakavimpien katkosten määrässä oli sen sijaan laskua. Yksittäisissä katkoksissa häiriöitä aiheutui alueellisiin palveluihin tai hätäliikenteen hetkellisesti, mutta katkot olivat pääasiassa lyhytaikaisia. Sääolosuhteet olivat edellisvuotta huomattavasti myrskyisämmät, mikä osaltaan vaikutti siihen, että sähkökatkoista johtuneiden häiriöiden määrä kaksinkertaistui vuoteen 2022 verrattuna. Pitkällä aikavälillä tarkasteltuna yleisten viestintäpalveluiden toimivuushäiriöiden ja erityisesti vakavimpien vikatilanteiden määrä jatkaa laskuaan, vaikka tilastollisesti poikkeukselliseen edellisvuoteen verrattuna merkittävien toimivuushäiriöiden lukumäärä kokonaisuudessaan kasvoikin huomattavasti.

Viranomaiset tekevät tiivistä yhteistyötä suomalaisten teleyritysten kanssa verkkojen toiminnan turvaamisessa.

Merenalaisen infrastruktuurin vaurioituminen lokakuussa 2023

Vuoden 2023 ehkä näkyvin kyberturvallisuustapaus oli merenalaisen infrastruktuurin vaurioituminen Suomenlahdella lokakuussa 2023: Suomen ja Viron välisessä Balticconnector-kaasuputkessa havaittiin 8.10. aamuyöllä vuototilanne ja sen aiheuttama häiriö. Sunnuntaina 8.10. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus sai tiedon suomalaiselta teleyritykseltä Viron ja Suomen välisen merikaapelin katkeamisesta Suomenlahdella ja samaisena viikonloppuna myös toisen teleyrityksen merikaapeli Ruotsin ja Viron välillä vaurioitui siten, että se välitti liikennettä normaalia alhaisemmalla kapasiteetilla.

Yleisten viestintäverkkojen ja -palvelujen eli teletoiminnan toimintavarmuudesta ja varautumisesta huolehtiminen on ollut osa toimijoita koskevaa lainsäädäntöä ja viranomaisohjausta ja -valvontaa jo 1990-luvulta lähtien. Tällä ja Kyberturvallisuuskeskuksen jatkuvasti tekemällä teleyritysyhteistyöllä on merkittävä vaikutus siihen, että mm. merikaapelien katkeamisista on tuskin lainkaan näkyviä vaikutuksia teleyritysten asiakkaille. Lokakuun tapauksessakin normaalien varautumiskäytäntöjen mukaan, teleyritys siirsi Suomen ja Viron välisen kaapelin liikenteen välittömästi varayhteydelle ja tietoliikenne Suomen ja Viron välillä toimi siten ongelmitta. Katkoksella ei siis ollut vaikutusta suomalaisten tai virolaisten viestintäpalvelujen toimivuuteen.

Kyberturvallisuuskeskus muodosti tapauksesta tilannekuvaa. Keskus seurasi katkenneen kaapelin korjaustoimien edistymistä tiiviissä yhteistyössä teleyrityksen ja muiden viranomaisten kanssa, niin kansallisesti kuin kansainvälisesti. Tällä toiminnalla tuettiin valtioneuvoston päätöksentekoa.

Lokakuun tapauksen käsittely jatkuu edelleen Suomessa ja Virossa esitutkintaviranomaisten toimesta. Kyberturvallisuuskeskus jatkaa kansallista ja kansainvälistä yhteistyötä teleyritysten ja muiden viranomaisten kanssa viestintäverkkoinfrastruktuurin suojaamiseksi sekä mahdollisten ongelmien ennaltaehkäisemiseksi, havaitsemiseksi ja korjaamiseksi.

Traficomin Kyberturvallisuus-keskuksen vuosi 2023

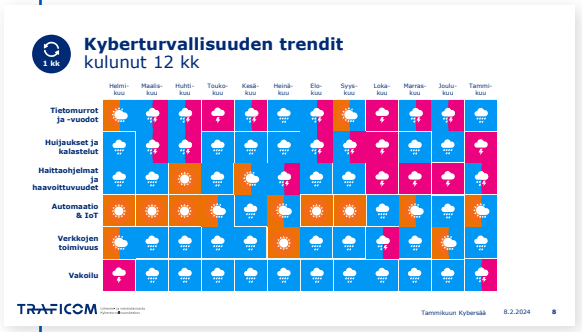
Liikenne- ja viestintäviraston ja erityisesti sen Kyber-turvallisuuskeskuksen merkitys yhtenä turvallisuus-viranomaisena koko yhteiskunnalle on vahvistunut muuttuneessa turvallisuusympäristössä viimeisten vuosien aikana. Havainnointikyvyn sekä verkostojen ja näissä vaihdettavan tiedon avulla Kyberturvallisuus-keskus kykenee yhdessä kumppaniensa kanssa vastamaan nopeasti yhteiskuntaan vaikuttaviin kyber-uhkiin ja merkittävästi vähentämään uhkien vaiku-tuksia yhteiskunnalle, digitaaliselle infrastruktuurille ja kansalaisille. Kyberturvallisuuskeskus arvioi, että yksin sen tietoturvaloukkausten käsittelyä ja kansa-laisten auttamista koskevat toimet tuottavat yhteis-kunnalle merkittävän euromääräisen nettohyödyn vuosittain.

Tukea yhteiskunnan kyberturvallisuutta koskevaan tilannetietoisuuteen

Kyberturvallisuuskeskuksen tehtäviin kuuluu tuottaa yhdistettyä kansallista kyberturvallisuutta koskevaa tilannekuvaa. Keskus kerää tietoja tietoverkkotapahtumista ja välittää sitä eri toimijoille. Tilannekuvan muodostamisessa hyödynnetään laajasti kansallisia ja kansainvälisiä lähteitä, kuten huoltovarmuuskriittisten organisaatioiden verkostoja, muita turvallisuusviranomaisia sekä Kyberturvallisuuskeskuksen virallisia, vapaaehtoisuuteen ja molemminpuoliseen luottamukseen perustuvia kansallisia ja kansainvälisiä yhteistyöverkostoja. Lisäksi Kyberturvallisuuskeskus saa vuosittain yli kymmenentuhatta vapaaehtoista ilmoitusta esimerkiksi kansalaisilta. Kyberturvallisuuskeskuksen asiakkaat hyödyntävät tilannekuvatietoa varautumisensa kehittämisessä sekä päivittäisessä toiminnassaan.

Esimerkkeinä keskuksen julkisista tilannekuvatuotteista voidaan mainita viikoittain ilmestyvä tilannekuvakooste Kyberturvallisuuskeskuksen viikkokatsaus, jossa analysoidaan kunkin viikon merkittävimmät kansalliset ja kansainväliset kybertapahtumat. Kuukausittain ilmestyvässä Kybersäässä tarkastellaan puolestaan kyberturvallisuuteen pidemmällä aikavälillä vaikuttavia kehityskulkuja. Sekä Viikkokatsaus että Kybersää ovat saatavilla Kyberturvallisuuskeskuksen verkkosivuilla. Kyberturvallisuuskeskus tuottaa myös kyberturvallisuutta koskevaa strategista tilannekuvaa ylimmän valtionjohdon käyttöön.

Kyberturvallisuuskeskuksen viikkokatsaus | Kyberturvallisuuskeskus



Kybersään tavoitteena on kertoa kybermaailman tapahtumista mahdollisimman ymmärrettävästi ja tiiviissä paketissa.

Kybersää – ajankohtaista tietoturvasta | Kyberturvallisuuskeskus

Kyberturvallisuuskeskuksen tuottamilla tilannekuvatuotteilla on tärkeä rooli yhteiskunnallisen kyberturvallisuutta koskevan tilanneymmärryksen, vaikuttavuuden ja varautumisen kehittämisessä. Keskuksen julkisista tilannekuvatuotteista laadittiin kysely vuoden 2023 aikana ja kyselyyn vastanneiden antama arvio tuotteista oli erinomainen (keskiarvo 4,3 asteikolla 0–5).

Kansainvälinen yhteistyö tiivistyi vuoden 2023 aikana

Kyberturvallisuuskeskus tekee päivittäin tiivistä yhteistyötä koti- ja ulkomaisten kumppanien sekä verkostojen kanssa. Tämä pitää sisällään esimerkiksi tietojen ja kyberturvallisuutta koskevan tilannekuvan vaihtoa, tapaamisia, koulutuksia ja harjoitustoimintaa. Kansainvälisen yhteistyön myötä osaaminen ja tietoisuus vallitsevasta kyberuhkatilanteesta kasvaa. Yhteistyö auttaa siten ennaltaehkäisemään Suomeen kohdistuvia kyberuhkia.

Kansainväliset verkostot ja yhteistyö ovat myös tärkeässä roolissa erilaisten akuuttien tietoturva- ja kyberpoikkeamatapausten selvityksessä. Myös Suomessa vallitsevan kyberuhkatilanteen skaalaaminen kansainväliseen tilanteeseen mahdollistuu verkostojen kautta.

Vuoden 2023 aikana Kyberturvallisuuskeskuksen asiantuntijat jatkoivat kahdenvälisten suhteiden tiivistämistä keskeisiin kumppanimaihin, kuten Ruotsiin ja Viroon. Keskuksen kansainvälisten asioiden vaikuttamista ja koordinaatiota vahvistettiin myös uudella kansainvälisten asioiden päällikön toimenkuvalla.

Kyberturvallisuuden kansainvälisessä yhteistyössä vuonna 2023 keskeiset teemat olivat operatiivinen yhteistyö, strategisen tason yhteistyön kehittäminen EU:ssa ja lukuisat kyberturvallisuutta koskevat sääntelyhankkeet niin ikään EU:n tasolla. EU-kokonaisuuksien rinnalla Kyberturvallisuuskeskus jatkoi kansallisia toimenpiteitä osana kansallista NATO-koordinaatiota. NATO-jäsenyyden myötä kansainvälinen yhteistyö laajeni uusille alueille.

Traficomin Kyberturvallisuuskeskuksen verkkosivuilta löytyy tietoa kyberturvallisuutta koskevaan harjoitustoimintaan

Harjoitustoiminta | Kyberturvallisuuskeskus

Harjoitustoiminta jatkui aktiivisena

Onnistunut toiminta erilaisissa turvallisuustilanteissa edellyttää ajantasaisten suunnitelmien lisäksi myös säännöllistä harjoittelua. Harjoitukset tarjoavat arvokasta tietoa organisaatioiden operatiivisen toiminnan, johtamisen, viestinnän ja tilannekuvatoiminnan kehittämiseen.

Vuoden 2023 aikana kyberturvallisuutta koskeva harjoitustoiminta jatkui aktiivisena niin koti- kuin ulkomailla. Edellisvuosia enemmän harjoituksiin osallistui kotimaassa keskeisiä palveluntarjoajia ja -toimittajia. Harjoituksissa korostui operatiivisten rajapintojen vastuualueiden ja niihin liittyvien sopimusten tarkastelu. Kyberuhka voi myös kohdistua palvelukumppaniin ja heijastua sitä kautta omaan toimintaan.

Tulevaisuudessa, erityisesti isommissa kansallisissa harjoituksissa, tullaan tarkastelemaan laajemmin toimialojen sisäisiä toimitusketjuja ja toimialojen välisiä riippuvuuksia.

Ennakointityö tukee tulevaisuuden ilmiöihin varautumista

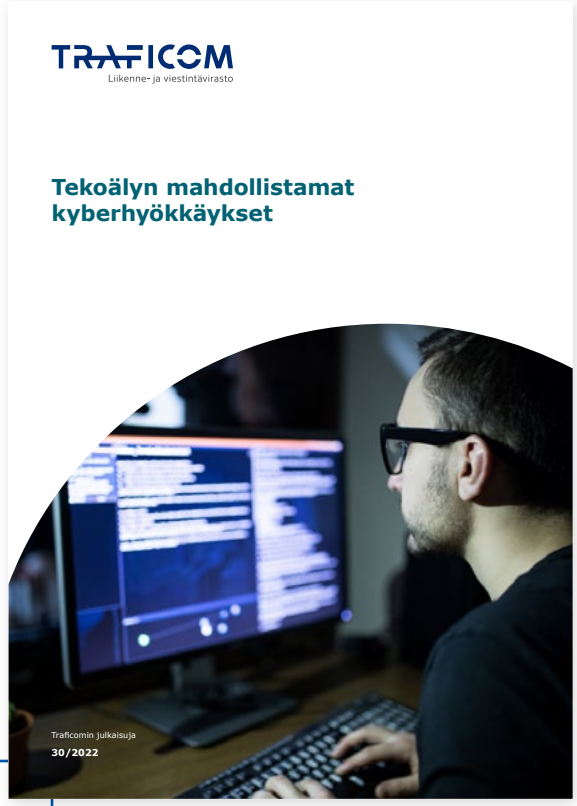
Tulevaisuus- ja ennakointityötä kehitettiin tulevaisuuden ilmiöihin ja teknologiseen kehitykseen varautumiseksi ja ennakointiajattelun vahvistamiseksi koko keskuksessa. Lisäksi jatkettiin yhteistyön rakentamista yhteiskunnan eri sektorien kanssa.

Tulevaisuus- ja ennakointityön keskeisenä painopistealueena oli vuonna 2023 tarkastella erilaisten kyberskenaarioiden toteutumista tulevaisuuden toimintaympäristön mahdollisten kehityskulkujen ymmärtämiseksi. Ennakointityössä jatkettiin tekoälyn vaikutuksien arvioimista, ja Traficom käynnisti kolmannen tekoälyä käsittelevän selvityksen laatimisen. Talvella 2024 julkaistavassa selvityksessä pureudutaan tekoälyn hyödyntämiseen kyberturvallisuuden edistämisessä ja tekoälypohjaisiin kyberturvallisuusratkaisuihin. Selvitys on aihepiirinsä kolmas, ja täydentää aiempia tekoälyselvityksiä, jotka käsittelivät tekoälyn riskienhallintaa ja tekoälyn mahdollistamia kyberhyökkäyksiä. Selvityksissä on kuultu laajaa joukkoa tietoturva-alan ammattilaisia yksityiseltä ja julkiselta sektorilta sekä tutkimuslaitoksista. Selvitykset on toteutettu yhteistyössä Huoltovarmuuskeskuksen kanssa.

Ennakointityössä käsiteltiin lisäksi paikallisten matkaviestinverkkojen toteuttamisen kyberturvallisuutta ja riskienhallintaa. Monet yhteiskunnan toimintojen kannalta kriittiset toimijat tulevat todennäköisesti tulevaisuudessa hyödyntämään paikallisia omiin tarpeisiin räätälöityjä matkaviestinverkkoja toimintansa digitalisoimiseen ja tehostamiseen. Näihin verkkototeutuksiin liittyy uudenlaisia riskejä ja osaamisvaatimuksia, jotka on tärkeää ottaa huomioon verkkoja toteutettaessa. Edellä mainituista teemoista tuotettiin myös julkaisut Kyberturvallisuuskeskuksen verkkosivuille. Selvitykset ja ohjeet toteutettiin yhdessä Huoltovarmuuskeskuksen kanssa.

Traficom järjestää 2024 kolmannen 5G hackathonin. Hack the Networks -tapahtuma järjestetään toukokuussa, ja tämän vuoden hackathonin keskiössä ovat kriittisessä infrastruktuurissa käytettävien paikallisten 5G-verkkojen turvallisuus. Lisätietoja hackthenetworks.fi

- Tekoälyn mahdollistamat kyberhyökkäykset | Traficom
- Tekoälyn soveltamisen kyberturvallisuus ja riskienhallinta | Traficom
- Ohje paikallisten matkaviestinverkkojen kyberturvallisuudesta ja riskienhallinnasta | Kyberturvallisuuskeskus



Traficomin Kyberturvallisuuskeskuksen ja Huoltovarmuuskeskuksen teettämän selvityksen toinen osa Tekoälyn mahdollistamat kyberhyökkäykset esiteltiin loppuvuodesta 2023.

Tietoisuuden lisääminen ja viestintä

Kyberuhkiin varautumisessa ja vastaamisessa viestinnällä on keskeinen rooli. Yhteiskunnan digitalisoituessa vauhdilla tietoturvataitojen hallinta ja niiden jatkuva kehittäminen ovat tärkeitä taitoja. Ilman tietoisuutta erilaisista uhkista niihin ei voida varautua eikä niitä voida torjua.

Kyberturvallisuuteen liittyvät asiat, erityisesti uhkat nousevat hyvin nopeasti julkiseen keskusteluun. Ne kiinnostavat ja herättävät myös huolta. Kun kyberturvallisuudesta keskustellaan, on tärkeää, että keskustelua käydään oikean ja ajantasaisen tiedon perusteella. Tähän tiedontarpeeseen Traficom vastaa tuottamalla ja jakamalla jatkuvasti kyberturvallisuutta koskevaa tietoa eri kohdeyleisölle. Ylimmän valtionjohdon kyberturvallisuutta koskevan päätöksenteon tueksi tuotetaan strategista tilannekuva-analyysiä. Viikoittain julkaistava Kyberturvallisuuskeskuksen viikkokatsaus ja kuukausittain julkaistava kybersää kertovat suurelle yleisölle esimerkiksi, millaisiin huijausviesteihin tai tietojenkalastelukampanjoihin he voivat arjessaan törmätä.

Vuosittain yhdessä Huoltovarmuuskeskuksen kanssa järjestettävä Tietoturvaseminaari kokosi viime vuonna lokakuussa yli 2000 osallistujaa. Traficomin verkkosivujen ja sosiaalisen median tilien kautta tavoitetaan päivittäin laajasti erilaisia kohdeyleisöjä. Lisäksi keskuksen asiantuntijat antavat säännöllisesti haastatteluja medialle. Verkkosivuilla jaetaan ohjeita ja oppaita sekä vinkkejä arjen tietoturvataitojen kehittämiseen. Messuihin ja tapahtumiin sekä eri kohdeyleisöille suunnatut ja viestintäkampanjat kuuluvat osana keinoihin, joilla pyritään lisäämään kyberturvallisuutta koskevaa tietoisuutta yhteiskunnassa.

Digikaistan tietoturvakampanja tavoitti Metassa tehokkaasti kohderyhmää hyvin edullisella CPM-hinnalla.

Lue lisää kansalaisten tietoturvataidoista sivulta 29.

Vuonna 2023 käynnistettiin valtakunnallisen suuren yleisön kyberturvallisuutta koskevan laajan viestintäkampanjan suunnittelu ja konseptointi. Kampanja toteutetaan yhdessä Digi- ja väestötietoviraston sekä Keskusrikospoliisin kanssa loppukeväästä 2024.

Verkostoyhteistyötä kehitettiin edelleen vuonna 2023

Vuonna 2023 Kyberturvallisuuskeskuksen verkostoyhteistyö kehittyi voimakkaasti. ISAC-tiedonvaihtoryhmien merkitys korostui etenkin tilannekuvan tuottamisessa sekä yhteiskunnan kriittisten toimialojen keskinäisessä tiedonvaihdossa varautumiseen ja häiriötilanteiden hallintaan liittyen.

Kiinnostus verkostotoimintaa kohtaan kasvoi viime vuoden aikana. ISAC-tiedonvaihtoryhmiin (Information Sharing and Analysis Centre) liittyi useita uusia organisaatioita ja hyvinvointialueet kutsuttiin osaksi sosiaali- ja terveysalan tiedonvaihtoryhmää. Vuoden aikana perustettiin uudet ISAC-tiedonvaihtoryhmät kunta-alalle, tietoturvayrityksille sekä energia-alan toimijoille. Sama kehitys jatkuu myös vuonna 2024, sillä kuluvan vuoden aikana on suunniteltu perustettavaksi tiedonvaihtoryhmät muun muassa kiinteistö- ja rakennusalalle sekä korkean teknologian toimijoille.

Verkostoihin liittyvä tiedonvaihto kansainvälistyi vuoden 2023 aikana. Suomi on ollut aiempaa aktiivisempi jäsen kansainvälisillä foorumeilla ja myös kahdenvälinen verkostoituminen kansainvälisesti on tehostunut huomattavasti.

Myös viranomaisten välinen yhteistyö ja tiedonvaihto olivat aktiivisen kehittämisen kohteena. Valvovien viranomaisten välinen nk. NIS-yhteistyöryhmä valmistautui NIS2-direktiivin kansalliseen toimeenpanoon. NIS2-direktiivi mm. lisää valvottavien toimialojen määrää ja tuo olemassa oleville valvoville viranomaisille lisätehtäviä. Vuoden 2024 aikana NIS-yhteistyöryhmä laajentuu huomattavasti, kun mukaan liittyvät myös uudet NIS2-direktiiviä valvovat viranomaiset. Tätä ennakoiden Traficom laajensi vuoden 2023 aikana olemassa olevaa tietoturvallisuuden neuvontapalveluaan valvoville viranomaisille. Lisäksi jo entuudestaan aktiivinen turvallisuusviranomaisten tiedonvaihto on edelleen aktivoitunut turvallisuusympäristön muutoksesta johtuen.

Luottamusverkostoina toimivien tiedonvaihtoryhmien yhteiskunnallinen merkitys on kasvanut kuluneen vuoden aikana ja verkostot ovat entistäkin merkittävämpi osa kyberturvallisuuden kansallista tilannekuvaa ja häiriötilanteiden hallintaa. Vuoden 2023 aikana luottamusverkostojen tiedonvaihtoa tehostettiin ja myös toimialarajat ylittävää tiedonvaihtoa parannettiin. Tiedonvaihtoryhmissä varautuminen ja hybridivaikuttaminen olivat aiempaa enemmän esillä. Lisäksi kyberharjoitteluun on panostettu aiempaa enemmän.

Kyberturvallisuuskeskus panosti myös ajantasaiseen tiedonjakoon eri verkostoille. Tästä esimerkkeinä ovat syksyllä pilotoitu viikoittainen sektoriraportti sekä tarvittaessa lyhyellä varoitusajalla järjestettävät operatiiviset tiedontasaukset vakaviin ja akuutteihin tietoturvauhkiin liittyen. Osa tiedontasauksista on järjestetty luottamusverkostojen lisäksi laajemmin huoltovarmuuden kannalta kriittisille toimijoille. Merkittävää tietoturvauhkaa käsitelleeseen operatiivisen tiedontasaukseen saatiin päivän varoitusajalla yli kuusisataa osallistujaa.

> ” Vuoden aikana perustettiin uudet ISAC-tiedonvaihtoryhmät kunta-alalle, tietoturvayrityksille sekä energia-alan toimijoille.

Yhteiskunnan turvallisuutta edistettiin kyberturvallisuuden turvallisuuden kehittämishankkeilla

Kyberturvallisuuskeskus on toteuttanut viime vuosina useita hankkeita yhteiskunnan elintärkeiden toimijoiden kyberturvallisuuden ja sitä kautta koko yhteiskunnan varautumisen ja kyberturvallisuuden parantamiseksi. Huoltovarmuuskeskuksella on ollut näissä hankkeissa keskeinen rooli niin hankkeiden rahoittajana kuin myös tukijana niiden toteuttamisessa. Myös valtiovarainministeriö on osallistunut Kyberturvallisuuskeskuksen toteuttamien kehittämishankkeiden rahoittamiseen.

Huoltovarmuuskeskuksen rahoittamien ja tukemien kehittämishankkeiden kohteena ovat yhteiskunnan kannalta elintärkeät yritykset ja niiden kyberturvallisuus. Valtiovarainministeriön rahoittamien ja tukemien kehityshankkeiden kohteena on puolestaan julkisen hallinnon kyberturvallisuuden kehittäminen.

Toteutettuja palveluita ovat esimerkiksi

- **Havaro**, joka havainnoi suomalaisiin yrityksiin kohdistuvia vakavia tietoturvauhkia ja varoittaa niistä. Havaro.fi
- **Hyöky**, Kansallinen Hyökkäyspintakartoitus kyberturvallisuuden parantamiseksi kunnissa. Hyöky | Kyberturvallisuuskeskus
- **Kybermittari**, ilmainen kyberturvallisuuden arviointi- ja kehittämispalvelu. Se on organisaatioiden johdolle ja tietoturvaammattilaisille suunnattu, konkreettinen väline kyberturvallisuuden hallintaan, toimialakohtaiseen vertailuun ja kehityspanostusten ohjaamiseen. Kybermittari.fi

Huoltovarmuuskeskuksen rahoittamat kehityshankkeet rahoitetaan Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030 -ohjelmasta ja ne noudattavat ohjelmassa asetettuja tavoitteita.

Valtiovarainministeriön rahoittamat kehityshankkeet on rahoitettu valtiovarainministeriön Julkisen hallinnon digitaalisen turvallisuuden toimeenpano 2020–2023 (Haukka) -ohjelmasta.

Tukea yritysten tietoturvan kehittämiseen

Vuonna 2023 Kyberturvallisuuskeskus myönsi tietoturvan kehittämisen tukea 251 yritykselle yhteensä noin 5,2 miljoonan euron edestä yrityksien oman tietoturvan parantamiseen. Tästä enintään 15 000 euron tukina myönnettiin noin 3,2 miljoonaa euroa ja enintään 100 000 euron tukina 2 miljoonaa euroa. Kaiken kaikkiaan Kyberturvallisuuskeskus käsitteli vuoden aikana 409 yrityksen tukihakemukset.

Noin 40 prosenttia tukihakemuksista hylättiin muun muassa johtuen siitä, että yritys ei täyttänyt lainsäädännön asettamia vaatimuksia tuen myöntämiseksi tai tukihakemus oli puutteellinen, jolloin ei voitu varmistua tuen myöntämiseksi asetettujen vaatimusten täyttymisestä. Kaiken kaikkiaan tukea oli vuoden loppuun mennessä hakenut 740 yritystä noin 19 miljoonan euron edestä, kun määrärahaa tukien myöntämiseksi oli varattua vain 6 miljoonaa euroa. Varatusta 6 miljoonan euron määrärahasta loput noin 0,8 miljoonaa euroa myönnetään vuoden 2024 alkupuoliskolla.

Kokemuksia Tietoturvamerkistä hyödynnetään aktiivisesti EU:n kyberturvallisuusvaatimusten sääntelyn seurannassa ja vaikuttamisessa

Kyberturvallisuuskeskuksen vuonna 2019 julkaisema Tietoturvamerkki kertoo siitä, että merkillä varustettu tuote tai palvelu täyttää Traficomin vaatimukset tietoturvan hyvästä perustasosta. Merkin vaatimukset pohjaavat eurooppalaiseen standardiin. Merkki voidaan myöntää kuluttajien internetiin yhdistettävälle älylaitteelle, eli niin sanotulle IoT-laitteelle. Näitä laitteita ovat esimerkiksi älytelevisiot, älyrannekkeet ja kodin reitittimet.

Vuoden 2023 aikana Tietoturvamerkki myönnettiin yhdelle uudelle laitteelle. Merkki on tällä hetkellä voimassa 25 laitteella. Merkkimäärää on kasvattanut viime vuosina osaltaan vuonna 2021 aloitettu yhteistyö Singaporen kyberturvallisuusviranomaisen kanssa.

Tietoturvamerkin rooli tuotteiden tietoturvallisuuden osoittamisessa vähenee tulevina vuosina voimaan tulevien EU:n sääntelymuutosten myötä. Tietoturvamerkkitoiminnan tuottamaa tietoa hyödynnetään aktiivisesti EU:n kyberturvallisuusvaatimusten sääntelyn seurannassa ja vaikuttamisessa. Traficomin Kyberturvallisuuskeskus varautuu muuttamaan toimintaansa edellä mainitun sääntelyn tehtäviin.

Kansallisen koordinointikeskuksen toiminta

Liikenne- ja viestintävirastossa sijaitsevaan Kyberturvallisuuskeskukseen perustettiin vuoden 2023 alussa uusi Kyberturvallisuuden tutkimuksen, kehityksen ja innovaatioiden Suomen kansallinen koordinointikeskus (National Coordination Centre Finland, NCC-FI), jonka tehtävänä on luoda edellytyksiä suomalaiselle kyberturvallisuustoimialalle, kuten yrityksille, korkeakouluille ja tutkimuslaitoksille osallistua kansainväliseen tutkimus- ja kehitystoimintaan. Kansallinen koordinointikeskus on osa Euroopan unionin jäsenvaltioiden kansallisten koordinointikeskusten ja Euroopan kyberturvallisuuden kompetenssikeskuksen (European Cybersecurity Competence Centre, ECCC) muodostamaa osaamis- ja yhteistyöverkostoa.

Kansallisen koordinointikeskus (NCC-FI) sai Digitaalinen Eurooppa -ohjelmasta kaudelle 2023–2024 hankerahoitusta, jota se voi jakaa eteenpäin kolmansille osapuolille modernien kyberturvallisuusratkaisujen ja -innovaatioiden käyttöönottoon ja levittämiseen. Rahoitusohjelmalla Euroopan komissio tavoittelee kyberturvallisuuskapasiteetin ja strategisen omavaraisuuden kasvattamista jäsenmaissaan.

Ensimmäinen rahoitustukihaku kolmansille osapuolille oli auki 16.6.–16.8.2023. Tukea pystyivät hakemaan Suomeen rekisteröidyt pk-yritykset. Kansallisen koordinointikeskuksen järjestämän ensimmäisen rahoitustukihaun päätökset annettiin 15.11.2023. Rahoitustukea myönnettiin 13 hakijalle yhteensä noin 485 000 eurolla. Rahoitustukea oli haettavissa yhteensä 500 000 euroa ja tukea haettiin yhteensä noin 633 000 euron edestä.

Tietoturva

> ” Rahoitusohjelmalla Euroopan komissio tavoittelee kyberturvallisuuskapasiteetin ja strategisen omavaraisuuden kasvattamista jäsenmaissaan.

Kyberturvallisuuskeskus tuki lainsäädännön kehittämistä

Kyberturvallisuuden sääntelyyn on niin EU- kuin kansallisellakin tasolla kiinnitetty kiitettävästi ja enenevässä määrin huomiota. Keskeisempiä säädöshankkeita vuonna 2023 olivat muun muassa NIS2-direktiivin kansallinen täytäntöönpanotyö ja täytäntöönpanotyötä koskeva koordinaatio EU:n tasolla, kyberkestävyyssäädöstä koskevien neuvotteluiden loppuunsaattaminen, kybersolidaarisuussäädöstä koskevat neuvottelut sekä uuden eIDAS-asetuksen valmistelu. Virastolle ja siten myös keskukselle suunnitellaan myös enenevässä määrin uusia tehtäviä kyberturvallisuuslainsäädännön noudattamisen valvomiseksi.

Liikenne- ja viestintäviraston osana Kyberturvallisuuskeskus tukee lainsäädännön kehittämistä tarjoamalla lainvalmisteluun asiantuntijaosaamistaan. Keskus lausui vuonna 2023 kymmeniin EU- ja kotimaisiin säädösvalmisteluihin ja se osallistuu aktiivisesti alansa yhteistyöryhmiin niin sääntelyn laadukkaasti valmistelemiseksi kuin olemassa olevan sääntelyn noudattamisen varmistamiseksi.

Kyberturvallisuuskeskus ohjaa ja valvoo teletoiminnan tietoturvaa, toimintavarmuutta ja varautumista sekä vahvojen sähköisten tunnistus- ja luottamuspalvelujen ja EU:n verkko- ja tietoturvadirektiivissä (NIS-direktiivi) tarkoitettujen digitaalisen infrastruktuurin ja digitaalisten palvelujen tarjonnan tietoturvaa. Lisäksi se valvoo luottamuksellisen viestinnän suojan toteutumista sähköisessä viestinnässä. Osana Liikenne- ja viestintävirastoa keskus myös antaa lakia tarkentavia määräyksiä valvomilleen toimijoille ja neuvoo päivittäin niin kansalaisia kuin yrityksiä sääntelyn noudattamisesta.

Määräyksiä uudistetaan säännöllisesti vastaamaan kyberturvallisuusympäristössä ja teknisessä kehityksessä tapahtuviin muutoksiin. Tästä esimerkkinä on vuoden 2023 aikana uudistettu teletoiminnan tietoturvaa koskevaa määräystä ja uusittu määräys tullaan antamaan alkuvuoden 2024 aikana.

Sääntelyn noudattamista valvottiin vuonna 2023 mm. käsittelemällä satoja toimintavarmuuden ja tietoturvan häiriöilmoituksia sekä antamalla tapauskohtaisia valvontapäätöksiä mm. koskien evästeiden käyttöä verkkosivuilla. Keskus myös toteutti mm. laitetilojen kulunvalvontojen ja merikaapelien maihinnousupaikkojen tarkastuksia teleyrityksiin.

Sääntelyn osalta keskeisempiä EU-hankkeita vuonna 2023 olivat muun muassa NIS2-direktiivin kansallinen täytäntöönpanotyö ja täytäntöönpanotyötä koskeva koordinaatio EU:n tasolla, kyberkestävyyssäädöstä koskevien neuvotteluiden loppuunsaattaminen, kybersolidaarisuussäädöstä koskevat neuvottelut ja lukuisat työryhmäkeskustelut kriittisen infrastruktuurin suojaamisen vahvistamiseksi.

Kyberturvallisuuden trendejä vuonna 2024

Kyberturvallisuuden uhkataso pysyy vuonna 2024 edelleen kohonneena.

Näkymiä kyberturvallisuuden yleiseen uhkatasoon vuonna 2024

Vuoden 2024 aikana kiristyshaittaohjelmatapauksia nähdään maailmalla todennäköisesti yhä enemmän ja ne ovat vakavampia ja kehittyneempiä. Tämä tilanne heijastuu myös Suomeen, mutta yritysten aktiivisilla ja huolellisilla suojaus- ja torjuntatoimilla ja yhteistyöllä kyetään myös jatkossa rajoittamaan uhkaa merkittävästi.

Kiristyshaittaohjelmat palvelutarjontana -ilmiö (Ransomware-as-a-Service, RaaS) tulee yleistymään entisestään, mikä tarkoittaa sitä, että eri tavoin motivoituneet kyberuhkatoimijat voivat helpommin hyödyntää kiristyshaittaohjelmia osana toimintaansa. Todennäköistä on myös uusien haittaohjelmaversioiden ilmaantuminen ja kiristyshaittaohjelmatoimijat pyrkivät parantamaan hyökkäysmenetelmiään ja pitävät todennäköisesti myös nollapäivähaavoittuvuudet osana toiminnallisissa työkaluissaan.

Vuoden 2024 aikana kyberrikolliset tulevat enenevissä määrin hyödyntämään tekoälypohjaisia teknologioita. Tekoälyä kehitetään esimerkiksi julkaistujen ohjelmistopäivitysten analysointiin haavoittuvuuksien ja niiden hyväksikäyttömenetelmien luomiseksi. Tekoälytekniikoita kehitetään myös automatisointiin. Näiden menetelmien kehittyessä rikolliset voisivat etsiä automatisoidusti miljardeista verkkolaitteista haavoittuvuuksia hyvin pian päivitysten julkaisun jälkeen. Tämä voi tehdä esimerkiksi kiristyshaittaohjelmatoimijoiden kampanjoista erittäin tehokkaita.

Kriittisiä haavoittuvuuksia kartoitetaan Suomessa vuonna 2024 edelleenkin. Kymmeniltä tai sadoilta kotimaisilta organisaatioilta vaaditaan pikaisia toimenpiteitä esimerkiksi kriittisten verkkolaitehaavoittuvuuksien paikkaamiseksi.

Kuluttajamarkkinoille tulee edelleen nopealla tahdilla paljon tuotteita, joissa on puutteelliset tietoturvallisuusominaisuudet.

Palvelunestohyökkäykset eri organisaatioiden verkkosivuja ja -palveluja kohtaan jatkuu aktiivisena. Palvelunestohyökkäysten toteuttaminen ei vaadi erityisiä teknisiä taitoja. Hyökkäyksen voi ostaa esimerkiksi palveluna rikollisilta. Organisaatioiden tulee varautua osana päivittäistä toimintaansa palvelunestohyökkäyksiin.

Kybervakoilu jatkuu aktiivisena myös vuonna 2024. Vakoilua harjoittavalle valtiolle kybervakoilu on edullinen ja tehokas keino hankkia merkittäviä määriä luottamukselliseksi tarkoitettua tietoa. Kybervakoilun kohde ei välttämättä itse huomaa joutuneensa vakoilun kohteeksi. Valtiolliset toimijat pyrkivät erilaisia haavoittuvuuksia hyödyntämällä pääsemään käsiksi erilaisiin luottamuksellisiin tietoihin. Suomessa Suojelupoliisin tehtävänä on torjua vieraiden valtioiden vakoilua myös verkossa.

Yksi Älyä ostoksiin -kampanjan teemoista muistutti tietoturvallisista kodinlaitteista.

Älyäostoksiin.fi

PalvelunestohyökkäysToiminta-ohje.pdf | Kyberturvallisuuskeskus

Tärkeitä muutoksia lainsäädäntöön

Vuonna 2024 kyberturvallisuuden sääntelyn lisääminen niin EU- kuin kansallisella tasolla jatkuu. Keskuksen toiminnan kannalta vuoden yksi merkittävimpiä asioita on syksyksi 2024 suunniteltu uuden verkko- ja tietoturvadirektiivin (nk. NIS2) kansallisen implementoinnin valmistuminen. Uuden lain myötä Kyberturvallisuuskeskus tulee saamaan uusia tehtäviä ja se valmistautuukin vuoden 2024 aikana käynnistämään näitä sekä tarjoamaan lain voimaantulon jälkeen tukea myös valvottavilleen.

Yritysten kannalta yksi ensimmäisistä askelista on perehtyä alkuvuodesta 2024 julkistettaviin perustason tietoturvakäytäntöihin, jotka toimivat konkreettisena oppaana toteutuksen aloittamiseksi. Näiden käytäntöjen noudattaminen on olennaista, kun yritykset pyrkivät täyttämään NIS2-direktiivin asettamat vaatimukset. Yritysten on oltava valmiita muuttamaan ja tehostamaan kyberturvallisuuskäytäntöjään vastaamaan paremmin nykyajan digitaalisiin uhkiin.

Digitaalisten tuotteiden valmistajille on tiedossa tuotteiden turvallisuuteen liittyvää sääntelyä. Radiolaitedirektiivin (Radio Equipment Directive, RED) tietoturvavaatimusten soveltamispäivämäärä on siirtynyt elokuulle 2025, mikä antaa yrityksille enemmän aikaa valmistautua sen vaatimuksiin. Direktiivi koskee kaikkia suoraan tai välillisesti internetiin liitettäviä laitteita. Tarkemmat määritykset vaatimuksenmukaisuudelle julkaistaan vuoden 2024 aikana. Kyberkestävyyssäädöksen (Cyber Resilience Act, CRA) odotetaan tulevaan voimaan vuoden 2024 aikana. CRA tulee koskemaan kaikkia internet-kytkentäisiä tuotteita ja koko niiden elinkaarta. Säädöksen soveltamisen odotetaan alkavan asteittain siten, että haavoittuvuuksista tiedottamisen velvotteita tullaan soveltamaan vuonna 2026 ja muita velvotteita vuonna 2027. Valmistajien onkin viisasta aloittaa varautuminen jo nyt perustason tietoturvavaatimuksiin. Kyberkestävyyssäädös haastaa valmistajat kehittämään vahvat kyberturvallisuuskäytännöt ja integroimaan ne tuotantoprosesseihinsa jo etukäteen.

Ensi vuonna myös jatkuu oikeusministeriön vetämä valmiuslain kokonaisuudistus, johon Traficom ja Kyberturvallisuuskeskus tuottavat jatkossakin näkemyksiä oman toimialansa kannalta.

Teknologinen kehitys jatkuu vauhdikkaana 2024

Eräs vuoden 2023 keskeisistä trendeistä oli generatiivisen tekoälyn nopea kehitys. Generatiivisin menetelmin on tuotettu realistisen näköisiä väärennettyjä kuvia, videoita ja tekstiä. Tämän kehityskulun on yleisesti todettu johtavan disinformaation leviämiseen ja lisäävän vaikeutta erottaa totuus fiktiosta.

On todennäköistä, että generatiivisillä tekoälymenetelmillä voidaan luoda videota reaaliajassa vuoden 2024 aikana. Tämä mahdollistaa myös sellaisten videoiden luomisen, joissa keksittyjen tai olemassa olevien henkilöiden kasvojen liikkeet ja puhe synkronoidaan realistisesti luoden vaikutelman aitoudesta. Näiden videoiden luomiselle kohdehenkilön suostumuksella on monenlaisia liiketoimintatarpeita, ja on todennäköistä, että niiden käyttö yleistyy nopeasti.

Erityisesti silloin kun videoita luodaan harhauttamistarkoituksessa ja ilman kohteen suostumusta, puhutaan ns. deepfake-videoista, suomeksi syvävääreennöksistä tai yleisemmin väärennösvideoista. Reaaliaikainen väärennösvideoiden generointi voi lisätä entisestään huijausmahdollisuuksia monilla eri aloilla. Yrityksiä vastaan tehdyissä huijauksissa voidaan käyttää väärennösvideoita esimerkiksi yritysjohtajien kasvojen liikkeiden ja äänen muokkaamiseen luomaan vaikutelman, että kyseessä on aito viesti.

Kun kasvojen ja äänen mallintamiseen käytettävä tekniikka arkipäiväistyy, voidaan uskottavia väärennösvideoita tehdä myös yksityishenkilöistä. Tällaiset väärennösvideot voivat helpottaa identiteettivarkauksia ja erilaisia huijauksia, joissa yksilön henkilöllisyyttä käytetään petollisiin tarkoituksiin.

Yksityishenkilöihin kohdistuvissa huijauksissa todellisia tai keksittyjä henkilöitä mallintavat väärennösvideot voivat antaa vaikutelman henkilökohtaisemmasta vuorovaikutuksesta huijareiden ja uhrien välillä. Tämä voi lisätä uhrien tunneyhteyttä huijariin ja tehdä heistä alttiimpia petoksille. Erityisesti sukulaishuijausten ja romanssihuijausten kaltaisissa petoksissa aletaan todennäköisesti käyttää väärennettyä ääntä ja videokuvaa. Huijarit voivat esimerkiksi esittää kuvitteellisia kriisejä tai mitä erilaisempia tarinoita rahallisen tuen toivossa. Generatiivisilla tekoälytekniikoilla voidaan myös helposti tuottaa uskottavan näköisiä väärennöksiä erilaisista dokumenteista huijaustarinoita tukemaan. Erilaisia huijaustyyppejä keksitään todennäköisesti aina uusia sitä mukaa kun edellisiä opitaan varomaan.

Yhteistyö teollisuuden, tutkijoiden ja viranomaisten välillä on keskeistä väärennettyjen sisältöjen torjunnassa. Kehitettäviä palveluita tulisi mahdollisimman aikaisesta vaiheesta lähtien arvioida myös väärinkäytösten näkökulmasta ja pyrkiä luomaan erilaisia tapoja havaita ja estää väärinkäytöksiä. Yhteiset ponnistelut voivat johtaa parempiin tunnistusmenetelmiin ja suojamekanismeihin. Jo nyt on esimerkiksi kehitetty edistyneitä tekniikoita väärennettyjen videoiden tunnistukseen. Tekoälypohjaiset järjestelmät pyrkivät havaitsemaan merkkejä siitä, että video tai kuva on generoitu, ja ne pyrkivät erottamaan aidon sisällön väärennöksestä. Myös erilaisia sisällön aitouden varmistamiseen pyrkiviä tekniikoita on esitetty.

Väärennösvideoita voidaan käyttää osana laajempia informaatiovaikuttamisen kampanjoita. Tällaiset kampanjat voivat pyrkiä vaikuttamaan yleiseen mielipiteeseen, levittämään vääriä tietoja tai luomaan hämmennystä yhteiskunnassa.

Lisääntynyt tietoisuus väärennettyjen sisältöjen olemassaolosta ja mahdollisista riskeistä voisi kannustaa yleisöä olemaan varovainen ja kriittinen digitaalisen sisällön suhteen. Myös sääntelytoimet voivat edistää vastuullista tekoälyn käyttöä ja asettaa tiukempia vaatimuksia generatiivisten mallien kehittäjille. Teknologian kehitykselle on ominaista jatkuva kilpailu kehittäjien ja turvallisuusasiantuntijoiden välillä. Samalla kun turvallisuustoimenpiteitä tehdään, myös hyökkääjät kehittävät uusia tapoja kiertää ne.

Tekoälymenetelmiä ja erityisesti generatiivista tekoälyä tullaan kehittämään muillakin tavoilla puolustuksellisiin tarkoituksiin. Niiltä odotetaan erityisesti parempia työkaluja turvallisten järjestelmäasetusten ylläpitoon ja tietoturvapoikkeama-analyysiin, sekä mahdollisuuksia automatisoituun turvallisuusuhkiin reagointiin. Vuonna 2024 tullaan näkemään erilaisia ratkaisuja tekoälyavusteiseen tietoturvapoikkeamien havainnointiin ja selvittämiseen.

Tekoälyn käyttö ohjelmistotuotannossa voi vaikuttaa monin tavoin luotujen järjestelmien kyberturvallisuuteen. Niitä on käytetty varsinaisen ohjelmistotuotannon lisäksi esimerkiksi testitapausten luomiseen, mikä on omiaan helpottamaan järjestelmän kehitystä ja ylläpitoa. Tekoälymallien kehityksen myötä ne voisivat auttaa kehittäjiä tuottamaan turvallisempaa koodia ja tunnistamaan potentiaalisia riskialtista koodia tai huonoja käytäntöjä. Ne voisivat vastaavasti myös auttaa tunnistamaan ohjelmistojen haavoittuvuuksia ja tietoturva-aukkoja.

” Samalla kun turvallisuustoimenpiteitä tehdään, myös hyökkääjät kehittävät uusia tapoja kiertää ne.

Tietoturvataitojen hallinta korostuu entisestään

Kyberrikokset ja -rikollisuus muuttavat jatkuvasti muotoaan. Esimerkiksi erilaisissa huijauksissa ja tietojenkalastelukampanjoissa käytetyt teknologiat ja tekniikat kehittyvät ja muuttuvat jatkuvasti entistä hienostuneemmiksi ja kierommiksi. Niiden tunnistaminen muuttuu entistä haastavammaksi kenelle tahansa.

Yhteiskunnan digitalisoituessa vauhdilla tietoturvataitojen hallinta ja niiden jatkuva kehittäminen ovat tärkeitä kansalaistaitoja. Yksittäiset kansalaiset ovat entistä useammin kyberhyökkäysten, kuten tietojen kalastelun, tietomurtojen, sosiaalisen median tilien kaappausyritysten, kiristyshaittaohjelmien ja huijausviestien kohteena. Tämä pitää sisällään myös informaatiovaikuttamisen erilaiset muodot, kuten disinformaation levittämisen. Tämän vuoksi on tärkeää, että kansalaisten tietoturvaosaamiseen sekä media- että teknologialukutaidon ylläpitämiseen ja kehittämisen panostetaan.

Kansalaisten kyberturvallisuustaidot vaihtelevat merkittävästi. Toiset tarvitsevat tukea perusasioiden, kuten salasanojen ja ohjelmistopäivitysten kanssa sekä huijausten tunnistamisessa. Toisten tietoturvataidot ovat erinomaisella tasolla.

Kyberturvallisuudessa on kysymys myös luottamuksesta. Jos ihmiset eivät luota jonkin yrityksen tai organisaation tarjoamiin sähköisiin palveluihin tai tuotteisiin, ei niitä myöskään haluta käyttää. Mitä enemmän yhteiskunta ja sen tarjoamat palvelut digitalisoituvat, sitä tärkeämpää on kiinnittää huomiota hyvään tietoturvaan ja luottamuksen säilyttämiseen. Aktiivisella, avoimella ja säännöllisellä viestinnällä tuetaan luottamuksen säilyttämistä. Sekä hyvistä asioista että myös ongelmista tulee viestiä avoimesti ja läpinäkyvästi. Digitalisoituneessa yhteiskunnassa on myös kiinnitettävä huomiota osallisuuden toteutumiseen.

Tänä päivänä julkisessa kyberturvallisuutta koskevassa keskustelussa näkyvät paljon tekoäly ja sitä hyödyntämällä tehdyt syvävääärennökset eli deepfaket. Kun uhkista puhutaan, on myös hyvä muistaa, että niihin myös varaudutaan. Samalla tavalla kuin tekoäly mahdollistaa uudenlaisia huijauksia ja kyberhyökkäyksiä, se tarjoaa myös keinoja niiltä suojautumiseen.

Kyberturvallisuuskeskus tukee kaikilla tietoturvan tasoilla olevien kansalaisten kybertaitoja.

Kyberturvallisuuskeskus.fi

Viestintäasiantuntijamme esittelevät, miten teknologia mahdollistaa yhä petollisemman harhaanjohtamisen kyberhuijauksien ja informaatiovaikuttamisen apuvälineenä.

Deepfake: miten syvävääärennökset tehostavat kyberrikollisuutta ja informaatiovaikuttamista? | Youtube

Toimintamme tunnuslukuja 2023

Varoitukset
1
(2022: 1 kpl)

Huijaus
4 963
(2022: 3 519 kpl)

Kalastelu[1]
9 266
(2022: 5 787 kpl)

Tietovuodot
111
(2022: 104 kpl)

Tieto-murrot[2]
1 014
(2022: 1 026 kpl)

Tietomurron yritys[3]
383
(2022: 127 kpl)

Automaattinen tapauskäsittely
209 416
(2022: 188 561 kpl)

Tietoturva-poikkeamia yhteensä
18 625
(2022: 12 947 kpl)

Facebook-seuraajat
7 190
(2022: 6 939 kpl)

X-seuraajat
17 200
(2022: 16 805 kpl)

Media-yhteydenotot
152
(2022: 142 kpl)

Tilannekuvatuotteiden asiakastyytyväisyys
4,3
(2022: 4,3)

1 Vuonna 2023 saimme 3 881 ilmoitusta pankkitunnusten kalastelusta.
2 Mukana kansalaisten sometilit, 3 Suhteessa eniten kasvua edellisvuoteen

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
PL 320, 00059 TRAFICOM
p. 029 534 5000

Kyberturvallisuuskeskus.fi

Traficomin julkaisuja 10/2024
ISSN 2669-8757 (verkkojulkaisu)
ISBN 978-952-311-909-3

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus