TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Tietoturvan vuosi 2022

Sisällys

Traficomin julkaisuja 16/2023
ISSN 2669-8757 (verkkojulkaisu)
ISBN 978-952-311-876-8

Tiedonvaihto, yhteistyö ja varautuminen – Kyberturvallisuus tehdään yhdessä

Vuoden 2023 päästyä kunnolla käyntiin on hyvä palauttaa mieliin monellakin tapaa poikkeuksellisen vuoden 2022 tärkeimmät kybertapahtumat.

Viime vuonna kyberturvallisuuden uhkataso nousi korkeammalle kuin koskaan aiemmin. Muutoksesta on tullut pysyvä. Pitkään jatkunut kyberhäiriöiden määrän kasvu tasaantui, mutta kyberhäiriöt muuttuivat Ukrainan sodan myötä entistä vakavammiksi ja kohdennetuimmiksi. Huijaukset, palvelunestohyökkäykset, haittaohjelmat ja kiristyshyökkäykset organisaatioiden ICT-ympäristöihin sekä tietojenkalastelu vaikuttivat suomalaisten ja Suomessa toimivien organisaatioiden arkeen.

Traficomin Kyberturvallisuuskeskus ja muut viranomaiset varoittivat Venäjän helmikuussa 2022 Ukrainaan käynnistämän laajamittaisen hyökkäyksen jälkeen eri kanavissa mahdollisesta kyberuhkien kasvusta. Kyberturvallisuuskeskukselle ilmoitettujen vakavien kyberhäiriöiden, kuten merkittävien kiristyshaittaohjelmatapauksien määrä lähtikin heinäkuussa 2022 kasvuun. Näitä tapauksia todettiin vuonna 2021 vain muutama ja vuonna 2022 kirjattiin jo toistakymmentä tapausta yhteiskunnan kriittisissä toiminnoissa. Kyberturvallisuuskeskus tuki näissä tapauksissa uhriorganisaatiota toipumisessa.

Vuonna 2023 kyberturvallisuuden uhkataso pysyy kohonneena ja kyberturvallisuus pysyy tärkeänä yhteiskunnallisena teemana. Kyberuhkat kiinnostavat ja herättävät paljon julkista keskustelua ja ymmärrettävästi myös huolta. Kun tätä keskustelua käydään, on tärkeää, että keskustelua uhkista ja niihin varautumisesta ja vastaamisesta käydään ajantasaisen ja oikean tiedon perusteella. Viranomaisilla on kyky ja velvollisuus tuottaa tätä tietoa.

Tässä katsauksessa tarkastellaan viime vuoden kyberturvallisuuden yleisiä tapahtumia ja ilmiöitä Suomessa, kyberturvallisuuden kehittämistoimia sekä Traficomin Kyberturvallisuuskeskuksen toimintaa.

> ”Kyberturvallisuutta edistettiin vuonna 2022 monin eri tavoin.

Vuonna 2022 kyberturvallisuutta koskevaa tilannekuvaa, yhteistyötä ja tiedonvaihtoa kehitettiin ja tiivistettiin

Kyberuhkat eivät noudata maiden tai yhteiskunnan eri sektorien välisiä rajoja. Kyberuhkat, kuten muutkin nykyajan uhkat, ovat luonteeltaan laaja-alaisia ja viranomaisten näkökulmasta poikkihallinnollisia. Digitalisaation myötä toimialat ovat riippuvaisia toisistaan ja harva häiriötilanne tänä päivänä koskettaa vain yhtä hallinnonalaa tai yhteiskunnan sektoria. Moderneihin uhkiin varautuminen ja vastaaminen edellyttävät sitä, että yhteistyö toimii ja johtamisen, tilannekuvan ja viestinnän väliset yhteydet ovat kunnossa. Päätöksiä on tehtävä oikein tiedoin ja oikean tilannekuvan perusteella. Valmiuteen ja varautumiseen liittyvällä yhteiskunnan eri sektorien välisellä yhteistyöllä on Suomessa pitkät perinteet.

Vuonna 2022 kybertuvallisuuden kehittämistyötä jatkettiin tiivistämällä turvallisuudesta vastaavien ministeriöiden ja kyberturvallisuusviranomaisten sisäistä ja keskinäistä yhteistyötä. Viranomaisten välisen yhteistyön ja tiedonvaihdon varmistamiseksi sekä yhteisen tilannekuvan tuottamiseksi perustettiin erillinen ministeriötason ryhmä keväällä 2022. Ryhmän tehtävänä on tarvittaessa tukea valtionjohdon päätöksentekoa vakavissa kyberhäiriö- tai vaikuttamistilanteissa. Lisäksi Digitalisaation, datatalouden ja julkisen hallinnon kehittämisen ministeriryhmän tehtävää täydennettiin maaliskuussa 2022 kyberturvallisuuden ja julkisen hallinnon varautumisen osalta.

Traficom ja Kyberturvallisuuskeskus sen osana kehittivät toimintansa painopisteitä vastaamaan kohonneeseen uhkatasoon. Uusia kyvykkyyksiä kehitettiin tekniseen havainnointikykyyn sekä nopeamman avun tarjoamiseen vakavissa kyberhäiriöissä. Kyberturvallisuuskeskus alkoi tuottaa muun muassa uutta kyberturvallisuuden strategista tilannekuvaa valtionjohdon tarpeisiin.

Tietoliikenneyhteyksien toimintavarmuuden ja turvallisuuden varmistaminen sekä teleyritysten varautumisen tukeminen säilyi keskeisenä tavoitteena ohjaus- ja valvontatoiminnassa. Vuoden aikana edistettiin myös useita lainsäädäntöhankkeita, joiden tarkoituksena on kehittää yritysten tietoturvaa, riskien hallintaa ja varautumista sekä tukea viranomaisten kyberturvallisuutta koskevaa yhteistyötä ja parantaa tiedonvaihdon edellytyksiä.

Vuoden 2022 aikana Kyberturvallisuuskeskus tiivisti kotimaista ja kansainvälistä yhteistyötään.

Vaikutimme kotimaisissa ja kansainvälisissä verkostoissa ja osallistumme aktiivisesti lainsäädännön valmisteluun ja kehittämiseen. Toteutimme, koordinoimme ja olimme mukana useissa kyberturvallisuutta kehittäneissä hankkeissa.

Venäjän helmikuussa 2022 käynnistämässä laajamittaisessa hyökkäyksessä Ukrainaan kyberulottuvuus on ollut tiiviisti mukana. Kyberturvallisuuskeskus on seurannut ja analysoinut tiiviisti Ukrainassa nähtyjä kyberhyökkäyksiä ja tukenut suomalaisen yhteiskunnan eri sektorien varautumista ja valmiuksia vastata erilaisiin kyberympäristössä nouseviin uhkiin. Tästä esimerkkinä on nopean reagoinnin kybervarautumisten hankkeet, joissa kehitettiin nopean ensivasteen palveluita ja uusi strateginen kyberturvallisuuden tilannekuva-analyysi, joka jaetaan muun muassa ylimmälle valtionjohdolle. Kyberturvallisuuskeskus on myös tehnyt tiivistä yhteistyötä suomalaisten teleyritysten kanssa viestintäverkkojen ja -palvelujen toimivuuden turvaamiseksi ja erilaisiin uhkiin varautumiseksi.

Kyberturvallisuudessa viranomaisten roolit ja tehtävät ovat selvät

Työtä kyberturvallisuuden ylläpitämiseksi ja kehittämiseksi tehdään Suomessa joka päivä. Viranomaisten kesken työnjako kyberturvallisuudessa on selvä ja perustuu lainsäädäntöön. Operatiivista yhteistyötä tehdään päivittäin ja viranomaisilla on hyvin organisoidut koordinaatioryhmät ja -toimintamallit. Kyberturvallisuushäiriötilanteessa kyberturvallisuusjohtaja tuottaa yhdessä ministeriötason ryhmän kanssa tilannekuvaa valtionjohdolle ja koordinoi tilannetta. Lisäksi liikenne- ja viestintäministeriö koordinoi tilannetta muiden ministeriöiden kesken horisontaalisesti.

Kyberturvallisuutta ja -uhkia koskevaa tietoa ja tilannekuvaa vaihdetaan koti- ja ulkomaisten kumppaneiden ja sidosryhmien kesken koko ajan. Yhteistyö toimijoiden kesken sekä yhteiskunnan eri sektorien välillä on tiivistä.

Kyberturvallisuuden kehittäminen on jatkuvaa ja strategista toimintaa

Kyberturvallisuuden ylläpitäminen ja kehittäminen edellyttävät panostuksia. Se on pitkäjänteistä ja strategista toimintaa, jolle ajantasainen lainsäädäntö sekä vuonna 2019 voimaan tullut kyberturvallisuusstrategia ja kyberturvallisuuden kehittämisohjelma luovat hyvät puitteet ja suuntaviivat. 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.

Varautumista ja valmiuksia vastata kyberuhkiin kehitetään jatkuvasti harjoitustoiminnalla ja sääntelyä kehittämällä. Tulevaisuuden ennakointia tehdään esimerkiksi skenaariotyössä analysoimalla teknologisia ja yhteiskunnallisia kehityskulkuja. Ilman näkymää tulevaan, on vaikea tehdä oikeita toimenpiteitä ennakoivasti ja oikea-aikaisesti. Kyberturvallisuuden kehittäminen on strategista toimintaa, joka pohjautuu ajantasaiseen tilannekuvaan ja -analyysiin.

Kyberturvallisuutta edistetään ja tuetaan myös monin muin tavoin. Esimerkkeinä näistä voi mainita vuoden 2022 lopussa valtioneuvoston päättämän yhteiskunnan toimintojen kannalta elintärkeille yrityksille suunnatun tietoturvan kehittämisen tuen, eli niin kutsutun Tietoturvasetelin, Huoltovarmuuskeskuksen viisivuotisen Digitaalinen turvallisuus 2030 -ohjelmakokonaisuuden sekä valtiovarainministeriön rahoittamat kehityshankkeet, jotka rahoitetaan Julkisen hallinnon digitaalisen turvallisuuden toimeenpano 2020–2023 (Haukka) -ohjelmasta.

Kyberturvallisuuskeskus tukee koko yhteiskunnan ja sen eri sektorien kyberresilienssiä

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus ohjaa ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta, vahvojen sähköisten tunnistus- ja luottamuspalvelujen tietoturvallisuutta sekä erilaisten digitaalisen infrastruktuurin ja palvelujen tarjoajien tietoturvaa ja riskien hallintaa. Osallistuimme tiiviisti sekä koti- että kansainvälisen alaa koskevan sääntelyn ja standardoinnin kehittämiseen.

Traficomin Kyberturvallisuuskeskus on Suomessa viranomainen, jonka tehtäviin kuuluu tuottaa laaja-alaista, yhteiskunnan eri sektorit kattavaa tieto- ja kyberturvallisuuden tilannekuvaa ja analyysia sekä tukea sektori- ja hallinnonalarajojen ylittävää kyberturvallisuuden kehittämistä. Tuottamaamme strategista tilannekuvaa ja analyysia hyödynnetään laajasti, kuten esimerkiksi ylimmän valtionjohdon päätöksenteossa ja huoltovarmuuskriittisillä sektoreilla.

Kyberturvallisuuskeskus osallistuu aktiivisesti kyberturvallisuutta koskevaan kotimaiseen ja kansainväliseen yhteistyöhön ja tiedonvaihtoon. Keskuksen ennakointi- ja skenaariotyössä seurataan ja analysoidaan laajasti kyberturvallisuuteen yleisesti vaikuttavia yhteiskunnallisia ja teknologisia kehitystrendejä, kuten esimerkiksi tekoälyn hyödyntämistä kyberhyökkäyksissä. Toiminta tukee yhteiskunnan eri sektoreiden kyberturvallisuuden varautumista ja kehittämistä.

Kyberturvallisuuskeskus palvelee koko Suomea ja sen tehtäviin kuuluu tiedottaa yleisesti kyberuhkista, kuten käytössä olevissa ohjelmistoissa olevista haavoittuvuuksista. Kyberturvallisuuskeskus tuottaa ja päivittää jatkuvasti kansalaisten kuin organisaatioidenkin käyttöön tarkoitettuja ohjeita, joilla kerrotaan, miten esimerkiksi erilaisia tietoturvapoikkeamia voi ennaltaehkäistä. Kyberturvallisuuskeskus neuvoo yrityksiä, yhteisöjä ja kansalaisia tieto- ja kyberturvallisuuteen liittyvissä asioissa ja tukee esitutkintaviranomaisia kyberrikosten selvittämisessä. Keskuksen verkkosivuilla julkaistaan joka viikko Kyberturvallisuuden viikkokatsaus, jossa kerrotaan tuoreista kyberturvallisuuteen vaikuttaneista tekijöistä ja havainnoista. Kuukausittain julkaistavassa Kybersää-katsauksessa tarkastellaan pidemmän aikavälin trendejä kyberturvallisuudessa. Keskuksen sivuilta löytyy myös ohjeita arjen kyberturvataitojen ylläpitämiseen ja kehittämiseen kaikille.

Kyberturvallisuuskeskus arvioi, että yksin sen tietoturvaloukkausten ennaltaehkäisyä ja kansalaisten auttamista koskevat toimet tuottavat yhteiskunnalle merkittävän euromääräisen nettohyödyn vuosittain.

> ” Kyberturvallisuuskeskus tuottaa laaja-alaista kyberturvallisuuden tilannekuvaa.

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.

Kyberturvallisuudessa on kysymys myös luottamuksesta

Kyberturvallisuudessa on myös kysymys ihmisten luottamuksesta yhteiskuntaan, sen instituutioihin ja palveluihin. Jos palveluihin ja niiden tietoturvaan ei luoteta, ei niitä myöskään haluta käyttää. Luottamuksen ylläpitäminen ja vahvistaminen on tärkeää. Luottamus on liima, joka pitää yhteiskuntamme koossa. Tähän myös luottamus digitaalisiin palveluihin ja kyberturvallisuuteen kuuluu. Tekemällä oikeita asioita ja viestimällä niistä avoimesti, voimme osaltamme tukea luottamuksen säilymistä. Ongelmista ja virheistä on myös tärkeä puhua avoimesti ja läpinäkyvästi.

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. Tällainen keskustelu tukee ja edistää yhteiskunnan kriisitietoisuutta ja resilienssiä. Kyberturvallisuutta kehitetään joka päivä, toimintaa ja toimintatapoja muutetaan muuttuvan uhkaympäristön mukaisesti. Kyberympäristössä nousevia uhkia analysoidaan jatkuvasti ja niihin vastataan.

Vuosi 2022 oli usean samanaikaisen kriisin vuosi. Turvallisuusympäristön muutos, koronapandemia, energiakriisi, taloudellisen taantuman uhka ja ilmastonmuutos koskettivat jokaista meistä. Julkisessa keskustelussa esiin nousevat nopeasti kriisien taloudelliset vaikutukset, mutta yhtä tärkeää on myös kiinnittää huomiota niiden sosiaalisiin ja yhteiskunnallisiin vaikutuksiin. Nämä vaikutukset saattavat ilmetä vasta pitkän ajan jälkeen.

Turvallisuudessa on kysymys myös tunteesta. Ihmisten tulkinnat ja kokemukset riskeistä ja kriiseistä voivat erota hyvin paljon viranomaisten ja muiden toimijoiden käsityksistä. Tähän tiedontarpeeseen viranomaisten ja muiden yhteiskunnallisten toimijoiden on vastattava kuuntelemalla ja keskustelemalla sekä aktiivisella, oikea-aikaisella ja avoimella viestinnällä. Tämä koskee myös kyberuhkia.

Kyberuhkat koskettavat konkreettisesti koko yhteiskuntaa aina yksilötasolta koko yhteiskunnan tasolle. Häiriöt digitaalisissa verkoissa tai sähköisissä palveluissa vaikuttavat arkeemme. Mitä enemmän ja pitkään kestävää sitkosta arjessa on, sen suurempi mahdollisuus sillä on vaikuttaa yhteiskunnan henkiseen kriisinkestävyyteen. Kyberuhkiin varautumisessa ja niistä puhuttaessa on myös tärkeä muistaa henkisen kriisinkestävyyden ulottuvuus.

Lopuksi on hyvä muistuttaa, että kyberturvallisuuden kehittäminen on kuin ultramaraton. Erona reaalimaailmassa toteutettavaan juoksutapahtumaan, kyberissä maaliviiva siirtyy aina ja puskista saattaa hypätä uusia kilpakumppaneita mukaan matkaan. Jotta pysymme vauhdissa mukana ja menestymme, tarvitaan kestävyyttä, oikeat ja sopivat välineet, suunnitelmallisuutta ja strategisuutta, yhteistyötä huoltojoukkojen ja muiden kumppanien kanssa sekä ennakointia. Tiedämme, millainen reittiprofiili on, ja missä muut kanssajuoksijat menevät. Lisäksi osaamme sovittaa vauhtimme, huoltomme ja askeleemme sen mukaisesti. Tässä onnistuimme vuonna 2022 hyvin. Sama tavoite meillä on tänä ja ensi vuonna.

Tietoturvan vuosi 2022

Uhkataso nousi vuoden 2022 aikana

Koronapandemia ja Venäjän helmikuussa 2022 käynnistämä laajamittainen hyökkäys Ukrainaan vaikuttivat myös Suomen turvallisuustilanteeseen. Vuoden 2022 aikana turvallisuusympäristömme muuttui merkittävästi. Viranomaiset, kuten Suojelupoliisi, varoittivat keväällä laajamittaisen hybridivaikuttamisen mahdollisuudesta suomalaista yhteiskuntaa ja sen eri sektoreita vastaan. Suojelupoliisi myös otti kantaa joidenkin kyberhäiriöiden taustalla oleviin toimijoihin. Erityisesti kyberhyökkäyksiin ja informaatiovaikuttamiseen varautumiseen ja vastaamiseen kehotettiin kiinnittämään huomiota. Näin myös toimittiin. Kyberturvallisuuden puolella varautumisen ja valmiuden kehittämiseen panostettiin yhteiskunnan eri sektoreilla. Kyberturvallisuuskeskus tuki organisaatioita tässä työssä.

Vuoden 2022 aikana kiristyshaittaohjelmat, kohdistettu tietojenkalastelu ja haitallinen liikenne lisääntyivät niin valtionhallintoon kuin huoltovarmuuskriittisiin organisaatioihin. Hyökkäysten toimintatapa myös muuttui. Muutoksen vuoksi Kyberturvallisuuskeskus nosti ja tiedotti syyskuussa kyberympäristön uhkatason noususta ensimmäistä kertaa. Tämä koordinoitiin yhdessä Suojelupoliisin kanssa. Kyberturvallisuuskeskus arvioi, että Suomi on selviytynyt hyvin uhkatason noususta – muun muassa varautumiskulttuurin ja avoimen viranomaisten välisen keskustelu-ympäristön johdosta.

Rikollisten toiminta on hyvin opportunistista ja he seuraavat tarkasti aikaansa. Esimerkiksi pandemian aikana on nähty huijausyrityksiä, joissa ihmisiä yritetty saada luovuttamaan tietojaan koronaan liittyvillä teemoilla ja aiheilla. Myös valtioiden poliittiset ratkaisut, turvallisuusympäristön muutokset ja yritysten päätökset voivat aktivoida rikollisia kohdistamaan hyökkäyksiä suomalaisiin organisaatioihin.

On myös hyvä muistaa, että vaikkei kyberhyökkäys kohdistuisi suoraan Suomeen, voi syntyä heijastevaikutuksia, kun digitaaliset järjestelmät ovat globaalisti sidoksissa toisiinsa.

> ”Suomi on selviytynyt hyvin uhkatason noususta.

Palvelunestohyökkäykset lisääntyivät selvästi loppuvuonna

Vuoden 2022 aikana erityisesti palvelunestohyökkäykset suomalaisia organisaatiota ja yrityksiä kohtaan lisääntyivät. Niistä tehtiin ilmoituksia Kyberturvallisuuskeskukselle selvästi enemmän kuin vuonna 2021. Osa tästä kasvusta johtui kuitenkin myös julkisesta keskustelusta ja sen myötä tapahtuneesta ilmoituskynnyksen madaltumisesta.

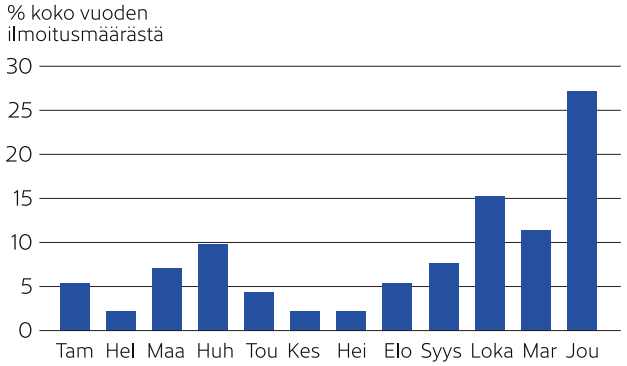
Vuoden 2022 aikana palvelunestohyökkäyksissä korostui haktivismi ja hyökkäysten näkyvä sitominen osaksi poliittista ideologiaa. Vaikka ilmiönä haktivismi ei ole uusi, palvelunestohyökkäysten tekeminen kannanottona näkyi julkisuudessa enemmän kuin aiempina vuosina.

Palvelunestohyökkäyksiä on tehty pitkään ympäri maailmaa, mutta vuonna 2022 niitä valjastettiin enemmän kyber- ja informaatiovaikuttamisen keinoiksi. Esimerkkeinä tästä olivat hyökkäykset, jotka kohdistuivat kansalaisten käyttämiin verkkopalveluihin, joiden pääsyn estymisen seurauksena hyökkäyksen tekijän oli mahdollista pyrkiä luomaan julkisuudessa mielikuvaa vakavammasta hyökkäyksestä kuin siinä todellisuudessa oli kyse.

Ukrainan sodan seurauksena kannanottona tehdyt palvelunestohyökkäykset lisääntyivät. Myös monet muut kansainväliset poliittiset tai muut merkittävät tapaukset aktivoivat haktivisteja tekemään palvelunestohyökkäyksiä. Näkyvimpiä tapauksia Suomeen tehdyissä hyökkäyksissä olivat Venäjä-mielisten haktivistiryhmien, kuten NoName057(16) ja Killnetin tekemät hyökkäykset. Kohteena olivat erityisesti valtionhallinnon sekä sote-sektorin, finanssialan, liikenne- ja logistiikka-alan ja media-alan toimijat, joiden palveluihin kohdistuvilla katkoksilla sai suoraa näkyvyyttä kansalaisille, vaikka organisaatioiden sisäisiin järjestelmiin niillä ei vaikutusta ollutkaan ja vaikutukset ulkoisiinkin palveluihin olivat valtaosin lyhytaikaisia.

Palvelunestohyökkäykset ovat olleet arkipäivää Suomessa jo vuosia. Niitä todetaan vuosittain yli 10 000. Palvelunestohyökkäyksen toteuttaminen ei vaadi erityistä teknistä osaamista, vaan sen voi tilata rikollisilta kaupallisena palveluna. Keinona palvelunestohyökkäys on näyttävä, ja sen toteuttamisella saa helposti julkisuutta. Haitta hyökkäyksestä on lyhytaikainen ja niillä saa harvoin mitään todellista vahinkoa aikaan. Vaikuttamiskeinona palvelunestohyökkäys sijoittuu kyber- ja informaatiovaikuttamisen väliselle harmaalle vyöhykkeelle.

Kyberturvallisuuskeskuksen käsittelemät ilmoitukset palvelunestohyökkäyksistä 2022



Palvelunestohyökkäyksiä tehtiin vuoden 2022 aikana myös aiempaa sinnikkäämmin ja hyökkääjä muun muassa vaihteli tekniikoita sitä mukaa kun torjuntatoimia tehtiin. Kyberturvallisuuskeskus ylläpiti tilannekuvaa palvelunestohyökkäyksistä, avusti organisaatioita niiden torjunnassa ja jakoi julkisuudessa tietoja niiden todellisista vaikutuksista. Organisaatioiden tekemät ilmoitukset palvelunestohyökkäyksistä lisääntyivät Kyberturvallisuuskeskukselle vuoden aikana ja myös eri menetelmin tehtyihin sinnikkäisiinkin hyökkäyksiin kyettiin tekemään hyökkäystä rajoittavia suojautumistoimia, joilla estettiin hyökkäysten vaikutus. Joulukuussa Kyberturvallisuuskeskukselle ilmoitettiin neljäsosa koko vuoden 2022 palvelunestohyökkäyksistä Suomessa.

Suomalaisia organisaatioita joutui kiristyshaittaohjelmien uhriksi entistä useammin

Vuonna 2022 Kyberturvallisuuskeskukselle ilmoitettiin edellisvuotta enemmän kiristyshaittaohjelmien uhriksi joutumisesta. Julkisuudessa esimerkiksi Suomen Tietotoimisto STT:n, Wärtsilä Oyj:n, Vahanen Oy:n ja Uponor Oyj:n tapaukset olivat näkyvästi esillä. Kiristyshaittaohjelmat lisääntyivät myös kansainvälisesti. Suomeenkin ilmiöt ja trendit rantautuivat muista maista. Globaalit tapaukset koskettivat Suomea vuoden 2022 aikana aiempaa enemmän, ja osa hyökkäyksistä liitettiinkin julkisuudessa maailmanpoliittiseen tilanteeseen.

Vuoden aikana kiristyshaittaohjelmien levittäminen Suomessa nähtiin aiempaa kohdennetumpana ja Suomessa havaituissa tapauksissa tunnistetut haittaohjelmat olivat kansainvälisestikin aktiivisesti käytössä. Vuoden 2022 aikana kiristyshaittaohjelmatapaukset lisääntyivät erityisesti kesällä, mutta syksyllä ilmoitukset niistä vähenivät. Loppuvuotta kohti tapaukset jälleen lisääntyivät. Kesällä uhriorganisaatioon selvästi kohdennettuja kiristyshaittaohjelmahyökkäyksiä kohdistui suuriin ja merkittäviin yrityksiin ja loppuvuodesta uhreiksi joutui toimijoita myös kunta-alalta.

Vaikka hyökkäysten kohteina oli merkittäviäkin suuryrityksiä ja huoltovarmuuden kannalta kriittisiä organisaatioita, hyökkäyksessä käytetyt menetelmät olivat varsin tavanomaisia. Suuri osa kiristyshaittaohjelmiin johtaneista hyökkäyksistä aiheutui sähköpostitse välitetyn tietojenkalasteluviestin avulla. Myös muiden tavanomaisten suojausmenetelmien, kuten hyvien salasanakäytänteiden tai ohjelmistopäivitysten puuttumista käytettiin kiristyshaittaohjelmahyökkäyksissä hyväksi.

> ” Vuoden aikana kiristyshaittaohjelmien levittäminen Suomessa nähtiin aiempaa kohdennetumpana.

Suomen tietotoimisto STT sai vuonna 2022 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.

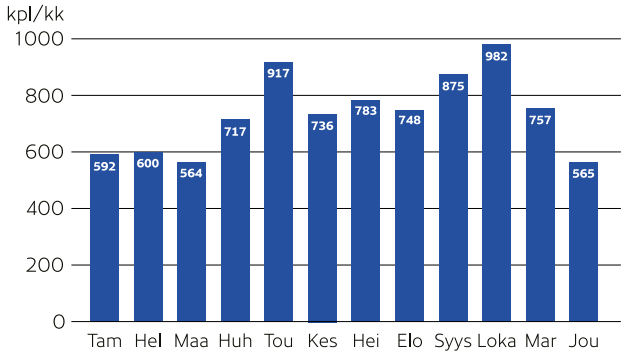
Tietojenkalastelu ja huijaukset olivat arkipäivää myös vuonna 2022

Tietojenkalastelu ja huijausten yrittäminen jatkuivat aktiivisesti myös vuonna 2022. Vuoden aikana esimerkiksi pankkien ja viranomaisten nimissä lähetettiin viestejä, joilla yritettiin saada ihmisiä luovuttamaan pankkitunnuksensa tai luottokortti- tai henkilötietonsa huijareille. Kyberturvallisuuskeskukselle raportoitujen sosiaalisen median tilien kaappausten tai niiden yritysten määrät jatkoivat kasvuaan. Erityisen haitallisina sosiaalisen median tilin kaappaukset ovat näkyneet henkilöille, joiden pääasiallinen toimeentulo liittyy sosiaalisen median kanavaan.

Tietojenkalastelun ja huijausten yrityksissä nähtiin vuonna 2022 uudenlaisia toimintatapoja. Usein huijauksissa korostuvat kuitenkin edelleen tietyt perustoimintatavat. Vetoaminen kiireeseen, uhkailu tai luotettavana tahona esiintyminen ovat kautta linjan huijauksissa käytettyjä peruskeinoja. Rikolliset ovat myös kohdentaneet tietojenkalastelua ja huijauksia kohteen mukaan, esimerkiksi yrityksiin on vuoden aikana kohdistunut totuttuun tapaan toimitusjohtaja- ja laskutushuijauksia.

Esimerkkeinä vuonna 2022 nähdyistä uusista toimintatavoista voi mainita laajan huijauskampanjan, jolla yritettiin vaihtaa palkanmaksutili huijarin pankkitiliksi. Samaa huijausta on nähty aiemminkin, mutta nyt sitä yritettiin järjestelmällisesti. Samankaltaisella huijauksella yritettiin saada vuokranmaksut siirrettyä huijareille tekstiviestikampanjassa 2023 alkupuolella. Lisäksi poliisiteemaiset kiristyshuijaukset levisivät vuonna 2022 maailmalta Suomeen. Euroopassa jo aiemmin nähdyt värikkäillä leimoilla ja virallisilla titteleillä koristellut dokumenttiliitteet uhkailivat räikeillä syytteillä ja seuraamuksilla, ellei uhri maksaisi lunnaita virtuaalivaluutalla. Huijarit yrittivät lisätä huijauksen uskottavuutta käyttämällä poliisiviranomaisen dokumentissa Palloliiton logoa. Samoin uutena isompana ilmiönä on alkuvuonna 2023 ollut henkilöpapereiden kopioiden ja sen kautta henkilötietojen kalastelu mahdollista identiteettivarkautta varten.

Kyberturvallisuuskeskuksen käsittelemät ilmoitukset huijauksista ja tietojenkalasteluista 2022



Haavoittuvuuksissa vuosi 2022 oli edellisiä vuosia rauhallisempi

Vuosi 2021 muistetaan lukuisista haavoittuvuuksista, jotka vaikuttivat maailmanlaajuisesti ja julkaisimme osasta näistä myös varoituksia. Vuonna 2022 yksittäisiltä erittäin merkittävästi yhteiskuntaan vaikuttavilta haavoittuvuuksilta vältyttiin. Vuoden 2022 aikana julkaisimme kymmenen haavoittuvuustiedotetta vähemmän kuin kahtena edellisenä vuonna.

Uusia haavoittuvuuksia löydetään jatkuvasti. Haavoittuvuuksien hyväksikäyttöyrityksiä tehdään myös vanhojen haavoittuvuuksien osalta. Kyberturvallisuuskeskukselle on tehty ilmoituksia, joissa vuosia vanhoja haavoittuvuuksia on käytetty hyväksi rikollisten toimesta. Unohtuneet päivitykset tai epätäydelliset korjaukset voivat altistaa organisaation monille uhkille. Organisaatioiden tulisikin tunnistaa omat haavoittuvat järjestelmänsä, ja ylläpitää ohjelmistot ajan tasalla.

Varoituksia julkaisemme vuosittain keskimäärin 1–3 kpl, ja vuoden 2022 ainoa varoitus koski FluBot-haitta-ohjelmaa. Vuonna 2021 varoituksia julkaistiin yhteensä viisi, joka on huomattavasti keskiarvoa enemmän.

Viestintäverkot toimivat Suomessa vakaasti vuonna 2022

Vuonna 2022 viestintäverkkojen toiminta oli Suomessa vakaata. Palvelukatkoksia tapahtui edellisvuotta selvästi vähemmän, ja vakavilta katkoksilta sekä seurauksilta vältyttiin. Yksittäisissä katkoksissa häiriöitä aiheutui alueellisiin palveluihin tai hätäliikenteen hetkellisesti, mutta katkot olivat lyhytaikaisia. Yleisten viestintäpalveluiden toimivuushäiriöiden määrä väheni kokonaisuudessaan 38 prosenttia vuodesta 2021.

Viranomaiset tekevät tiivistä yhteistyötä suomalaisten teleyritysten kanssa tietoliikenneyhteyksien rakentamisessa ja verkkojen toiminnan turvaamisessa. Rakentamista ohjaavalla sääntelyllä varmistetaan omalta osaltaan viestintäverkkojen toimivuus eri tilanteissa.

Suomen tietoliikenneyhteydet kotimaassa sekä maailmalle on varmennettu ja turvattu useilla eri tavoilla. Häiriöt yhteyksissä ovat kuitenkin aina mahdollisia. Mahdollisessa häiriötilanteessa tietoliikenne ohjataan ja hoidetaan muiden kaapelien tai varajärjestelmien kautta. Toiminta on hyvin automatisoitunutta, jolloin käyttäjä ei edes huomaa, että viestintäverkoissa olisi edes häiriöitä.

Kybervakoiluyritykset jatkuivat aktiivisena

Vuonna 2022 kybervakoiluyritykset jatkuivat aktiivisena edellisvuoden tapaan. Suomalaisiin organisaatioihin kohdistui jatkuvasti toimintaa, jolla pyrittiin tunnistamaan käytettyjä palveluita, löytämään erilaisia haavoittuvuuksia tai heikkoja salasanoja. Haavoittuvat verkkolaitteet ja -palvelut ovat olleet kybervakoilussa kiinnostuksen kohteena, koska niiden kautta on mahdollista päästä kiinni luottamukselliseen tietoon ja viestintään tai päästä sisälle muihin järjestelmiin. Lisäksi kohdistettuja haitallisia sähköpostiviestejä hyödynnetään edelleen yleisesti kybervakoilussa. Osa toiminnasta viittaa julkisten, kaupallisten, viranomais- tai muiden lähteiden pohjalta valtiollisten toimijoiden toimintaan.

Venäjän hyökkäys Ukrainaan näkyi vuoden aikana kybervakoilussa ja -vaikuttamisessa monin tavoin. Ukrainassa havaittiin vuoden aikana esimerkiksi useita uusia tietoja salaavia haittaohjelma sekä erilaisia tietojenkalastelu- ja haittaohjelmien levityskampanjoita. Muualla Euroopassa kybervakoilua on kohdistunut esimerkiksi sotaan ja humanitaariseen apuun liittyviin toimijoihin. Yksi esimerkki sodanaikaisten kybertoimien merkittävistä vaikutuksista myös Ukrainan ulkopuolella oli Viasat-satelliittipalvelun häiriö.

> ” Vuonna 2022 kybervakoiluyritykset jatkuivat aktiivisena edellisvuoden tapaan.

Valtiolliset toimijat hyödyntävät edelleen haavoittuvia koti- ja pienyritysreitittimiä sekä verkkolevypalvelimia osana hyökkäysinfrastruktuuriaan. Päivittämättömät tai heikosti suojatut laitteet, jotka ovat saavutettavissa internetistä, ovat alttiina yleisemminkin pahantahtoisille toimille, mikä on muodostumassa kasvavaksi ongelmaksi. Haavoittuvia laiteita ei välttämättä hyödynnetä niiden käyttäjiä vastaan, vaan niitä hyödyntäen voidaan toteuttaa huomaamattomammin kyberhyökkäyksiä kotimaisiin kohteisiin.

Traficomille raportoitiin GPS-häiriöistä

Venäjän hyökkäyssota Ukrainaan aiheutti merkittäviä muutoksia lentoreitteihin Venäjän ilmatilan sulkeutuessa. Ilma-alusten satelliittinavigointijärjestelmien häiriöitä havaittiin erityisesti konfliktialueiden läheisyydessä. Euroopan lentoturvallisuusvirasto EASA julkaisi aiheesta uutisen maaliskuussa. Myös Suomessa julkaistiin maaliskuun alussa kaikkia lentäjiä GPS-häiriöstä varoittava NOTAM-tiedote, joka peruttiin 15.3.2022.

Vuonna 2022 Traficomille ilmoitettiin Suomessa ilma-alusten lennonaikaisia GPS-signaalin katkeamisia tai signaalin heikentymistä 65 kpl. Edeltävinä koronavuosina ilmoituksia tuli 8 kpl vuonna 2021 ja 27 kpl vuonna 2020. Vuosina 2017–2019 ilmoituksia saatiin yhteensä 9 kpl. Suomen ulkopuolelta suomalaisilta ilma-aluksilta saatiin 1327 ilmoitusta GPS-häiriöistä. Ilmailua koskien häiriötilanteiden määrää seurataan ja asiaa käsitellään kansainvälisesti sekä EASA:n, Eurocontrolin sekä kansainvälisen televiestintäliiton ITU:n toimesta. Ilmailun poikkeamailmoituksia koskevat tarkat EU-tason vaatimukset muun muassa ilmoittajan yksityisyydensuojan osalta. Poikkeamailmoitukset ovat myös julkisuuslain mukaan salassapidettäviä. Maanpäällisiltä liikennesektorin toimijoilta satelliittiradionavigointiin liittyviä GNSS-häiriöilmoituksia ei vuoden 2022 aikana ole saatu.

Maanpäälliset radiohäiriömäärät ovat olleet laskusuunnassa

Maanpäälliset radiohäiriömäärät ovat olleet yleisesti laskusuunnassa. Vuoden 2022 aikana ilmoitettiin Traficomille kokonaisuudessaan yhteensä 86 radiohäiriöitä, joista 32 vaati kenttäselvitystä. Vuoden 2021 aikana häiriöitä ilmoitettiin 115 kpl. Vuoden 2022 aikana ilmoitetuista radiohäiriöistä 11 liittyi satelliittiradionavigointiin (GNSS). Valtaosa näistä oli yksittäisten kansalaisten ilmoituksia GNSS-poikkeamista, joissa esimerkiksi urheilukello, auton navigaattori tai karttaplotteri on näyttänyt väärää paikkaa.

Traficomin havaitsee omassa monitoroinnissaan säännöllisesti pieniä häirintälähettimiä eli jammereita ympäri maan. Jammerihavaintoja on tehty virastossa vuoden 2022 aikana 422 kappaletta.

Traficomin Kyberturvallisuuskeskuksen vuosi 2022

Varautumista tehostettiin ja yhteistyötä tiivistettiin

Turvallisuusympäristön muutoksen ja kyberympäristön uhkatason nousun vuoksi viranomaiset tehostivat varautumista ja tiivistivät yhteistyötään sekä koti- että ulkomaisten yhteistyökumppaneiden kanssa. Varautumisen tasoa nostettiin viranomaisissa, julkishallinnossa ja kriittisen infrastruktuurin toimijoilla. Kyberturvallisuuskeskus antoi keväällä 2022 huoltovarmuuskriittisten organisaatioiden johdolle tarkentavaa ohjeistusta ja tukea, jotta ne ovat voineet tehostaa varautumista ja jatkuvuudenhallintaa. Myös Suojelupoliisi kehotti yrityksiä varautumaan kyber- ja informaatiovaikuttamisen uhkaan.

Vuoden 2022 aikana erilaisten tiedonvaihdon ja tilannekuvatiedon tuottamisen ja jakamisen verkostojen välistä yhteistyötä tiivistettiin ja samalla panostettiin reaaliaikaisen tiedon- ja kokemusten vaihtoon. Yhteistyötä teleyritysten kanssa jatkettiin suomalaisten verkkojen ja palvelujen toimivuuden turvaamiseksi. Työssä hyödynnettiin muun muassa Ukrainasta saatuja havaintoja ja oppeja viestintäinfrastruktuurin suojaamisesta.

Kybersuojauksesta vastaavien ministeriöiden ja kyberturvallisuusviranomaisten sisäistä ja keskinäistä yhteistyötä tiivistettiin vuonna 2022 entisestään. Viranomaisten välisen yhteistyön ja tiedonvaihdon varmistamiseksi sekä yhteisen tilannekuvan tuottamiseksi perustettiin erillinen ministeriötason ryhmä keväällä 2022. Ryhmän tehtävänä on tarvittaessa tukea valtionjohdon päätöksentekoa vakavissa kyberhäiriö- tai vaikuttamistilanteissa.

Verkostoyhteistyötä kehitettiin vuonna 2022

Jatkuva tiedonvaihto on olennainen osa Kyberturvallisuuskeskuksen toimintaa ja keskeinen palvelutehtävämme. Osallistumme useisiin kansainvälisiin yhteistyöryhmiin ja fasilitoimme kotimaassa tiedonvaihtoa kaikilla yhteiskunnan huoltovarmuuskriittisillä toimialoilla. Tietoja vaihdetaan niin päivänpolttavista kyberuhista kuin varautumisesta ja kyberturvallisuuden hallinnastakin.

Suomessa keskukselle tärkeimpiä verkostoja ovat ISAC-tiedonvaihtoryhmät (information sharing and analysis centre). Ne ovat tietyn toimialan organisaatioista koostuvia luottamuksellisia ja itsenäisiä ryhmiä. Ryhmiä on elintarvike-, energia-, finanssi-, ICT-, media- ja vesihuoltoaloilla, sekä internetpalveluntarjoajien, kemian ja metsäteollisuuden, logistiikan ja liikenteen, sosiaali- ja terveydenhuollon ja valtionhallinnon aloilla. ICT-ISAC perustettiin alan yrityksiltä tulleen toiveen kannustamana syksyllä 2022. Lisäksi Kyberturvallisuuskeskuksen havainnointi- ja varoituspalvelu HAVARO:n käyttäjillä on omat tiedonvaihtoryhmänsä.

Vuoden 2022 aikana suurimpia ISAC:eissa käsiteltyjä aiheita ovat olleet Ukrainan sodan vaikutukset kyberturvallisuuteen, EU:n NIS2- ja CER-direktiivit sekä DORA-asetus, ja yhteiskunnan riippuvuus ulkomailla tuotetuista ICT-palveluista. Aiheista keskusteltiin ISAC:ien kokouksissa, ja myös ISAC:ien jäsenille tehtiin erikseen kyselyitä niistä. Kyberturvallisuuskeskus hyödynsi saatuja tietoja osana kyberturvallisuuden kansallisen tilannekuvan muodostamista ja asioista raportoitiin myös julkisesti. Yhteistyöhön aktiivisesti osallistumalla tiedonvaihtoryhmien jäsenet myös saavat itse ajantasaista tietoa vertaisiltaan.

Vuonna 2021 alkanut operaattoreiden ja Kyberturvallisuuskeskuksen yhteistyö johti uuden suositukseen antamiseen alkuvuodesta 2022 eri keinoista estää soittajan numeron väärentäminen ja huijaussoittojen välittäminen puhelun vastaanottajille Suomessa. Tavoitteena on estää suomalaisten numeroiden käyttö kansainvälisessä tietoverkkorikollisuudessa ja vähentää ulkomailta tulevia huijauspuheluita. Keskusrikospoliisin mukaan huijauspuheluissa menetettyjen eurojen määrät ovatkin laskeneet merkittävästi aiemmista vuosista.

Kansainvälinen yhteistyö laajeni ja jatkui tiiviinä

Kansainvälisen yhteistyön tavoitteena on tukea erityisesti kansallisen ja kansainvälisen kyberturvallisuutta koskevan tilannekuvan muodostamista ja edistää sitä kautta Suomen kyberturvallisuutta koskevien tavoitteiden saavuttamista. Kansainvälinen vastavuoroinen tiedonvaihto on elinehto kyberturvallisuuden ylläpitämiseksi ja kehittämiseksi kansallisella tasolla. Kansainvälisistä verkostoista tai toiselta valtiolta saatu tieto tai varoitus kyberlouk-kauksesta tai esimerkiksi tietojärjestelmähaa-voittuvuudesta voi olla kriittisessä asemassa kansallisen varautumisen näkökulmasta.

Vuoden 2022 aikana kansainvälistä yhteistyötä tiivistettiin ja kehitettiin eri tasoilla. Koko kansainvälistä yhteistyötä leimasi vuoden 2022 aikana erityisesti Ukrainan sota ja korostunut tiedon jakamisen tarve eri kumppanimaiden kesken. Kansainväliset kyberturvallisuuden yhteistyöverkostot osoittivat myös käytännön kykynsä sopeutua nopeastikin muuttuviin tilanteisiin turvallisuusympäristössä.

Suomi toimii aktiivisesti kansainvälisissä organisaatioissa, instituutioissa ja verkostoissa. Operatiivisessa yhteistyössä korostuvat vakiintuneet luottamukseen perustuvat yhteistyöryhmät eri maantieteellisillä alueilla. Tärkeimpiä yhteistyöryhmiä ovat Pohjoismaiden välinen NCC-ryhmä (Nordic Cert Cooperation), eräiden eurooppalaisten valtioiden muodostama EGC-ryhmittymä (European Governmental Certs) sekä globaali International Watch and Warning Network. Lisäksi eri toimialoilla tehdään laajaa kansainvälistä yhteistyötä, johon myös Kyberturvallisuuskeskus osallistuu. Esimerkki tällaisesta on pohjoismaisten finanssi-instituutioiden yhteistyöryhmä Nordic Financial Cert.

Myös EU-tasoinen yhteistyö kehittyy jatkuvasti. Kyberturvallisuuskeskus osallistui aktiivisesti EU:ssa teknistä ja operatiivista kybertilannekuvaa keräävän EU:n jäsenvaltioiden välisen kansallisten kyberturvallisuuskeskusten CSIRT-verkoston toimintaan. Strategisemman tason yhteistyötä kehitettiin EU:ssa vuoden 2022 aikana erityisesti CyCLONe-verkostossa, jonka tarkoituksena on tuottaa muun muassa tilannekuvaa ja analyysiä neuvoston kybertyöryhmälle erityisesti laajoissa kyberturvallisuutta koskevissa kriisitilanteissa. EU:n verkostojen ohella suomalaisten viranomaisten yhteistyö myös Naton eri kyberturvallisuusverkostojen kanssa tiivistyi vuoden 2022 aikaan.

Kyberturvallisuuskeskus osallistuu Euroopan kyberturvallisuusvirasto ENISA:n toimielimiin ja asiantuntijaryhmiin ja se toimii ENISA:n kansallisena yhteyspisteenä. Olemme mukana myös Tallinnassa sijaitsevan NATO:n kyberpuolustuksen osaamiskeskus NATO CCDCOE:n toiminnassa.

Sääntelyyn tai vakiintuneiden instituutioiden alaisuuteen kuuluvien yhteistyöverkostojen ohella Kyberturvallisuuskeskus osallistui aktiivisesti useiden muidenkin kansainvälisten verkostojen toimintaan ja yhteistyöhön, kuten esimerkiksi Pohjoismaiden väliseen kyberturvallisuusyhteistyöhön. Mainittujen kansainvälisten verkostojen toiminta perustuu vahvasti luottamukseen eri osallistujavaltioiden kesken. Sääntelyn kehittämisessä oppeja ja tietoa vaihdetaan aktiivisesti pohjoismaisten sisarvirastojen kanssa ja osana laajempia EU-yhteistyöfoorumeja.

Operatiivisen yhteistyön kehittämisen ohella EU:ssa on ollut vuoden 2022 aikana ennätysmäärä kyberturvallisuutta koskevia aloitteita tai hankkeita eri työryhmien käsittelyssä. Näistä keskeisempiä ovat olleet muun muassa sähköisen viestinnän tietosuojaa ja tunnistuspalveluja koskevien säädöskokonaisuuksien edistäminen, NIS2-direktiivin viimeistely, kyberkestävyyssäädöstä koskevat neuvottelut ja lukuisat työryhmäkeskustelut kriittisen infrastruktuurin suojaamisen vahvistamiseksi. Kyberturvallisuuskeskuksen asiantuntijat osallistuivat tiiviisti EU-tason kyberturvallisuuden kehittämishankkeisiin, ennakkovaikuttamiseen ja säädösvalmisteluun. Myös kansainvälinen harjoitustoiminta oli aktiivista vuoden 2022 aikana. Harjoitustoiminnassa painottui vuoden 2022 aikana aikaisempaa vahvemmin myös strateginen taso ja päätöksentekoprosessien harjoittelu kriisitilanteissa.

Yhteiskunnan turvallisuutta edistettiin kyberturvallisuuden ja digitaalisen 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. Huoltovarmuuskeskuksen rahoittamat kehityshankkeet rahoitetaan Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030 -ohjelmasta ja ne noudattavat ohjelmassa asetettuja tavoitteita. Viimeisten vuosien aikana kyberturvallisuuden kehitystyötä on saatu laajennettua, kun myös valtiovarainministeriö on osallistunut näiden kyberturvallisuuden kehityshankkeiden rahoittamiseen ja tukemiseen. Valtiovarainministeriön rahoittamat kehityshankkeet rahoitetaan valtiovarainministeriön Julkisen hallinnon digitaalisen turvallisuuden toimeenpano 2020–2023 (Haukka) -ohjelmasta.

Huoltovarmuuskeskuksen rahoittamien ja tukemien kehittämishankkeiden kohteena ovat yhteiskunnan kannalta elintärkeät yritykset ja niiden kyberturvallisuus, kun valtiovarainministeriön rahoittamien ja tukemien kehityshankkeiden kohteena ovat julkisen hallinnon, pääasiassa yhteiskunnan kannalta elintärkeät toimijat ja niiden kyberturvallisuus. Yhteisinä tavoitteina Huoltovarmuuskeskuksen ja valtiovarainministeriön rahoittamilla kehityshankkeilla on tarjota uutta tietoa, työkaluja ja palveluja, jotka auttavat sekä yksityisen että julkisen sektorin elintärkeitä toimijoita varautumaan, ylläpitämään, kehittämään ja parantamaan omaa kyberturvallisuuttaan ja sitä kautta koko yhteiskunnan kyberturvallisuutta ja turvallisuutta. Valtiovarainministeriön mukaan tulolla kyberturvallisuuden kehityshankkeisiin ja yhteistyön tiivistämisellä on saatu merkittäviä synergioita ja säästöjä aikaan, kun kehityshankkeiden tuloksena syntynyttä tietoa, työkaluja ja palveluja on voitu hyödyntää ristiin niin yksityisen kuin julkisen sektorin kyberturvallisuuden kehittämisessä ja parantamisessa eikä samoja kehityshankkeita ole ollut tarvetta toteuttaa erikseen yksityiselle ja julkiselle sektorille suunnattuna.

Harjoitustoiminnan, tilannetietoisuuden ja ennakointityön kehittämistä jatkettiin myös vuonna 2022

Varauduttaessa ja vastattaessa erilaisiin häiriötilanteisiin on tärkeää, että johtamisen, viestinnän ja tilannekuvan väliset yhteydet toimivat sekä roolit ja vastuut ovat selvät ja ne on harjoiteltu. Vuonna 2022 jatkettiin tilannetietoisuuden kehittämistä esimerkiksi kehittämällä toimintaympäristön ennakointitoimintaa ja Kyberilmastoa. Kyberilmaston tavoitteena on kehittää Kyberturvallisuuskeskuksen kykyä hyödyntää dataa ja informaatiota kansallisen kyberturvallisuuden tilannekuvan muodostamiseksi, uusien palveluiden ja toimintamallien synnyttämiseksi sekä kyberturvallisuusuhkiin ja -poikkeamiin vastaamiseksi.

Ennakointityössä pureuduttiin tekoälyn hyödyntämiseen kyberhyökkäyksissä ja rikollisuudessa sekä arvioitiin, milloin ja missä muodossa teknologian tuomat vaikutukset alkavat näkyä. Toisena erityisenä teemana ennakointityössä käsiteltiin 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[1,2] Kyberturvallisuuskeskuksen verkkosivuille.

Ennakoinnin osalta jatkettiin myös yhteistyön rakentamista erilaisten toimijoiden kanssa. Toimintaympäristön muuttuessa ja monimutkaistuessa yhteistyön rooli tulevaisuuden ilmiöiden ja niiden erilaisten vaikutusten tunnistamisessa korostuu entisestään. Yhteistyöllä tuetaan tiedon jakamista ja hyödyntämistä kaikessa toiminnassa.

Vuoden 2022 aikana jatkettiin HAVARO- ja Kybermittari-palveluiden kehittämistä. HAVARO havainnoi suomalaisiin yrityksiin kohdistuvia vakavia tietoturvauhkia ja varoittaa niistä. Kybermittari on kansallinen kyberturvallisuuden arviointimalli, joka mahdollistaa organisaatioiden kyberturvallisuuden jatkuvan arvioinnin, kehittämisen ja vertailun viiteryhmän toimijoiden välillä.

Vuoden 2022 aikana toteutettiin useita kyberharjoituksia. Hyvätkään toimintamallit ja ohjeistukset eivät välttämättä riitä, jos niitä ei osata käyttää tositilanteessa. Harjoittelun avulla hyvät ja oikeat prosessimallit saadaan helposti jalkautettua organisaation toimintaan, mikä on selkeästi kasvattanut kiinnostusta kyberharjoittelua kohtaan. Vuoden 2022 aikana toteutettiinkin useita toimialakohtaisia kyberturvallisuuden yhteisharjoituksia. Organisaatiot näkevät itsensä selkeämmin osana laajempaa organisaatioverkostoa tai toimitusketjua ja tästä syystä kumppaneiden kanssa yhteisten prosessien harjoittelu on myös viime aikoina koettu aiempaa tärkeämmäksi. Kyberturvallisuuskeskus tukee kyberharjoittelua neuvontapalveluilla, ohjeistuksilla, tarjoamalla käyttöön skenaarioideoita harjoitusten sisällöksi sekä tukemalla kansallisesti merkittävien yhteisharjoitusten suunnittelua ja toteutusta.

[1] Tekoäly tulee muuttamaan myös kyberhyökkäyksiä | Traficom (kyberturvallisuuskeskus.fi)
[2] Uudessa ohjeessa tietoa paikallisiin matkaviestinverkkoihin liittyvistä kyberuhkista ja riskienhallinasta | Kyberturvallisuuskeskus

Tietoisuutta kyberuhkista pyrittiin lisäämään monin eri tavoin

Vuoden 2022 aikana tietoisuutta kyberuhkista pyrittiin lisäämään aktiivisesti Suomessa. Esimerkiksi eri viranomaiset, yritykset ja järjestöt viestivät säännöllisesti kyberuhkista ja antoivat ja julkaisivat ohjeita sekä varoituksia ajankohtaisesta kyberturvallisuustilanteesta, kuten havaituista huijausviesteistä.

Kyberturvallisuuskeskuksen eri viestintäkanavissa, esimerkiksi verkkosivuilla ja sosiaalisessa mediassa viestittiin aktiivisesti keskuksen toimintaan, kyberuhkiin ja ajankohtaiseen turvallisuustilanteeseen liittyvistä asioista. Vuoden 2022 aikana järjestettiin useita tilaisuuksia, kuten Tietoturvamerkki- ja Tietoturvaseminaarit, joiden tarkoituksena oli lisätä suomalaisen tietoturvayhteisön ja johdon tietoa tulevasta kyberturvallisuutta ja tietoturva-alaa koskevasta sääntelystä, turvallisuusympäristön muutoksista ja niiden vaikutuksista kyberturvallisuuteen. Lokakuussa Huoltovarmuuskeskuksen kanssa järjestetty Tietoturvaseminaari kokosi yli 1 000 osallistujaa. Tapahtuman pääpuhujana toimi Ukrainan digitaalisesta transformaatiosta vastaava varaministeri George Dubynskyi.

Vuonna 2022 lanseerattiin uusi Kyberturvallisuuden viikkokatsaus, jossa jaetaan tietoa ajankohtaisista kyberilmiöistä.

Kuukausittain julkaistussa Kybersää-katsauksessa kerrottiin kuluneen kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Tuote on ensisijaisesti suunnattu tietoturvasta vastaaville henkilöille, mutta arjen kyberturvallisuusosiossa on hyviä neuvoja kaikille. Katsauksesta saa nopean kokonaiskuvan siitä, mitä kyberturvallisuuskentällä on tapahtunut. Kybersää-katsausta uudistettiin loppuvuonna. Tuote suunnataan jatkossa organisaatioille ja se luo yhteisen kokonaisuuden Viikkokatsauksen kanssa siten, että ajankohtaiset teemat nostetaan esille Viikkokatsauksessa, jotta tieto saadaan nopeasti jaettua. Kybersää puolestaan koostaa kuun tapahtumat lyhyesti yhteen, mutta keskittyy lyhyen ja pitkän aikavälin trendeihin sekä uhkiin, joihin organisaatioiden suositellaan varautuvan.

Kyberuhkat muuttavat jatkuvasti muotoaan. Organisaatioiden, tietoturva-alan ammattilaisten ja suuren yleisön tietoisuutta ja kykyä tunnistaa ja vastata kyberuhkiin sekä parantaa omaa tietoturvaansa tuettiin julkaisemalla keskuksen verkkosivuilla useita oppaita ja toimintaohjeita. Vuonna 2022 julkaistuja oppaita ja ohjeita olivat esimerkiksi toimintaohjeet kiristyshaittatilanteeseen johdolle, katsaus palveluestohyökkäystilanteeseen, ohjeita vuotaneisiin tunnuksiin liittyen, katsaus viestintäverkkojen tehonsyötön turvaamiseen sekä kuvaus Suomen kansainvälisistä tietoliikenneyhteyksistä ja niihin kohdistuviin toimivuusuhkiin varautumisesta. Lisäksi julkaistiin vinkkejä informaatiovaikuttamisen tunnistamiseen sekä ohjeistus monivaiheisen tunnistautumisen käyttämiseen suojaamaan käyttäjätilejä.

Vuoden 2022 aikana Kyberturvallisuuskeskus toteutti tai osallistui useisiin viestintäkampanjoihin. Kampanjoita olivat esimerkiksi loppuvuonna toteutettu Älyä ostoksiin -kampanja, jonka tarkoituksena oli lisätä kuluttajien tietoa älylaitteisiin liittyvistä tietoturva-asioista ja lokakuussa toteutettu Euroopan kyberturvallisuuskuukausi. Lisäksi Yleisradio lähetti syksyllä yleishyödyllisenä mainoksena TV-kanavillaan kyber- ja informaatiovaikuttamisen tunnistamista koskevan tietoiskuvideon.

Keskuksen asiantuntijat ja johto luennoivat säännöllisesti alueellisilla ja valtakunnallisilla maanpuolustuskursseilla kyberuhkiin ja niihin varautumiseen liittyvistä aiheista. Asiantuntijat antoivat myös säännöllisesti haastatteluja koti- ja ulkomaiselle medialle ja esiintyivät seminaareissa ja tapahtumissa niin Suomessa kuin ulkomailla. Teimme tiivistä yhteistyötä alan korkeakoulujen ja oppilaitosten kanssa. Aktiivisella ja avoimella tiedonjaolla tuimme osaltamme kyberturvallisuutta koskevan tiedon ja osaamisen leviämistä yhteiskunnassa.

Tietoturvan kehittämisen tuella nopeutetaan tietoturvan parantamista huoltovarmuus-kriittisissä yrityksissä

Valtioneuvosto teki lokakuussa 2022 päätöksen määräaikaisesta yhteiskunnan toiminnan kannalta elintärkeille yrityksille suunnatusta tietoturvan kehittämisen tuesta (nk. Tietoturvaseteli). Tuen tavoitteena on nostaa nopeasti yritysten tietoturvallisuuden tasoa ja sitä kautta parantaa koko yhteiskunnan kykyä suojautua kyberturvallisuusuhkia vastaan. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus vastaa tuen myöntämisestä. Tuen hakemista ja myöntämistä varten virastossa kehitettiin nopealla aikataululla järjestelmät ja prosessit, jotka mahdollistavat tuen hakemisen, käsittelyn ja maksatuksen sähköisesti. Näin tuet voidaan myöntää mahdollisimman nopeasti tukea hakeneille yrityksille.

Tietoturvasetelin haku käynnistyi joulukuussa ja jo ensimmäisten viikkojen aikana tukihakemuksissa haettu euromäärä ylitti valtioneuvoston tukina myönnettäväksi osoittaman kuuden miljoonan euron määrärahan. Toden teolla tukihakemuksia päästiin käsittelemään vuoden 2023 alusta ja ensimmäiset myönteiset tukipäätökset annettiin tammikuussa 2023. Tukihakemusten käsittelyn jälkeen Kyberturvallisuuskeskuksen tehtävänä on käsitellä tukea saaneiden yritysten selvitykset tuen käytöstä. Samalla tehdään arviointia tuella toteutetuista toimenpiteistä ja saavutetuista hyödyistä.

> ”Tuen tavoitteena on nostaa nopeasti yritysten tietoturvallisuuden tasoa ja sitä kautta parantaa koko yhteiskunnan kykyä suojautua kyberturvallisuusuhkia vastaan.

Tietoturvamerkki myönnettiin 15 uudelle laitteelle

Liikenne- ja viestintävirasto Traficomin 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 2022 aikana Tietoturvamerkki myönnettiin 15 uudelle laitteelle. Yhteensä merkki on tällä hetkellä 25 laitteella. Merkkimäärää kasvatti osaltaan vuonna 2021 aloitettu yhteistyö Singaporen kyberturvallisuusviranomaisen kanssa. Tietoturvamerkin rooli tuotteiden tietoturvallisuuden osoittamisessa vähenee tulevina vuosina voimaan tulevien EU:n sääntelymuutosten myötä. Traficomin Kyberturvallisuuskeskus varautuu muuttamaan toimintaansa edellä mainitun sääntelyn tehtäviin.

Kyberturvallisuuden tutkimus- ja kehitystoimintaan vahvistusta Suomessa ja Euroopassa

EU:n kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen Suomen kansallinen koordinointikeskus aloitti virallisesti toimintansa vuoden 2023 alusta Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksessa. Suomen kansallisen koordinointikeskuksen valmistelutyöt käynnistettiin syksyllä 2022. Koordinointikeskus tukee suomalaisten toimijoiden osallistumista rajat ylittäviin EU-hankkeisiin ja edistää kansallisten prioriteettien mukaisen EU-rahoitusmahdollisuuksien avaamista. Lisäksi koordinointikeskus järjestää rahoitushakuja suomalaisille toimijoille kyberturvallisuutta kasvattaviin toimiin.

Kansallinen koordinointikeskus on osa koko unionin laajuista EU:n kyberturvallisuuden osaamiskeskuksen koordinointikeskusten verkostoa. Verkoston tehtävänä on parantaa kyberomavaraisuutta, tukea kyberturvallisuusalan tutkimusta ja vauhdittaa teknologian kehittämistä koko EU:ssa. Koordinointikeskusten muodostaman verkoston avulla yhteistyö jäsenvaltioiden välillä lisääntyy ja tiivistyy. Yhteistyön myötä EU:n kyberturvallisuusvalmiudet sekä toimialan kilpailukyky vahvistuvat. Koordinointikeskuksen toimintaa rahoittavat EU ja Suomen valtio.

Sääntelyn kehittämisellä tuetaan kyberturvallisuutta

Yleisten viestintäverkkojen ja -palvelujen (eli teletoiminnan) varautumisesta ja tietoturvallisuudesta huolehtiminen on ollut osa toimijoita koskevaa lainsäädäntöä ja viranomaisohjausta ja -valvontaa jo 1990-luvulta lähtien. Traficomin Kyberturvallisuuskeskus ohjaa ja valvoo vahvojen sähköisten tunnistus- ja luottamuspalvelujen sekä EU:n verkko- ja tietoturvadirektiivissä (NIS-direktiivi) tarkoitettuja digitaalisen infrastruktuurin ja palvelujen tarjoajia. Lisäksi se valvoo luottamuksellisen viestinnän suojan toteutumista sähköisessä viestinnässä.

Kyberturvallisuuskeskus antaa lakia tarkentavia määräyksiä valvomilleen toimijoille. Määräyksiä uudistetaan säännöllisesti vastaamaan kyberturvallisuusympäristössä ja teknisessä kehityksessä tapahtuviin muutoksiin. Tästä esimerkkinä on vuoden 2022 aikana annettu uudistettu sähköisiä tunnistus- ja luottamuspalveluja koskeva määräys. Lisäksi se ohjaa valvomiaan toimijoita antamalla suosituksia ja ohjeita sekä tukemalla lainsäädännön tulkinnassa.

Kyberturvallisuuskeskus valvoo toimialaansa usein eri tavoin, kuten keräämällä häiriöilmoituksia, antamalla valvontapäätöksiä ja tekemällä tarkastuksia. Voit lukea lisää keskuksen ohjaus- ja valvontatoiminnasta verkkosivuiltamme: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta

Vuoden 2022 aikana Kyberturvallisuuskeskus käsitteli satoja häiriöilmoituksia ja kymmeniä evästeiden käyttöä verkkosivuilla koskevia valituksia. Se neuvoi päivittäin lainsäädännön noudattamisessa ja lausui kymmeniin esimerkiksi lainsäädännön kehittämistä koskeviin pyyntöihin. Kyberturvallisuuskeskus teki jatkuvasti toimivaa yhteistyötä valvomiensa yritysten kanssa.

> ” Kansallinen koordinointikeskus on osa koko unionin laajuista EU:n kyberturvallisuuden osaamiskeskuksen koordinointikeskusten verkostoa.

Kyberturvallisuuden trendejä vuonna 2023

Vuoden 2023 aikana kyberturvallisuusympäristön uhkataso pysyy hyvin todennäköisesti edelleen kohonneena ja teknologinen kehitys jatkuu nopeana. Sääntely tiukkenee ja yritykset joutuvat noudattamaan kiristyvää sääntelyä kyberturvallisuuden alalla. Tämä vaatii resursseja ja aikaa. Samaan aikaan ilmassa on uhka talouden taantumasta ja kyberosaajista on pula. Yritysten on suojattava tietonsa ja järjestelmänsä kasvavilta kyberuhilta ja niiden on myös tehtävä merkittäviä investointeja kyberturvallisuuteen. Lisäksi yritykset ja organisaatiot joutuvat ratkomaan uudenlaisia kyberturvallisuushaasteita, kuten deepfake-videoiden tuomia huijausyrityksiä ja botti-hyökkäysten torjumista.

Vuonna 2023 rikolliset pyrkivät hyödyntämään ja ottamaan käyttöön uutta teknologiaa, jotta he saavuttaisivat tavoitteensa entistä tehokkaammin. Samalla kun tekoälyn arkipäiväistyminen ja yleistyminen luovat uudenlaisia mahdollisuuksia ja keinoja hyökkäyksille, se tarjoaa uusia välineitä myös niiden torjunnalle. Esimerkiksi tekoälypohjaiset keskustelubotit tarjoavat tehokkaan apuvälineen huijauksien ja petosten torjunnassa. Nämä botit pystyvät tunnistamaan epäilyttävät viestit ja varoittamaan käyttäjiä mahdollisista huijauksista. Tämä on tärkeää, sillä huijarit ovat yhä luovempia ja keksivät uusia tapoja päästä käsiksi tietoihin ja varoihin.

Kehitetyt kyberpuolustusjärjestelmät, kuten koneoppiminen ja data-analytiikka, tulevat olemaan lähivuosien aikana yhä tärkeämpiä kyberturvallisuuden näkökulmasta. Nämä järjestelmät tarjoavat reaaliaikaisen suojauksen ja ennaltaehkäisevän suojan tietoturvahyökkäyksiltä. Tämä on tarpeen, sillä myös huijarit käyttävät yhä kehittyneempiä tekniikoita ja bottijärjestelmiä hyökätäkseen tietojärjestelmiin. Kehitetyt kyberpuolustusjärjestelmät tarjoavat tärkeää suojaa tällaisilta hyökkäyksiltä.

Miten kyberuhkatason nousu näkyy arjessa?

Kyberuhkatason nousu näkyy eri toimijoiden arjessa useilla tavoilla. Tärkeimmät näkymät ovat

Lisääntynyt tietoturvariski:
yritysten ja muiden organisaatioiden on suojattava tietonsa ja järjestelmänsä kasvavilta kyberuhilta.

Tiukempi sääntely:
yrityksiin ja organisaatioihin tulee kohdistumaan tulevina vuosina enemmän sääntelyä kyberturvallisuuden alalla, mikä vaatii resursseja ja osaamista.

Investoinnit kyberturvallisuuteen:
yritysten ja organisaatioiden on varauduttava tekemään uusia investointeja kyberturvallisuuteen, jotta ne voivat suojata tietonsa ja järjestelmänsä.

Uuden teknologian tuomat haasteet:
yritykset ja organisaatiot joutuvat ratkomaan uudenlaisia kyberturvallisuushaasteita, kuten deepfake-videoiden ja botti-hyökkäysten torjumista.

Jotta yrityksen ja organisaatiot voivat vastata näihin haasteisiin, niiden on tehtävä seuraavia muutoksia

Päivitettävä tietoturvastrategiansa:
tarvitaan ajan tasalla olevan tietoturvastrategia, joka vastaa uusimpiin kyberuhkiin.

Panostettava koulutukseen ja henkilöstöön:
henkilöstön koulutukseen ja kyberturvallisuuden osaamiseen tulee panostaa entistä enemmän.

Huolehdittava säännöllisestä kyberriskien arvioinnista ja kehittämisestä:
yritysten ja muiden organisaatioiden on huolehdittava säännöllisestä kyberriskien arvioinnista ja kehitettävä järjestelmiään ja prosessejaan tarvittaessa.

Yhteistyö kumppaneiden kanssa:
kyberturvallisuutta on mahdollista tehostaa yhteistyössä kumppaneiden kanssa ja hyödyntämällä heidän tarjoamia ratkaisuja.

Taloudellisen taantuman uhka ja pula kyberosaajista muodostuu haasteeksi

Haasteeksi muodostuu yritysten ja muiden organisaatioiden kyky hankkia ja ylläpitää tarvittavia kyberturvallisuusresursseja talouden mahdollisten lähitulevaisuuden haasteiden vuoksi. Tämän vuoksi toimijat saattavat priorisoida säästöjä kyberturvallisuuden alalla ja jättää joitain toimenpiteitä toteuttamatta. Tämä tullee johtamaan esimerkiksi yrityksissä ulkoistusten ja toimitusketjujen lisääntyvään käyttöön, säästötarpeiden myötä edelleen näiden karsintaan ja priorisointiin.

Kyberosaajien puute vaikeuttaa yritysten ja muiden organisaatioiden kykyä reagoida ja ratkaista kyberuhkia, ja tekee niistä entistä haavoittuvaisempia hyökkäyksille. Tämän vuoksi yritysten ja organisaatioiden on tärkeää varautua ja mukautua näihin haasteisiin kehittämällä tehokkaita ja joustavia ratkaisuja sekä hankkimalla ja kouluttamalla riittävästi osaavia henkilöstöresursseja.

Kyberturvallisuutta koskeva hankintaosaamista tulee jatkuvasti kehittää

Yritysten ja muiden organisaatioiden tulee jatkuvasti kehittää kyberturvallisuutta koskevaa hankintaosaamistaan. Tämä edellyttää esimerkiksi yrityksissä kykyä ja osaamista sovittaa kyberturvallisuuden tarpeet yhteen liiketoiminnan tarpeiden kanssa.

Ostetut palvelut ja toimitusketjut voivat olla merkittävä osa yritysten kyberturvallisuuden ratkaisemisessa. Ne tarjoavat mahdollisuuden ulkoistaa osa kyberturvallisuusvastuista ja hyödyntää asiantuntemusta ja teknologiaa, joita organisaatiolla ei välttämättä itsellään ole.

Ostaessaan kyberturvallisuuspalveluita ja -tuotteita organisaatioiden tulee varmistaa, että ne täyttävät niille asetetut toiminnalliset ja laadulliset vaatimukset. Tämä edellyttää ymmärrystä kyberturvallisuuden eri osa-alueista ja niihin liittyvistä standardeista, teknologioista ja toimintatavoista. Lisäksi hankkija tarvitsee tietämystä tarjolla olevista palveluista ja tuotteista, markkinoiden hintatasosta ja tarjouksista sekä ymmärrystä tietoturva- ja tietosuoja-asioista. Hankkijalla tulee myös olla osaamista arvioida palveluntuottajan luotettavuutta ja kykyä tarjota jatkuvaa tukea ja päivityksiä.

Onko hankinnoissa käytettäville tietoturva- ja tietosuojavaatimuksille olemassa helposti käyttöön otettavissa olevia parhaita käytäntöjä? Kyllä on, näitä ovat esimerkiksi EU:n tietosuojadirektiivit ja tietoturvasäädökset, NIST Cybersecurity Framework ja ISO/IEC 27001 ja 27002 ovat tietoturvastandardit.

Lainsäädäntö muuttuu – on hyvä olla etupainotteisesti liikkeellä ja valmistautua

Yritysten ja muiden organisaatioiden on hyvä varautua sääntelyn tiukkenemiseen ja muutoksiin. Tämä on tarpeen, sillä kyberhyökkäykset ovat yhä yleisempiä ja monimutkaisempia. Lainsäädäntö auttaa suojaamaan yksityisiä ja liike-elämän tietoja sekä parantamaan yleistä tietoturvaa ja toimivuutta. Hyvästä tietoturvasta on mahdollista tehdä kilpailuetu.

EU-sääntely kyberturvallisuuden alalla tulee lisääntymään. Helmikuussa 2022 radiolaitedirektiiviä (RED) täydennettiin pakollisilla tietoturvavaatimuksilla. Asetuksessa on valmistajille siirtymäaika, jonka jälkeen 1.8.2024 lähtien markkinoille saatettavien langattomien laitteiden on täytettävä vaatimukset. Kriittisen infrastruktuurin NIS2-kyberturvasäädökset tulevat voimaan 18.10.2024.

Yritysten on hyvä valmistautua EU:n kyberturvallisuussääntelyyn seuraavilla tavoilla vuonna 2023:

- **Tutustuminen säädöksiin ja varautuminen niiden kansalliseen implementointiin:** yritysten tulisi tutustua tuleviin sääntelyihin, kuten RED-direktiiviin ja NIS2-kyberturvasäädöksiin, ja selvittää niiden vaatimukset itselle.
- **Arviointi ja riskien hallinta:** yritysten tulisi arvioida nykyisiä kyberturvatasojaan ja tunnistaa mahdolliset puutteet sääntelyn vaatimusten noudattamisessa.
- **Toimenpiteiden suunnittelu ja toteutus:** yritysten tulisi suunnitella ja toteuttaa tarvittavat toimenpiteet sääntelyvaatimusten noudattamiseksi, esimerkiksi tietoturvaohjelman ja -prosessien päivittäminen.
- **Henkilöstön koulutus ja viestintä:** yritysten henkilöstön tulisi olla tietoinen sääntelystä ja sen vaatimuksista. Henkilöstölle tulisi tarjota tarvittava koulutus ja tiedotus sääntelyn noudattamiseksi.
- **Yhteistyö:** yritysten tulisi yhteistyössä alan toimijoiden ja mahdollisten tukipalvelujen kanssa valmistautua tulevaan sääntelyyn ja noudattaa sitä tehokkaasti.

Miten tuetaan kansalaisten tietoturvataitoja myös tulevaisuudessa?

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. Kyberturvallisuuskeskus tukee kaikille tietoturvan tasoilla olevien kansalaisten kybertaitoja.

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.

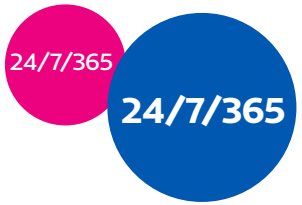
Aktiivisella, avoimella ja säännöllisellä viestinnällä tuetaan luottamuksen säilyttämistä. Sekä hyvistä asioista että myös ongelmista tulee viestiä avoimesti ja läpinäkyvästi.

Digitalisoituneessa yhteiskunnassa on myös kiinnitettävä huomiota osallisuuden toteutumiseen. Miten pidämme kaikki mukana digiyhteiskunnassa? Miten turvaamme eri väestöryhmien osallisuuden ja osallistumisen?

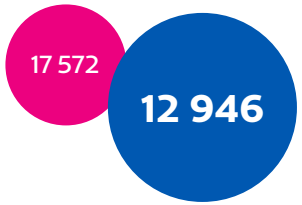
> ” Aktiivisella, avoimella ja säännöllisellä viestinnällä tuetaan luottamuksen säilyttämistä.

Toimintamme tunnuslukuja

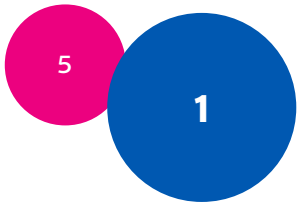
2021 2022



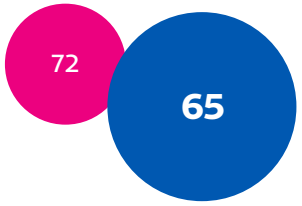
Katkeamaton päivystys



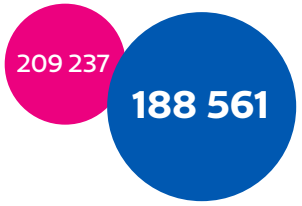
Käsitellyt tapaukset



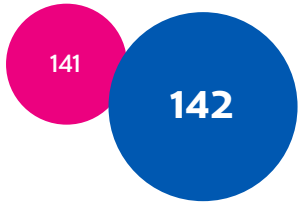
Varoitukset



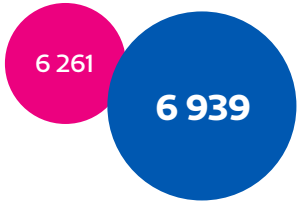
Haavoittuvuuskoordinaation käsittelemät tapaukset



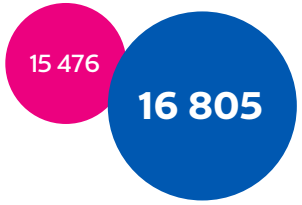
Autoreporter



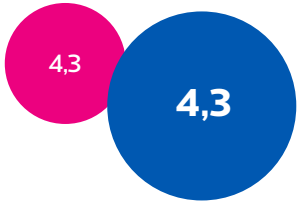
Media-yhteydenotot



Facebook-seuraajat

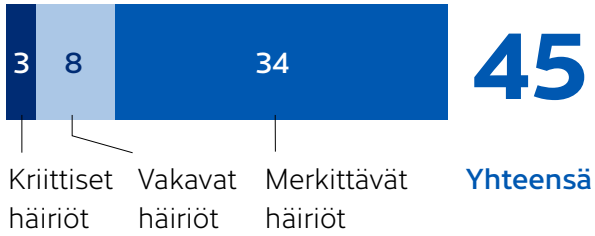


Twitter (nyk. X) -seuraajat



Tilannekuvatuotteiden asiakastyytyväisyys

Häiriömäärät



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

Kyberturvallisuuskeskus.fi

Traficomin julkaisuja 16/2023
ISSN 2669-8757 (verkkojulkaisu)
ISBN 978-952-311-876-8

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus