TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

TIETOTURVAN VUOSI 2019

Kyberturvallisuuskeskuksen vuosikatsaus

Traficomin julkaisuja

5/2020

SISÄLTÖ

Yhteiskunta tarvitsee tietoturvallisia arjen tekoja – yhdessä olemme vahvin lenkki

Vuoden 2019 laajin yhteiskunnallinen keskustelu käytiin 5G-teknologian kyberturvallisuudesta. Olimme valmiita, sillä asiantuntijamme ovat arvioineet uuden teknologian ja standardin tuomia teknisiä haasteita sekä mahdollisuuksia jo vuodesta 2017. Kykymme tuottaa teknistä tietoa kansalliseen riskiarvioon oli kansainvälisestikin arvokasta.

Huippuhetkiimme kuuluivat myös kansainväliset tapahtumamme: maailman ensimmäinen 5G Hackathon sekä Galileo Innovation Challenge. Tapahtumat todistivat, että yhteistyö teleoperaattorien, laitevalmistajien ja viranomaisten välillä on ollut sujuvaa. Yhteistyö on vahvuutemme, josta täytyy pitää kiinni.

Mennyt vuosi tullaan muistamaan myös uusien haavoittuvuuksien nopeasta hyödyntämisestä, laajavaikutteisista kiristyshaittaohjelmista ja käänteestä, jolloin huijauksista ja tietojenkalastuksesta tuli arkeamme - uusi normaali. Takana on myös kyberturvallisuuden sääntelyn supervuosi, kun useat tietoturvallisuutta koskevat lait astuivat voimaan. Muuan muassa TUPAS jäi historiaan ja tunnistus- ja luottamuspalveluiden muutokset toivat kilpailua tunnistuspalveluihin.

Vuoden näkyvimpiä kyberherättelijöitä olivat kuntasektoriin kohdistuneet kyberhyökkäykset. Ne osoittivat yhteiskuntamme haavoittuvuuden ja haittasivat muun muassa kansalaisten peruspalveluita sekä arkea. Tapaukset ja niiden perusteella tehdyt selvitykset ovat herättäneet keskustelua valtionhallinnossa, kunnissa ja yritysmaailman ylimmässä johdossa. On äärimmäisen tärkeää, että asia ei jää keskustelun asteelle, vaan tilanteen parantamiseksi on tehtävä välttämättömiä ja konkreettisia toimenpiteitä sekä päätöksiä.

Vuonna 2019 Suomeen rantautui uusi merkittävä ilmiö "big game hunting", jossa rikolliset havittelevat suuria lunnaita kiristyshaittaohjelmahyökkäyksillä, joiden kohteina ovat suuret yritykset. Hyökkäykset ovat aiheuttaneet yrityksille vakavia toiminnan häiriöitä ja jopa keskeytyksiä sekä mittavia taloudellisia tappioita. Ilmiö on nostanut yritysten johdon agendalle kokonaisvaltaisen, myös toimitusketjut ja kumppanit huomioivan, kyberriskien hallinnan.

Viime vuonna kuluttajalaitteiden turvaamiseksi kehittämämme Tietoturvamerkki sai ilahduttavan laajaa julkisuutta. Merkki tarjoaa ihmisille helpon keinon parantaa henkilökohtaista kyberturvallisuuttaan. Kampanjoimme sosiaalisessa mediassa, TV:ssä ja radiossa ja tavoitimme yli 2,4 miljoonaa kansalaista. Aktiivinen kansalaiskampanjointi sai ihmiset kiinnostumaan tietoturvasta!

Tuleva vuosi tuo uusien haasteiden lisäksi mukanaan positiivista kehitystä. Alkuvuodesta julkaistun yritysten hallituksille suunnatun kyberturvallisuusoppaan aikaansaama kiinnostus on hyvä osoitus halusta tarttua toimeen.

Minulla on ollut ilo aloittaa Kyberturvallisuuskeskuksen johtajana vuoden 2020 alusta alkaen. Aktiivinen toiminta sidosryhmiemme kanssa tarjoaa erinomaisen perustan yhteiskunnan kyberturvallisuuden kehittämiselle myös vuonna 2020.

Helsingissä 19.2.2020,
Kalle Luukkainen
Ylijohtaja
Kyberturvallisuuskeskus
Liikenne- ja Viestintävirasto Traficom

TETOTURVAUHAT JA SUOJAUTUMISKEINOT - TOP 3

Uhat ja ratkaisut yksityishenkilöille

Laadukkaat salasanat, säännölliset tietoturvapäivitykset ja hätiköimätön nettikäyttäytyminen. Lähivuosina yksityishenkilöihin kohdistuvat tietoturvauhat ja -ratkaisut eivät juuri ole muuttuneet. Samoilla periaatteilla suojaat itsesi ja tärkeimmät tietosi nyt sekä tulevina vuosina.

UHAT

Huijausviestit vievät tietosi ja rahasi

Huijausten ja tietojenkalastelun kohteeksi päätyvät kaikki. Huijauksista kärsivät päivittäin niin yritykset, julkishallinto, yhdistykset, rahastot, säätiöt kuin oppilaitoksetkin. Huijaukset voivat olla ilmiselviä tai täysin uskottavia, taitavasti tehtyjä ja kohdennettuja. Huijausten avulla rikolliset yrittävät päästä organisaation tietojärjestelmiin tavoitteenaan esimerkiksi valelaskujen lähettäminen tai liikesalaisuuksien selvittäminen.

Huonot salasanat ja helppo pääsy sähköisiin palveluihin

Käytössämme voi olla jopa satoja verkkopalveluita. Koska monen ainutkertaisen salasanan muistaminen ei ole mahdollista, helposti ajautuu käyttämään samoja yksinkertaisia salasanoja useissa palveluissa. Se nostaa riskejä, kun tietomurron tai -vuodon sattuessa kaikki samalla salasanalla suojatut tilit ovat vaarassa.

Suojaamattomat älylaitteet

Kännykkäsi, äly-tv:si ja tietokoneesi sisältävät varmasti arvokasta tietoa sinusta. Osaatko huolehtia niiden turvallisuudesta ja päivityksistä? Suuri osa tietoturvapäivityksistä sisältää korjauksia, joilla paikataan laitteen tai ohjelmiston turvallisuuspuutteita. Päivittämättömän laitteen käyttö on aina riskialtista. Samalla kutsut tietomurrot kylään.

RATKAISUT

Kaikkia tietoja ei tarvitse antaa

Viranomainen tai palveluntarjoaja ei kysy verkossa käyttäjätunnuksiasi tai pankkitunnuksiasi. Jos tietojasi kysellään yllättäen, voit hyvin kysyä, miksi ja pohtia, onko viesti aito. Älä käytä sinulle tarjottua linkkiä, vaan kirjaudu palveluun palveluntarjoajan sivuilta. Näin voit turvallisesti tarkistaa, tarvitaanko tietojasi tai toimiasi oikeasti.

Suojaa tietosi laadukkailla salasanoilla ja vahvalla tunnistautumisella

Hyvä salasana on vähintäänkin pitkä. Käytä yhtä salasanaa vain yhdessä palvelussa. Ota käyttöösi salasanojen hallintaohjelma. Se muistaa salasanat puolestasi. Ryhdy myös 2-vaiheisen tunnistautumisen ja vahvan sähköisen tunnistamisen käyttäjäksi aina, kun siihen on mahdollisuus. Näin turvaat esimerkiksi pankki- ja sometilisi paremmin.

Päivitykset ja tuoteturvallisuus kuntoon

Päivittämällä laitteesi ja pitämällä ne ajan tasalla suojaat ne myös tietoturvauhkilta. Kun otat automaattiset päivitykset käyttöön, sinun ei tarvitse muistaa niitä itse. Laitteesi hoitaa ne itsenäisesti ja säännöllisesti.

Oletko hankkimassa uutta älylaitetta?
Tietoturvamerkkimme kertoo laitteen turvallisuudesta.

Uhat ja ratkaisut organisaatioille

Organisaatiossa hallittu kyberturvallisuus näkyy riskienhallinnassa, varautumisessa ja henkilöstön koulutuksessa. Kokonaisuus on monen eri osa-alueen hallitsemista, siksi kyberturvallisuuden tulisi olla koko työyhteisön toimintatapa.

UHAT

Päivittäinen tietojenkalastelu ja huijaukset

Huijausten ja tietojenkalastelun kohteina ovat päivittäin yritykset, julkishallinto, yhdistykset, rahastot, säätiöt ja oppilaitokset. Ne voivat olla ilmiselviä tai täysin uskottavia, taitavasti tehtyjä ja kohdennettuja. Huijausten avulla rikolliset yrittävät päästä organisaation tietojärjestelmiin tavoitteenaan esimerkiksi valelaskujen lähettäminen tai liikesalaisuuksien selvittäminen.

Uusien haavoittuvuuksien nopea hyödyntäminen - perinteiset torjuntakeinot eivät enää riitä

Rikolliset hyödyntävät hyökkäyksissään julki tulleita haavoittuvuuksia lähes välittömästi. Organisaatioiden onkin varauduttava päivittämään tietojärjestelmiään ja sovelluksiaan yhä nopeammin. Tämä koskee etenkin huipputeknologian ja innovaatioiden parissa työskenteleviä organisaatioita, jotka ovat sekä rikollisten että teollisuusvakoilijoiden erityisen tarkkailun kohteita. Tunnetteko tietoympäristönne ja käytössänne olevat sovellukset ja järjestelmät? Ilman tätä tietoa, tietoympäristöönne kohdistuvia hyökkäyksiä ei voi esimerkiksi tietoturvapäivityksin torjua.

Palveluja keskitetään ja ulkoistetaan ilman suunnittelua ja vastuuttamista

Keskeisten palvelujen ulkoistaminen tai palvelujen tarjoaminen yhteistyökumppaneille lisää kyberhyökkäyksen riskiä. Rikolliset hyödyntävät kumppaneita tai alihankkijoita pyrkiessään sisään varsinaisen kohteensa tietojärjestelmiin muun muassa varastamalla kumppanille luovutettuja käyttöoikeuksia. Erilaiset häiriötilanteet voivat levitä laajalle ja yllättäviinkin paikkoihin, jos omien palveluiden keskitystä tai ulkoistusta ei ole suunniteltu kunnolla.

RATKAISUT

Juurruta kyberturvallisuus riskienhallintaanne

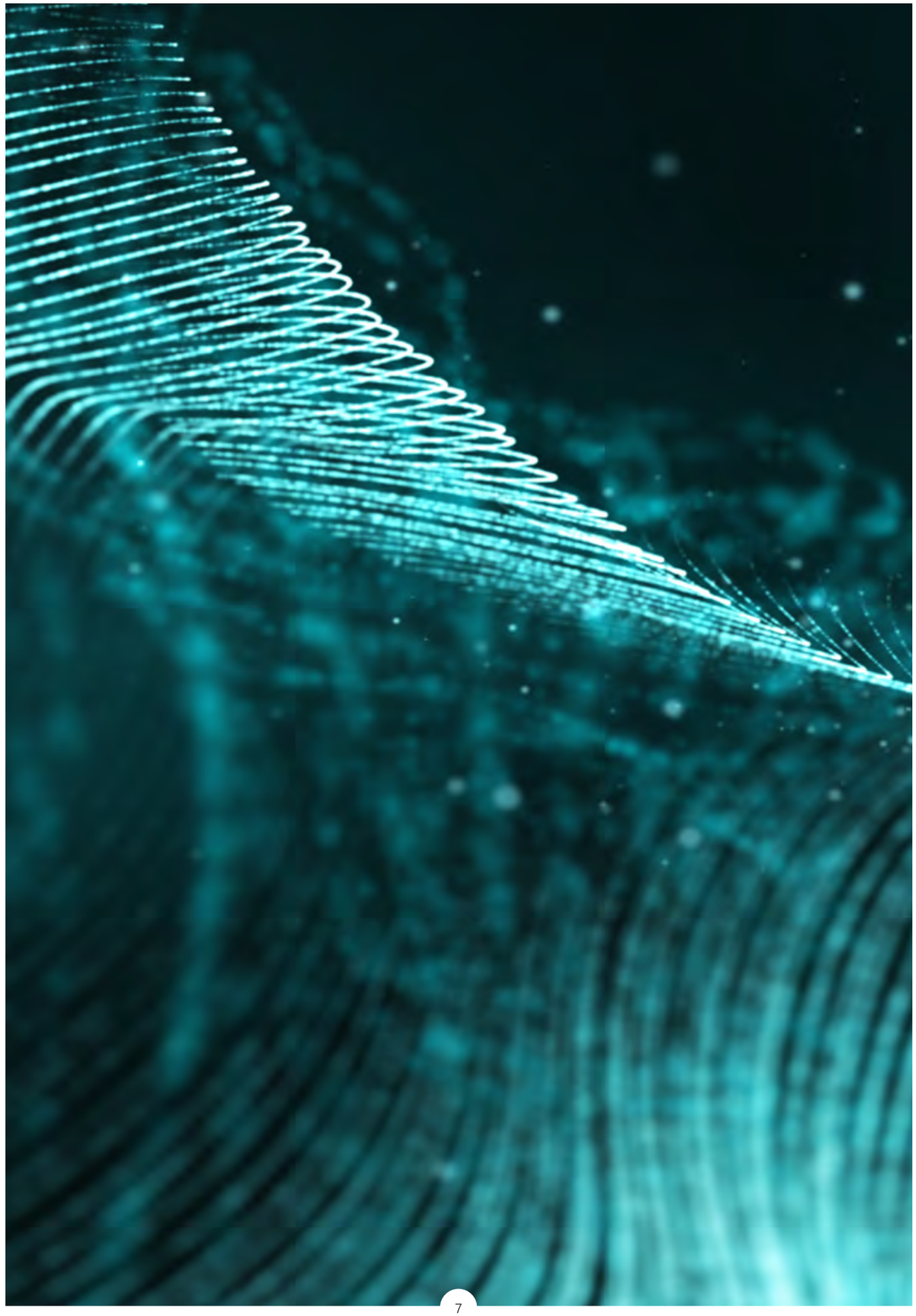
Kyberturvallisuuden riskit on otettava huomioon. Riskeihin pätevät samat mekanismit kuin perinteisempiin riskeihin: riski voidaan poistaa esimerkiksi ottamalla palvelu pois käytöstä tai sen todennäköisyyttä voidaan pienentää vahvaa tunnistautumista käyttämällä. Jäljelle jäänyt jäännösriski voidaan hyväksyä, kun se on sellaisella tasolla, jonka organisaation johto voi hyväksyä.

Harjoittele häiriö- ja poikkeamatilanteissa toimimista

Kuinka toimitte, jos verkkorikollinen on päässyt murtautumaan sähköpostiinne ja lähettää nimissänne huijauslaskuja? Kouluttautumalla ja erilaisia kyberhäiriötilanteita harjoittelemalla selvitätte parhaat käytännöt. Usein tämä on myös edullisin tapa havaita puutteita. Jos tunnette oman tietoympäristönne ja olette harjoitelleet esimerkiksi järjestelmien päivittämis- ja varmuuskopiointirutiinit, tulette selviytymään paremmin niin harjoituksissa kuin myös oikeissa kriiseissä.

Vastuuta toimittajat ja selvitä palveluidenne liitännäisyydet

Toimittajien vastuut, poikkeamatilanteissa toiminta ja palveluidenne liitännäisyydet pitää tietää, ennen kuin niitä ulkoistetaan. Sopikaa toimintamalleista ja vastuista kumppaneidenne sekä kolmansien osa-puolten kanssa jo sopimusneuvotteluissa. Näin tiedätte roolinne, vastuunne ja toistenne toimintatavat esimerkiksi häiriötilanteen kohdatessa.



Vuoden 2019 merkittävät kybertapahtumat

POSITIIVISIA SAAVUTUKSIA

- **Uusien teknologioiden turvallisuutta rakennetaan:**
  - 5G Hackathon
  - Galileo Innovation Challenge
- **KYBER 2020 -hankkeen vaikutukset:**
  - Kyberturvallisuuden harjoittelu lisääntynyt organisaatioissa - Harjoitusohjeestamme harjoittelun perusteet haltuun.
- **Kansalaisten tietoturvatietoisuus ja -taidot parempaan kuntoon:**
  - Tietoturvamerkki
  - Turvalistit
  - Turvallisesti netissä -oppaat lapsille ja vanhemmille
  - Spoofy - lasten oma tietoturvapeli
- **Kriittisen infrastruktuurin kyberturvallisuus kehittyy:**
  - Kyberturvallisuuden tason arviointiin Kybermittari
  - HAVARO-palvelu
  - DNSSEC

MIELENKIINTOISIA ILMIÖITÄ

- **Haittaohjelma QSnatch**
- **Peilaavat palvelunestohyökkäykset**
- **Onnistuneet vaalit ja EU-puheenjohtajuuskausi**

HUOLESTUIMME

- **Uusi normaali: Office 365 -tietomurrot ja tietojenkalastelu**
- **Big game hunting - suurta saalista metsästävät verkkorikolliset**
- **Kuntien kyberturvallisuus**

MUUTOKSIA TIETOTURVAVAATIMUKSISSA

- **TUPAS historiaan**
- **Kilpailua tunnistuspalvelumarkkinoille**
- **Tukea pilvipalvelujen hankintaan kriteeristöstämme**

Verkkojen toimivuus

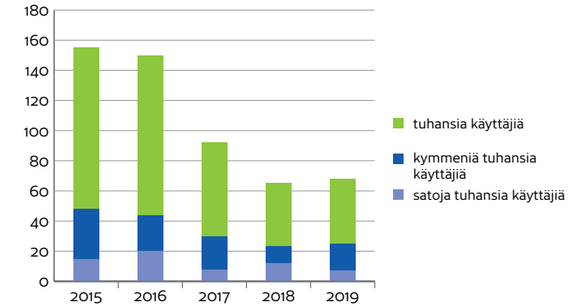
Myrskytuulet ja salamat katkoivat puheluja ja internetyhteyksiä

Vuoden 2019 pitkäkestoisimmat häiriöt saivat alkunsa sääolosuhteista. Tammikuussa Aapeli-myrsky katkoi sähköjä ja aiheutti useita pitkäkestoisia toimivuushäiriöitä. Kesäkuussa salamoinnin synnyttämät virtapiikit rikkoivat useita viestintäverkon voimalaitejärjestelmiä ja saivat aikaan muutamia merkittäviä toimivuushäiriöitä. Salaman aiheuttamia voimalaitejärjestelmien vikoja ei voida täysin välttää, mutta usein viestintäverkon komponenttien ylijännitteeltä suojaaminen estää laiterikot.

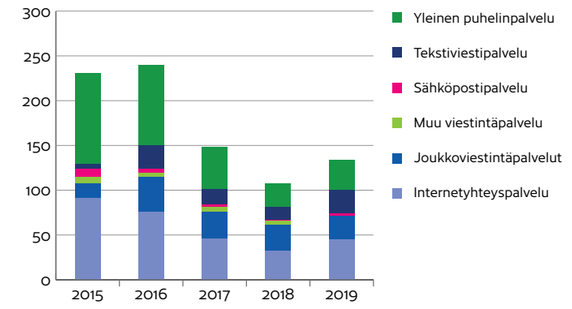
Kotimaisissa viestintäpalveluissa vakavimpien häiriöiden määrä on puolittunut vuodesta 2018. Erityisesti ovat vähentyneet antenni-TV-verkon laajat ja vakavat viat. Sen sijaan häiriöt, jotka vaikuttivat noin 1000 - 10 000 viestintäpalvelujen käyttäjään, hieman lisääntyivät vuoteen 2018 verrattuna. Suurimmat häiriöt syntyivät erilaisista laite- ja ohjelmistovioista sekä sähkökatkoista. Kuitenkin merkittävien häiriöiden kokonaismäärä on selvästi vähentynyt vuosista 2015 ja 2016.

Arviomme mukaan merkittävien toimivuushäiriöiden vuosittainen määrä on laskenut ainakin seuraavista syistä:

- yleisten viestintäverkkojen suuret muutostyöt ovat vähentyneet
- muutostöillä teleyritykset ovat saaneet aikaan paremmin hallittavat ja rakenteeltaan vikasietoisemmat verkot ja palvelut
- keskeisiä tietoliikennekaapeleita katkeaa kaivuutöissä entistä harvemmin
- teleyritysten ja sähköverkkoyhtiöiden yhteistyö on parantunut.



Merkittävät häiriöt viestintäpalvelujen käyttäjämäärien mukaisesti vuosina 2015–2019



Merkittävät häiriöt viestintäpalveluittain vuosina 2015–2019. Yksi häiriö voi vaikuttaa kerralla useampaan viestintäpalveluun.

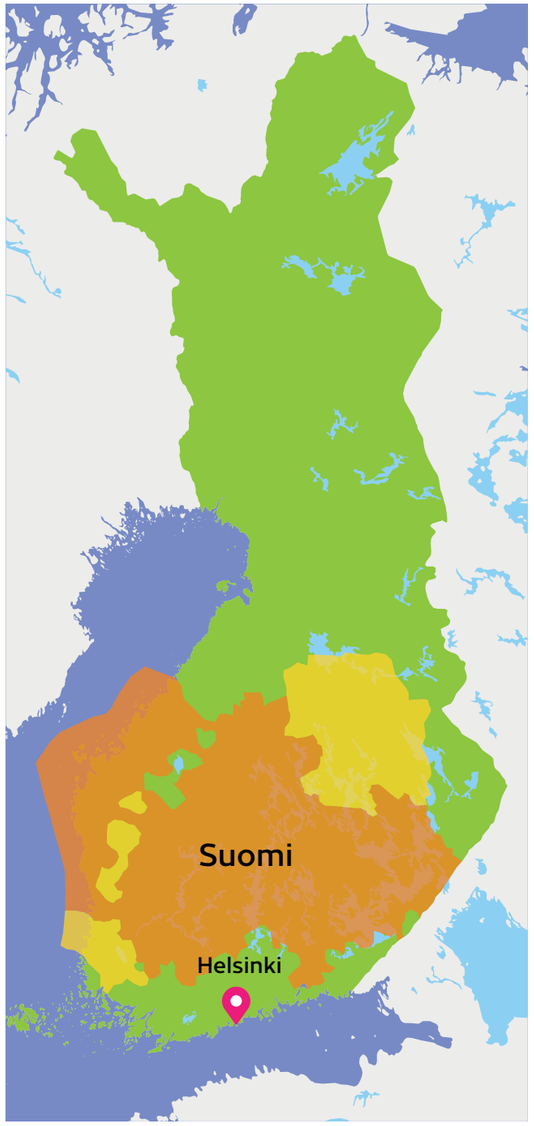
Aapelin ennätykselliset tuulet katkoivat sähköt 120 000 asiakkaalta

Aapeli-myrsky vaikutti 1.-2.1.2019 voimakkaimmin Pohjanmaan ja Ahvenanmaan maakuntiin. Kova tuuli kaatoi paljon puita, jotka sähkölinjojen päälle kaatuessaan katkaisivat sähköjä matkaviestinverkkoja toiminnassa pitäviltä laitteilta. Merkittäviä matkaviestintäpalveluiden häiriöitä oli yli kolmasosassa Suomea. Myös viranomaisradioverkko VIRVE kärsi häiriöistä. Kiinteille puhelinverkoille ja TV:lle myrsky ei aiheuttanut merkittäviä häiriöitä.

Ahvenanmaalla Ålands radion radioasemalta sähköt katkesivat pariksi tunniksi. Uutistietojen mukaan myös hätäliikenne oli poikki lähes vuorokauden ajan. Manner-Suomessa matkaviestintäpalveluissa saattoi olla paikallisia päällekkäisiä katveita, siksi hätäpuheluita ei paikoittain ollut mahdollista soittaa matkapuhelimella. Hätäkeskuslaitoksen mukaan saapuneiden hätäpuheluiden määrä oli kuitenkin odotetun suuri, joten mahdolliset katvealueet olivat olleet pieniä.

Matkaviestintäpalveluiden häiriöt olivat laajimmillaan keskiviikkoaamuna 2.1.2019. Manner-Suomessa merkittävät häiriöt saatiin korjattua 3.1. mennessä. Ahvenanmaan yleisten viestintäpalveluiden tilanne jäi epäselväksi. Lehtitietojen mukaan merkittäviä häiriöitä esiintyi vielä 4.1.

Aapelin vuoksi sähköt olivat poikki noin 120 000 taloudelta tai asiakkaalta. Vertailun vuoksi Rauli (2018) ja Seija (2013) -myrskyissä sähköt katkesivat noin 200 000 asiakkaalta. Ennätyksellisen kovista tuulista huolimatta Aapelin vaikutus jäi aiempia vuosia vähäisemmäksi. Kehityksestä voimme kiittää tele- ja sähköyhtiöitten sekä viranomaisten toimivaa yhteistyötä, joka on sujuvoitunut vuosi vuodelta. Myrskykokemuksista ja yhteistyön hyödyistä on otettu opiksi.



Näkymä Traficomin julkisesta MONITORi-palvelusta 2.1.2019 kello 10.31. Eri teleyritysten häiriöalueet on merkitty keltaisen eri sävyillä. Kahden teleyrityksen palvelut ovat heikentyneet merkittävästi.

Muiden ICT-palveluiden toimintavarmuus

Niin julkishallinnon kuin yritystenkin ICT-palveluiden huomattavia häiriöitä on värittänyt se, että vaikka toimintavarmuutta parantavia toimenpiteitä on suunniteltu, suunnitelmat eivät ole toimineet käytännössä.

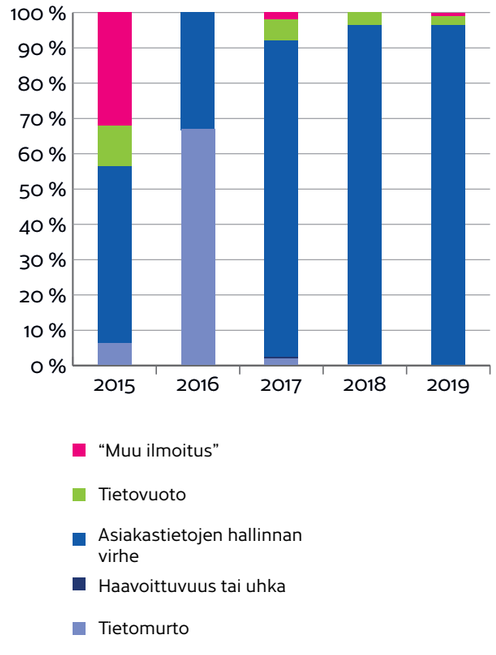
Etenkin terveydenhuollossa häiriöillä on merkittäviä vaikutuksia, vaikka asiakkaita onkin varauduttu hoitamaan ilman tietoliikenneyhteyksiä. ICT-häiriöt hidastavat terveydenhuollon toimintaa ja palvelukykyä esimerkiksi hoitotilanteissa, joissa potilastietoihin ei päästä käsiksi.

Teleyritysten tietoturvaloukkausilmoitusten määrä on vakiintunut

Virastollemme ilmoitettujen tietoturvaloukkauksien määrä on viime vuosien voimakkaan kasvun jälkeen pysähtynyt ja jopa laskenut hieman vuoden 2018 tasosta.

Tietoturvaloukkausilmoitukset liittyvät tapauksiin, joissa henkilötiedot tuhoutuvat, häviävät, muuttuvat tai niitä luovutetaan eteenpäin vahingossa tai luvattomasti. Tyypillisin ilmoitus liittyy henkilötietojen käsittelyssä tapahtuneeseen virheeseen, jossa yksittäisen asiakkaan henkilötiedot päätyvät tai paljastuvat väärälle henkilölle.

Tässä kuvattuna teleyritysten ilmoitukset henkilötietojen loukkauksista ja niiden kehityksestä vuosina 2015 - 2019.



Heinäkuu 2019

10.7 Potilastietojärjestelmä Apotti oli poissa käytöstä Kemin kaupungin sisäverkon tietoliikennekytkimen vian vuoksi.

11.–18.7. Eurooppalainen satelliittipaikannusjärjestelmä Galileo ei toiminut viikkoon. Syynä olivat viat järjestelmän molemmissa maa-asemissa, minkä vuoksi satelliittien tarkkoja sijainteja kiertoradoillaan ei saatu laskettua.

Syyskuu 2019

Syyskuussa vanha hätäkeskusjärjestelmä ELS palautettiin käyttöön viikoksi, jotta Erica-järjestelmän käytettävyys saatiin varmistettua. Erica on toistuvasti kärsinyt valtion turvallisuusverkko TUVE:n verkkoliikennehäiriöistä.

27.9. Potilastietojärjestelmä Apotti poissa käytöstä Vantaalla tietoliikennekuidun katkettua.

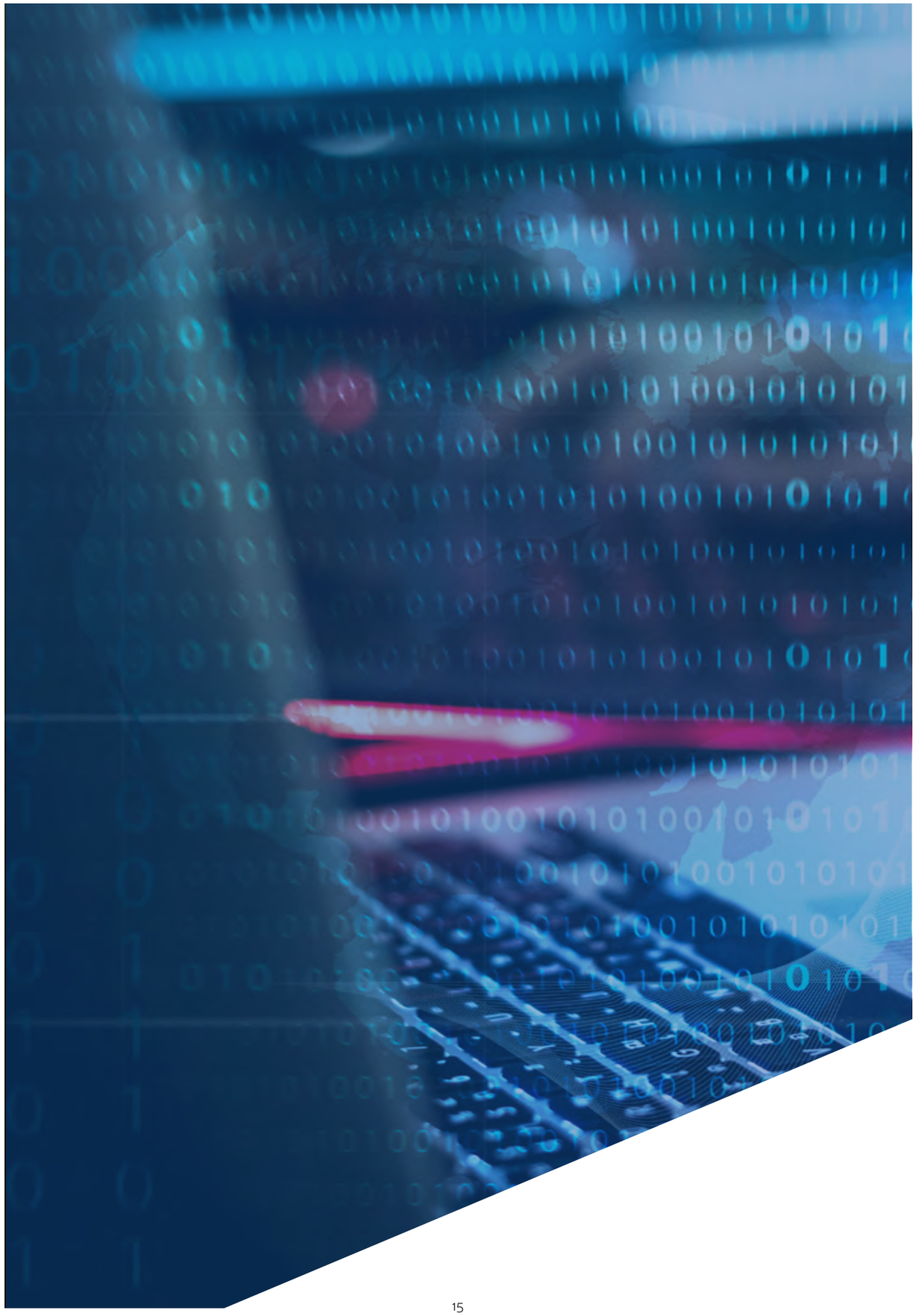
Lokakuu 2019

Julkishallinnon ICT-palveluissa oli lokakuun aikana useita häiriöitä:

10.–18.10. Väestörekisterikeskuksen VTJ-rajapinnassa esiintyneet häiriöt haittasivat useiden viranomaisten työtä.

13.–14.10. Valtorin ylläpitämän VY-verkon häiriöt estivät useiden valtion viranomaisten verkkosivujen ja sähköisten asiointipalveluiden toimintaa.

14.10. Nesteen tietojärjestelmissä esiintynyt toimivuushäiriö laski hetkellisesti yhtiön osakkeen arvoa. Häiriö johtui laiteviasta Nesteen käyttämän ICT-palveluntarjoajan datakeskuksessa.



Palvelunestohyökkäykset: usein motiivina häirintä tai rahan kiristäminen

Erityisesti kotimaisten yritysten varautuminen palvelunestohyökkäyksiin on parantunut. Hyökkäysliikennettä näkyi teleyritysten verkoissa edellisvuotta enemmän, mutta meille ilmoitettujen hyökkäysten vaikutukset jäivät vähäisemmiksi.

Määrällisesti lyhyet hyökkäykset ovat hyvin yleisiä. Vuonna 2019 noin 80 % kaikista Suomessa nähdyistä hyökkäyksistä oli kestoltaan alle 15 minuuttia. Hyökkäysten kohteet vaihtelevat, mutta yksi kohde, joka korostuu vuodesta toiseen, on koulujen Wilma-järjestelmä. Lyhyiden hyökkäysten takana voi olla nuoria, jotka kokeilevat palvelunestohyökkäysten tekemistä ja sen vaikutuksia. Palvelunestohyökkäyksen tekeminen tai sen yrittäminen voidaan tulkita rikokseksi, josta voi seurata tekijälle sakkoa tai enintään kaksi vuotta vankeutta.

Hyökkäysten tekeminen on teknisesti helppoa, koska internetissä on tarjolla niin kutsuttuja stresser-palveluita, joista hyökkäyksiä voi ostaa palveluna ilman omaa teknistä osaamista. Useat hyökkäyksiä myyvät sivustot tarjoavat lyhyitä näytehyökkäyksiä ilmaiseksi.

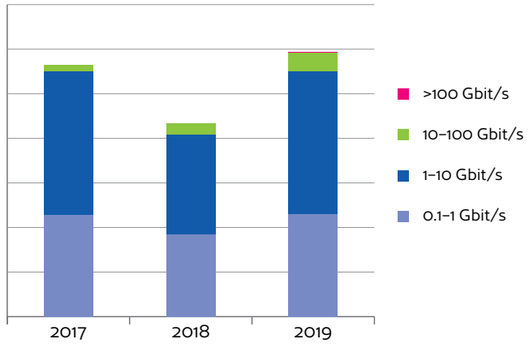
PALVELUNESTOHYÖKKÄYSTEN SYYT

1. Häirintä
2. Rahallisen hyödyn tavoittelu hyökkäyksellä uhkailemalla
3. Halu ja kiinnostus kokeilla hyökkäyksen vaikutuksia

Organisaatiot suojautuvat aiempaa paremmin, silti häiriöiltä ei ole vältytty

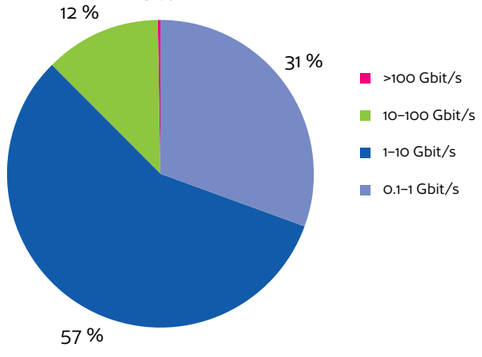
Etenkin suuret suomalaiset organisaatiot ovat varautuneet palvelunestohyökkäyksiin aiempia vuosia paremmin. Esimerkiksi pakettipesuripalveluiden ja pilvipalveluiden käyttöönotto on johtanut siihen, että hyökkäykset onnistutaan usein torjumaan ilman merkittäviä vaikutuksia palveluiden toimintaan.

Silti palveluissa nähdään välillä häiriöitä hankituista suojauksista huolimatta. Yleensä häiriöt johtuvat hyökkäysliikenteestä, joka ehtii kaataa palveluita ennen kuin torjuntatoimet aktivoituvat. Monissa tapauksissa esimerkiksi kohteen palomuuri on ylikuormittunut, eikä enää automaattisesti palaudu normaalitilaan edes sen jälkeen, kun varsinaista hyökkäysliikennettä ei enää saavu kohteeseen. Oman organisaation palveluiden kykyä sietää hyökkäysliikennettä kannattaa testata, jolloin palvelussa olevat mahdolliset pullonkaulat tai muut heikot kohdat voi löytää hallitusti. Tästä hyvänä esimerkkinä on LähiTapiolan tekemä harjoitus, josta **Leo Niemelä** kertoo vieraskynässä.



Palvelunestohyökkäysten volyymien kehitys Suomessa. Lähde: Telia

Palvelunestohyökkäysten määrä on lukumääräisesti kasvanut edellisvuodesta. Eniten kasvua on ollut yli 1 Gbit/s ja yli 10 Gbit/s hyökkäyksissä.



Palvelunestohyökkäysten volyymien jakauma Suomessa 2019. Lähde: Telia

Noin 69 % kaikista hyökkäyksistä on volyymiltaan yli 1 Gbit/s ja 12 % yli 10 Gbit/s. Suomessa nähdään volyymiltaan yli 10 Gbit/s hyökkäyksiä ja lukuisia pienempiä päivittäin.

”DDoS-harjoitus on myrkkyä palvelunestohyökkääjille

LähiTapiolassa olemme pyrkineet jo vuosien ajan kehittämään tietoturvaamme ennakoluulottomalla otteella. Toimintatapoihimme on vakiintunut muun muassa yhteistyö valkohattuhakkereiden kanssa, bug bounty -palkkio-ohjelma ja avoin viestintä tietoturvasta. Tänä vuonna pääsimme toteuttamaan palvelunestohyökkäyksen omiin verkkopalveluihimme.

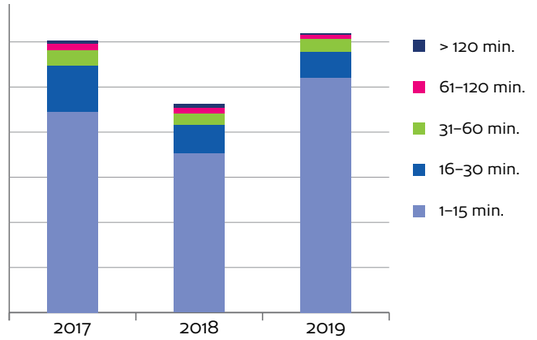
Hyökkäsimme omiin verkkopalveluihimme tammikuussa 2019 käyttäen samoja työkaluja kuin verkkorikolliset. Kuormitimme verkkopalveluitamme nörttisydämemme kyllyydestä: satoja hyökkäyskoneita oli viritetty globaalisti tarkoituksenaan kaataa LähiTapiolan verkkopalvelut. Tarkoituksenamme oli hakea kyvykkyyttä torjua palvelunestohyökkäyksiä sekä oppia miten LähiTapiolan infrastruktuuri kestää kuormitusta, joka poikkeaa normaalista verkkokäyttäytymisestä.

Harjoitus vaati todella paljon ennakkosuunnittelua tietoliikenteen, infran, palvelinten, sovelluksien ja tietokantojen osalta. Jouduimme arvaamaan suurimman osan riskeistä ja hyväksymään sen, ettei kaikkia harjoituksesta aiheutuneita riskejä voi ennustaa. Valmistelu, suunnittelu, tiedottaminen ja itse harjoituksen toteutus vaativat kuukausien suunnittelun, johdolta rohkeutta ja – mikä tärkeintä – harjoituksen näkemisen investointina tulevaisuuteen.

Palvelunestohyökkäyksien torjuntapalvelut ovat myrkkyä hyökkääjille. Torjuntapalvelut vaativat kuitenkin toimiakseen todella tarkkaa optimointia sekä konfigurointia, jotta pienikin palveluita hidastava hyökkäysliikenne havaitaan ja voidaan estää normaalista tietoliikenteestä. Me opimme, että useat palvelut kaatuvat yllättävänkin pienellä liikennemäärällä.

Kannustan yrityksiä toteuttamaan käytännön harjoituksia, koska ne auttavat mitoittamaan puolustustoimet oikealle tasolle ja ymmärtämään konkreettisesti ne riskialueet, joihin organisaation tulee kiinnittää erityistä huomiota.

Leo Niemelä
LähiTapiola



Palvelunestohyökkäysten kestojen kehitys Suomessa. Lähde: Telia

Hyökkäysten kestoajoissa alle 15 minuutin hyökkäysten lukumäärä on kasvanut edellisvuodesta. Lyhyet alle 15 minuutin hyökkäykset ovat todennäköisesti stresser-palveluiden ilmaisia näytehyökkäyksiä.

Hyökkäysten kestoon vaikuttavat eniten toteutetut torjuntatoimet, koska yleensä rikolliset jatkavat hyökkäystään, kunnes sillä on näkyviä vaikutuksia kohteen toimintaan.

PALVELUNESTOHYÖKKÄYSTEN TEKNIIKKA VUONNA 2019

Aiempien vuosien tapaan valtaosa palvelunestohyökkäysten volyymistä muodostui niin sanotuista UDP (User Datagram Protocol) -amplifikaatiohyökkäyksistä, esimerkiksi aika- tai nimipalveluita hyödyntäen. Amplifikaatiossa käytetään avoimia palvelimia ympäri maailmaa, joista liikenne peilataan vahvistettuna hyökkäyksen kohteeseen. Myös sovellustason hyökkäyksiä nähtiin säännöllisesti.

Nousevana trendinä, etenkin vuoden loppupuolella, teimme havaintoja TCP (Transmission Control Protocol) -kättelyliikenteen peilaamisesta hyökkäyksen kohteena olevan organisaation verkkoon. Pakettimäärät olivat niin suuria, että ne aiheuttivat häiriöitä myös suomalaisille peilauksessa käytetyille palvelimille, vaikka ne eivät olleet hyökkäyksen kohde. Näiden hyökkäyksen torjuminen on myös ollut haastavaa, koska hyökkääjät pommittivat lukuisia kohteen verkko-osoitetta samanaikaisesti.

Vakoilu ja vaikuttaminen

Vuoden 2019 aikana valtiollisen kybervakoilun kehityssuunnat pysyivät pääosin samoina kuin aiempina vuosina. Myös suomalaiset yritykset ja julkishallinnon organisaatiot ovat edelleen kybervakoilun kohteena sekä poliittisista että taloudellisista syistä.

Maailmalla on jo aiemmin nähty, kuinka kohdistetuilla kyberoperaatioilla on saatu pahimmillaan aikaan merkittäviä vaikutuksia. Myös Suomen kriittiseen infrastruktuuriin kohdistuvasta mielenkiinnosta on nähty viitteitä. Organisaatioiden järjestelmistä etsitään heikkoja kohtia ja samalla jalansijaa niihin. Pääsyä järjestelmiin voidaan havitella myös kohdistetulla tunnustenkalastelulla.

Kybervakoilu apuna taloudellisen aseman parantamisessa

Vuoden aikana pinnalla oli jälleen teollisuusvakoilu, jossa pyrkimyksenä on varastaa yritysten tietopääomaa. Liiketoiminnalle merkityksellisiä tietoja varastamalla tavoitellaan taloudellista etumatkaa esimerkiksi hyötymällä muiden tekemästä kehitys- ja tutkimustyöstä. Vakoilun kohteelle se voi tarkoittaa esimerkiksi heikentynyttä myyntiä tai markkina-asemaa, kun vakoilun edesauttamana halvemmalla tuotetut kilpailevat tuotteet tai palvelut valtaavat markkinoita.

Valtiot voivat yrittää parantaa taloudellista asemaansa tai saavuttaa muita kansallisia tavoitteittaan yhtäaikaisesti kybervakoilun ja investointien tai muun taloudellisen vaikuttamisen keinoin. Esimerkiksi vuonna 2019 Kiinaan kohdistui useita syytöksiä ilmailuteollisuuden vakoilusta ja teknologian kopioimisesta maan oman lentokonetuotannon käynnistämiseksi.

Menetelmiä kehitetään vaikeasti havaittaviksi

Erilaisten julkisten palvelujen hyödyntäminen kybervakoilussa yleistyi selvästi. Jos hyökkääjä lisää omaa sisältöään, muun muassa piilotettuja käskyjä, esimerkiksi kuva-, video- tai pilvipalveluihin, sitä on hankala havaita tavanomaisilla verkkoliikenteen havainnointimenetelmillä.

Muun muassa näiden menetelmien yleistyessä päälaitteilla tapahtuvan havainnoinnin merkitys korostuu. Ratkaisujen käyttöönotto on kuitenkin ollut hidasta, vaikka tarjolla on sekä kaupallisia että maksuttomia ratkaisuja.

Toimitusketjuhyökkäys voi olla huomaamaton

Varsinaisen kohteen saavuttaminen toimitusketjuja hyödyntämällä on edelleen ajankohtainen uhka. Murtautuminen tai tietoihin käsiksi pääseminen voidaan toteuttaa esimerkiksi tunkeutumalla IT-palveluntarjoajan tai laitetoimittajan järjestelmiin.

Menneen vuoden aikana esiin nousivat myös yritysten ja organisaatioiden strategisten kumppanien hyödyntäminen vastaavalla tavalla. Riippuvuussuhteet tällaisiin yrityksiin ovat tiiviimmät, eikä kumppanuuksia voi helposti korvata.

Osana kohdistettuja hyökkäyksiä hyödynnettiin myös digitaalisen infrastruktuurin ja verkon toiminnalle keskeisiä palveluja, muun muassa nimipalveluja. Lisäksi tietoturvaratkaisujen luotettavuus oli vaakalaudalla, kun turvallisen verkkoyhdyskäytävän luomiseen käytettyihin Virtual Private Network (VPN) -palveluihin ja -ratkaisuihin yritettiin murtautua.

Tunkeutumisväylänä organisaation hallinnoimiin laitteisiin tai järjestelmiin voidaan pyrkiä käyttämään myös henkilöiden yksityisiä laitteita.

Kohteina myös toimittajat, tutkijat ja toisinajattelijat

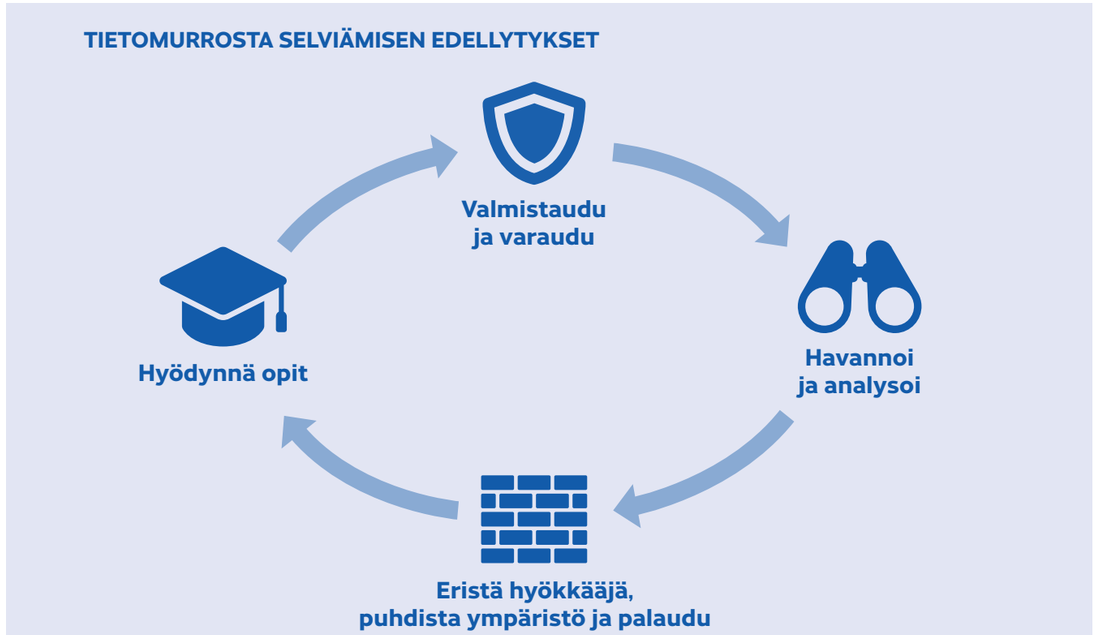
Kuluneen vuoden aikana myös yksittäisiä henkilöitä, kansanryhmiä ja tutkijoita vakoiltiin. Useissa uutisissa kerrottiin esimerkiksi Kiinan pyrkimyksistä seurata uiguurivähemmistöään.

Lisäksi valtiot voivat pyrkiä vakoilemaan tai seuraamaan myös ulkomailla asuvia kansalaisiaan, toisinajattelijoita ja aktivisteja tai näihin liittyvien asioiden parissa työskenteleviä toimittajia tai tutkijoita. Tällaisilla pyrkimyksillä voi olla vaikutuksia myös Suomessa asuviin ihmisiin tai toimiviin organisaatioihin.

Varautumistaso vaihtelee

Suomessa osa organisaatioista on varautunut vakoilun uhkaan selvästi paremmin osa taas heikommin. Varautumistarve ei myöskään koske vain kotimaan maaperällä toimimista, vaan länsimaisiin yrityksiin voidaan joskus kohdistaa poliittisista syistä vaikuttamista myös kybervakoilun keinoin.

Teknisten ratkaisujen lisäksi varautumista tulee kehittää tietoisuutta lisäämällä. Vakoilun kohteeksi päätyvät hyvin erilaiset organisaatiot oman toimintansa, hallussa pitämänsä tiedon tai toimitusketjuun liittyvän asemansa vuoksi.



1 Organisaatioosi on lähetetty kaksi kuukautta sitten kohdistettuja kalasteluviestejä. Saat tiedon lähettäjäosoitteesta.

- Pystytkö näillä tiedoilla löytämään viestin ja selvittämään, keille se on lähetetty?
- Saatko selville, onko viesti avattu ja onko käyttäjä klikannut viestissä ollutta linkkiä?

2 Saat tiedon organisaatiostasi lähtevästä haittaohjelman komentopalvelinliikenteestä. Ilmoittaja kertoo sinulle aikaleiman ja komentopalvelimen verkkotunnuksen.

- Pystytkö tunnistamaan, mistä laitteesta liikenne on peräisin?
- Saatko selville, mikä ohjelma tai prosessi liikenteen aiheutti?
- Miten varmistat, että mahdollista todistusaineistoa ei katoa tai tuhoudu poikkeamanhallintaprosessin aikana?

3 Yritämme tavoittaa organisaatiostanne tietoturvasta vastaavaa henkilöä mahdollisen valtiolliseen toimintaan liittyvän havainnon selvittämiseksi.

- Onko organisaatiossanne määritelty vastuut tietoturva-asioissa?
- Onko tietoturvavastaavanne yhteystiedot asiantuntijamme löydettävissä tai saako häneen muutoin yhteyden?
- Tiedätkö, mistä saat apua asian jatkoselvittämisessä?

Haittaohjelmat ja haavoittuvuudet

Vuosi 2019 muistetaan nopeista uusien haavoittuvuuksien hyödyntämisestä. Aika haavoittuvuuden julkaisusta sen hyväksikäyttöön lyheni huomattavasti aiempaan verrattuna. Organisaatioiden pitäisikin varautua tietoturvaprosesseissaan erityisesti kriittisten päivitysten nopeaan asentamiseen tai muiden torjuntakeinojen nopeaan käyttöönottoon. Erityisesti internetiin avoimet järjestelmät on syytä pitää jatkuvasti ajantasaisina. Kriittiset päivitykset tai muut rajoittamiskeinot tulisi ottaa käyttöön heti, eikä esimerkiksi vasta seuraavassa huoltokatkossa.

Exim-haavoittuvuutta hyödynnettiin tietomurroissa hurjan nopeasti

Exim-sähköpostipalvelinohjelmistosta julkaistiin etäkäytön mahdolliseksi tekevä haavoittuvuus torstaina 6.6.2019. Heti seuraavana viikonloppuna myös Suomessa toteutettiin lukuisia tietomurtoja haavoittuvuuden avulla. Tästä syystä annoimme varoituksen Exim-haavoittuvuuden hyväksikäytöstä maanantaina 10.6.

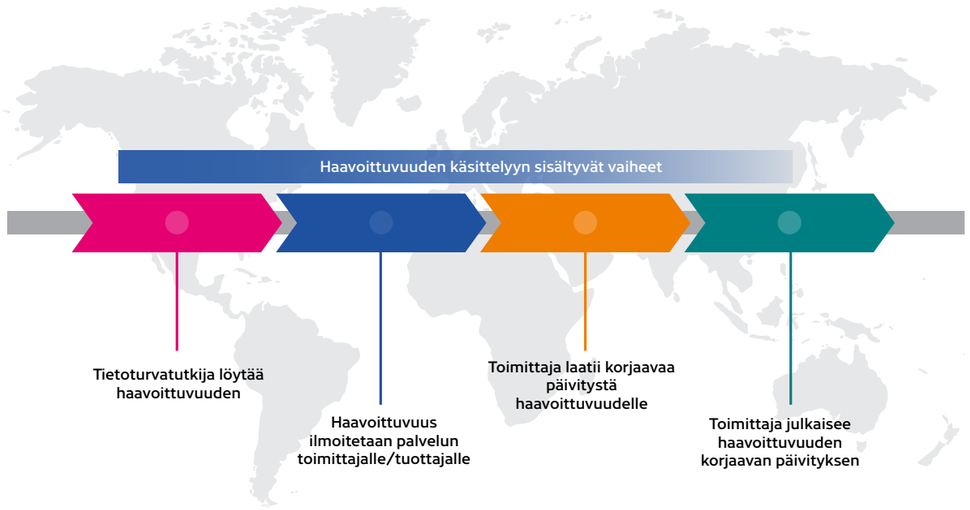
Haavoittuvuuden massamainen hyväksikäyttö ei välttämättä ala heti. Esimerkiksi Microsoft Windowsin RDP-etähallintapalvelun luvattomaan etäkäyttöön liittyvä niin sanottu BlueKeep-haavoittuvuus julkaistiin toukokuussa 2019. Kesti useita kuukausia ennen kuin haavoittuvuudesta oli saatavilla julkinen hyödyntämismenetelmä (exploit). Tätä ennen haavoittuvuutta oli hyväksikäytetty yksittäisissä tapauksissa. Haavoittuvuuden julkaisuhetkellä onkin vaikea ennakoida, kuinka nopeasti se päätyy rikollisten työkaluksi.

Osaa internetiin kytketyistä laitteista ei ylläpidetä lainkaan tai erittäin harvoin

Liian harva internetiin kytketty laite on ylläpidetty. Tämä kävi selväksi, kun selvittelimme muun muassa BlueKeep-haavoittuvuuden jälkiä kotimaassa.

Toukokuun loppupuolella skannasimme Suomen internetosoitteet ja löysimme 414 haavoittuvuudelle altista järjestelmää kytkettynä internetiin. Näiden laitteiden omistajiin olimme teleyritysten välityksellä yhteydessä. Lähes kahden viikon kuluttua löysimme yhä 353 haavoittuvaa järjestelmää, eli määrä oli laskenut vain noin 15 %:lla. Verkkoon kytkettyjä ja haavoittuvaksi jääviä järjestelmiä etsivät myös rikolliset.

Nollapäivähaavoittuvuuden aikajana



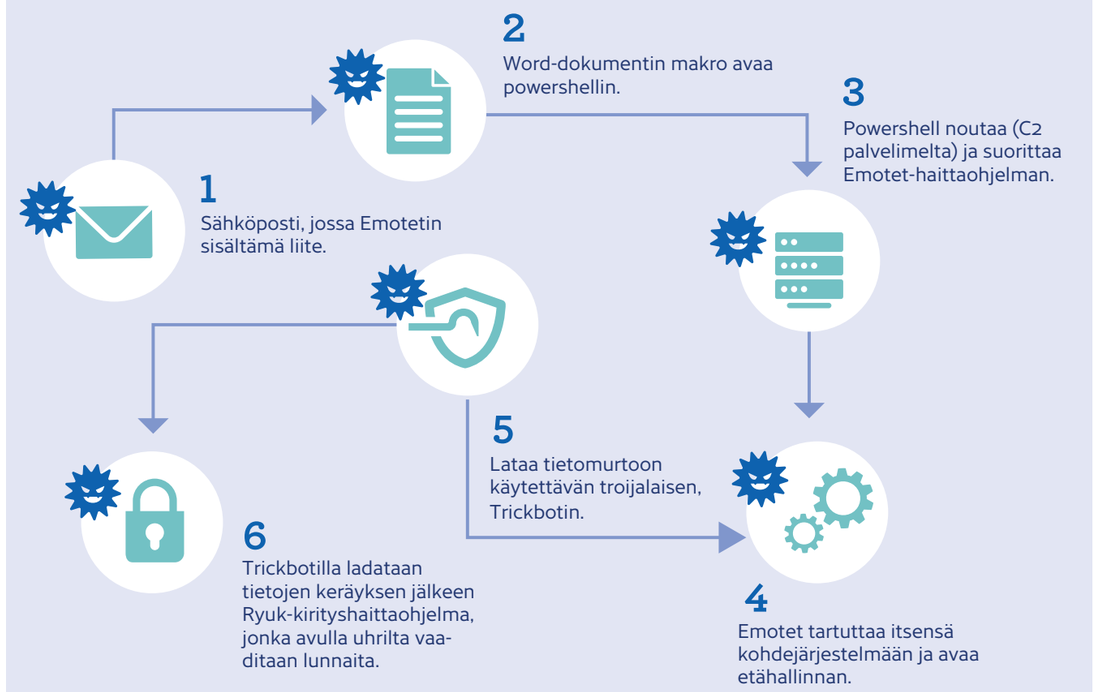
Laajavaikutteinen kiristyshyökkäys voi aiheuttaa kymmenien miljoonien kustannukset

Kuluneena vuonna laajavaikutteiset kiristyshaittaohjelmahyökkäykset puhuttivat paljon. Englanninkielisellä nimellä big game hunting kulkevassa ilmiössä edistyneet rikollisryhmät saalistavat kohteikseen yrityksiä tai organisaatioita, joiden toimintaa laajalle levinnyt kiristyshaittaohjelmatapaus haittaisi merkittävästi.

Rikollisryhmät ovat erikoistuneet kyberrikollisuuden eri osa-alueisiin ja jälleenmyyvät palveluitaan toisilleen

Yksi ryhmä keskittyy haittaohjelman levittämiseen mahdollisimman laajalle esimerkiksi käyttämällä varastettuja sähköpostiketjuja, haitallisilla liitetiedostoilla höystettynä. Toinen joukko kerää haittaohjelman avulla tietoja, esimerkiksi salasanoja ja luottokorttinumeroita, ja luokittelee niitä jälleenmyyntiä varten. Kolmas taas ostaa pääsyn sopivimpiin kohteisiin ja asentaa kiristyshaittaohjelman, joka salaa kohteen koko tietoverkon palvelimet, verkkolevyt ja tärkeimmät työasemat. Samalla kohteen toiminta lamaantuu. Tietojen vapauttamiseksi uhrilta vaaditaan kymmenien tai satojen tuhansien eurojen lunnaita. Samalla kohteen toiminta lamaantuu.

Näin etenee big game hunting -ilmiöön liittyvä haittaohjelmahyökkäysketju:



Uskottavia huijausviestejä vaikea erottaa aidoista

Emotet-haittaohjelmaa levittävä rikollisryhmä on kehittänyt tehokkaaksi osoittautuneen tavan huijata vastaanottajia sähköpostiviesteillä.

Tietomurron uhriksi joutuneen sähköpostiviestiketjuja varastetaan ja niitä lähetetään edelleen uhrin osoitekirjan osoitteisiin haittaohjelman sisältävällä liitteellä höystettynä. Viestin sisältö on siis aidosta keskustelusta lainattu, jolloin sitä voi olla vaikea tunnistaa haitalliseksi. Haittaohjelma leviää siis ketjumaisesti uhrilta toiselle hyödyntäen olemassa olevaa luottamusta. Tällä tavoin muodostuneet haittaviestit muistuttavat uskottavuudeltaan jopa valtiollisten uhkatoimijoiden lähettämiä kohdistettuja viestejä (spearphishing).

Organisaatioihin kohdistuva uhka on entistä vakavampi

Euroopassa big game hunting -ilmiön uhreja ovat olleet esimerkiksi tanskalainen terveysteknologiavalmistaja Demant, norjalainen alumiiniyhtiö Norsk Hydro, saksalainen automaatioteknologiavalmistaja Pilz, ranskalainen tv-kanava M6 ja espanjalainen mediakonserni Prisa.

Kustannukset kipuavat kiristyshaittaohjelmatapauksissa huomattaviksi. Esimerkiksi oman raportointinsa mukaan Norsk Hydrolle aiheutui vuoden 2019 ensimmäisellä puoliskolla 55-65 miljoonan euron kokonaiskustannukset. Demant puolestaan arvioi sille aiheutuneet kustannukset vielä tätäkin suuremmiksi, jopa sataa miljoonaa dollaria lähenteleviksi.

Hyökkääjä hankaloittaa tietoisesti palautumista

Kun rikollisryhmä saa jalansijan organisaatioon, se pyrkii huomaamattomasti levittäytymään mahdollisimman laajalle kohdeorganisaatiossa. Tällaisesta hyökkäyksestä organisaation on hyvin vaikea palautua tavanomaisin keinoin. Haittaohjelman käynnistämisen jälkeen tiedot salataan vahvalla salauksella, jonka purkaminen nykyisillä työkaluilla on usein mahdotonta. Rikolliset tyypillisesti myös hankaloittavat hyökkäyksestä toipumista esimerkiksi salaamalla tiedostojen ja järjestelmien ohella myös varmuuskopiot ja keskitetyn käyttövaltuushallinnan tiedot. Tämän jälkeen hyökkääjä vaatii huomattavaa lunnassummaa vastineeksi salausavaimen luovuttamisesta. Julkisuudessa kerrotuissa tapauksissa lunnasvaatimukset ovat olleet jopa yli puoli miljoonaa euroa.

Menetelmiä, joilla organisaation järjestelmiin alun perin tunkeudutaan ja joilla sisäverkossa levittäydytään, on useita. Suojautumisessa korostuukin kokonaisvaltainen tietoturvan hallinta ja sen perustasosta huolehtiminen kaikilla osa-alueilla.

Jos hyökkääjä kuitenkin saa jalkansa ovenrakoon, on erittäin tärkeää, että organisaatio pystyy havaitsemaan epätavalliset tapahtumat ja hyökkääjän levittäytymisyritykset ennen salauksen käynnistämistä.

Joskus tämäkään ei riitä, vaan hyökkääjä etenee salausvaiheeseen. Silloin auttavat muun muassa harjoitellut palautuskäytännöt ja sellaiset varmuuskopiot, jotka on mahdollista ottaa käyttöön myös laajassa häiriötilanteessa. Nämä kopiot pitää olla suojattuna niin, ettei hyökkääjällä ole mahdollisuutta päästä niihin käsiksi, vaikka tämä olisi odotellut järjestelmissä sopivaa hetkeä.

Lunnaiden maksu kannustaa etsimään lisää uhreja

Todennäköisiä uhreja on vaikea määritellä etukäteen. Maailmalla on nähty viitteitä siitä, että rikolliset ovat kiinnostuneita erityisesti isoista ja maksukykyisistä yrityksistä sekä organisaatioista, joiden tuotantoa kiristyshaittaohjelmalla voidaan haitata merkittävästi. Myös esimerkiksi aluehallinto sekä kunta- ja terveydenhuoltosektori ovat olleet tulilinjalla.

On myös mahdotonta sanoa, yleistyvätkö kiristyshaittaohjelmatapaukset Suomessa. Niin kauan kuin hyökkääjille ei makseta lunnaita, heille viestitään, ettei kyberrikollisuus kannata. Tällöin Suomesta ei myöskään tule hyökkääjiä houkuttelevaa kohdetta. Jos taas lunnaiden maksu yleistyy, on lähes varmaa, että myös rikolliset toteavat tilaisuutensa koittaneen.

MUISTILISTA

ENNALTAEHKÄISE JA VARAUDU

- Huolehdi perustietoturvasta.
- Toteuta varmuuskopiointi siten, että varmuuskopiot saadaan palautettua myös kiristystilanteessa.
- Huomioi uhka riskiarviossa.
- Tee toimintasuunnitelma kriisitilanteen varalta ja varaudu myös viestintätarpeisiin.
- Harjoittele varmuuskopioiden palauttamista.
- Testaa havainnointikykynne.

HAVAITSE AJOISSA

- Ota käyttöön kattava lokitus.
- Pyri havaitsemaan levittäytyminen organisaation verkossa.
- Tunnista komentokanavat.
- Havaitse käyttäjätunnusten luvaton käyttö tai uusien pääkäyttäjätunnusten luonti.
- Hyödynnä jo hankittujen ratkaisujen ja järjestelmien tietoturvaominaisuuksia.

VARMISTA PALAUTUMINEN

- Varmistu varmuuskopioiden saatavuudesta myös häiriötilanteessa.
- Turvaa keskitetty käyttövaltuushallinta.
- Varmistu varmuuskopioiden puhtaudesta.
- Ilmoita hyökkäyksestä viranomaisille. Kyberturvallisuuskeskus tarjoaa apuaan tietoturvaloukkauksen urheille. Tee myös rikosilmoitus poliisille.

Tietomurrot ja tietovuodot

Viime vuoden tapahtumissa erottuvat edelleen Office 365 -tietomurrot. Office 365 -tietomurtoja tehdään pääasiassa kalastelluilla tunnuksilla. Tietomurroilla pyritään pääsemään käsiksi luottamukselliseen materiaaliin, tekemään laskutuspetoksia haltuun saaduilla tiedoilla tai tekemään uusia tietomurtoja haltuun saatuja tunnuksia hyödyntäen.

> ”Kesän aikana useampaan suomalaiseen kuntaan kohdistui tietomurto. Kuntasektorin tietomurtoja sekä kyberturvallisuuden tilannetta käsitellään erillisessä artikkelissa sivulla 36.

Kuntien tietomurrot kesällä 2019

Kevään aikana yleistyi ilmiö, jossa kyberrikolliset etsivät kohteikseen isoja yrityksiä tai julkishallinnon organisaatioita, joiden toimintaa haittaamalla ne voivat yrittää kiristää huomattavia summia rahaa. Big game hunting –ilmiö on aiheuttanut merkittäviä tappioita kohteeksi joutuneille organisaatioille. Lisätietoa aiheesta saat sivulta 36.

Epäselvät vastuunjaot aiheuttavat tietomurtoja

Ulkoistuksia ja palvelusopimuksia suunniteltaessa on syytä ottaa huomioon vastuut järjestelmien ja ohjelmistojen ylläpidosta ja päivityksistä. Kuluneen vuoden aikana tietoomme on tullut useita järjestelmän tai laitteiston päivittämättömyydestä johtuvia tietomurtoja, joissa ylläpitovastuut ovat olleet epäselviä. Monitoimijaympäristössä vastuiden lisäksi myös oikeudet järjestelmien sulkemisesta ja esimerkiksi lokien käsittelystä on syytä sopia jo etukäteen. Yhteiset harjoitukset palvelutoimittajien kanssa ovat yleensä hyvä keino käydä läpi vastuita ylläpidossa ja ongelmatilanteissa.

Työntekijöiden ohjeistus ja yhteiset toimintatavat estävät tietovuotoja

Suojattavien tietojen käsittely esimerkiksi julkisissa pilvipalveluissa saattaa aiheuttaa tietovuotoriskin. Niin ikään toiminta esimerkiksi työmatkoilla on syytä ohjeistaa siten, ettei suojattava tieto ainakaan helposti päädy vääriin käsiin. Valitettavasti organisaation omien ratkaisujen tai toimintatapojen puute tai toimimattomuus saattaa aiheuttaa tilanteita, missä helpoin toimintatapa aiheuttaa tietovuodon riskin.

Tietomurto on rikos

Mitä enemmän saamme ilmoituksia tietomurroista ja tietovuodoista, sitä paremmin voimme luoda kyberturvallisuuden tilannekuvaa sekä auttaa myös muita tietomurtojen uhreiksi joutuneita. On hyvä muistaa, että tietomurto tai sen yritys on rikos, joten suosittelemme tekemään tietomurroista rikosilmoituksen. Muistathan, että jos tietovuodossa päätyy henkilötietoja vääriin käsiin, siitä on tehtävä ilmoitus tietosuojavaltuutetulle.

> ”Kohdistetut kiristyshaitta-ohjelmatapaukset yleistyivät keväällä ulkomailla.
> Lisää ilmiöstä voit lukea sivuilta 21-23.

Tietojenkalastelu ja huijaukset

Käyttäjätunnusten ja salasanojen kalastelu värittivät vuotta 2019. Huijausviestit ohjasivat vastaanottajiaan erilaisille tietojenkalasteluun tarkoitetuille verkkosivuille. Verukkeita oli monia: hyväksy pankkisi uudet direktiivin mukaiset käyttöehdot; avaa kollegasi sisäverkossa jakama tiedosto; kirjaudu palveluun uudelleen; vahvista kirjautumisesi pilvipalveluun tai sometilille. Yhdessäkään tapauksessa viestin mukana tullut linkki ei ollut oikea, vaan huijarin lähettämä. Näin kalastelusivuille syötetyt pankkitunnukset ja salasanat päätyivätkin huijarille tietomurtotarkoituksiin. Vuonna 2019 tapaukset olivat valitettavan arkipäiväisiä.

Office 365 -tietojenkalastelu ja -tietomurrot ovat jo arkea

Jo kesäkuussa 2018 julkaisimme varoituksen Office 365 -sähköpostitunnusten tietojenkalastelusta. Varoitus ehti olla voimassa yli vuoden, kunnes viimein poistimme sen 16.9.2019. Ilmiö ei kuitenkaan ole vähentynyt tai kokonaan poistunut, sillä Office 365 -käyttäjätunnuksia menetetään rikollisille yhä päivittäin.

Syksyllä poistimme varoituksen, koska uusiin hyödyntämistapoihin liittyvät ilmoitukset olivat rauhoittuneet. Tietojen kalastelun ja tietomurtojen uhka ei kuitenkaan ole vähentynyt, vaan saamme edelleen lähes joka päivä ilmoituksia Office 365 -tietomurroista. Lisäksi kalastelulla haltuun saatujen tunnusten käyttö tietomurroissa on nopeutunut kuluneen vuoden aikana ja tämän trendin odotetaan jatkuvan.

Julkaisimme kesällä 2019 oppaan Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta suojautumiseksi. Oppaan saat verkkosivuiltamme suomeksi ja englanniksi. Suojautumisessa auttaa etenkin monivaiheisen tunnistautumisen käyttöönotto, joka oikein toteutettuna auttaa torjumaan vääriin käsiin päätyneiden tunnusten hyväksikäytön. Microsoftin mukaan lähes kaikki Office 365 -tietomurroista olisi estettävissä kaksivaiheisella tunnistautumisella.

Valitettavasti näyttää siltä, että Office 365 -tietomurrot tulevat jatkumaan myös vuoden 2020 aikana. Suosittelemme, että Office 365 -ympäristön, kuten muidenkin pilviratkaisujen ylläpidossa käytetään erillisiä ylläpitotunnuksia, jolloin käyttäjätunnusten päätyminen vääriin käsiin aiheuttaa pienemmän haitan koko pilviratkaisulle.

Kuva Office 365 -huijauksen vaiheista

Murretut sähköpostitilit petosten välineinä

Vuosi 2019 kului myös toimitusjohtajahuijausten ja muiden laskutuspetosten parissa. Tekaistujen sähköpostiviestien ja väärennettyjen pikaviestien virta oli jatkuvaa. Huijausviestejä lähetettiin myös murretuilta sähköposti- ja sometileiltä. Suomessa toimitusjohtajahuijauksiksi kutsutaan huijauksia, joissa organisaation maksuliikenteestä vastaavaa lähestytään johtajaksi tekeytyen ja pyydetään suorittamaan jokin maksu pikaisesti yleensä ulkomaiselle tilille. Huijari vetoaa kiireeseen ja luottamuksellisuuteen, väittää olevansa tilanteessa jossa viestiminen on hankalaa ja vaatii nopeaa toimintaa.

Yritysten lisäksi toimitusjohtajahuijausten kohteiksi ovat päätyneet kaikenlaiset organisaatiot urheiluseuroista ja kirjastoista sairaaloihin ja seurakuntiin. Sähköpostitse tällaiset viestit on helppo väärentää näyttämään oikean johtajan lähettämiltä, mutta myös muunlaisia viestikanavia käytetään. Vuoden 2019 uutuuskikkoja ovat olleet palkkatilien muutospyynnöt huijarien tilille ja erilaisten verkkopalveluiden lahjakorttien ostaminen ja koodien lähettäminen huijarille. Erityisesti lahjakorttien ostamiseen liikelahjaksi sopii hyvin salamyhkäisyys, joka auttaa huijaria uskottaviin huijauksiin.

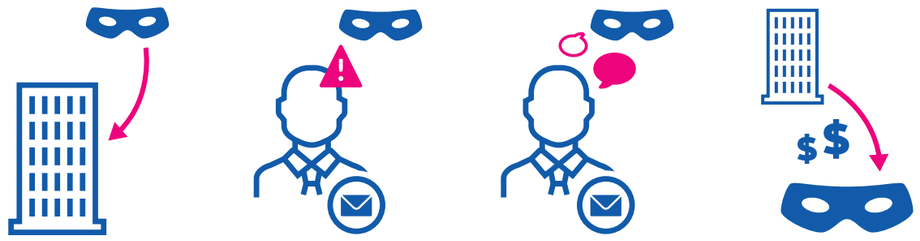
Tekstiviesteihin ei voi luottaa

Tekstiviestien osuus kaikesta huijausliikenteestä jatkoi kasvuaan 2019. Muun muassa tilausansat, sijoitus- ja rahanpesuhuijaukset kilahtelivat mobiililaitteisiin juuri tekstiviesteinä. Olemme jo oppineet pitämään sähköpostia huijareiden vedätyskanavana, mutta tekstiviesteillä ei vielä ole samaa mainetta. Tätä käsitystä huijarit osasivat hyödyntää. Älypuhelimella luettu tekstiviesti vie linkkien kautta epäluotettaville tietojenkalastelu- ja huijaussivuille siinä missä sähköpostikin.

Suurimmat tekstiviestihuijauskampanjat nähtiin jo alkuvuodesta ja keväällä Postin nimissä. Postin nimiin väärennetty saapumisilmoitus näkyi vastaanottajan puhelimessa samassa viestiketjussa kuin oikeatkin Postin tekstiviestit, siksi ne vaikuttivat uskottavilta. Kannattaa kuitenkin epäillä petkutusta, jos paketti-ilmoituksen sijaan "Postin" ilmoittamasta linkistä avautuu kilpailu, arvonta ja mahdollisuus ostaa eurolla satojen eurojen arvoisia viihdelaitteita.

Tilausansojen ja huijausten lisäksi tekstiviestejä käytettiin myös pankkitunnusten kalasteluun ja vahvan tunnistautumisen ohittamiseen.

Tilausansoihin voi joutua montaa eri reittiä: mainoksesta, huijauksesta, someviestistä, tekstiviestistä, nettihausta, ketjukirjeestä. Verukkeena voi olla arvonta, kilpailu, kysely, saapumisilmoitus, tai muu viesti, mutta lopputulos on kuitenkin useimmiten sama: huijattu luulee osallistuneensa kilpailuun ja saaneensa palkinnon, kuten puhelimen tai television eurolla, mutta pienellä painetussa tekstissä kuluttaja onkin sitoutunut kuukausimaksulliseen turhaan palveluun. Huijattu jää ilman kaipaamaansa palkintoa, mutta luottokorttinumeron saaneelle huijarille kilahtaa 80 euroa joka kuukausi.



BEC – Business Email Compromise eli laskutushuijaus.

SUOMESSA HAVAITTUJA HUIJAUKSIA 2019

ESIMERKKEJÄ KIRISTYSHUIJAUSISTA

- **Pornokiristys:**
  Sähköposti, jossa huijari väittää murtaneensa uhrin tietokoneen ja asentaneensa sille vakoiluohjelman, jolla on tallentanut uhrin katsomassa esimerkiksi aikuisviihdettä. Huijari vaatii lunnaita, jottei julkistaisi arkaluonteista tallennetta. Toisinaan kiristyksestä yritetään tehdä uskottavampi jonkin vanhan salasanavuodon avulla: "Tiedän salasanasi, joten varmasti puhun totta".

- **Tappouhkauskiristys:**
  Huijari väittää olevansa palkkamurhaaja, joka on palkattu murhaamaan uhrinsa. Mutta tästäkin pinteestä uhri selviäisi kovat lunnaat maksamalla.

- **Roskapostikiristys:**
  Kiristäjä uhkaa pilata yrityksen maineen aloittamalla valtavan roskapostikampanjan yrityksen nimissä, ellei lunnaita makseta.

- **Palvelunestokiristys:**
  Kiristäjä uhkaa kaataa yrityksen tietoverkon suurella liikennetulvalla, ellei yritys maksa lunnaita. Toisinaan näihin uhkauksiin voi liittyä pieni palvelunestohyökkäyksen näyte, jollaisia verkkorikolliset toteuttavat ilmaiseksi.

ESIMERKKEJÄ LASKUTUSHUIJAUKSISTA

- **Toimitusjohtajahuijaus:**
  Huijari esiintyy johtajana ja lähestyy organisaation kirstunvartijaa sähköpostilla, someviestillä tai muuta kanavaa pitkin. Tarkoituksena on saada jollain verukkeella tehtyä rahasiirto huijarin käyttämälle tilille.

- **Palkanmaksuhuijaus:**
  Huijari esiintyy johtajana ja pyytää organisaation palkanlaskijaa muuttamaan palkkatilin huijarin tiliksi.

- **Lahjakorttihuijaus:**
  Huijari esiintyy johtajana ja pyytää järjestämään nopeasti lahjakortteja, joiden koodit huijari pystyy muuttamaan rahaksi muualla.

Esineiden internet

Aiemmin tulevaisuuden ilmiönä pidetty esineiden internet on nyt arkipäiväämme. Älylaitteet ovat tulleet meille tutuiksi esimerkiksi erilaisten viihdepalvelujen, urheilutapahtumien ja kotiteknologioiden kautta. Palveluja voidaan tuottaa myös paikoista, joissa se ei aiemmin ollut mahdollista. Tällaisia palveluita ovat muun muassa lapsen monitorointiin tarkoitetut pehmolelut, jotka sisältävät seurantamahdollisuuden etäältä tai kodin ohjaamiseen käytettyjä äänikomennoin toimivia laitteita. Laitteiden sisältämät haavoittuvuudet voivat antaa ulkopuoliselle mahdollisuuden päästä käsiksi sekä videokuva- että äänimateriaaleihin.

Internetiin liitettävät laitteet ovat yhä haavoittuvaisia. Laiteohjelmistojen turvallisuus ei parantunut myöskään vuonna 2019. Tietoturvayritys Cyber ITL:n tekemä laaja tutkimus (https://cyber-itl.org/2019/08/26/iot-data-writeup.html) osoitti, että Internet of Things eli IoT-tuotteiden valmistajat toistavat tuotteissaan vuodesta toiseen samoja virheitä, eikä kehitystä ole tapahtunut yli kymmeneen vuoteen.

Turvattomat IoT-laitteet koskevat myös meitä

Havaitsemme internetiin avoinna olevia ja haavoittuvia IoT-laitteita paljon myös Suomessa. Tietoturvapuutteita sisältävät laitteet voidaan esimerkiksi valjastaa bot-verkkoihin palvelunestohyökkäyksiä tehostamaan. Esimerkiksi IoT-laitteet ovat kasvattaneet Mirai-bot-verkkoa vuonna 2019 erityisen runsaasti. Valitettava tosiasia on, että esineiden internetin leviämisen myötä myös rikolliset saavat uusia ansaintamahdollisuuksia.

Toistaiseksi IoT-laitteiden tietoturvan taso on ollut heikko. Onneksi kansainvälisten IoT-standardien tarpeeseen on herätty niin Euroopassa kuin Yhdysvalloissa. Loppuvuosi 2019 toikin kuluttajille ja yrityksille helpotusta esimerkiksi sääntelyn keinoin ja Tietoturvamerkin avulla. Toivomme niiden auttavan mahdollisimman monia kuluttajia älylaiteita koskevissa ostopäätöksissä.

Testaus kunniaan! Parempaa IoT:tä jo tuotekehitysvaiheessa

IoT on tuonut mukanaan etuja, mutta myös tietoturvahaasteita. Näihin haasteisiin on puututtava ennen kuin IoT-laite liitetään internetiin.

Haasteet vaihtelevat laitekohtaisesti. Esimerkiksi kodin lukituksiin liittyvien laitteiden turvallisuushaasteet ovat merkittäviä. Haasteisiin vastataan parhaiten, kun älylaitteiden tietoturvaominaisuudet otetaan mukaan jo suunnittelu- ja kehitysvaiheessa.

Kokonaistilanteen ja haasteiden arviointi vaatii lisää tutkimusta. Silti voimme todeta, että IoT-teknologian hyödyt saadaan parhaiten irti, kunhan perusteet on hoidettu hyvin. Turvallinen esineiden internet perustuu teknologioiden turvalliseen ohjelmistokehitykseen, huolelliseen testaamiseen ja säännöllisiin päivityksiin. IoT-laitteiden avulla tuotetuissa palveluissa on haasteiden lisäksi paljon mahdollisuuksia.

Keskeiset tietoturvariskit yksityishenkilöille, organisaatioille ja valtionhallinnolle

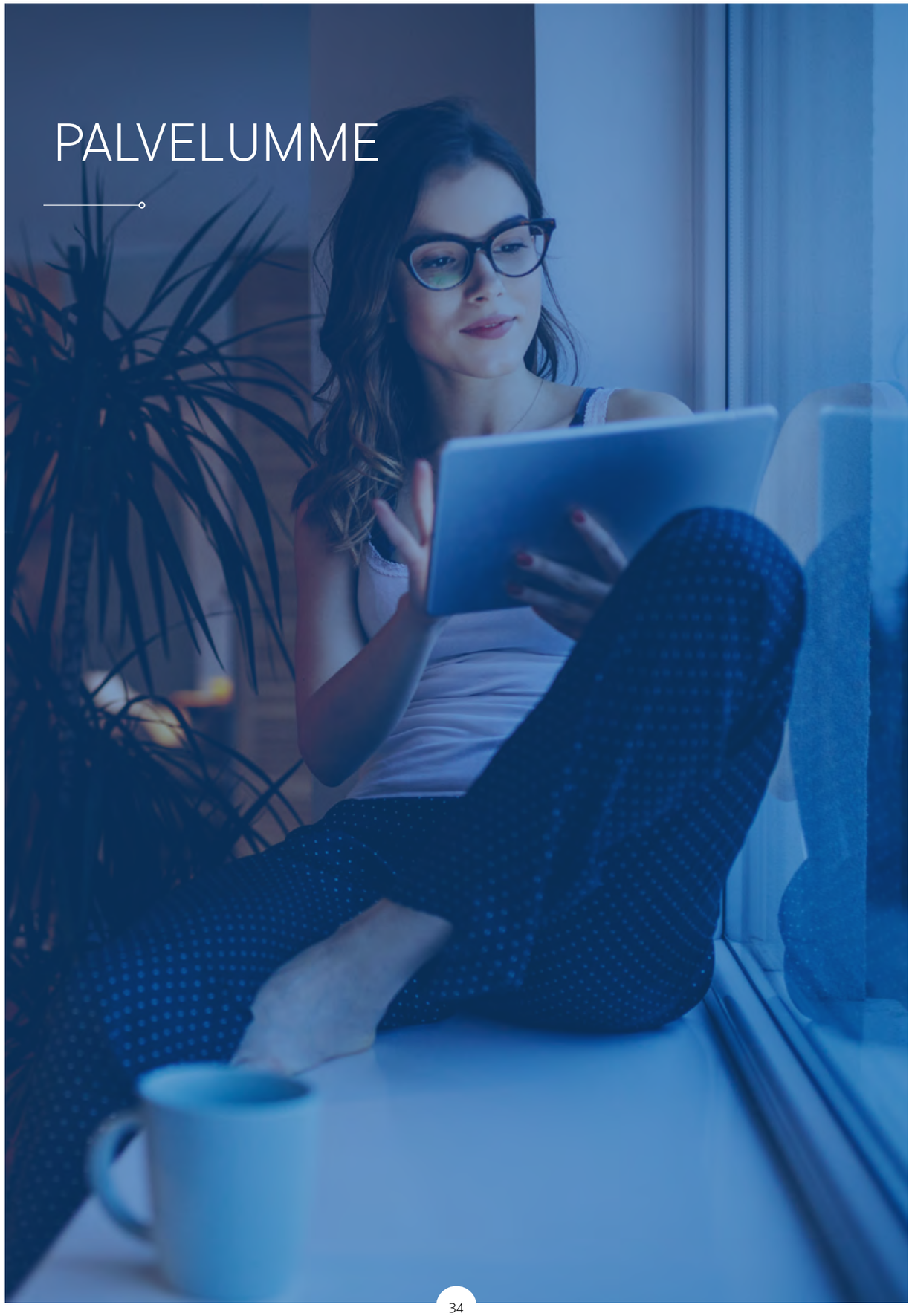
Tässä arviomme keskeisiin kyberturvallisuusilmiöihin liittyvistä merkittävimmistä riskeistä vuonna 2019. Olemme nostaneet esiin esimerkkitapauksia, jollaisina riskit ovat voineet näyttäytyä yksityishenkilöille, yrityksille, kunnallisille organisaatioille tai valtionhallinnolle.

Nuolen suunta kertoo tilanteen kehityksestä vuoteen 2018 verrattuna. Näkemyksemme mukaan vuonna 2019 Suomen yleinen kyberturvallisuuden riskitaso pysyi lähes ennallaan vuoteen 2018 verrattuna. Riskeihin liittyvät uhat eivät ole pienentyneet, paremminkin ne ovat pysyneet ennallaan tai vakavoituneet.

= Riski on pysynyt samana ▲ Riski on kohonnut

VIESTINTÄVERKKOJEN TOIMIVUUS	= Digitaalisten palveluiden käyttö kasvaa, mutta niiden toimivuudesta ei olla syvästi riippuvaisia.	= Entistä useampi organisaatio on varautunut ICT-palveluiden toimivuushäiriöihin. Varatoimet eivät kuitenkaan aina ole riittäviä.	▲ Vanhojen ICT-järjestelmien ylläpito syö resursseja yhteisten järjestelmien toimintavarmuudelta, niiden ylläpidolta ja kehittämiseltä.
PALVELUNESTOHYÖKKÄYKSET	= Murrettuja kotireitittimiä ja muita kodin IoT-laitteita käytetään yhä yhtenä palvelunestohyökkäysliikenteen lähteenä.	= Palvelunestohyökkäyksiin varautuminen tulisi huomioida organisaation verkkopalveluita suunniteltaessa ja hankittaessa.	= Julkiset palvelut ovat valitettavan suosittu kohde palvelunestohyökkäyksille. Etenkin kriittisten palveluiden toimivuus tulisi taata kaikissa tilanteissa.
VAKOILU JA VAIKUTTAMINEN	= Suomalaisten yksityishenkilöiden todennäköisyys joutua vakoilun kohteeksi on pysynyt pääosin samana. Autoritäärisiin maihin liittyvillä toisinajattelijoilla ja poliittisilla vaikuttajilla on riski joutua vakoilun kohteeksi.	▲ Yrityksiä vakoillaan sekä taloudellisten että poliittisten päämäärien edistämiseksi. Organisaatioiden toimintaa häiritsemällä voidaan myös pyrkiä vaikuttamaan yhteiskuntaan.	= On yhä vakoilun keskeinen kohde. Vakoilun avulla edistetään omia poliittisia asemia, hankitaan tietoa päätöksenteosta, arvioidaan varautumista ja kyvykkyyttä sekä voidaan valmistella muuta ei-toivottua vaikuttamista.
HAITTAOHJELMAT JA HAAVOITTUVUUDET	= Haavoittuvat IoT-laitteet saastuvat haittaohjelmilla nopeasti. Ohjelmistot päivittyvät entistä useammin automaattisesti.	= Internetiin kytkettyjä haavoittuvia laitteita etsitään ja murretaan nopeasti. Myös automaatiolaitteiden haavoittuvuuksia hyödynnetty.	▲ Erityisesti haavoittuvuuksien hallinnan ja ylläpidon tärkeys korostunut.
TIETOMURROT JA TIETOVUODOT	= Tietomurtoriski on pysynyt lähes samana vuoden takaiseen. Suurien tunnustietovuotojen määrä on kasvanut.	▲ Kiristyshaittaohjelmatapaukset ovat yleistyneet. Lisäksi etenkin O365 – tietomurtojen määrä on kasvanut.	▲ Valtionhallintoa koskevat samat uhat ja riskit kuin organisaatioitakin. Tietomurtojen ja tietovuotojen määrä on lisääntynyt.
TIETOJENKALASTELU JA HUIJAUKSET	▲ Kansalaisia huijataan entistä etevämmin. Kiristyshuijaukset, pankkikalastelut ja tilausansat kehittyvät jatkuvasti vaikeammiksi torjua.	▲ Yritystilien tietojenkalastelun huippua ei ehkä vielä kään ole nähty, valitettavasti.	= Toimitusjohtaja- ja laskutushuijaukset ovat arkea myös valtionhallinnossa, mutta riskit ymmärretään entistä paremmin.
ESINEIDEN INTERNET	= Kuluttajatuotteiden ohjelmistojen turvallisuus ei ole kehittynyt vuosiin. Tietoturvamerkki ja kehittyvä standardointi tukee turvallisten laitteiden valintaa.	▲ Laiteohjelmistojen turvallisuus ei ole kehittynyt vuosiin.	= Haasteet pysyvät ennallaan, täysin uusia mittavia riskejä ei ole ilmaantunut.

PALVELUMME



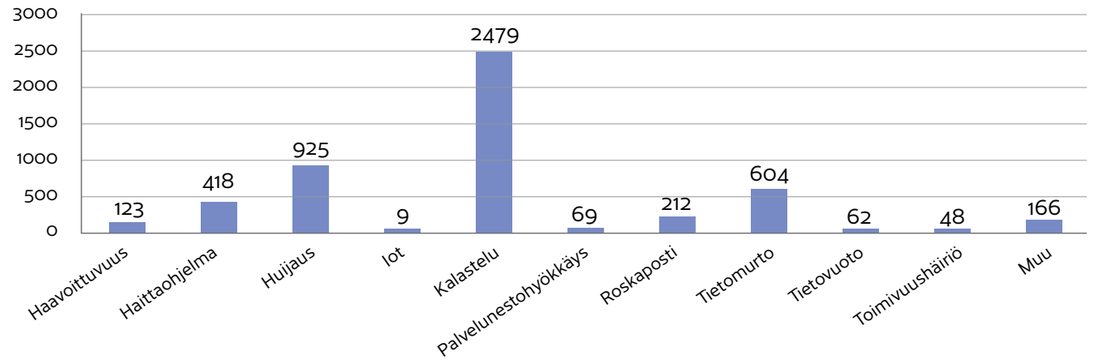
Tilannekeskuksessa käsitellään tuhansia tapauksia vuodessa

Tilannekeskuksessamme neuvotaan ja tuetaan päivittäin lukuisia tietoturvaloukkausten uhreja. Apua tarvitseva voi olla yksittäinen kansalainen kuin myös suuryritys tai kunta. Palvelumme tunnetaan englanninkielisellä termillä incident responce (IR).

Tietoturvaloukkausten vakavuutta arvioidaan kahden henkilön voimin. Usein apu voidaan antaa jo ensiyhteydenoton aikana. Tarkkaa teknistä analyysiä tai pitkäaikaista koordinaatiota vaativat tapaukset siirretään eteenpäin yksityiskohtaisempaan tarkasteluun.

mennään, millaisia toipumis- tai suojautumistoimia on tehty ja millaisia jatkotoimia oli suunnitteilla seuraavaksi.

Nopeat – parhaassa tapauksessa myös ennalta harjoitellut – toimintatavat ja oman ympäristön sekä järjestelmien tuntemus auttavat, jos hyökkäys osuu omalle kohdalle.



Vuonna 2019 Tilannekeskuksemme käsitteli noin 4500 tapausta. Kuvaajan tapausmäärissä eivät näy Autoreporter-järjestelmämme automaattisesti käsittelemät tapaukset.

Käsittelemme vuosittain tuhansia tapauksia. Tietomurtotapausten määrää kasvattivat erityisesti Office 365 -tapaukset. Lisäksi erilaiset huijaukset, muun muassa sähköpostitse ja tekstiviestein lähetetyt tilausansat ovat olleen tämän vuoden riesa.

Vuoden mieleenpainuvimpia asiakkaitamme olivat Kokemäen, Porin ja Lahden kunnat. Ne kokivat, mitä kyberhyökkäyksen kohteeksi joutuminen tarkoittaa.

Kaikissa tapauksissa kaupungit ilmoittivat tapauksista Tilannekeskukseemme nopeasti, heti tilanteen havaittuaan. Näin pystyimme tukemaan ja neuvomaan kyberhyökkäyksen uhreja parhaalla mahdollisella tavalla.

Lahden ja Kokemäen kanssa pidimme säännöllisiä tilannepalavereita, joissa selvitimme missä

Kunnilla on merkittävä rooli arjen toimintojen tuottajana ja kuntalaisten turvaajina

Kun kuntien palvelut toimivat, asiaan ei kiinnitetä sen enempää huomioita. Kunnilla on paljon erilaisia palveluita, joita niiden tulee ylläpitää. Vuoden 2019 aikana useampi suomalainen kunta joutui kyberhyökkäyksen kohteeksi ja kuntien kyberturvallisuus nousi puheenaiheeksi.

Kuntien kyberturvallisuuden taso vaihtelee ja resursseja, niin taloudellisia kuin henkilöstöön liittyviä, on käytettävissä hyvin eri tavalla. Usein ongelmana on, että kyberturvallisuuteen ei panosteta tarpeeksi. Palveluita toteutetaan edullisesti ja siten, ettei niiden

Kyberhyökkäys horjuttaa yhä Lahden terveyspalveluja – Krp: "Kaikki voitava tehdään, että pahuuden levittäjä saadaan kiinni"

YLE:n uutiset 13.6.2019

"Kiristäjät vaativat lunnaita Kokemäen kaupungilta – haittaohjelma pisti kaupungin verkon polvilleen"

YLE:n uutiset 30.7.2019

"Taas tietomurto Satakunnassa: Tällä kertaa kohteena Porin kaupunki"

YLE:n uutiset 8.8.2019

ylläpitoa suunnitella. Lisäksi ylläpito toteutetaan resurssisyistä yksinkertaisesti, joka voi tarkoittaa esimerkiksi sitä, että yhdessä ja samassa verkossa on useita eri palvelukokonaisuuksia. Hyökkäämällä verkkoon voidaan yhdellä kertaa saada laaja-alaiset vaikutukset.

Kokemäen, Lahden ja Porin kyberkesä oli työntäyteinen

Kokemäellä kaupungin tietoverkkoon kohdistunut hyökkäys aiheutti laajaa haittaa ja häiriöitä kaupungin palveluiden ja toimintojen järjestämisessä. Esimerkiksi kaupungin sähköpostiliikenne ja maksuliikenne eivät hyökkäyksen myötä toimineet.

Lahdessa kaupungin tietoverkkoon kohdistuneen hyökkäyksen suorat kustannukset olivat nousseet vuoden vaihteeseen mennessä jo noin 900 000 euroon. Myös epäsuorien kustannusten määrän arvioidaan olevan sadoissa tuhansissa euroissa, kun verkon toimimattomuus haittasi verkon käyttäjien työtehtäviä. Varotoimena muun muassa Lahden kaupungin ja Päijät-Hämeen hyvinvointiyhtymän verkkojen välinen yhteys jouduttiin katkaisemaan.

Porissa hyökkäyksestä selvittiin pienemmällä, mutta ainekset laajempaan vahinkoon olivat olemassa.

Osallistuimme kesän ja syksyn aikana niin Porin, Lahden kuin Kokemäenkin kuntiin kohdistuneiden kyberhyökkäysten selvitykseen. Tapauksia yhdisti välittömät vaikutukset etenkin ICT-palveluihin. Kohteiksi osuneisiin kuntiin kohdistui tietomurto, jossa haittaohjelman avulla päästiin sisälle kunnan tietoverkkoon. Hyökkääjä ei välttämättä valinnut kohteikseen juuri näitä kuntia, paremminkin hyökkääjän haaviin osui helppoja saaliita, joiden tietoturvan taso oli heikko. Tällöin hyökkääjä sai pienellä vaivalla suuren vaikutuksen.

Suurimmassa kuntatapauksessa hyökkääjä pääsi toimimaan verkon sisällä puutteellisen verkon eriyttämisen ja laajalti käytössä olleiden ylläpito-oikeuksien avulla. Toisaalta ajantasainen tietoturvaohjelmisto reagoi haittaohjelman tavallisuudesta poikkeavaan toimintaan nopeasti, ja kunnan erittäin asiantunteva palveluntarjoaja esti nopeasti mahdolliset suuret lisävahingot. Silti kyberhyökkäyksen kokonaiskustannukset nousivat satoihin tuhansiin euroihin ja vaikutukset olivat pitkäkestoisia.

Muissa tapauksissa hyvin toteutetut verkon eri osien eriyttämiset estivät haittaohjelman laajemman leviämisen. Myös varmuuskopiot tekivät mahdolliseksi nopeamman toipumisen.

Kesän tapahtumien vuoksi selvitimme kuntien tietoturvallisuuden tasoa. Havaintojemme mukaan kuntien verkkoympäristöissä on paljon internetiin avoimia palveluita, jotka eivät sinne kuulu. Tällaisia ovat esimerkiksi suojaamattomat toimistolaitteet, verkon hallintalaitteet, erilaiset tietokantapalvelimet ja sisäiset palvelut kuten koko intranet. Ongelmia aiheuttavat myös vanhentuneet ohjelmistot ja palvelimet. Raportoimme havaintomme kuntiin, jotta tietoturvapuutteet saataisiin korjattua.

Yhteistyö ja verkostot osana kuntien kyberturvallisuuden kehitystä

Turvallisuuskomitea teki syksyllä 2019 suosituksen kuntien kyberturvallisuuden parantamiseksi: "Viimeaikaiset tapahtumat ovat koetelleet eri tavoin kuntien kyberturvallisuutta. Vastuu toimenpiteistä ja kustannuksien kattamisesta on kunnilla, mutta Liikenne- ja viestintäviraston Kyberturvallisuuskeskus ja muut viranomaiset tarjoavat kunnille neuvonta- ja tutkintatukea."

Tällä hetkellä Kyberturvallisuuskeskuksessa ei ole kuntien kyberturvallisuuden tilanteesta kokonaiskuvaa, koska ilmoitusvelvollisuutta poikkeamista ei ole. Osa kunnista teki vuoden 2019 aikana ilmoituksen, mikä helpotti tilanteesta toipumista. Yhdessä Kuntaliiton kanssa olemme todenneet tarpeen kuntien omalle verkostolle, jossa voidaan jakaa tietoa. Tätä varten on aloitettu työ yhteistyöryhmän perustamiseksi. Tilannetta saadaan huomattavasti parannettua, kun kuntien tavoitettavuus helpottuu ja tietoa voidaan jakaa kohdennetusti.

Tietoturvasääntely ja -arvioinnit

Takana kyberturvallisuuslainsäädännön supervuosi

Vuonna 2019 useat tietoturvallisuutta ja kyberturvallisuutta koskevat lait astuivat voimaan. Muun muassa tunnistus- ja luottamuspalvelulakien muutokset toivat mukanaan kilpailua tunnistuspalveluihin. Puolestaan kyberturvallisuusasetuksen voimaan tulo vakinaisti Euroopan unionin verkko- ja tietoturvaviraston ENISA:n aseman ja antoi mahdollisuuden eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän perustamiselle.

Lisäksi useat lainsäädäntöön liittyvät valmistelutyöt jatkuivat. Esimerkiksi sähköisen viestinnän palveluista annetun lain sisältöjä uudistettiin, jotta se voisi vastata EU:n sähköisen viestinnän direktiivipaketin säädöksiä. Myös sähköisen viestinnän ePrivacy- eli tietosuoja-asetusta valmisteltiin EU:ssa.

Kuluneen vuoden säädösprojektien lisäksi valvoimme ja veimme käytäntöön myös aiemmin voimaan tullutta säädäntöä.

Kaivattua kilpailua tunnistuspalvelumarkkinoille

§

Vuoden alkupuolella voimaan tulleet tunnistus- ja luottamuspalvelulain muutokset toivat kaivattua kilpailua vahvojen sähköisten tunnistuspalvelujen markkinoille. Myös niin sanottujen tunnistuspalveluvälittäjien toiminta pääsi alkuun. Saavutimme tilanteen, jossa sähköisen palvelun tarjoaja voi kilpailuttaa tunnistuspalvelujen tarjoajia ja tarvittaessa saada kaikki tunnistusvälineet asiakkaidensa käyttöön tekemällä sopimuksen yhden välityspalvelun tarjoajan kanssa. Aiemmin sopimuksia oli tehtävä useita. Lisäämällä kilpailua markkinoilla alennetaan palveluista maksettuja hintoja ja edistetään vahvan tunnistuksen käyttöä sähköisissä palveluissa. Mitä enemmän vahvaa tunnistusta käytetään, sitä turvallisemmaksi digitaalinen yhteiskuntamme rakentuu.

TUPAS tuli tiensä päähän

§

Suomalaisille verkkopankeista tuttu ja vahvassa sähköisessä tunnistamisessa pitkään käytetty TUPAS-yhteyskäytäntö sai historiallisen päätöksensä. Suomessa kehitetty TUPAS oli vahvan tunnistamisen edistyksellinen ratkaisu. Siitä päätettiin kuitenkin luopua, koska se ei enää täyttänyt nykyaikaisia vahvan sähköisen tunnistamisen turvallisuusvaatimuksia. Tilalle otettiin OIDC- ja SAML-yhteyskäytännöt, jotka täyttävät nykyvaatimukset ja ovat kansainvälisesti paljon käytettyjä. Kehitys on hyvä muistutus siitä, että järjestelmiä ja palveluja on jatkuvasti kehitettävä sekä tämänhetkisiä että tulevaisuuden turvallisuusvaatimuksia ajatellen.

Seutuverkkojen toimintavarmuus tarkastajien kohteena

Olemme viime vuosina tehneet tarkastuksia erityisesti uusiin käyttöön otettuihin seutuverkkoihin ja niitä pyörittäviin toimijoihin. Tavoitteenamme on ollut varmistaa riittävä verkkojen ja verkossa tarjottavien palvelujen toimintavarmuus heti käyttöönotosta alkaen. Seutuverkoilla tarkoitetaan kymmeniä paikallisia valokuituverkkoja, joita erilaiset paikalliset toimijaryhmät ovat rakentaneet laajakaistayhteyksien tarjoamista varten.

Tarkastuksissa käydään läpi viestintäverkon toimivuuden ja sähkönsyötön varmistamiseen, maadoituksiin ja häiriönhallintaan liittyvät vaatimukset. Tavoitteena on parantaa toimijoiden tietoisuutta vähimmäisvaatimuksista ja antaa neuvoja toimintavarmuuden kehittämiseksi. Tarkastusten perusteella voidaan myös velvoittaa korjaamaan havaitut puutteet. Vaikka tarkastusten kohteena on aina yksittäinen toimija, keräämme samalla myös tietoa sääntelyn toimivuudesta ja muutostarpeista. Tarkastukset ovat tärkeä osa myös toimintavarmuutta koskevan sääntelyn ja koko yhteiskunnan turvallisuuden kehittämisessä.

Porinaa evästeistä

Euroopan unionin tuomioistuin antama niin kutsuttu Planet 49 -ratkaisu lisäsi evästeistä käytävää julkista porinaa yleisen tietosuoja-asetuksen, GDPR:n, vanavedessä. Valitettavasti tuomioistuimen ratkaisu ei tuonut tapauksiin selkeää linjausta.

Ratkaisun mukaan evästeiden käyttöä koskevaan suostumukseen vaaditaan käyttäjältä aktiivinen toimenpide. Lisäksi palveluntarjoajan on annettava tiedot evästeiden toiminta-ajasta ja siitä, onko kolmansilla mahdollisuus käyttää kyseisiä evästeitä. Tuomioistuimen ratkaisussa ei kuitenkaan käsitelty sitä, tuleeko suostumus pyytää esimerkiksi ponnahdusikkunalla. Nähtäväksi jää, tuoko valmisteltavana oleva sähköisen viestinnän tietosuoja-asetus muutoksia tilanteeseen.

Kansainvälisen turvallisuusluokitellun tiedon suojaamiseen sopivat järjestelmät kovassa huudossa

Kansallisen ja kansainvälisen turvallisuuspolitiikan ilmiöt näkyivät myös arviointikohteissamme, joissa keskityttiin erityisesti kansainvälisen turvallisuusluokitellun tiedon suojaamiseen. Arvioimme useita yhteiskunnan toiminnan kannalta merkittäviä tietojenkäsittely-ympäristöjä, joiden käytön ehdoksi turvallisuusluokitellun tiedon omistajat olivat asettaneet kansallisen viranomaishyväksynnän. Tietojenkäsittely-ympäristöjen lisäksi hyväksyimme useita kotimaisten salaustuotteiden uusia versioita.

NCSA:n kuluneen vuoden yleistunnelmat olivat positiiviset pystyessämme tukemaan useita viranomaisia ja yrityksiä turvallisuusluokitellun tiedon käsittelyyn liittyvissä, paikoin poikkeuksellisenkin kriittisissä tarpeissa. Vuoden merkittävimmille arviointikohteillemme pystyttiin myöntämään viranomaishyväksyntä. Kansallisten ja kansainvälisten ilmiöiden kehittyminen lupaa erittäin mielenkiintoisia haasteita myös vuodelle 2020!

> Eväste (cookie) on pieni tekstitiedosto, jonka internetselain tallentaa käyttäjän laitteelle. Evästeiden avulla on mahdollista muun muassa kerätä verkkokaupassa ostoksia ostoskoriin ennen niiden maksamista. Evästeistä säädetään sähköisen viestinnän palveluista annetun lain 205 §:ssä. Se perustuu EU:n sähköisen viestinnän tietosuojadirektiiviin, joka ollaan korvaamassa asetuksella.

Neuvontapalvelumme on otettu hyvin vastaan - tarkastusten läpimenoajat nopeutuivat

Edellisvuoden tapaan tietoturvaneuvonnan tarve kasvoi. Vuonna 2019 tukea ja ohjeistusta tarvittiin erityisesti yhteiskuntamme kriittisen infrastruktuurin suojaamiseen sekä turvallisuusluokitellun tiedon suojaamiseen tietojärjestelmissä. Neuvontapalvelumme tulokset näkyivät arviointikohteissamme aiempaa parempina valmiusasteina, mikä nopeutti muun muassa tarkastusten läpimenoaikoja.

Kriteerit pilvipalvelujen turvallisuuden arviointiin

Jo pitkään pilvipalveluiden tietoturvallisuus on herättänyt kysymyksiä niin hallinnossa kuin elinkeinoelämässä. Julkaisemamme kriteeristö pilvipalveluiden turvallisuuden arvioinnin tueksi otettiinkin positiivisesti vastaan.

§

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) tukee viranomaisia uuden tiedonhallintalain soveltamisessa. Se sisältää myös työkaluja pilvipalvelujen turvallisuuden ja niihin liittyvien riskien arviointiin. Lisäksi se kertoo pilvipalvelujen turvallisuuteen vaikuttavista hyvistä käytännöistä, joita kaupallisetkin toimijat voivat hyödyntää.

Olemme saaneet kriteeristöstä paljon hyvää palautetta ja kehitysehdotuksia. Alkuvuodesta 2020 julkaisemme siitä uuden version, joka perustuu sekä palautteeseen että omiin havaintoihimme.

Päivitetty arviointikriteeristö tukee tunnistuspalvelujen turvallisuuden kehittämistä

Vuoden 2019 aikana päivitimme vahvan sähköisen tunnistamisen arviointikriteeristön tunnistuspalvelujen arviointikertomuksista ja tietoturva-auditoinneista saatujen kokemusten pohjalta. Kriteeristö tukee tunnistuspalvelujen tarjoajia ja niille auditointeja tekeviä arvioitsijoita palvelujen turvallisuuden kehittämisessä ja arvioimisessa. Kriteeristön perusteella myös me arvioimme sekä tarjolla olevien että uusien tarjolle tulevien tunnistuspalvelujen turvallisuutta ja vaatimustenmukaisuutta. Vaikka kriteeristö on ensisijaisesti tarkoitettu vahvan sähköisen tunnistuspalvelujen tarjoajille ja niitä arvioiville, se luo hyvän perustan myös muiden tunnistuspalvelujen kehittämiselle.

Päivitetyssä kriteeristössä on myös oma kokonaisuus tunnistuspalveluissa käytettäville mobiilitunnistusratkaisuille ja -sovelluksille. Sen tavoitteena on nykyisin käytössä olevien ja tulevaisuudessa käyttöönotettavien sovellusten turvallisuuden tason parantaminen. Kriteeristö pohjautuu The Open Web Application Security Projectin (OWASP) mobiilisovellusstandardiin, joka mielestämme luo parhaimmat lähtökohdat turvallisten sovellusten kehittämiselle. Kriteeristö ei olisi valmistunut ilman erinomaista valmistajien ja tunnistuspalvelun tarjoajien asiantuntijoista koostunutta asiantuntijatyöryhmää.

Kriteeristömme on maailmanlaajuisesti ainutlaatuinen, ja se on herättänyt myös kansainvälistä kiinnostusta. Useat sääntelyviranomaiset ja tunnistusratkaisuja sekä -palveluja tarjoavat toimijat ovat ottaneet kriteeristömme lämpimästi vastaan.

Mobiilitunnistusratkaisut ovat yleistyneet hurjaa vauhtia ja on selvää, että suurin osa tunnistusratkaisuista tulee jatkossa perustumaan mobiilipäätelaitteeseen ja siihen asennettavaan tunnistusapplikaatioon. Mobiiliratkaisut ovat myös näkyneet EU:n jäsenmaiden eIDAS-asetuksen perustella tehdyissä ilmoituksissa ja niitä edeltävissä jäsenmaiden yhteistoimintaverkoston antamissa lausunnoissa. Erityisesti lausunnoissa ovat nousseet esille kryptografisten avaimien säilyttämiseen liittyvät turvallisuusarvioinnit ja biometrisen todentamistekijöiden soveltuvuus. Voit tutustua ohjeeseemme 211/2019 O Sähköisen tunnistuspalvelun arviointiohje verkkosivuillamme.
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/O211_Sähköisen_tunnistuspalvelun_arviointiohje_211_2019_O.pdf

Laitevelmistajat heräsivät Galileon hyötyihin

Euroopan unionin rahoittama Galileo-paikannussatelliittipalvelu saavutti vuonna 2019 tärkeän etapin: Galileon avoimen palvelun käyttöä tukevia päätelaitteita, lähinnä älypuhelimia, oli myyty miljardi syyskuuhun 2019 mennessä. Laitevalmistajien heräämi-nen Galileon hyödyntäjiksi olikin vuoden merkittävin muutostrendi.

Brexit karsi järjestelmän globaalia kattavuutta

Galileo-järjestelmä toimi vuonna 2019 yhteensä 22 satelliitin varassa. Sillä saavutetaan globaali kattavuus. Britannian irtautumisaikomus EU:sta sai aikaan sen, että Galileo-järjestelmän maasegmentin brittiläiset osuudet - turvallisuushallintakeskus Iso-Britanniassa, maatukiasemat Falklandilla ja Ascensionilla - irrotettiin kokonaisuudesta. Tilanteen tasaamiseksi aloitettiin Espanjaan sijoittuvan turvallisuushallintakeskuksen rakentaminen.

Palvelut monipuolistuvat suunnitelmallisesti aina 2024 asti

Galileon paikannuspalvelut ovat toistaiseksi Initial Services -vaiheessa. Kaikille avoimen paikannuspalvelun (OS, Open Service) virallinen käyttöönotto tapahtunee vuoden 2020 loppupuolella. Muut Galileon palvelut otetaan käyttöön yksi kerrallaan ja erillisen hyväksymisprosessin mukaisesti vuosina 2021-2024. Suurin mielenkiinto tullee kohdistumaan ilmaiseksi tarjottavaan tarkkuuspalveluun (HAS, High Accuracy Service), jolle on luvattu 20 senttimetrin paikannustarkkuus. Palvelua pidetään merkittävänä erityisesti autonomisia liikennemuotoja kehitettäessä.

Heinäkuinen palvelukatkos herätti huomiota

Heinäkuussa 2019 palvelut katkesivat lähes viikoksi, Search and Rescue eli SAR-palveluita lukuun ottamatta. Tämä herätti ymmärrettävästi huomiota paitsi ammattipiireissä, myös julkisessa sanassa. Palvelujen käyttäjät eivät havainneet suurta muutosta satelliittipohjaisissa paikannuspalveluissaan, koska kuluttajapäätelaitteet käyttävät tyypillisesti rinnan kaikkia saatavilla olevia globaaleja paikannussatelliittijärjestelmiä, joita Galileon ohella ovat GPS, Glonass ja Beidou. Palvelukatkoksen aiheutti inhimillinen virhe järjestelmää päivitettäessä. Tapahtuma on tutkittu perin pohjin ja vastaavan virheellisen toiminnan välttämiseksi on otettu käyttöön tukku varmistavia toimenpiteitä.

GALILEO SAATTAA OLLA SINUNKIN TASKUSSASI

EU:n rakentama satelliittinavigointijärjestelmä Galileo tuottaa erittäin tarkkaa sijainti- ja aikatietoa. Galileo-järjestelmää operoi Euroopan satelliittipaikannusvirasto (GSA) EU:n jäsenmaiden ohjauksessa. Sinäkin voit olla Galileon käyttäjä, sillä suuri osa nykyisistä, kuluttajille suunnatuista matkapuhelimista ja älylaitteista hyödyntää jo Galileon satelliittien signaaleita.

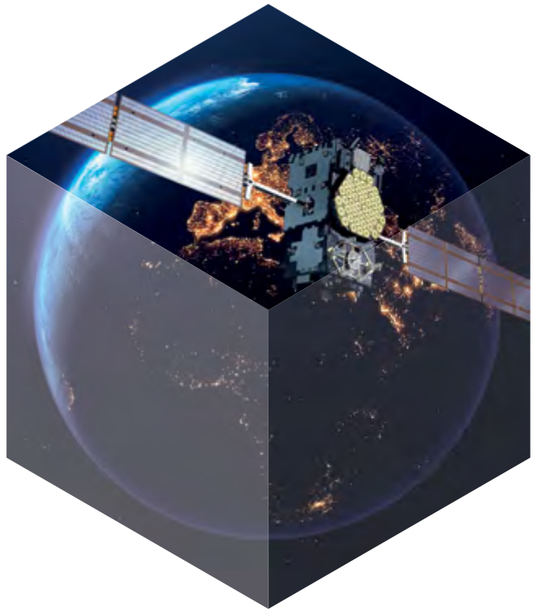
Parempi tarkkuus ja vähemmän häiriöitä, kun yhdysvaltalaislaitteiden Galileo-vastaanottokyky huomattiin

Galileo-taajuuksien käytön tultua hyväksytyksi myös Yhdysvalloissa, sikäläiset laitevalmistajat aktivoituivat vuoden 2019 kuluessa Galileon hyödyntämisessä. Osassa yhdysvaltalaisvalmisteisia päätelaitteita piilevänä tähän asti ollut Galileo-vastaanottokyky pystyttiin aktivoimaan ohjelmistopäivitysten kautta. Älypuhelimissa ja muissa kehittyneissä mobiilipäätelaitteissa otettiin käyttöön prosessoreja, jotka sisälsivät Galileon - osittain myös GPS:n - signaalien vastaanottomahdollisuuden kahdella erillisellä taajuuskaistalla, mikä vaikuttaa positiivisesti paitsi paikannustarkkuuteen myös signaalin vastaanotettavuuteen kaupunkiolosuhteissa. Laajimmalle levinnyt tällainen piiri oli Qualcommin Snapdragon 855.

Galileo-työ jatkuu ja saamme lisää vastuita

Suomen PRS- eli Galileo Public Regulated Service -viranomaisena jatkoimme PRS-palvelun käyttöönoton valmisteluja Liikenne- ja viestintäministeriön ohjauksessa. Useat valtionhallinnon alat sekä myös yhteiskunnan kriittisistä toiminnoista vastaavat yritykset ilmaisivat tarpeensa varmennetun paikannus- ja aikapalvelun käyttöönottamisesta. Tarkoituksena on, että kansallisen PRS-käytön mahdollistava palveluarkkitehtuurin suunnittelu alkaisi vuonna 2020.

Liikenne- ja viestintäministeriö siirsi vuoden 2019 aikana virastoomme myös muiden Galileo-palveluiden operatiivisen toiminnan valmisteluvastuun. Marras-joulukuun vaihteessa 2019 järjestimmekin mittavan Galileo Innovation Challenge -tapahtuman, joka keräsi Helsinkiin runsaan ja kansainvälisen osallistujajoukon. Tapahtumassa kehitettiin Galileon palveluiden uudenlaisia käyttötapoja, tutkittiin häiriöiden havaitsemistekniikoita ja innovoitiin Galileon palveluiden yhdistämistä robotiikkaan. Tapahtuma kuului ministeriömme vuonna 2017 julkaisemaan satelliittinavigoinnin toimenpideohjelmaan.



GALILEO
INNOVATION
CHALLENGE

Yhteistyö ja tiedonjako

Tiedonvaihtoryhmiemme kootut kuulumiset

Tiedonvaihtoryhmämme, eli ISAC:it (ISAC=Information Sharing and Analysis Centre), ovat eri toimialoille perustettuja kyberturvallisuuden yhteistyöelimiä. Niiden päätarkoituksena on jakaa tietoa ja kokemuksia ja näin lisätä organisaatioiden sekä toimialojen kykyä suojautua digitaalisilta uhkilta.

Käytämme ISAC-ryhmien tuottamaa tietoa kansallisen kyberturvallisuuden tilannekuvan koostamisessa.

Tässä eri toimialojen keskeiset kuulumiset ja nostot vuodelta 2019.

TOIMIALA	ERITYISPIIRTEET	AJANKOHTAISTA
VALTIONHALLINTO	Valtionhallinnon organisaatiot kohtaavat samoja tietoturvauhkia kuin muutkin toimijat. Sovittujen käytäntöjen noudattaminen on pelastanut valtionhallinnon toimijat monelta huijausyritykseltä, muun muassa laskutus- eli BEC-huijaukselta.	Vaalien ja EU-puheenjohtajuuskauden varautuminen siivittivät vuotta 2019. PiTuKri ja Pilvistrategia toivat yhteistä näkemystä pilvipalvelukeskusteluihin. Uuden kyberturvallisuusstrategian myötä kansallinen kyberturvallisuuden johtaminen on vahvistunut.
FINANSSI	Toiminta aloitettiin keväällä 2019. Jäsenet ovat aktiivisia ja tekevät toimialaa kehittävää yhteistyötä. Pankkien nimissä lähetetyt huijausviestit, sekä toimijoihin kohdistuvat palvelunestohyökkäykset ovat arkipäivää.	EU:n suosittelema TIBER-EU-kehikko ohjaa toimialaaa säännölliseen ja skenaariopohjaiseen uhkien harjoittelemiseen. Harjoittelun tulisi perustua mahdollisimman realistisiin tilanteisiin. TIBER-FI-kehikkoa päivitetään, ja yhdessä NIS-direktiivin kanssa ne ovat osaa toimijoita koskevaa suositus- ja regulaatiokehikkoa.
VESIHUOLTO	Liiketoiminnan ydin on automaatiojärjestelmien toimivuus, joten näiden suojaaminen ja ylläpito on etusijalla.	Ryhmän ensimmäinen vuosi takana. On jaettu kokemuksia, ohjeistuksia, tietoa ja työkaluja kyberturvallisuuden parantamiseksi. Vuoden 2018 KYBER-VESI-hankkeelle ollaan suunnittelemassa jatkoa. Tähän myös ISAC-ryhmä osallistuu.
TELEYRITYKSET (ISP)	Teleyritykset ja internetyhteyspisteet ovat erityisasemassa tietoturvauhkien havainnoinnissa ja torjunnassa. Uhkakuvia, joiden torjumisesta keskustellaan, ovat esimerkiksi palvelunestohyökkäykset ja pahantahtoisesti toteutetut internetliikenteen reititysmuutokset.	Jaettu tietoa ajankohtaista tapauksista, keskusteltu sääntelyn vaikutuksesta liiketoimintaan ja miten toimintatapoja tulisi kehittää, jotta uusiin kyberturvallisuusuhkiin voitaisiin vastata. Kesällä 2019 tiedonvaihtoryhmän puheenjohtajuus siirrettiin Traficomilta toimialalle.
SOTE	Potilas- ja asiakastietojen luottamuksellisuus ja tietosuoja ovat jatkuvia haasteita, joita ratkotaan muun muassa tietoturvan keinoin. STM julkaisi SOTE-alan ensimmäisen valtakunnallisen kyberturvallisuusohjeen. STM luo alalle valtakunnallista toimintamallia kyberturvallisuuden poikkeamista ilmoittamiseksi ja tilannekuvan luomiseksi.	Kyber-Terveys-hankkeen tulosten levittäminen käynnistyi. Uusia kehittämishankkeita suunnitellaan. Lääkinnällisten laitteiden EU-tason säädäntö muuttuu, ja sen myötä tulee kyberturvallisuutta koskevia vaatimuksia. Tiedonhallintalaki muutti SOTE-alaa koskevia tietoturvavaatimuksia.
ENERGIA	Toimialalla on paljon yhteistä ja omaa harjoitustoimintaa. Toimijoiden kesken vallitsee erittäin vahva luottamus, joka tekee mahdolliseksi aktiivisen tiedonjaon.	IoT:n ja pilvipalveluiden hyödyntämiseen ja tietoturvaan liittyvät näkökulmat. Keskustelua NIS-direktiivistä ja siihen liittyvästä kyberturvallisuuden maturiteetin arvioinnista. Alalla on testattu Kyberturvallisuuskeskuksen ja Huoltovarmuuskeskuksen tuottamaa Kybermittari-arviointityökalua, jonka avulla yrityksen on mahdollista tehdä itsearvio kyberturvallisuuden maturiteettitasostaan.
KEMIA JA METSÄTEOLLISUUS	Toiminnan kansainvälinen luonne sekä voimakas riippuvuus automaatiojärjestelmistä.	Office 365-huijaukset olleet koko vuoden ajankohtaisia. Erityisesti riippuvuus palveluntarjoajista ja niiden prosesseista puhuttaa.
ELINTARVIKE JA KAUPPA- JA JAKELU	Elintarviketuotanto ja kauppa- ja jakelutoimiala ovat täysin digitalisoituneita. Automaation, robotiikan ja IoT:n hyödyntäminen liiketoiminnan tehostamiseksi on arkipäivää.	Tälläkin toimialalla erityisesti O365-huijaukset ovat olleet toimijoiden riesana. Lisäksi uuden teknologian käyttöönotto liiketoimintaprosesseissa on nopeaa. Tämä aiheuttaa merkittäviä haasteita tietoturvan proaktiiviselle hallinnalle.
MEDIA	Alalla korostuu verkkoyhteyksien ja järjestelmien toimintavarmuus sekä nopeatempoisessa uutistyössä että sähköisessä viestinnässä. Lisäksi toimintaan ja toimittajiin kohdistuu mielenkiintoa, joka yhtiöiden on huomioitava myös tietoturvasta huolehtiessaan.	Media-alan varautumista kyberuhkiin on vahvistettu niin henkilöstön kouluttamisella kuin tietoteknisillä uudistuksilla, kuten pilviratkaisujen käytöllä.
LOGISTIIKKA JA LIIKENNE	Liikenteen- ja logistiikka-alan voimakkaan digitalisaation myötä on nähty tarve lisätä tietoturvaan liittyvää tiedonvaihtoa toimialalla.	L-ISAC aloitti toimintansa vuoden 2019 alussa, ja verkostotyö on käynnistynyt hyvin.

Verkko- ja tietoturvadirektiivi NIS: EU:n jäsenvaltiot raportoivat ensi kerran yhteiskunnalle merkittävistä tietoturvahäiriöistä

Vuosi 2019 oli ensimmäinen täysi kalenterivuosi verkko- ja tietoturvadirektiivin, tutummin NIS-direktiivin, voimaantulon (5/2018) jälkeen. Helmikuussa 2020 EU:n jäsenvaltiot raportoivat ensimmäisen kerran koko vuoden (2019) aikana tapahtuneet yhteiskunnalle merkittävät tietoturvahäiriöt. Raportoitua tietoa hyödynnetään kyberturvallisuuden kehittämisessä sekä kansallisesti että EU:ssa.

NIS-direktiivi asettaa yhteiskunnan kriittisen infrastruktuurin tarjoajille ja toimijoille minimivelvoitteita verkko- ja tietoturvajärjestelmien riskienhallintaan, tietoturvan seurantaan ja raportointiin. Velvoitteet on saatettu osaksi kansallisia toimialakohtaisia lakeja. Suomessa näitä velvoitteita ja niiden kohteena olevia toimijoita valvovat sektorikohtaiset viranomaiset. Ne myös raportoivat poikkeamat meille Kyberturvallisuuskeskukseen.

> Vuodelta 2019 Suomi raportoi yhden merkittävän tietoturvahäiriön terveydenhuollon sektorilta. Muita huomionarvoisia poikkeamia raportoitiin 8.

Kuluneelta vuodelta Suomi raportoi yhden merkittävän tietoturvahäiriön terveydenhuollon sektorilta. Tapahtuma liittyi kuntasektorille suunnattuun kyberhyökkäykseen ja tietomurtoon (lue lisää s. 36-37). Muita huomionarvoisia poikkeamia raportoitiin vuodelta 2019 kahdeksan. Kaikkiaan ne olivat hyvin samankaltaisia kuin vuoden 2018 tapahtumat, jotka koskivat Office 365 -aiheisia tietojenkalastelu-, murrettuja salasanoja ja luvattomia kirjautumisia järjestelmiin. Direktiivin ensimmäisen vajaan voimassaolovuoden 2018 ajalta Suomi ei raportoinut yhtään merkittävää tietoturvapoikkeamaa.

Toimimme Suomen yhteyspisteenä EU:n jäsenvaltioiden välisessä tiedonvaihdossa. Koordinoimme myös kansallista ja kansainvälistä yhteistyötä. Suomen sektorikohtaiset valvontaviranomaiset ovat järjestäytyneet NIS-yhteistyöverkostoksi, joka kokoontui vuonna 2019 neljä kertaa. Yhteinen sähköinen häiriöilmoituslomake on toimijoiden käytössä verkkosivuillamme. Viranomaistyöryhmässä on myös tuotettu toimijoille esitysmateriaaleja ja tiedotteita.

Häiriöilmoituslomake merkittävistä verkko- ja tietojärjestelmähäiriöistä yhteiskunnan kriittisten sektoreiden toimijoille: https://www.kyberturvallisuuskeskus.fi/fi/asioi-kanssamme/ilmoita-tietoturvapoikkeamasta-nis-ilmoitusvelvollisuus

Energia
Energiavirasto

- Sähkönjakeluverkon ja suurjännitteisen jakeluverkon haltijat
- Sähkön kantaverkonhaltija: Fingrid
- Maakaasun siirtoverkonhaltija: Gasum

Terveydenhuolto
Valvira

- Sosiaali- ja terveyspalvelujen antajat
- Lääkinnällisten laitteiden valmistajat
- SOTE-tietojärjestelmien valmistajat

Finanssiala
Finanssivalvonta

- Pankit
- Pankkien keskusyksiköt
- EU-pankkien sivuliikkeet

Finanssialan infrastruktuuri
Finanssivalvonta

- Pörssi: Nasdaq

Liikenne
Traficom

- **Ilmailu**: Air Navigation Services Finland, Finavia Helsinki-Vantaa lentokenttä
- **Merenkulku**: Vessel Traffic Services Finland Oy; Turun, Naantalin, HaminaKotkan ja Helsingin satamat
- **Rautatieliikenne:** Väylävirasto rataverkon haltijana, Finrail Oy
- **Maantieliikenne:** Tieliikennekeskus liikenteenohjausyhtiönä

Vesihuolto
Maa- ja metsätalousministeriö
ELY-keskukset

- Vesilaitokset: jotka toimittavat/vastaanottavat yli 5000m³/vrk vettä

Digi-infrastruktuuri
Traficom, Kyberturvallisuuskeskus

- Teleyritykset (DNS)
- Yhdysliikennepisteet (IXP)
- DNS nimipalveluiden tarjoajat
- .FI-maatunnusrekisteri

Digitaaliset palvelut
Traficom, Kyberturvallisuuskeskus

- Pilvipalvelut
- Hakukoneet
- Verkon keskitetyt markkinapaikat

Ei koske pieniä-/mikroyrityksiä

Tietoturvallisuus- ja häiriöraportointivelvoitteet koskevat energia-, liikenne-, finanssi-, ja terveydenhuoltoalan toimijoita sekä vesilaitoksia, jotka toimittavat/vastaanottavat vettä yli 5000 m³/vrk. Myös digitaalisten palveluiden tarjoajat eli pilvipalveluita, hakukoneita ja verkon markkinapaikkoja tarjoavat suuret ja keskisuuret toimijat ovat direktiivin säätelyn piirissä.

Rutinoitunut yhteistyö loi perustan rauhallisille vaaleille ja sujuvalle EU-puheenjohtajuuskaudelle

Varautuminen pitää pinnalla, vaikka vaalitulosten luotettavuus ei huolettaisi

Mennyt vuosi toi mukanaan kahdet vaalit – kansalliset eduskuntavaalit sekä Euroopan unionin eurovaalit. Ne ovat yksi demokratian peruspilareista. Vaalimme ovat ainakin yhdet maailman turvallisimmista, ellei turvallisimmat.

Turvallisuus on tunne, joka horjuu erilaisten uhkien ja riskien edessä. Siihen vaikuttaa muun muassa luottamus viranomaisten kykyyn ehkäistä turvallisuusuhkia. Esimerkiksi vaaliprosessiin luottaminen on tässä avainasemassa. Halusimme olla mukana turvaamassa luotettavia vaaleja muiden keskeisten vaaleihin liittyvien viranomaisten kanssa, jotta maailmalla nähty vaalihäirintä ei saisi jalansijaa Suomessa.

Ruotsissa tehtiin palvelunestohyökkäys vaalituloksia käsittelevään järjestelmään vuoden 2018 vaaleissa. Ranskassa murtauduttiin puolueen tietojärjestelmiin ja pyrittiin aiheuttamaan skandaali tietovuodon avulla vuonna 2017, Yhdysvaltojen 2016 presidentinvaaleista puhumattakaan.

Suomen eduskuntavaalien aikaan nähtiin yksi palvelunestohyökkäys, jota Keskusrikospoliisi tutkii epäiltynä törkeänä tietoliikenteen häirintänä. Muuten vaalihäirintä kohdistui yksittäisiin ehdokkaisiin.

Lähes häiriöttömien vaaliemme taustalla vaikutti tiivis viranomaisyhteistyö, jossa saimme olla mukana. Yhteistyön ansiosta muun muassa kunkin organisaation rooli mahdollisissa häiriötilanteissa sai selvät rajat. Jokainen tiesi, kehen ottaa yhteyttä, jos eteen tulisi ongelmia.

Suomi EU:n puheenjohtajana

Vaalit sujuivat mukavasti, mutta jo parin kuukauden hengähdyksen jälkeen alkoi pidempi ponnistus. Suomi toimi heinäkuusta joulukuuhun vuonna 2019 EU:n puheenjohtajamaana. Tämän puolivuotiskauden aikana järjestettiin useita ministeri- ja virkamieskokouksia Helsingissä, jolloin Suomi oli korostetusti ainakin eurooppalaisen median kiinnostuksen kohteena. Mahdollinen maineriski haluttiin minimoida. Kyberulottuvuuden turvaaminen tehtiin jälleen hyvässä yhteistyössä keskeisten viranomaisten kanssa.

Yksi ei muutu: yhteistyössä on voimaa

Vaalit ja EU-puheenjohtajuuskausi sujuivat yhteistyön näkökulmasta monella tapaa rutiinilla. ISAC-yhteistyönä tehtävä valtionhallinnon verkosto tarjoaa erinomaisen alustan luottamukselle myös erityistapauksissa, joissa Suomi on vahvemmin valokeilassa. Vuoden 2018 aikana tiivistetty yhteistyö presidentti Trumpin ja presidentti Putinin vierailua varten loi yhteisiä hyviä käytänteitä, joita hyödynnettiin myös vuonna 2019. Vaikka yhteistyötahot saattavat hieman vaihtua, yhteistyö ja luottamus auttavat kunkin varautumistoimen käynnistämisessä. Näin voidaan tarvittaessa reagoida yllättäviinkin normaaliolojen häiriötilanteisiin nopeasti.

Vaalihäirinnällä pyritään rapauttamaan kansalaisten luottamusta yhteiskuntaan ja sen perustana olevaan demokraattiseen järjestelmään ja päätöksentekoon. Vaalihäirintä voi liittyä myös laajempaan suunnitelmalliseen toimintaan tai hybridivaikuttamiseen.

Vaikuttamisella voidaan pyrkiä muun muassa ohjailemaan yhteiskunnallista keskustelua. Muualla maailmassa vaalihäirintää on havaittu kohdistuneen äänestysjärjestelmään, äänestäjiin, puolueisiin ja mediaan.

KYBERTURVALLISUUSKESKUS VARMISTAMASSA TURVALLISIA VAALEJA

Vuosi 2019 oli tietoturvan ja informaatioturvallisuuden näkökulmasta erityisen merkittävä vuosi suomalaiselle yhteiskunnalle. Vuonna 2019 Suomessa järjestettiin peräkkäin kahdet merkittävät vaalit. Lisäksi samana vuonna Suomi otti vastaan Euroopan Unionin puheenjohtajuuden.

Tapahtumissa turvallisuuden takaaminen yhteistyössä eri viranomaisten kanssa oli selvää ja erittäin tärkeää. Erilaiset signaalit maailmalta osoittivat, että myös Suomessa uhkiin sekä niiden toteutumiseen tulisi varautua. Jo ennen ensimmäisiä vaaleja viranomaiset aloittivat tiiviin yhteistyön, jotta vaalit voitaisiin Suomessa käydä vapaasti, ilman häiriöitä. Tiivis yhteistyö myös takasi, että viranomaiset voisivat jakaa tietoa eri toimijoiden kesken mahdollisimman nopeasti.

Keskusrikospoliisin näkökulmasta molemmat vaalit pystyttiin toteuttamaan ilman merkittäviä häiriöitä. Eduskuntavaalien alla vaalien online-tulospalvelu joutui voimakkaan palvelunestohyökkäyksen kohteeksi, jolloin tulospalvelujen verkkosivusto lakkasi hetkellisesti toimimasta. Tekoa voidaan jo tässä vaiheessa luonnehtia yksittäiseksi teoksi, eikä siinä ole nähtävissä laajempaa organisoitua toimintaa juuri vaaleja kohtaan. Palvelunestohyökkäyksen avulla ei ollut mahdollisuutta päästä vaikuttamaan vaalien lopputulokseen. Ilmiönä se on kuitenkin vakava, sillä se kohdistui vapaan demokraattisen yhteiskunnan merkittävään kulmakiveen.

Keskusrikospoliisin näkökulmasta varautuminen vaalien turvaamiseen oli riittävää ja panostus siihen varsin kannattavaa. Tieturvallisuuden näkökulmasta vaalit pystyttiin toteuttamaan varsin mallikkaasti, josta erityisesti voi kiittää kaikkien sen turvaamiseen osallistuneita tahoja.

Keskusrikospoliisin ja Kyberturvallisuuskeskuksen yhteistyön kannalta vuosi 2019 oli varsin vilkas. Panostimme muun muassa varoittavaan ja ennalta ehkäisevään toimintaan Office 365 -tietomurtoihin liittyen. Laajamittaisella tietojen vaihdolla ja tiedotuskampanjoilla lisättiin suomalaisten tietoisuutta ilmiöstä merkittävällä tavalla. Panostuksemme on noteerattu myös maailmalla. Keskusrikospoliisi jatkaa tietomurtojen tutkimista edelleen, mutta kansainvälisissä piireissä Suomi nauttii tällä hetkellä varsinkin tähän ilmiöön liittyen erityisen hyvää mainetta.

Marko Leponen
KRP

Suomessa vaalit ovat monella tavalla riippuvaisia tietojärjestelmistä ja niiden turvallisuudesta, vaikka äänestyslippu täytetään kynällä ja paperilla. Oikeusministeriön omistama vaalitietojärjestelmä, joka sisältää muun muassa äänioikeusrekisterin ja jonka kautta välitetään vaalien tulokset, on vaalien onnistumisen kannalta keskeinen.

Vaalihäirinnän vastaista työtä tehtiin ennen kevään 2019 eduskuntavaaleja ja europarlamenttivaaleja aiempaa tiiviimmin. Kyberturvallisuuskeskus otti aktiivisen roolin vaalien kyberturvallisuuden tilannekuvan muodostamisessa, viranomaisyhteistyön parantamisessa ja vaalitietojärjestelmän ylläpidon tukemisessa. Kyberturvallisuuskeskus kokosi Vaali-VIRT-viranomaisverkoston, johon kuuluivat kaikki vaalien kannalta keskeiset sidosryhmät. Verkosto harjoitteli yhdessä häiriötilanteiden hallintaa, vaihtoi tietoja ja ylläpiti vaalien aikana tilannekuvaa yhteisillä tilannekatsauksilla.

Oikeusministeriön näkökulmasta Kyberturvallisuuskeskuksen panos vaalien turvaamiseen oli keskeinen. Viranomaisyhteistyön fasilitointi tuotti konkreettisia tuloksia. Kyberturvallisuuskeskuksen asiantuntijat tunnistivat keskeiset toimijat, auttoivat kansainvälisen tilannekuvan luomisessa ja tukivat yhteistyötä.

Heini Huotarinen
OM

Harjoittelemalla kyberturvallisuus hallitaan paremmin

Hankkeesta osaksi peruspalveluita

Harjoitustoiminnan tuesta on vuoden 2019 aikana tullut osa peruspalveluitamme. Huoltovarmuuskeskuksen rahoittaman KYBER 2020-hankkeen yhteydessä käynnistetty suunnittelutyö on tuottanut uuden keskeisen osan palvelupakettiimme. Harjoitustoiminta yhdessä muiden palveluiden kanssa auttaa meitä palvelemaan yhteiskunnan kyberturvallisuutta yhä monipuolisemmin. Harjoitustoiminnan tukemme keskittyy palvelemaan pääasiassa huoltovarmuuskriittisiä organisaatioita opastamalla ja tukemalla harjoitustoimintaan liittyvissä asioissa.

Harjoittelun avulla organisaatio kehittää toiminta-valmiuksia ja reaktio- sekä palautumiskykyä ja siten pienentää häiriöistä ja hyökkäyksistä aiheutuvia haittavaikutuksia. Harjoituksiin osallistuminen on pitkään ollut osa toimintaamme. Osallistumalla harjoituksiin ja simuloimalla niissä omia palveluitamme olemme kehittäneet omaa toimintaamme ja auttaneet muita organisaatioita harjoittelemaan todentuntuisesti. Harjoitustoiminnan tukitoiminnon tarkoituksena onkin jakaa tämä osaaminen myös muiden kriittisten toimijoiden tietoisuuteen.

Vuosi 2019 toi mukanaan runsaasti kyberharjoituksia, joiden avulla yritykset kohensivat omaa varautumistaan ja kyvykkyyttään. Saamamme palautteen perusteella harjoitustoiminnan tukipalvelu koettiin hyödylliseksi ja tarpeelliseksi myös jatkossa. Vuosi 2019 näytti, että huoltovarmuuskriittisten organisaatioiden halukkuus parantaa omia kybervalmiuksiaan harjoittelun keinoin on lisääntynyt. Tukemiemme harjoitusten määrä onkin kasvanut tasaisesti vuodesta 2016 alkaen.

Kyberharjoitusohje ja harjoitusskenaariot 2020

Vuonna 2019 julkaisimme Kyberharjoitusohjeen, johon kokosimme keskukseemme kerääntyneet opit ja kokemukset kymmenistä kyberharjoituksista, niiden suunnittelusta, pelaamisesta sekä tulosten analysoinnista. Ohjeen avulla organisaatio voi suunnitella alusta loppuun kyberharjoituksen joko yksin tai asiantuntevan kumppanin kanssa.

Vuoden 2019 lopulla järjestimme myös Kyberharjoitusskenaariot 2020 -työpajan. Työpajaan osallistui keskeisten tietoturva-alalla toimivien yritysten edustajia ja viranomaisia. Työpajan tuloksena syntyi 20 harjoitusskenaariota organisaatioiden harjoittelun tueksi. Skenaariot ovat kaikkien saatavilla verkkosivuillamme.

Jatkamme harjoitustoiminnan kehittämistä

Jatkamme huoltovarmuuskriittisten organisaatioiden harjoitustarpeiden kartoittamista ja tunnistamista myös tulevina vuosina. Jokavuotisen kyselyn avulla kartoitetaan organisaatioiden toiveita ja haasteita sekä seurataan muutoksia harjoittelukyvykkyydessä ja -halukkuudessa. Kartoituksen avulla tulemme jatkossakin olemaan yhteydessä kohdeorganisaatioihin ja tuemme aktiivisesti organisaatioiden kyberharjoittelua.

Huoltovarmuuskriittisille organisaatioille kohdistuvien harjoitustukitoimien lisäksi isot yhteisharjoitukset, kuten TAISTO-, TIETO-, KYHA ja Cyber Europe, tuovat yhteen useita huoltovarmuuskriittisiä sekä muita organisaatioita.

FINEST19-harjoitus toi Viron ja Suomen tietoturvaviranomaiset yhteen

Maaliskuussa harjoittelimme yhdessä Viron CERT-EE-tietoturvaviranomaisen kanssa kriittisen infrastruktuurin kyberhäiriötilannetta FINEST19-harjoituksessa. Harjoitus oli ensimmäinen suunnittelemamme ja järjestämämme Suomen ja Viron CERT-tiimien kansainvälinen yhteisharjoitus. Harjoitus toteutettiin yhteistyössä Suomen kantaverkkoyhtiö Fingridin ja Viron kantaverkkoyhtiö Eleringin kanssa.

Harjoittelimme molempia maita koskevan kyberkriisin yhteistä selvittämistä kriittisessä infrastruktuurissa. Harjoituksen painopisteenä oli erityisesti tehokas ja turvallinen viestintä sekä yhteisen, jaetun tilannekuvan luominen. Harjoituksen skenaario keskittyi sähkönjakelun häiriöön, ja siinä oli myös kyberrikollisuutta käsittelevä näkökulma.

Harjoitustoiminnan tuki auttaa kyberharjoituksissa seuraavilla tavoilla:

- harjoituksen suunnittelun käynnistäminen
- sopivan harjoitusyhteistyökumppanin löytäminen
- skenaariosuunnittelun tuki
- kyberturvallisuuskeskuksen palveluiden simulointi harjoituksessa
- havainnoijan rooli harjoituksessa
- avustaminen harjoituksen jälkianalyysissa.

Tulevaisuustyö ja toiminnan kehittäminen

Tietoturvamerkin voi saada IoT-kuluttajalaite, jonka perustietoturva on kunnossa

Tietoturvamerkki auttaa kuluttajia tunnistamaan myymälässä ja verkkokaupassa tietoturvalliset laitteet ja tekemään tietoturvallisia hankintoja. Merkki myös lisää kuluttajien tietoisuutta siitä, miten älylaitteita käytetään turvallisesti. Tietoturvamerkin avulla kannustamme yrityksiä sisällyttämään laitteisiinsa tietoturvaominaisuuksia heti tuotesuunnittelun ensimetreistä lähtien

Myönsimme ensimmäisenä Tietoturvamerkin kolmelle eri tuotteelle: Polar Ignite -fitnesskellolle, Cozify Hub -älykotiratkaisulle sekä DNA:n Wattinen-älytermostaattipalvelulle. Pilottikumppaniyrityksemme Polar Electro Oy, Cozify Oy ja DNA Oyj ovat kiinnittäneet jo ennen Tietoturvamerkin hankkimista erityistä huomiota laitteidensa tietoturvallisuuteen. Tämä kyvykkyys yhdistettynä haluun viestiä tietoturvan merkityksestä sidosryhmille olivat keskeisiä tekijöitä pilottikumppaneiden valinnassa.

Tietoturvamerkki näyttämässä suuntaa älylaitteiden eurooppalaisille standardeille

Jotta laite tai palvelu voi saada Tietoturvamerkin, sen pitää täyttää todennetusti asettamamme vaatimukset. Ne perustuvat pääasiassa vielä luonnosvaiheessa olevaan eurooppalaiseen standardiin ETSI EN 303 645 Cyber Security for Consumer Internet of Things. Osallistumme aktiivisesti standardin kehittämiseen, millä pyrimme varmistamaan yhteensopivuuden mahdollisten myöhemmin voimaan tulevien yleiseurooppalaisten vaatimusten kanssa. Näin helpotetaan esimerkiksi IoT-laitteita valmistavien suomalaisyritysten siirtymistä kansainvälisille markkinoille.

IoT:n sertifiointi on herättänyt – ja herättää yhä – laajaa kiinnostusta. Aihetta on pohdittu myös EU:n kesäkuussa 2019 asettaman kyberturvallisuuden sertifiointijärjestelmän yhteydessä. Valmistuessaan ETSIn standardia pidetään yhtenä mahdollisena pohjana IoT-sertifioinneille. Sertifiointijärjestelmän käynnistämistä valmisteleva viranomaisryhmä on ollut kiinnostunut Tietoturvamerkistämme, ja kokemuksiamme pyritään hyödyntämään myös eurooppalaisen sertifioinnin kehitystyössä.

Televisiostakin tuttu, verkkosivuilta lisätietoja

Tietoturvamerkki julkistettiin 26.11.2019. Teimme merkkiä tunnetuksi televisio- ja somekampanjoin. Kun kuluttajat oppivat tuntemaan Tietoturvamerkin ja merkin saaneiden laitteiden tarjonta lisääntyy, voimme olla tyytyväisiä Tietoturvamerkin vaikuttavuuteen. Lisätietoa muun muassa Tietoturvamerkin vaatimuksista ja sen hakemisesta saat osoitteessa www.tietoturvamerkki.fi

Vaikka Tietoturvamerkki on tarkoitettu kuluttajalaitteille ja -palveluille, myös yritysratkaisuja tarjoavat valmistajat ovat olleet kiinnostuneita siitä. Auditointien kustannukset ja niihin käytetty aika ovat herättäneet keskustelua siitä, pitäisikö merkistä tehdä myös itsearviointiin perustuva versio.

Tulemme tarkastelemaan kehitysmahdollisuuksia ja hiomaan Tietoturvamerkki-konseptia kokemustemme perusteella. Jatkamme myös eurooppalaisten vaatimusten kehityksen seuraamista. Niiden mahdollisesti muuttuessa meillä on valmiudet päivittää myös omat vaatimuksemme. Näin voimme parhaiten tukea suomalaisyritysten kansainvälistymistä.

Tietoturva

Nimipalvelun tietoturvalaajennuksen käyttö laajeni merkittävästi

Turhan harvat mukana - maksuton palvelu tarjolla jo vuodesta 2011

Suomen FI-juurinimipalvelussa DNSSEC otettiin käyttöön vaiheittain 2010-luvun alussa. FI-juuren DNSSEC-allekirjoituksen lisäksi tarjosimme fi-verkkotunnusten käyttäjille DNSSECin käyttömahdollisuutta maksutta.

Palvelun varhaisesta käyttöönotosta, maksuttomuudesta ja monista DNSSEC- kampanjoista huolimatta, DNSSECin käyttö ei juuri lisääntynyt Suomessa.

Vuoden 2019 alkuun mennessä fi-verkkotunnuksia jälleenmyyvät verkkotunnusvälittäjät eivät käytännössä tarjonneet DNSSECiä asiakkailleen lainkaan. Fi-tunnuksista vain noin 5 000 oli DNSSEC-suojattuja. Noin 7% Suomen internetliikenteestä kulki DNSSECiä validoivien nimipalvelinten kautta.

Kampanja lisäsi DNSSECin käyttöä ilahduttavan paljon

Alkuvuodesta 2019 kävimme keskusteluja sidosryhmiemme kanssa, ja syntyi ajatus järjestää kansallinen DNSSECin käyttöönottopäivä, DNSSEC Launch Day. Sen ajatuksena oli koota yhteen DNSSECin käyttöön sitoutuvat verkkotunnusvälittäjät ja internetyhteyspalvelujen tarjoajat, pitää näistä yllä julkista listaa sekä tuoda julkiseen keskusteluun DNSSECin tarpeellisuus.

Käytöönottopäiväksi sovittiin 5. syyskuuta 2019. Kampanjaan osallistui 33 verkkotunnusvälittäjää sekä 3 internetpalveluntarjoajaa.

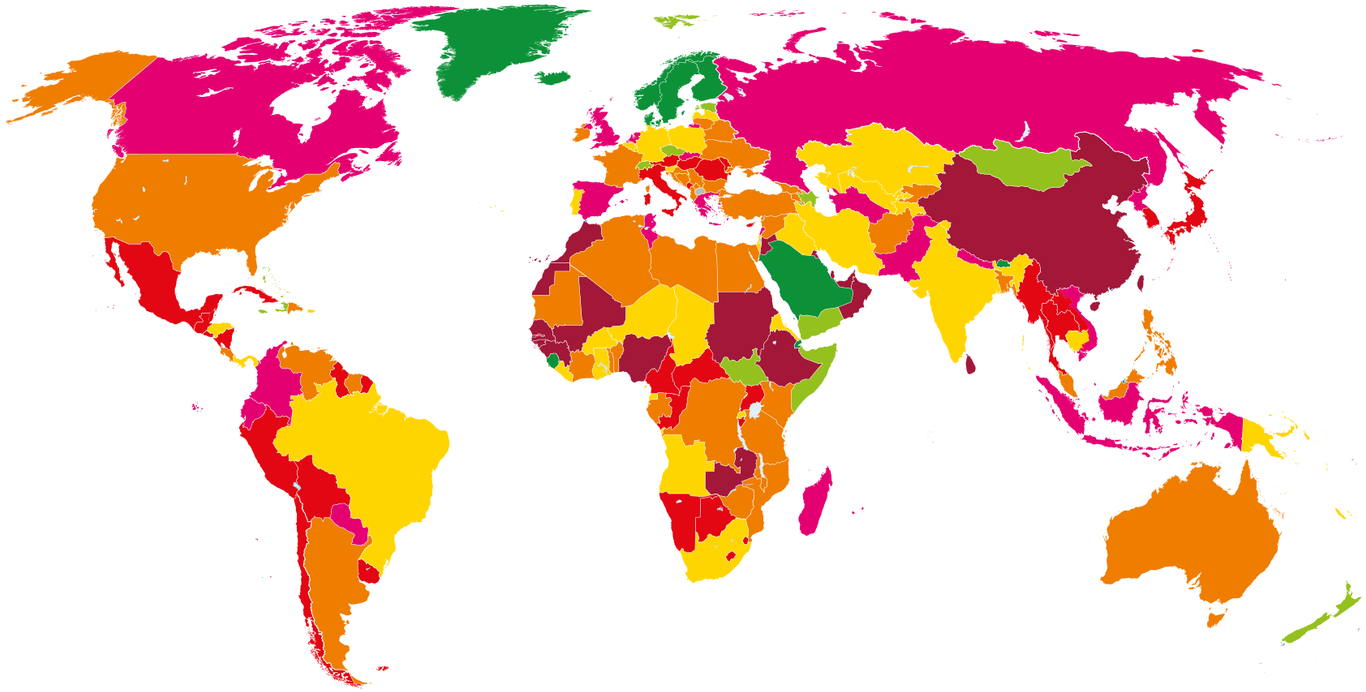
DNSSECiä tarjoavien verkkotunnusvälittäjien määrä kasvoi merkittävästi. Vuoden 2019 lopulla DNSSECiä tarjosi asiakkailleen jo yli 250 fi-verkkotunnusvälittäjää, ja DNSSEC-allekirjoitettuja fi-verkkotunnuksia lähes 10 000. Luku on kaksinkertainen vuoteen 2018 verrattuna.

DNSSEC-validointiaste nousi vuoden aikana 7 prosentista yli 90 prosenttiin suurten kotimaisten internetyhteyspalveluntarjoajien otettua validoinnin käyttöön resolverinimipalvelimissaan. Maailmanlaajuisestikin vertailtuna saavutettu validointiaste on korkea.

Domain Name Security Extensions (DNSSEC) on tekniikka, jolla varmistetaan nimipalvelun antaman vastauksen aitous ja muuttumattomuus. DNSSECin avulla on mahdollista todentaa nimipalvelun antaman vastauksen tai resolverinimipalvelimen välimuistin väärentäminen. DNSSEC on yksi keskeisimmistä tietoturvaominaisuuksista, joilla varmistetaan esimerkiksi, että käyttäjän avaaman www-sivun osoite ja sisältö vastaavat toisiaan ja että sähköposti päätyy osoitteen mukaiselle vastaanottajalle.

Verkkotunnuksen suojaaminen DNSSECillä ei kuitenkaan ole riitä, jotta se hyödyttäisi internetin käyttäjää. DNSSEC-allekirjoitus on myös todennettava internetliikenteestä, muutoin internetin käyttäjälle päätyvät myös ne DNS:n vastaukset, joissa DNSSEC-allekirjoitus on viallinen. Todentamisesta eli validoinnista ovat vastuussa resolverinimipalvelimet, joita tyypillisesti ylläpitävät internetyhteyksien tarjoajat.

DNSSEC Validation Rate by country (%)



LUKUJA

265 DNSSECiä asiakkailleen tarjoavien fi-verkkotunnusvälittäjien lukumäärä (kpl):

10 255 DNSSEC-suojattujen fi-verkkotunnusten lukumäärä (kpl):

92,2% DNSSEC-validointiaste Suomessa:

Työ 5G-verkkojen tietoturvallisuuden varmistamiseksi jatkuu

Vuonna 2018 5G-verkkojen kyberturvallisuusselvityksestä alkanut työ sai jatkoa. Vuonna 2019 selvitystä seurasivat kansallinen ja EU-tasoinen 5G-riskiarvio.

Nyt EU tekee töitä 5G-verkkojen riskienhallintaa tukevan työkalupakin kehittämiseksi. Työn tuloksena syntyy tietoa, jonka avulla 5G-teknologiaa tarjoavat ja käyttävät toimijat kykenevät tekemään realistisia riskiarvioita ja rakentamaan turvallisia ratkaisuja.

Osana työtä on tunnistettu, että 5G-teknologiaan siirtyminen tuo mukanaan suuremman paradigmamuutoksen kuin yksikään aikaisempi matkaviestinverkkosukupolvi on tuonut. 5G-teknologian uusien ominaisuuksien ja toimintamallien käyttöönotto muuttaa operaattoreiden roolia, se tuo mukanaan paikallisiin tarpeisiin räätälöidyt verkot, saattaa laajentaa viranomaisohjauksen toimintakenttää ja tuo täysin uudenlaisia riskienhallintavaatimuksia 5G:n ominaisuuksia hyödyntäville toimijoille. Verkko muuttuu tiedonsiirtoputkesta yhä enemmän jaetuksi tietojenkäsittelyn ja tietojen tuottamisen alustaksi, jossa verkon reunojen rajat hämärtyvät. Tämä mahdollistaa uusia toiminnallisuuksia ja mahdollisuuksia, joita myös yhteiskunnan kriittisiä toimintoja tarjoavat toimijat tulevat hyödyntämään. Samalla yhä tärkeämmät yhteiskunnan toiminnot tulevat lepäämään 5G-verkkojen varassa.

Muutos aiemmista verkkosukupolvista kohti 5G-maailmaa tulee vaatimaan tiedon aktiivista jakamista, viranomaisohjauksen rajojen uudelleentarkastelua ja yhä laajempaa vuoropuhelua eri toimijoiden välillä sekä lopulta myös uudenlaisia viranomaismääräyksiä. Kansainvälisesti oman haasteensa 5G:n tietoturvamaisemaan tuovat myös maakohtaiset ja EU-laajuiset suositukset, lait ja säädökset.

Teoreettisen lähestymisen lisäksi halusimme edistää EU-tasoisena yhteistyönä myös 5G-teknologian ympärille rakentuvan tietoturvallisuusekosysteemin teknistä osaamista. Tuodaksemme hakkeri- ja tietoturvallisuustestausyhteisöä, laitevalmistajia, Kyberturvallisuuskeskusta ja tiedemaailmaa lähemmäs toisiaan, järjestimme 29.11.-1.12.2019 2019 Oulun yliopiston, Ericssonin ja Nokian kanssa yhteistyössä 5G Cyber Security Hackathonin, joka on ensimmäinen 5G:n tietoturvallisuuteen keskittynyt hackathon-tapahtuma maailmassa.

Hackathoniin osallistui lähes 100 hakkeria yli 10 eri maasta, ja se tarjosi ainutlaatuisen tilaisuuden kaikille osapuolille uuden oppimiseen. Tuloksien analysointi on kesken ja hackathonin oppeja tullaan jakamaan ja kokemuksista keskustellaan digitaalisen maailman päätöksentekijöiden kanssa 5G leading Edge Forumissa 13. helmikuuta 2020.

KYBER 2020 ja Digitaalinen turvallisuus 2030

Takana on aktiivinen toimintamme kehitysvuosi. Esimerkiksi verkostojohtamista (ISAC-toiminta) ja harjoitustoimintaa paransimme Huoltovarmuuskeskuksen KYBER 2020 -ohjelman mukaisesti. Myös HAVARO -palvelun kehitystyössä etenimme ratkaisevasti. Asiakaspalautteen perusteella kehittämistyömme on koettu tarpeelliseksi.

Lisää tukea huoltovarmuuskriittisille yrityksille

Juuri huoltovarmuuskriittisille yrityksille toimintamme kehitys on näyttäytynyt uusina palveluina ja kyvykkyyksinä sekä entistä toimivampana yhteistyönä. Yhdessä Huoltovarmuuskeskuksen kanssa olemme rakentaneet luottamusta muun muassa osallistumalla sektori- ja poolikohtaiseen kyberturvallisuuden kehittämiseen.

Vahvaa kansallista kyberturvallisuutta rakentamassa

Huoltovarmuuskeskuksen KYBER 2020 -ohjelma saa jatkoa Digitaalinen turvallisuus 2030 -ohjelmalla, jonka suunnittelutyö aloitettiin vuonna 2019.

Digitaalinen turvallisuus 2030 -ohjelman tarkoituksena on kehittää kansallista kyberturvallisuutta aiempaa syvemmin ja suuremmalla joukolla. Olemme olleet tiiviisti mukana ohjelman suunnittelussa, johon on kutsuttu mukaan myös elinkeinoelämä ja poolitoiminta.

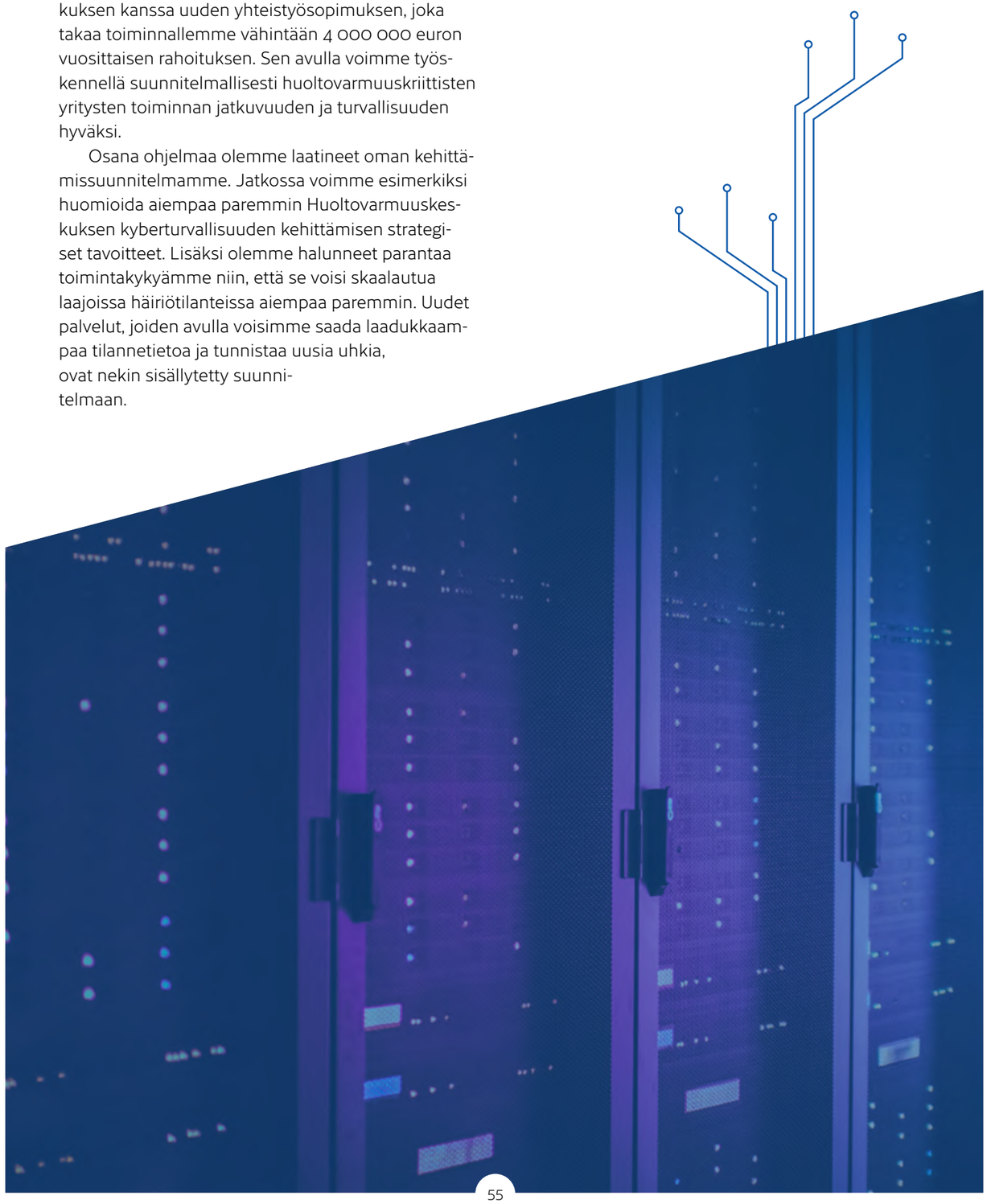
Vuonna 2019 ohjelma sai strategisen tavoitteen, keskeiset sisällöt ja toimintatavat, joiden avulla tavoitteet saavutetaan. Ohjelmaa viedään eteenpäin ketterän kehitysmallin mukaisesti, ja siihen halutaan sitouttaa niin elinkeinoelämä kuin viranomaisetkin.

Uusi yhteistyösopimus antaa kauaskantoisia mahdollisuuksia

Kuluneena vuonna solmimme Huoltovarmuuskeskuksen kanssa uuden yhteistyösopimuksen, joka takaa toiminnallemme vähintään 4 000 000 euron vuosittaisen rahoituksen. Sen avulla voimme työskennellä suunnitelmallisesti huoltovarmuuskriittisten yritysten toiminnan jatkuvuuden ja turvallisuuden hyväksi.

Osana ohjelmaa olemme laatineet oman kehittämissuunnitelmamme. Jatkossa voimme esimerkiksi huomioida aiempaa paremmin Huoltovarmuuskeskuksen kyberturvallisuuden kehittämisen strategiset tavoitteet. Lisäksi olemme halunneet parantaa toimintakykyämme niin, että se voisi skaalautua laajoissa häiriötilanteissa aiempaa paremmin. Uudet palvelut, joiden avulla voisimme saada laadukkaampaa tilannetietoa ja tunnistaa uusia uhkia, ovat nekin sisällytetty suunnitelmaan.

Huoltovarmuuskeskus on meille luotettava yhteistyökumppani, joka myös tukee toimintaamme ja sen kehittämistä.



Tervetuloa uudistetun HAVARO-palvelun asiakkaaksi!

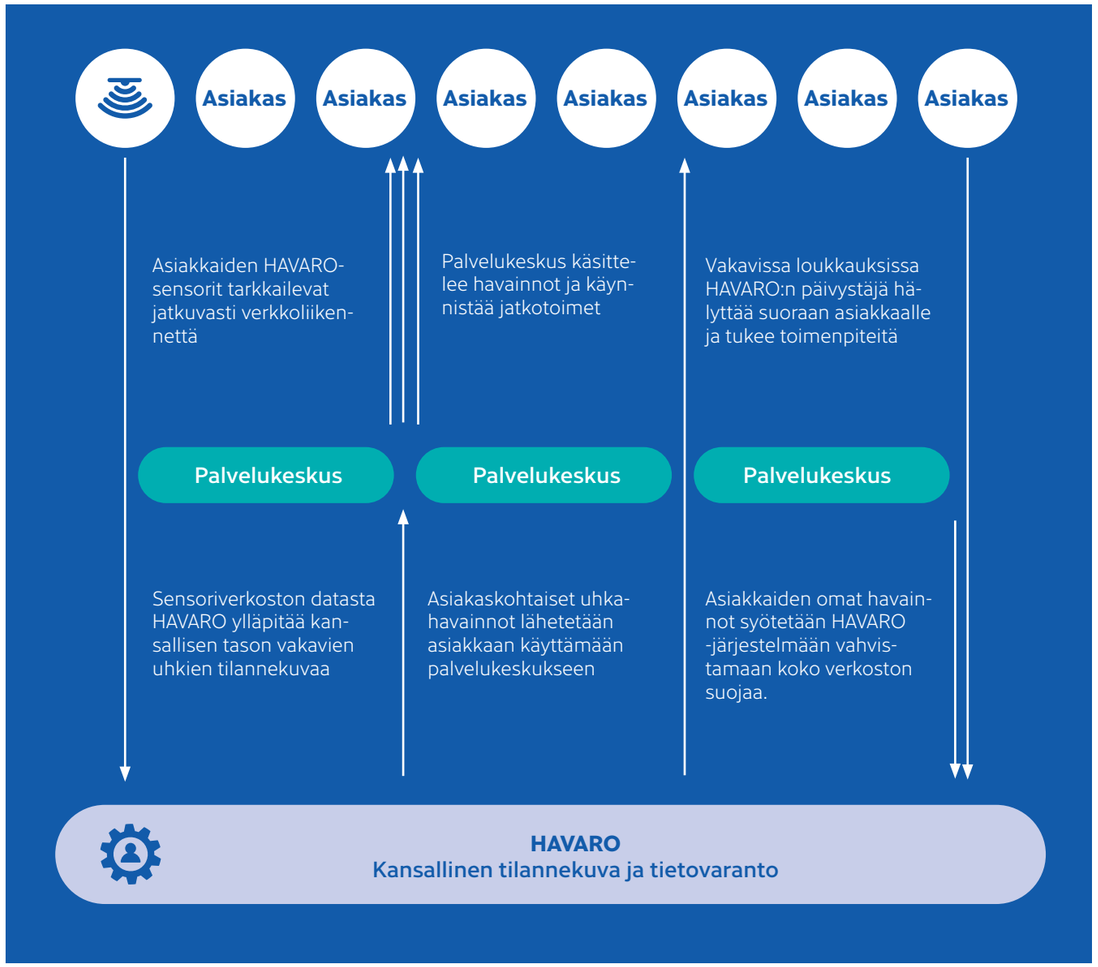
HAVARO-palvelumme varoittaa asiakkaita heihin kohdistuvasta haitallisesta liikenteestä ja tekee mahdolliseksi tietoturvauhkien torjumisen. Asiakkaina on nyt huoltovarmuuskriittisiä yrityksiä ja valtionhallinnon organisaatioita. Haitallista liikennettä hyödyntämällä ulkopuolinen toimija voi esimerkiksi päästä käsiksi asiakkaan liikesalaisuuksiin tai aiheuttaa taloudellisia menetyksiä asiakkaan rahaliikenteeseen vaikuttamalla.

HAVARO-palvelun uudistaminen aloitettiin vuonna 2017 osana Huoltovarmuuskeskuksen KYBER 2020 -hanketta. Uusi palvelu etenee tuotantovaiheeseen vuoden 2020 aikana.

Palvelun hankkiminen helpottuu

HAVARO tulee suomalaisten organisaatioiden saataville kesällä 2020, kun palvelu liittyy osaksi tietoturvapalveluita tarjoavien kaupallisten palvelukeskusten (SOC) valikoimaa.

Uusi palvelumalli korvaa vuodesta 2011 tuottamamme HAVAROn viranomaisversion. Kyberturvallisuuskeskuksen ja kaupallisten tietoturvatoimijoiden yhteistyöhön perustuva HAVARO tulee vastaamaan aiempaa kokonaisvaltaisemmin ja tarkemmin asiakkaiden tarpeisiin.



HAVARO-palvelumalli

Tulevaisuuden tarpeet

Uuden palvelun suunnittelussa ja toteutuksessa olemme huomioineet myös tulevaisuuden kehitystarpeet ja vaatimukset. Hankkeen aikana olemme käyneet lukuisia rakentavia keskusteluja sekä asiakkaidemme että muiden sidosryhmiemme kanssa. Olemme saaneet arvokasta palautetta ja kehitysideoita monissa työpajoissa ja yhteisissä tilaisuuksissa.

Yhteistyökumppanimme palvelun kehittämisessä on Reaktor Innovations Oy. Ketterän ohjelmistokehityksen menetelmillä uusi järjestelmä ja sen sovelluskomponentit on saatu hyvissä ajoin testattaviksi ja vaiheittain tuotantoon.

Uusille yhteistyökumppaneille on tilaa

Vuoden 2019 aikana HAVAROn uusi palvelu- ja toimintamalli tarkentui yhteistyössä palvelukeskusten kanssa. Selkeytimme palvelun ehtoja, jotka tekevät mahdolliseksi HAVARO-palvelun tarjoamisen laadukkaalla, mutta eri asiakastarpeisiin vastaavalla tavalla.

Myös uudet yhteistyökumppanit ovat tervetulleita HAVARO-palvelun muodostamaan ekosysteemiin. Otamme mielellämme mukaan esimerkiksi palvelukeskustoimijoita ja teknologiatoimittajia. Tervetuloa rakentamaan suomalaista kyberturvallisuuden peruspilaria!

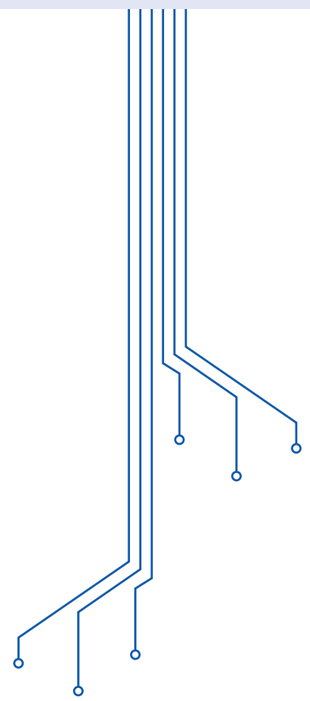
Haavoittuvuuskoordinaatio

Kuluneen vuoden haavoittuvuuskoordinaation tärkein tapaus liittyi Fidelix-merkkisiin rakennusautomaatiolaitteiden haavoittuvuuksiin.

Maaliskuussa 2019 Ylen julkaisemassa Team Whack -ohjelmasarjassa ryhmä hakkereita testasi Fidelix-merkkisiä rakennusautomaatiolaitteita ja löysi niistä useita haavoittuvuuksia. Koordinoimme näiden haavoittuvuuksien korjausta ja tiedotusta laitteiden omistajille. Tiedotustyöstämme huolimatta internetiin avoimien ja suojaamattomien laitteiden määrät vähenivät hitaasti kolmansien osapuolten hallinnoimia laitteita lukuun ottamatta.

Internetiin näkyvät avoimet rakennusautomaatiolaitteet ovat esiintyneet kotimaisten tietoverkkojen tietoturvakartoituksissamme jo vuosia. Rakennusautomaatiolaitteiden heikkouksien avulla hyökkääjät voisivat aiheuttaa vahinkoa rakennusten käyttäjille. Laitteiden omistajien tavoittaminen on kuitenkin ollut hankalaa, siksi avoimien laitteiden määrä ei ole juuri vähentynyt.

Haavoittuvuuskoordinaatiomme auttaa haavoittuvuuden tai vakavan ohjelmistovirheen löytäjää tekemään yhteistyötä esimerkiksi ohjelmistovalmistajien kanssa. Käsittelemme haavoittuvuustietoja aina vastuullisesti. Tavoitteenamme on, että tieto haavoittuvuudesta ja sen asianmukaisesta korjauksesta päivityksineen päätyy kaikille tietoa tarvitseville, myös tuotteen loppukäyttäjille. Pyrimme siihen, että mahdollisimman moni merkittävä haavoittuvuus myös korjataan ja korjaukset otetaan käyttöön.



Toimintamme tunnuslukuja

Lukujen perusteella vuosi 2019 oli meille työntäyteinen. Haitallisten sivujen alasajot ja tiedonvaihtoryhmien tilaisuudet pitivät meidät liikkeessä, mutta muutoin kulunut vuosi noudatteli edellisvuoden tahteja.

24/7/365
KATKEAMATON PÄIVYSTYS

2
VAROITUKSET

83208
AUTO-REPORTER

4500
KÄSITELLYT TAPAUKSET "TIKETTI"

25
HAAVOITTUVUUS-KOORDINAATION KÄSITTELEMÄT TAPAUKSET

4500
HAITALLISTEN SIVUSTOJEN ALASAJOT

5500
FACEBOOK-SEURAAJAT

11000
TWITTER-SEURAAJAT

HÄIRIÖMÄÄRÄT:

7
KRIITTISET HÄIRIÖT

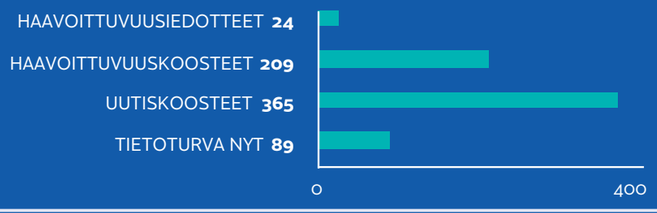
18
VAKAVAT HÄIRIÖT

43
MERKITTÄVÄT HÄIRIÖT

68
KAIKKI HÄIRIÖT YHTEENSÄ

Tilaisuudet ja harjoitukset

Viestintä ja tiedotteet



Toteutimme vuoden aikana asiakastyytyväisyyskyselyt tilannekuvatuotteisiimme ja tiedonvaihtoryhmiimme liittyen. Kyselyidemme arviointiskaala oli huonosta (1) kiitettävään (5).

Toimialakohtaiset tiedonvaihtoryhmät arvioitiin hyödyllisiksi. Erityisen tärkeäksi koettiin tiedonvaihdon mahdollistaminen ja verkostoituminen.

Tilannekuvatuotteisiimme ollaan tyytyväisiä

4,2
KESKIARVO

Kysely toimialojen tiedonvaihtoryhmille

4,4
ARVOSANA

KYBERSÄÄ 2019 JA KATSE KYBERVUOTEEN 2020

”Kyberrikollisuuden luonnetta ei tunneta riittävästi. Suurin osa kyberrikollisuudesta on opportunistista, kansainvälistä ja automatisoitua. Kun henkilö tai organisaatio arvioi omaa riskiään joutua tietoturvapoikkeaman kohteeksi, oletetaan että on oltava hyökkääjää kiinnostava kohde, vaikka tyypillisesti kohteeksi päädytään sattumanvaraisesti.

10 tietoturvanäkymää vuodelle 2020

Vuoden 2020 tietoturvanäkymät perustuvat Kyberturvallisuuskeskuksen ja yhteistyöverkostojemme yhteisarvioon. Osuimmeko näkymissämme oikeaan, se nähdään loppuvuodesta 2020.

1 Automatisoidut ja tekoälyä hyödyntävät tietoturvaratkaisut kehittyvät

Tarjonnan lisääntyessä myös muun muassa SOC-palveluiden käyttö monipuolistuu ja kasvaa.

2 Palveluja tuotetaan monikerroksisissa ja -kansallisissa alihankintaketjuissa

Ulkoistusvaiheessa on oleellista selvittää ja täsmentää tietoturvan kannalta olennaiset komponentit, riippuvuussuhteet ja vastuut. Jälkeenpäin muutokset ovat usein haastavia, etenkin jos puutteet tulevat esiin vasta poikkeamatilanteissa. Samat ongelmat koskevat niin yksityisiä kuin julkisia organisaatioita. Palvelujen häiriöillä voi olla myös yhteiskunnan toimintaa häiritseviä vaikutuksia.

3 Kyberturvallisuuden vaikutus liiketoimintaan huomioidaan aiempaa paremmin

Liiketoiminta on riippuvaista digitaalisuudesta. Siihen liittyvät riskit pitää sisällyttää riskienhallinnan toimenpiteisiin rutiininomaisesti. Tilanteeseen on herätty, mikä näkyy esiin nousseina tarpeina tietoturvan toimintaan liittyville riskilähtöisille tarkastelumalleille.

4 Suojautuminen ontuu, koska kyberrikollisuuden luonnetta ei tunneta riittävästi

Suurin osa kyberrikollisuudesta on opportunistista, kansainvälistä ja automatisoitua. Kun henkilö tai organisaatio arvioi omaa riskiään joutua tietoturvapoikkeaman kohteeksi, oletetaan että on oltava hyökkääjää kiinnostava kohde, vaikka tyypillisesti kohteeksi päädytään sattumanvaraisesti.

5 Kyberturvallisuuden harjoittelu lisääntyy

Toiminta on usein hyvin suunniteltua, mutta tositilanteessa hätäily ja kaaos voi yllättää. Tilanteen korjaamiseksi yhä useampi organisaatio harjoittelee häiriötilanteissa toimimista ja kehittää toimintaansa muun muassa havaittuihin puutteisiin perustuen.

6 Löydettyjä tietoturva-aukkoja hyödynnetään yhä nopeammin

Rutiinimaiset päivitysten julkaisu- ja päivitysprosessit eivät enää yksin riitä. Ohjelmistopäivitysten tueksi on otettava uudenlaisia suojautumisratkaisuja, joilla voidaan parantaa havainnointia.

7 Monipuolisten tietoturvaosaajien tarve kasvaa

Tietoturvan teknisten asiantuntijoiden osaaminen on eriytymässä eri osa-alueisiin. Osaajien joukkoon tarvitaan myös henkilöitä, joilla on liiketoimintaymmärrystä ja muun muassa hankintoihin liittyvää ei-teknistä osaamista.

8 Tiedot ja toiminta siirtyvät pilveen

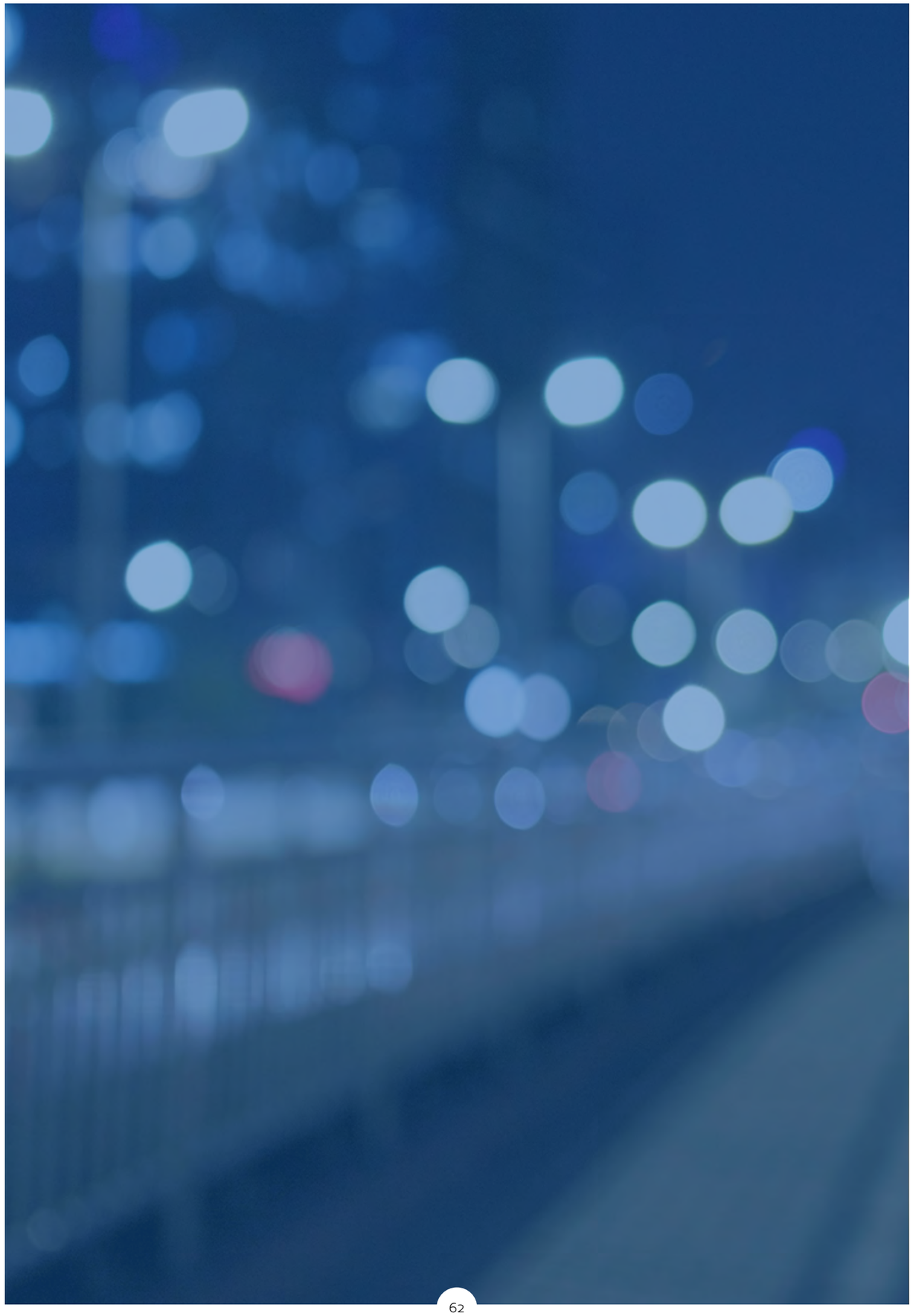
Pilvipalvelut monipuolistuvat. Pelkän tallennustilan sijaan pilvipalveluissa tarjotaan keskitettyjä toiminnallisuuksia, jotka ovat perinteisesti toteutettu omassa verkossa. Entistä merkittävämmäksi nousee kysymys palveluja käyttöönotettaessa: Onko vastuunjako pilvipalvelutoimittajan ja organisaation välillä selvä?

9 Tietoturva-arviointien suosio lisääntyy tietoisuuden noustessa.

Tietoturvaosaamisen ja -tason varmistaminen nousee entistä merkittävämmäksi. Sen osoittaminen esimerkiksi asiakkaille helpottuu, kun arvio on ulkopuolisen tekijän toteuttama.

10 Tietoturvan taso on sidoksissa henkilöstön valveutuneisuuteen

Organisaatioissa tietoturvallisuuden vahvuudet ja heikkoudet tulevat esiin henkilöstön kautta. Yksittäinenkin työntekijä voi torjua esimerkiksi tietojenkalastelua, laskutuspetoksia tai haittaohjelmia sisältäviä sähköposteja. Koulutuksiin ja harjoituksiin kannattaa panostaa!



Miten onnistuimme arvioimaan menneen vuoden tietoturvanäkymiä?

Arviomme pitivät hyvin! Kaikki näkymämme pysyivät ruodussa.

Oikein!

Pilvipalveluiden käytön lisääntymiseen ja uusien teknologioiden sekä niihin liittyvien haasteiden esiinmarssiin olimme varautuneet. Tarjonnan lisääntyessä näimme myös tietoturvan ulkoistamistrendin jatkuvan.

Hitaasti, mutta varmasti havaitsimme tietoturvan nousevan organisaatioiden kokonaisriskienhallintaan ja parantavan kyberuhilta suojautumista. Suojautumiskeinoja todella tarvitaan nettirikollisuuden yleistyessä ja valtiollisten toimijoiden kyberhyökkäysten tavanomaistuessa.

Kesällä kuntapalvelujen häiriöt puhuttivat. Tapaukset osoittivat ikävällä tavalla, kuinka riippuvuudet digitaalisista palveluista luovat yllättäviä, mutta myös vakavia tilanteita.

Tietoturvan perustaitojen tarve ja inhimillinen puoli nousivat esiin. Aihe on ajankohtainen myös nyt. Esimerkiksi henkilöstön tietoturvataidot ja kyky tunnistaa nettihuijauksia parantavat koko yhteisön turvallisuutta oleellisesti. Viattomilta vaikuttavat käyttäjätunnusten vuodot ja maksupetokset olivat Suomessakin arkipäivää.

Vaikka internetiin liitettävien laitteiden turvallisuus ei ole viimeiseen vuosikymmeneen parantunut, valonpilkahduksiakin on näkyvissä, sillä turvallisten kuluttajalaitteiden tunnistaminen helpottui Tietoturvamerkin avulla.

1 **Pilvi tulee voimalla, ja muutos riemastuttaa ja huolestuttaa** KYLLÄ

2 **Tietoturvan ulkoistaminen lisääntyy** KYLLÄ

3 **Valtiollisten toimijoiden kyberhyökkäykset ja niistä uutisointi jatkuu** KYLLÄ

4 **Organisaatioiden tietoturvan perusasioissa on yhä parannettavaa** KYLLÄ

5 **Tietoturva nousee osaksi liiketoimintalähtöistä riskienhallintaa** KYLLÄ

6 **Inhimillisen tietoturvan merkitys kasvaa** KYLLÄ

8 **Internetiin liitettävien kuluttajalaitteiden tietoturvan merkitys korostuu** KYLLÄ

7 **Riippuvuudet digitaalisista palveluista luovat yllättäviä tilanteita** KYLLÄ

9 **Vähäisiksi arvioidut tutut uhkat pahenevat hiljalleen** KYLLÄ

10 **Uudet teknologiat määrittävät 2020-luvun tietoturvahaasteet** KYLLÄ

+1 **Mobiililaitteisiin kohdistettuja haittaohjelmaepidemioita ei tulla näkemään** KYLLÄ

Vuoden 2019 kybersää

Tammi

Aapeli-myrsky riepotteli erityisesti Ahvenanmaan viestintäverkkoja

Internetiin avoimen RDP-etähallinnan kautta levitettiin haitallista toimintaa

Helmi

Toimitusjohtajahuijaukset lisääntyneet. Huijauksissa hyödynnetään murrettuja Office 365 -sähköpostitilejä

Kyberrikolliset ansaitsivat miljoonia toimitusjohtajahuijausten ja big game huntingin avulla

Maalis

Useissa Euroopan maissa palvelunestohyökkäyksiä, joiden tarkoituksena vaalihäirintä

Norsk Hydroon kohdistunut tietomurto aiheutti suuret taloudelliset tappiot

Suomessa paljon julkiseen internetiin näkyviä IoT-laitteita. Aihetta käsiteltiin Ylen Team Whack -ohjelmassa.

Eduskuntavaalien tulosten verkkopalveluun tehtiin palvelunestohyökkäys

Yhdysvaltojen NSA:n verkkovakoilutyökaluja epäillään päätyneen kiinalaisryhmän haltuun

Huhti

Touko

Bluekeep-haavoittuvuus voi johtaa itsenäisesti leviävään haittaohjelmaepidemiaan

Big game hunting -ryhmät hyödyntävät yleisiä haittaohjelmia

Varoitus 01/2019: Exim-sähköpostipalvelimen haavoittuvuuden avulla tehdään tietomurtoja

Kuntatapaus: Lahti

Pornokiristyshuijauksia ilmoitettiin runsaasti

Kesä

Heinä

Galileo-häiriö, palvelu poissa käytöstä viikon

Kuntatapaus: Kokemäki

Valtionhallinnon verkkosivut palvelunestohyökkäysten kohteena

Varoitus 02/2019: Microsoftin etätyöpöytäsovelluksen haavoittuvuuksia hyödynnetään tietomurroissa

Kuntatapaus: Pori

Elo

Syys

Poistimme Office 365 -tietomurtoja koskevan varoituksen

Kyberrikollisia saatu kiinni kansainvälisissä operaatioissa

15 vuodessa IoT-laitteiden tietoturva ei ole parantunut

Verkkolevyihin laajasti levinnyt haittaohjelmalöydös QSnatch

Vakoilijat muun muassa keksintöjen perässä, keräävät tietoa myös henkilöistä.

Peilaavia palvelunestohyökkäyksiä

Loka

Tietoturvamerkki auttaa kuluttajia tekemään turvallisempia kodin älylaitehankintoja – Suomi aloittaa älylaitteiden turvallisuuden varmistamisen ensimmäisenä Euroopassa

Monivaiheinen tunnistautuminen ehkäisisi suurimman osan Office 365 -tietomurroista

Marras

Vuosittainen kartoituksemme paljasti jälleen yli 1000 suojaamatonta laitetta kotimaisissa tietoverkoissa

Tilausansoja leviteltiin tekstiviestitse, sähköpostein ja mainoslinkkien sekä hakukoneoptimoinnin avulla

DNSSEC-tietoturvalaajennuksen käyttöönotto sai hyvän alun

Joulu

= Kansainvälinen uutisnosto

Vilkas julkaisujen, tapahtumien ja kampanjoiden vuosi

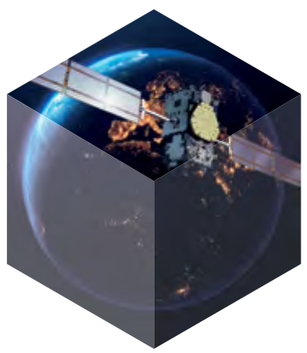
Tässä muutamia nostoja vilkkaasta julkaisuvuodestamme 2019. Toivottavasti mahdollisimman moni sai oppaistamme ja kampanjoistamme apua.

KAMPANJOITA JA TAPAHTUMIA

Turvalisti Teijo jakoi taas pointteja https://turvalistit.fi/

Tietoturvamerkki ohjaamassa fiksuihin älylaitehankintoihin https://tietoturvamerkki.fi/

Maailman ensimmäinen 5G-kyberturvallisuus-hackathon https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/70-maailmanluokan-hakkeria-kokoontui-ouluun-maailman-ensimmainen-5g



GALILEO INNOVATION CHALLENGE

Galileo Innovation Challenge: Kansainväliset joukkueet innovoivat palveluita EU:n Galileo-satelliittipaikannukselle https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kansainvaliset-tiimit-innovoivat-palveluita-eun-galileo-satelliittipaikannukselle

JULKAISUJA

Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta. Myös englanninkielinen käännös saatavilla. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Suojautuminen%20Microsoft%20Office%20365%20-tunnusten%20kalastelulta%20ja%20tietomurroilta%20web.pdf

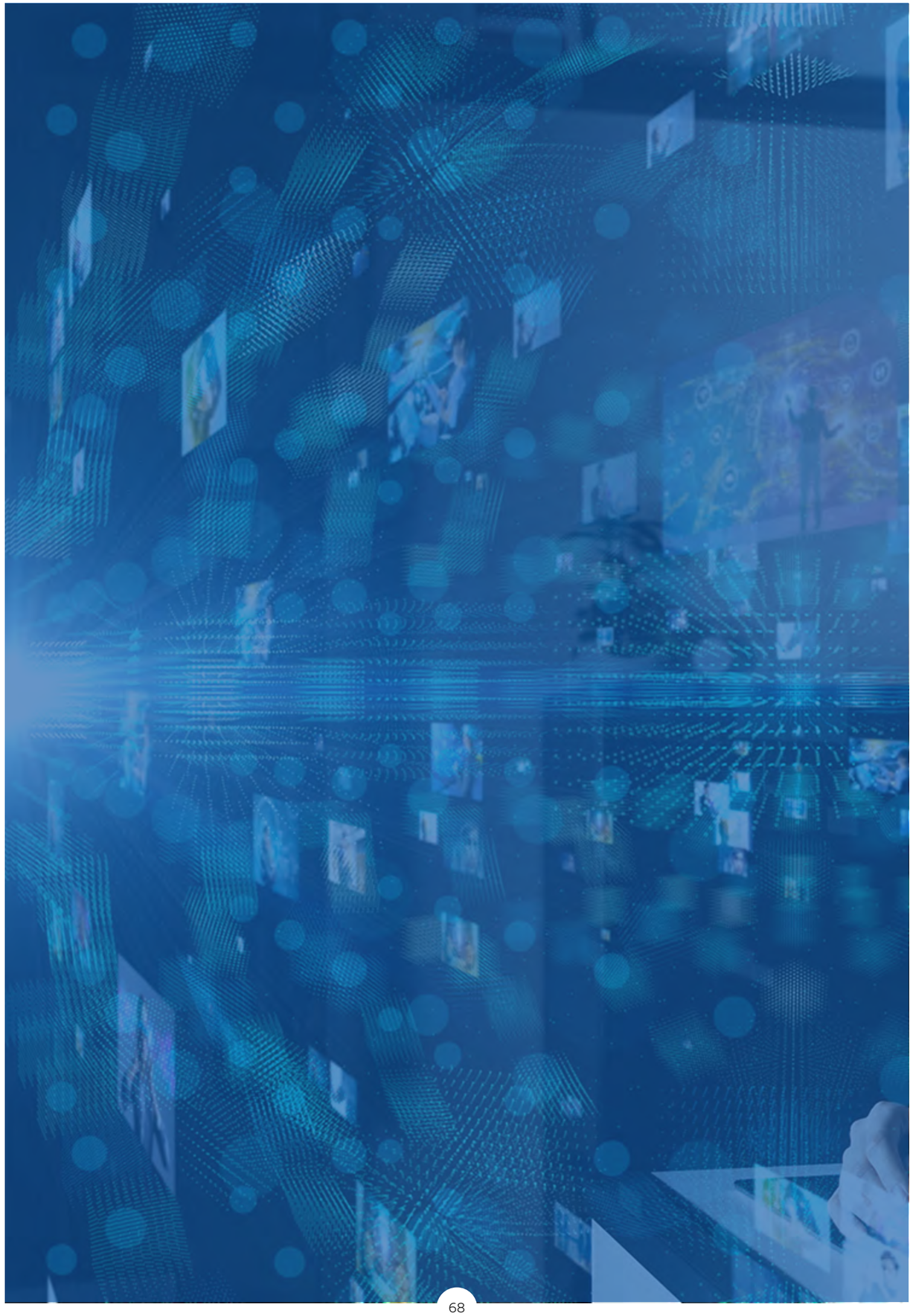
Pilvipalveluiden turvallisuuskriteeristö, englanninkielinen käännös https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/PiTuKri_v1_0_english.pdf

Kyberharjoitusohje – Käsikirja harjoituksen järjestäjälle https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusopas.pdf

Turvallisesti netissä -oppaat lapsille ja vanhemmille https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/turvallisesti-netissa-oppaat-lapsille

TUTUSTU MYÖS NÄIHIN

- Luottamuksen lähteillä – Näkökulmia tietoturvan standardointiin ja sertifiointiin https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf
- Näin suojaudut nettihuijaukselta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-nettihuijaukselta
- Näin pidät huolta tietoturvasta kotona ja työpaikalla https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvaohjeet/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla
- Kyber-Terveys-hanke: Sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimukset https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/sosiaali-ja-terveydenhuollon-hankintojen-tietoturva-ja
- Sähköisen tunnistuspalvelun arviointiohje https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/O211_Sähköisen_tunnistuspalvelun_arviointiohje_211_2019_O.pdf



Uutiskoonti kybersää 2019 tapahtumista

Tammikuu

- Aapeli-myrsky riepotteli erityisesti Ahvenanmaan viestintäverkkoja https://yle.fi/uutiset/3-10578072

Helmikuu

- Toimitusjohtajahuijaukset lisääntyneet. Huijauksissa hyödynnetään murrettuja Office 365 -sähköpostitilejä https://yle.fi/uutiset/3-10676320
- Kyberrikolliset ansaitsivat miljoonia toimitusjohtajahuijausten ja big game huntingin avulla https://www.crowdstrike.com/blog/pinchy-spider-adopts-big-game-hunting/

Maaliskuu

- Norsk Hydroon kohdistunut tietomurto aiheutti suuret taloudelliset tappiot https://www.tivi.fi/uutiset/kiristyshaittaohjelma-aiheutti-pohjoismaiselle-yhtiolle-viikossa-jopa-36-miljoonan-euron-tappiot/abfb80fb-6078-3c89-8869-9567673ea39d
- Suomessa paljon julkiseen internetiin näkyviä IoT-laitteita https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kuka-sammutti-valot-puutteellinen-rakennusautomaatiolaitteiden-suojaus-verkossa

Huhtikuu

- Eduskuntavaalien tulosten verkkopalveluun tehtiin palvelunestohyökkäys https://yle.fi/uutiset/3-10731312
- Yhdysvaltojen NSA:n verkkovakoilutyökaluja epäillään päätyneen kiinalaisryhmän haltuun https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html

Toukokuu

- Bluekeep-haavoittuvuus voi johtaa itsenäisesti leviävään haittaohjelmaepidemiaan https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/etatyopoytaratkaisun-kriittinen-bluekeep-haavoittuvuus-vaatii-kiireellista
- Big game hunting -ryhmät hyödyntävät yleisiä haittaohjelmia https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuuksien-hyvaksikaytto-synkensi-toukokuun-kybersaata

Kesäkuu

- Varoitus 01/2019: Exim-sähköpostipalvelimen haavoittuvuuden avulla tehdään tietomurtoja https://www.kyberturvallisuuskeskus.fi/fi/exim-sahkopostipalvelimen-haavoittuvuuden-avulla-tehdaan-tietomurtoja
- Kuntatapaus: Lahti https://www.tivi.fi/uutiset/kyberhyokkays-sekoitti-lahden-jarjestelmat-vakavat-hairiot-jatkuvat/30bfba87-5e49-461a-9443-4389ddb349e5

Heinäkuu

- Galileo-häiriö, palvelu poissa käytöstä viikon https://www.tekniikkatalous.fi/uutiset/undefined/ffb69bba-167a-4bae-b654-2ef46cc7c03b
- Kuntatapaus: Kokemäki https://yle.fi/uutiset/3-10899982

Elokuu

- Valtionhallinnon verkkosivut palvelunestohyökkäysten kohteena https://yle.fi/uutiset/3-10933059
- Varoitus 02/2019: Windows-käyttöjärjestelmän etätyöpöytäsovelluksen haavoittuvuuksilla levitettiin matomaisia haittaohjelmia sekä Suomessa että ulkomailla https://www.kyberturvallisuuskeskus.fi/fi/microsoftin-etatyopoyta-sovelluksen-haavoittuvuuksia-hyodynnetaan-tietomurroissa
- Kuntatapaus: Pori https://yle.fi/uutiset/3-10913191

Syyskuu

- Poistimme Office 365 -tietomurtoja koskevan varoituksen https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/office-365-sahkopostin-tietojenkalastelua-koskeva-varoitus-poistettiin
- Kyberrikollisia saatu kiinni kansainvälisissä operaatioissa https://www.fbi.gov/news/stories/operation-rewired-bec-takedown-091019

Lokakuu

- 15 vuodessa IoT-laitteiden tietoturva ei ole parantunut https://cyber-itl.org/2019/08/26/iot-data-writeup.html
- Verkkolevyihin laajasti levinnyt haittaohjelmalöydös QSnatch https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/qsnatch-qnap-nas-laitteisiin-suunnattu-haittaohjelma
- Vakoilijat muun muassa keksintöjen perässä; tietoa kerätään myös henkilöistä https://www.zdnet.com/article/iranian-hackers-credential-stealing-phishing-attacks-against-universities-around-the-world/
- Sivullisia hyödynnetään palvelunestohyökkäysliikenteen peilaamisessa varsinaiseen kohteeseen https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/2019-lokakuun-kybersaa

Marraskuu

- Tietoturvamerkki auttaa kuluttajia tekemään turvallisempia kodin älylaitehankintoja - Suomi aloittaa älylaitteiden turvallisuuden varmistamisen ensimmäisenä Euroopassa https://tietoturvamerkki.fi/
- Monivaiheinen tunnistautuminen ehkäisisi suurimman osan Office 365 -tietomurroista https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-mfa-get-started

Joulukuu

- Vuosittainen kartoituksemme paljasti jälleen yli 1000 suojaamatonta laitetta kotimaisissa tietoverkoissa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/hieman-yli-tuhat-automaatiolaitetta-suojaamattomana-suomalaisissa-verkoissa
- DNSSEC-tietoturvalaajennuksen käyttöönotto sai hyvän alun https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/dnssec-tietoturvalaajennuksen-kaytto-harppasi-suomessa-digitaalisten-palveluiden

Tarvitsetko sinä tai organisaatiosi apua tietoturva-loukkausten torjunnassa tai onko sinulla kysyttävää kyberturvallisuuteen liittyvästä säädännöstä? Arvioimme ja hyväksymme myös tietojärjestelmiä.

Kehitämme ja valvomme viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta. Tavoitat meidät näin:

sähköpostitse: cert@traficom.fi
asiakaspalvelu: 0295 345 630

Seuraa meitä ja uutisiamme
www.kyberturvallisuuskeskus.fi
@CERTFI
www.facebook.com/NCSC_FI

Ilmoita meille tietoturvaloukkauksesta
https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus

PL 320, 00059 TRAFICOM
p. 029 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-470-8
ISNN 2669-8757 (verkkojulkaisu)

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus