Tietoturvan vuosi

2018

TRAFICOM
Kyberturvallisuuskeskus

SISÄLLYS

Kyberturvallisuus kuuluu kaikille

Vuosi 2018 oli muutoksen aikaa. Muutimme kesällä uusiin toimitiloihin Kumpulaan ja vuoden lopussa siirryimme osaksi uutta Liikenne- ja viestintävirasto TRAFICOMia. Erittäin positiivisten, mutta myös työllistävien, kokemusten jälkeen vuonna 2019 voimme keskittyä täysipainoisesti toimintamme kehittämiseen.

Suomessa turvallisuuskulttuuri perustuu yksityisen ja julkisen sektorin vahvalle yhteistyölle. En ole törmännyt vastaavaan missään muualla maailmassa.

Yhteistyöperinteeseen on epäilemättä monia syitä. Ensinnäkin Suomessa tietoturvaihmiset tuntevat toisensa hyvin; nimet saavat nopeasti tutut kasvot. Tuttuihin on myös helpompi luottaa. Luja luottamus yhteistyökumppaneiden kesken on toinen yhteistyötä tukeva tekijä. Kolmanneksi kumppanit kokevat aidosti hyötyvänsä yhteistyöstä.

Yhteistyö on meille valtava voimavara. Saamme kumppaneiltamme erittäin luottamuksellisia tietoja ketterästi ja joustavasti ilman lakiin perustuvaa pakkoa. Yksi prioriteeteistamme on luottamuksellisen tiedon vastuullinen käsittely. Sujuva ja luotettava yhteistyö on sidosryhmiltämme saamamme palautteen mukaan keskeinen vahvuutemme, ammattitaitoamme unohtamatta. Näitä tulemme vaalimaan myös jatkossa.

Yhteistyössä on edelleen myös parannettavaa. Meidän on huolehdittava, että emme toimi vain tietoturva-ammattilaisten kuplassa ja myös kansalaiset hyötyvät yhteistyömme tuloksista.

Useat kyberturvallisuusuhkat voivat hiljalleen rikkoa luottamustamme digitaalisiin ympäristöihin, jos turvallisuuden ja hallinnan tunteemme katoavat. Vuonna 2018 merkittävimmäksi tietoturvauhkaksi nousi hiljalleen levittäytyvät, käyttäjiltä tietoja kalastelevat Office 365 -huijaukset. Inhimillisen tietoturvan merkitystä ei saa unohtaa eikä aliarvioida. Kyberturvallisuudesta ei voi tulla arjen kansalaistaitoa, jos emme viesti siitä inhimillisesti ja ymmärrettävästi. Toivon, että Teijo ja turvalistit sekä Pidempi parempi -salasanalinko ovat tuttuja mahdollisimman monelle. Näillä vuoden 2018 kansalaiskampanjoilla halusimme tuoda tietoturvan jokaiseen kotiin.

Tavoitteenamme on kehittää kotimaista kyberyhteistyötä niin, että tulevaisuudessa se toimisi entistä tiiviimmin. Kokonaisuus on tarkoitus rakentaa HAVARO-palvelumme ympärille, jolloin uhkatietoa voidaan jakaa ja jalostaa tehokkaasti. Tiivistyvän yhteistyön avulla kansalaisille tarjottavat kriittiset palvelut on mahdollista suojata entistä paremmin, koska tietoturvauhkilta suojautuminen ja niistä palautuminen olisi nykyistä nopeampaa. Uskon, että ”kyberekosysteemin” avulla sekä yksityinen että julkinen sektori pystyvät tuottamaan sellaisia sähköisiä palveluja, joita lapset, nuoret, aikuiset ja ikäihmiset voisivat käyttää tuntematta oloaan turvattomiksi.

Tervetuloa mukaan, sillä yhteiseen projektiin tarvitaan meitä kaikkia!

Helsingissä 31.1.2019,
Jarkko Saarimäki
Johtaja
Kyberturvallisuuskeskus
Liikenne- ja Viestintävirasto
Traficom

KESKEISET TIETOTURVAUHAT JA NIILTÄ SUOJAUTUMINEN

TOP 5 uhat ja ratkaisut yksityishenkilöille ja organisaatioille

YKSITYISHENKILÖT

UHAT

Rikolliset yrittävät varastaa käyttäjätunnuksesi
Varastetuilla tunnuksilla rikollinen yrittää päästä esimerkiksi uhrinsa sähköpostitilille. Sähköpostia käytetään usean nettipalvelun salasanan palautusosoitteena, siksi se on avain moneen paikkaan.

Huijaukset ovat internetin arkea
Etenkin valeverkkokaupat ja tilausansat vievät kuluttajilta rahaa. Myös arkaluonteisella materiaalilla kiristävät sähköpostit ja tech support -huijaukset ovat tehneet tuloaan.

Huonosti suojatut laitteet
Kuluttajille on tarjolla älypuhelimia, tietokoneita ja kodin IoT-laitteita, joiden tietoturva on olematonta: oletussalasanat käytössä, tuotetukea ja päivityksiä heikosti saatavilla. Niiden paikka ei ole internetissä - viestintäpalvelujen toimivuutta estämässä.

Valesovellukset virallisissa sovelluskaupoissa
Puhelimeen asennetut sovellukset voivat välittää eteenpäin enemmän tietoja, kuin olet hyväksynyt, jopa vakoilla ja varastaa tietojasi.

Verkkopalveluista vuotaa arvokkaita tietoja
Aidoista verkkokaupoista ja somepalveluista vuotaa jatkuvasti käyttäjä- ja maksutietoja, joita rikolliset voivat hyödyntää muun muassa huijausyrityksissään.

RATKAISUT

Älä anna sovelluksille tarpeettomia oikeuksia
Sovellusten oikeuksia voi useimmiten muokata myös asentamisen jälkeen. Taskulamppu toimii ilman pääsyä yhteystietoloosi tai kuviisi.

Tarkista, onko saamasi viesti liitteineen aito
Huijausviesti voi tulla sähköpostitse, tekstiviestinä, puheluna tai yksityisviestinä some-palveluun. Jos epäilet, varmista viestin sisällön oikeellisuus esimerkiksi puhelimitse.

Salasanaohjelmat ja 2-vaiheinen tunnistautuminen
Tarpeeksi pitkiä ja turvallisia salasanoja on jo vaikea muistaa. Ota 2-vaiheinen tunnistautuminen (2FA/MFA) käyttöön etenkin sähköpostitileillä, some-palveluissa ja yleisimmissä pilvipalveluissa, kun se on mahdollista.

Suojaudu tietoturvaohjelmistojen avulla
Haittaohjelmien torjunta ja palomuuri tulevat usein samassa paketissa. Käytä niitä. Noudata myös niiden antamia varoituksia ja ohjeita.

Tarkista luottokorttilaskusi säännöllisesti
Ole tarkkana etenkin nettiostosten jälkeen, koska aitojen verkkokauppojen tietomurrot ovat yleistyneet. Tarvittaessa voit kuolettaa korttisi. Huomaa, että verkkorikollinen ei jää kiinni ilman rikosilmoitusta.

ORGANISAATIOT

UHAT

Rikolliset pyrkivät rikastumaan tiedoillasi
Huijarit ja tietojenkalastelijat haluavat päästä organisaation tietojärjestelmiin ja hyötyä varastamistaan tiedoista. Osa huijauksista on hyvin uskottavia ja hyvin kohdennettuja, ja ne voivat aiheuttaa tuntuvia taloudellisia tappioita.

Ulkoistetut palvelut hyökkääjän lisäväylinä
Hyökkääjä voi päästä käsiksi yritykseen sen kumppanien ja alihankkijoiden järjestelmien kautta, etenkin jos yritys ulkoistaa keskeisiä palvelujaan ja tarjoaa niitä myös yhteistyökumppaneilleen. Hyökkäykset tai häiriöt järjestelmissä voivat levitä laajalle ja yllättäviin paikkoihin, jos yritys ei kykene kontrolloimaan omia teknisiä ympäristöjään.

Näkyvyyden puute
Omaa ympäristöä ei välttämättä tunneta riittävän hyvin. Hyökkäysten havainnointi ja paikallistaminen on erittäin vaikeaa, jos lokeja ei kerätä riittävästi. Esimerkiksi ohjelmistohaavoittuvuuksia hyödynnetään hyökkäyksissä lähes välittömästi, kun tieto haavoittuvuudesta on tullut julkisuuteen.

Arvokas tieto aktivoi vakoilijoita
Suomessa kiinnostavat poliittiset päätökset, huipputeknologia ja innovaatiot. Myös vaalit voivat kiinnostaa ulkomailla. Esimerkiksi EU-puheenjohtajuuskautena Suomi on potentiaalinen verkkovakoilun ja vaikuttamisen kohde. Median lisäksi aktivoituvat myös haktivistit ja poliittiset ryhmittymät.

Palvelunestohyökkäykset ovat arkipäivää
Jokaisen organisaation on varauduttava palvelunestohyökkäyksiin.

RATKAISUT

Sisällytä tietoturvavastuut sopimuksiin
Ulkoistamalla voi saada ammattimaista tietoturvaosaamista oman ydintoiminnan ulkopuolelta. Vastuuta ei voi ulkoistaa ilman, että ne on huomioitu sopimuksessa.

Laitteiden ja ohjelmistojen perushygienia
Ylläpidä ja päivitä kaikki verkkoon kytkettävät laitteet. Luo säännöllisille tiheille päivityksille ja varmuuskopioinnille rutiinitoimintamalli.

Kouluta, harjoittele ja testaa
Harjoittelulla testataan toimintaa ja löydetään kehityskohteet. Omista tapauksista oppien kerääminen on olennainen osa varautumista.

Juurruta tietoturva työyhteisön toimintatavaksi
Tietoturva pitää ottaa huomioon kaikessa toiminnassa. Sen on oltava osa kokonaisvaltaista riskienhallintaa ja varautumista.

Tunne järjestelmäsi ja palvelusi
Näin ylläpito ja varautuminen on tehokasta, lokitus on olennainen osa sitä. Harkitse automatisointia, jos se tekee työskentelystä tehokkaampaa ja parantaa prosessien toimintaa.

MERKITTÄVIMMÄT KYBERTURVALLISUUUSILMIÖT

Huijarit eivät levänneet

Sähköpostitileiltä laskutuspetoksiin

Huijausvuotta 2018 ovat värittäneet kiristyshuijaukset, Office 365 -aiheinen tietojenkalastelu ja toimitusjohtajahuijaukset. Jo aiempina vuosina tutuiksi tulleet tilausansat ja pankkitunnusten kalastelu eivät osoittaneet laantumisen merkkejä. Erilaiset huijaukset ovat vain lisääntyneet.

Vuosi 2018 tullaan varmasti muistamaan Microsoftin Office 365 -sähköpostipalvelun tunnusten kalastelusta. Ilmiö ei ole uusi, sillä erilaisten organisaatioiden tileille on aina yritetty päästä. Tähän saakka tietojenkalastelu on vaatinut aikaa vievää taustatyötä, kun rikollinen on tutustunut jokaisen organisaation etäkäyttöliittymään erikseen. Nyt yleisesti käytössä oleva Office-pilvipalvelualusta on yhtenäistänyt eri organisaatioiden sähköpostipalvelut. Samalla myös tietojenkalastelusta on tullut helpompaa: sama huijausviesti uppoaa useisiin samaa palvelua käyttäviin organisaatioihin.

Julkaisimme tietojenkalasteluista kriittisen varoituksen kesäkuussa 2018, kun kymmenien organisaatioiden sadat sähköpostitilit joutuivat vääriin käsiin. Rikollisten haltuun saamilta tileiltä lähti edelleen tuhansia uusia huijausviestejä, ja vuoden pahin tietojenkalasteluaalto jylläsi lumivyöryn tavoin organisaatiosta toiseen.

Kaapattuja sähköpostitilejä käytettiin myös muihin rikoksiin. Rikolliset pääsivät seuraamaan tilien liikennettä ja saivat haltuunsa organisaatioiden sisäisiä tietoja. Niiden avulla valmisteltiin laskutuspetoksia, väärennettiin laskuja ja huijattiin rahaa muun muassa organisaatiolta itseltään ja sen asiakkailta.

Petkutuksia ja harhautuksia

Kekseliäisyys ei verkkohuijareilta lopu. Kaikenlaisen tiedon voi käyttää väärin, esimerkiksi kiristyshuijauksiin. Erilaiset salasanavuodot ovat tulleet tutuiksi netinkäyttäjille, kun vuosia sitten unohdettujen palveluiden ikivanhoja salasanalistoja pulpahtelee pintaan. Jos vanhentuneita salasanoja on tarjolla tarpeeksi paljon, niillä voi helposti säikytellä ihmisiä luulemaan, että nyt heidän kaikki muutkin tietonsa on varastettu.

Maailmanlaajuisesti levinneissä ja huijauksiksi osoittautuneissa kiristyssähköposteissa yhdistyivät vanhat vuotaneet salasanat ja syyllistäminen pornon katselusta. Vaikka huijarilla ei ollutkaan hallussaan arkaluontoista materiaalia uhristaan, satunnainen vanha salasanavuoto lisäsi huijausviestin uskottavuutta: Maksa lunnaat, tai paljastan sinusta kaiken!

> *”Rikolliset pääsivät seuraamaan tilien liikennettä ja saivat haltuunsa organisaatioiden sisäisiä tietoja.*

Huijaustekstiviestejä mobiililaitteisiin

Nettiä selataan yhä enemmän mobiililaitteilla. Sinne ovat siirtyneet myös huijarit, jotka lähestyvät uhrejaan myös tekstiviesteillä. Huijausviestejä satelee niin sähköposteihin kuin älypuhelimiinkin. Tekstiviestin mukana tullut nettilinkki voi johtaa tilausansaan tai tietojenkalasteluun samoin kuin sähköpostiviesti.

Kuluttajia houkutellaan tilausansoihin valheellisella markkinoinnilla ja lupauksilla arpajaisvoitoista. Tunnetut tuotemerkit, parin euron televisiot ja kännykät ovat niissä tyypillisiä. Arvonnan tai toimitusmaksun varjolla kuluttajalta narrataan luottokortin numero. Palkintoa ei koskaan kuulu, mutta kuluttaja huomaakin sitoutuneensa nimelliseen palveluun, josta hänen luottokortiltaan veloitetaan kova kuukausimaksu.

Tepsiikö huijauksiin mikään?

Tiedotamme yleisöä meneillään olevista verkon vaaroista julkaisemalla tietoturvavaroituksia. Varoituksemme on huomattu hyvin, ja ne ovat ylittäneet median uutiskynnyksen tehokkaasti. Osa potentiaalisista uhreista on todennäköisesti välttänyt vaaran, mutta silti liian moni on mennyt vipuun. Erityisesti organisaatioiden on itse otettava vastuu henkilöstönsä valistamisesta ja pidettävä heidät tietoisena esimerkiksi huijausten vaaroista. Viranomaisena tarjoamme kaiken mahdollisen avun.

Rikokset suunnitellaan entistä tarkemmin

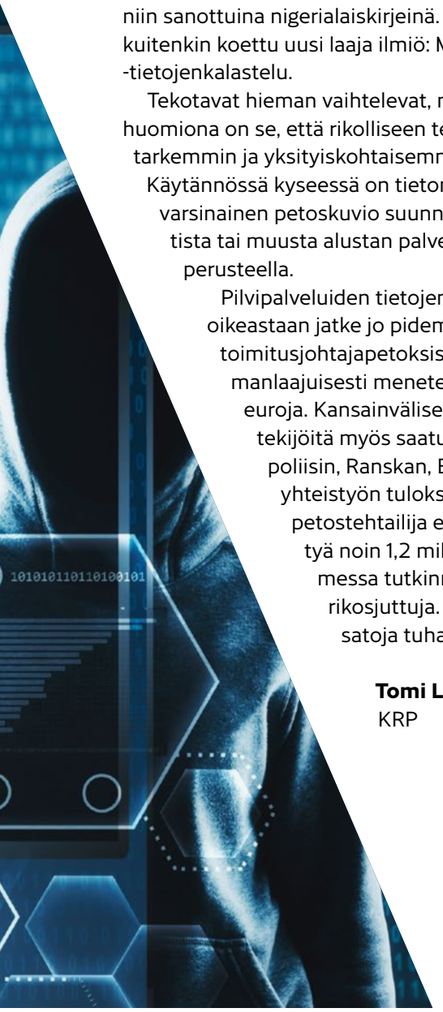
Mennyt vuosi on monella tavalla avannut silmiä myös poliisin näkökulmasta. Perinteisesti Suomessa on nähty internetiä hyödyntävää petosrikollisuutta kotimaisilla kauppapaikoilla, sähköpostihuijauksina sekä niin sanottuina nigerialaiskirjeinä. Vuoden aikana on kuitenkin koettu uusi laaja ilmiö: Microsoftin Office365 -tietojenkalastelu.

Tekotavat hieman vaihtelevat, mutta yleisenä huomiona on se, että rikolliseen tekoon paneudutaan tarkemmin ja yksityiskohtaisemmin kuin ennen.

Käytännössä kyseessä on tietomurto, jonka jälkeen varsinainen petoskuvio suunnitellaan sähköpostista tai muusta alustan palvelusta saadun tiedon perusteella.

Pilvipalveluiden tietojenkalasteluilmiö on oikeastaan jatke jo pidempään koetuista toimitusjohtajapetoksista, joissa on maailmanlaajuisesti menetetty satoja miljoonia euroja. Kansainvälisellä yhteistyöllä on tekijöitä myös saatu kiinni. Israelin poliisin, Ranskan, Belgian sekä FBI:n yhteistyön tuloksena kiinni saatu petostehtailija ehti kerätä rikoshyötyä noin 1,2 miljoonaa euroa. Suomessa tutkinnassa on kymmeniä rikosjuttuja. Menetykset ovat satoja tuhansia euroja.

Tomi Liesimaa
KRP



Office 365 -huijaukseen liittyvien tikettien määrät tammikuu 18 - tammikuu 19. Selvät piikit kesäkuussa, syyskuussa sekä marras- ja joulukuussa.

2017

8/2017 Saimme ilmoituksen Office365-tietojenkalastelusta ja tiedotimme siitä.

2018

2/2018 Helmi-maaliskuussa 2018 Office365-havainnot alkavat kiinnittää uudelleen huomiota.

11.6. Julkaistiin kriittinen varoitus.

8.8. Varoitus laskettiin kriittisestä vakavaksi.

21.9. Varoitus nostettiin takaisin vakavasta kriittiseksi.

26.9. Kaksivaiheinen tunnistus kierrettiin.

4.10. Huijausviestejä väärennettiin turvaposti-ilmoitukseksi.

26.10. Varoitus laskettiin kriittisestä takaisin vakavaksi.

27.11. Lisää uhreja: Sata tunnusta varastettiin PDF-liitetiedoston kalastelulinkillä.

11.12. Kirjautumisen aluerajoituksia kierrettiin VPN-yhteyksien avulla.

20.12. Huijausviestejä väärennettiin ääniviesti-ilmoitukseksi.

28.12. Huijausviestejä levitettiin SharePoint-sivuilla.

2019

1/2019 Tammikuussa 2019 tilanne on edelleen vakava.

Office 365 -huijauksen vaiheet

Kesäkuussa 2017 Suomessa havaittiin runsaasti tietojenkalasteluun tähtääviä sähköpostiviestejä. Kampanja oli kohdennettu lähinnä yritysten johdolle ja IT-ylläpidossa työskenteleville henkilöille. Onnistuneen sähköpostitunnusten kalastelun seurauksena organisaatioiden käyttämään Office 365 Exchange Online -pilvisähköpostipalveluun on esimerkiksi asetettu luvattomia sähköpostin edelleenohjaussääntöjä, joiden olemassaolon havaitseminen on vaikeaa tavallisilla ylläpitotyökaluilla.

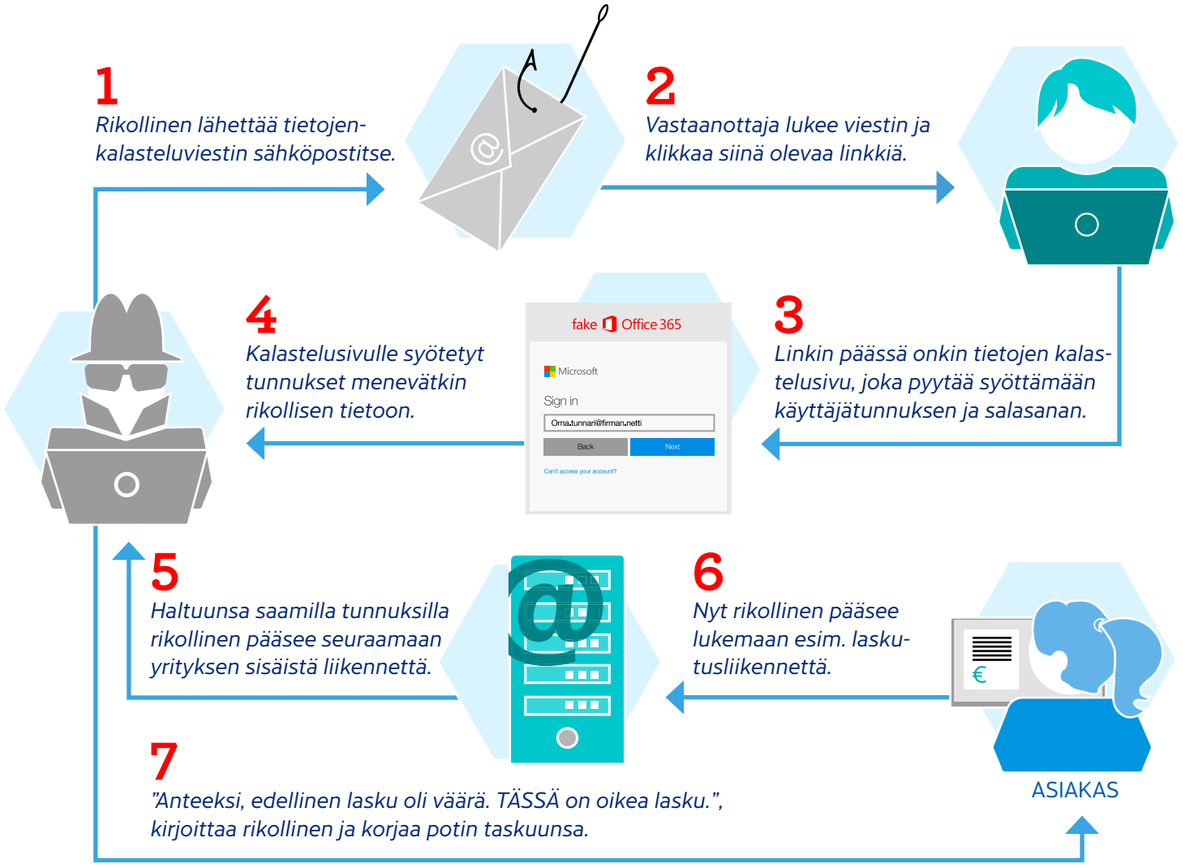
Elokuussa 2017 kehotimme kiinnittämään huomiota tunnistuksen turvallisuuteen ja Tietoturva nyt! -artikkelissamme ohjeistimme ottamaan käyttöön kaksivaiheisen tunnistuksen, koska salasanoja kalastellaan yleisesti. Syyskuussa varoittelimme jo kohdennetusta kalastelusta. Marraskuussa viestimme ongelmasta uudestaan, koska ilmiö ei näyttänyt laantuvan.

Helmikuussa 2018 herättelimme organisaatioita - jälleen kerran - tilanteen vakavuudesta. Julkaisimme TTN-artikkelin, johon liitimme esimerkkikuvat kalastelusivusta Office 365 ja OneDrive-teemalla. Varoitimme myös liikkeellä olevasta PDF-dokumentista, joka sisälsi linkin tietojenkalastelusivulle.

Aktiivisesta tiedotuksestamme huolimatta tietoomme saatettujen tapausten määrä kaksinkertaistui. Kesäkuussa päätimme julkaista aiheesta kriittisen varoituksen, sillä Office 365:a käyttävien organisaatioiden oli ryhdyttävä toimiin, jotta ongelma saataisiin kuriin! Varoitus sai julkisuudessa paljon huomiota ja näkyvyyttä, mutta ilmiö ei kuitenkaan poistunut, vaan jatkoi pahenemistaan.

Syyskuussa 2018 havaittiin, että kaksivaiheinen tunnistautuminen ei riittänyt, jos järjestelmä salli sen ohittamisen vanhemmilla päätelaitteilla. Lokakuussa huijausviestejä alkoi levitä myös turvaposti-ilmoituksiksi naamioituina. O365-huijarit vaikuttivat vain lisääntyvän, ja uudet uhrit erehtyivät antamaan tunnuksensa rikollisten kalastelusivuille.

Loppuvuodestakaan ilmoitettujen kalastelutapausten määrä ei merkittävästi vähentynyt, siksi varoituksen voimassaoloa ei ole voitu päättää.



Haavoittuvuudet ja haittaohjelmat

” Kotireitittimien ja IoT-laitteiden haitta-ohjelmahavainnot muodostavat lähes 60 % kaikista kyberturvallisuuskeskuksen haittaohjelmahavainnoista.

Haavoittuvuudet pysyivät kurissa ja epidemioilta vältyttiin

Vuonna 2018 merkittävin haavoittuvuusilmiö liittyi eri valmistajien suorittimista löytyneisiin haavoittuvuuksiin.

Vyyhti alkoi tammikuussa, kun Spectre- ja Meltdown-haavoittuvuudet osoittivat, että hyökkääjä voi päästä käsiksi samalla suorittimella ajettavan toisen ohjelman tai käyttöjärjestelmän tietoihin. Spectren ja Meltdownin vuoksi suorittimien haavoittuvuuksia tutkittiin maailmalla aiempaa enemmän ja lukuisia uusia tapauksia myös löydettiin. Suoritinhaavoittuvuudet ovat vaikuttaneet erityisesti pilvialustoihin ja muihin monikäyttöympäristöihin, mutta osa niistä koskee myös tavallisia kotikäyttäjiä.

Kuluneena vuonna myös käyttöjärjestelmien verkkototeutuksista löydettiin lukuisia kriittisiä haavoittuvuuksia. Haavoittuvuudet koskivat Windowsia, Unixia, MacOS:ää ja FreeRTOS:ia - käytännössä kaikkia käyttöjärjestelmiä. Eri haavoittuvuustyyppejä hyödyntämällä oli esimerkiksi mahdollista saada aikaan palvelunestotila. Vakavimmillaan haavan avulla pystyi suorittamaan omaa ohjelmakoodia kohdejärjestelmässä. Matomaisesti leviäviltä epidemioilta kuitenkin vältyttiin, koska haavoittuvuuksiin ei ollut heti tarjolla tehokasta hyödyntämismenetelmää.

Haittaohjelmat louhivat virtuaalivaluuttaa, klikkailivat mainoksia ja tunkeutuivat verkko-pankkeihin

Vuosina 2017 ja 2016 mellastivat notPetya, WannaCry ja Mirai, vuonna 2018 päästiin vähemmällä. Aiempina vuosina yleistyneet tietokoneen kovalevyn salaavat ja salauksen purkamisesta lunnaita vaativat kiristyshaittaohjelmat vähenivät ennusteistamme huolimatta.

Kiristyshaittaohjelmien sijaan kyberrikolliset saivat tuloja louhimalla virtuaalivaluuttoja uhrinsa tietokoneen resursseilla. Virtuaalivaluuttaa louhivia haittaohjelmia havaitsimme myös Suomessa. Näkyvin tapaus oli alkuvuodesta Lahden kaupungin tietojärjestelmiin vaikuttanut virtuaalivaluuttaa louhiva ja itsestään leviävä WannaMine-haittaohjelma. Louhija voidaan ujuttaa myös verkkosivun ohjelmakoodiin, jolloin valuutan louhinta onnistuu verkkosivuilla vierailevan käyttäjän selaimessa lähes huomaamatta. Haittaohjelmatartuntaa uhrin koneelle ei siis välttämättä edes tarvita.

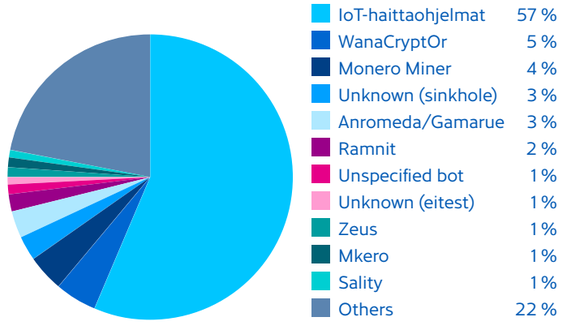
Maailmalla levinneistä Kovter ja Emotet -haittaohjelmista teimme havaintoja myös kotimaassa. Kovter on verkkomainoksia ”klikkaileva” haittaohjelma, jonka avulla verkkosivu voi keinotekoisesti lisätä omia mainostulojaan. Emotet puolestaan on monikäyttöinen haittaohjelma, jonka avulla voi esimerkiksi varastaa tunnuksia tai ladata jonkin toisen haittaohjelman.

” Jos laitteen säännöllinen päivittäminen ei ole mahdollista, se pitää erottaa internetistä.

Leviämisväylinä sähköpostin liitetiedostot, reitittimet ja päivittämättömät tietokoneet

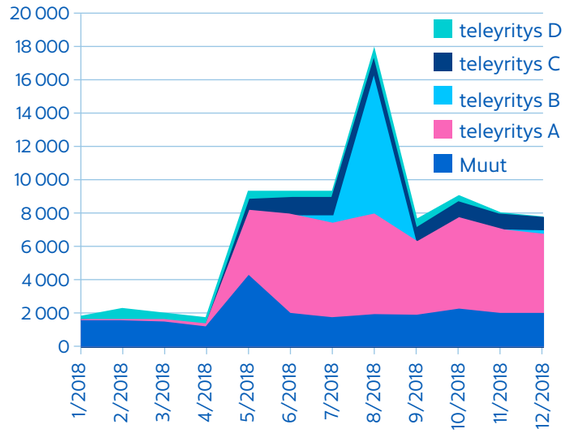
Sähköpostin liitetiedostot olivat yleisin tapa levittää haittaohjelmia vuonna 2018. Usein liitetiedosto on makroja sisältävä dokumentti, joka tartuttaa haittaohjelman tietokoneeseen.

Havaintomme kotireitittimien haittaohjelmatartunnoista lisääntyivät merkittävästi kesän 2018 aikana. Havainnot koskivat erityisesti muutaman teleyrityksen tiettyjä kotireititinmalleja. Tällä hetkellä erilaiset kotireitittimien ja muiden IoT-laitteiden haittaohjelmat muodostavat suuren osan, eli lähes 60 %, kaikista meille ilmoitetuista haittaohjelmahavainnoista.



IoT-haittaohjelmat muodostivat lähes 60 % kaikista vuoden 2018 haittaohjelmahavainnoistamme.

> *”Kotireittimien ja IoT-laitteiden haittaohjelmahavainnot muodostavat lähes 60 % kaikista kyberturvallisuuskeskuksen haittaohjelmahavainnoista.*



IoT-haittaohjelmahavainnot yleistyivät vuonna 2018. Havainnot keskittyivät muutamaan teleyritykseen. Piikki elokuussa 2018.

Teemme edelleen havaintoja myös hyvin vanhoista haittaohjelmista. Esimerkiksi vuonna 2007 löydettyä Zeus-haittaohjelmaa näkyy edelleen. Ilmiö on tyypillinen, ja johtuu luultavasti siitä, että osaa tietokoneista ei päivitetä tai käynnistetä uudelleen. Näiden laitteiden ylläpito on asentamisen jälkeen unohdettu, jolloin niistä on tullut otollista maaperää erilaisille haittaohjelmatartunnoille.

Olipa kyse suuryrityksen verkkopalvelimesta tai kotona käytettävästä verkkokamerasta, kaikkia internetiin kytkettäviä laitteita on syytä ylläpitää ja niiden päivityksistä tulee huolehtia. Jos esimerkiksi laitteen säännöllinen päivittäminen ei ole mahdollista, se pitää erottaa internetistä.

Rikolliset etsivät internetistä jatkuvasti haavoittuvia laitteita. Nettiin kytketty laite, jossa on haavoittuvuus ja haavoittuvuuteen julkinen hyödyntämismenetelmä, on nopeasti murrettu. Murrettu laite osallistuu esimerkiksi palvelunestohyökkäyksiin, louhii virtuaalivaluuttaa tai lähettelee roskapostia.

Vakoilu ja vaikuttaminen

> *”Kohteena ei enää ole vain tavanomainen ”toimistotietotekniikka” vaan myös automaatiojärjestelmät, joiden avulla pyöritetään yhteiskunnan elintärkeitä toimintoja.*

Tunkeutuminen toimitusketjun/ulkoituskumppanin kautta.

*Lähde: BAE Systems Threat Research Blog
https://baesystemsai.blogspot.com/2017/04/apt10-operation-cloud-hopper_3.html
https://2.bp.blogspot.com/-sBNjr4znWk/WN573VvsfmI/AAAAAAAAAno/OKLwDezpCFg-LwQt8k-EfvG7Ptn6nETefACLcB/s640/infographic.png

Vakoilurintamilta ei uutta

Jo vuonna 2017 puhtaasta vakoilusta siirryttiin vaikuttamiseen ja toimitusketjujen väärinkäyttö oli ilmeistä. Samat ilmiöt pysyivät pinnalla myös vuonna 2018.

Kybervakoilun, toisin sanoen tietoverkkojen avulla tehdyn laittoman tiedonhankinnan, lisäksi hyökkääjät halusivat häiritä tai lamaannuttaa kohteidensa tietojärjestelmien toimintaa. Kohteet vaihtelivat teollisuusautomaatiosta olympiakisoihin. Osassa tapauksista varsinaisia tihutöitä ei edes tehty, vaan tarkoituksena oli valmistella muun muassa jalansijaa mahdollisia tulevia operaatiota varten.

Vuonna 2018 julkisuudessa käsiteltiin useita tapauksia, joissa tietomurtoja oli käytetty sotilaallisten operaatioiden tukena. Tekijöiksi nimettiin niin Venäjän kuin Yhdysvaltainkin sotilasorganisaatioita. Kybertoimintaympäristöön liittyvät tunkeutumismenetelmät näyttävätkin tulleen kiinteäksi osaksi sotilaallisia hyökkäysoperaatioita.

Osumia automaatiojärjestelmiin ja hyökkääjille julkisia syytöksiä

Nykyaikaisen hybridivaikuttamisen työkalupakkiin kuuluu olennaisesti tietojärjestelmiin tunkeutuminen eri tavoin ja tarkoitusperin. Kohteena ei enää ole vain tavanomainen ”toimistotietotekniikka” vaan myös automaatiojärjestelmät, joiden avulla pyöritetään yhteiskunnan elintärkeitä toimintoja. Kun häiriöihin ja poikkeustilanteisiin varaudutaan, myös määrätietoisen valtiollisen toimijan torjuntakeinot tulee huomioida.

Selvä poikkeus aikaisempaan on se, että poliittiset päättäjät ovat halukkaampia syyttämään julkisesti muita valtioita ja jopa yksittäisiä virkamiehiä havaituista tietomurroista. Erityisesti Yhdysvallat ja Iso-Britannia ovat syyttäneet useasti sekä Venäjän että Pohjois-Korean tiedustelupalveluita erilaisista tietomurroista. Mutta kuohuntaa on ollut Euroopassakin, kun Belgia syytti Iso-Britanniaa tunkeutumisesta belgialaisen teleoperaattorin tietojärjestelmiin.

Pelkkien teknisten todisteiden perusteella on lähes mahdotonta osoittaa vedenpitävästi, kuka on istunut hyökkääjän näppäimistön ääressä ja miksi hyökkäys on tehty. Erityisesti julkisuudessa esitetyt syytökset perustuvat usein poliittisiin päätöksiin tai linjauksiin.

Nykyaikaista yritysvakoilua on entistä vaikeampaa havaita

Toimitusketjujen kautta tehtävät tietomurrot korostuivat yrityksiin kohdistuvassa vakoilussa myös vuonna 2018. Ohjelmistojen päivityspalvelimien ja tietojärjestelmien ylläpitopalveluiden kautta on mahdollista tunkeutua useisiin kohteisiin samalla kertaa. Toimitusketjujen kautta tehdyn hyökkäyksen havaitseminen on merkittävästi vaikeampaa esimerkiksi kohdistettuihin haitallisiin sähköposteihin verrattuna.

Jotta esimerkiksi EU-komissio voisi puuttua valtiollisten toimijoiden yritysvakoiluun, yritysten tulisi antaa arvio kyberhyökkäyksistä aiheutuneista taloudellisista menetyksistä. Arvioon pitäisi sisällyttää välittömien kulujen lisäksi myös välilliset kustannukset. Välittömiä kuluja ovat esimerkiksi tietomurron selvittelyyn ja tietojärjestelmien uudelleenrakentamiseen liittyvät kulut. Välillisiä kustannuksia ovat puolestaan immateriaaliomaisuuden varkaudesta ja menetetyistä liiketoimintamahdollisuuksista koituvat tappiot.

Tunkeutumisen eteneminen. Viimeisenä vaiheena on onnistunut tietomurto.

*Lähde: IBM X-Force IRIS Team
https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/

Palvelunestohyökkäykset

”Palvelunestohyökkäysten keskimääräinen koko jatkaa tasaista kasvuaan. Vuoden 2018 lopulla oli jo täysin normaalia, että yksittäisille kuluttajillekin osuvat hyökkäykset olivat > 10 Gbps. Memcachedia käyttävät hyökkäykset tulivat jäädäkseen, mutta eivät onneksi alun tulvan jälkeen ole generoineet suuria ongelmia. Hyökkäysten kasvulle ei ole näkyvissä loppua, joten palvelunestohyökkäysten aiheuttamiin ongelmiin on hyvä varautua.

Osmo Soinio
Telia

Kuka tahansa voi ostaa palvelunestohyökkäyksen haluamaansa kohteeseen

Palvelunestohyökkäyksiä tarjoavilta, niin sanotuilta stresser-palveluilta, saa myös ilmaisia lyhytkestoisia näytehyökkäyksiä. Tilastojen valossa valtaosa, eli noin 75 %, kaikista Suomessa nähtävistä palvelunestohyökkäyksistä kestävät alle 15 minuuttia. Näiden hyökkäysten lyhyen keston, mutta suuren kappalemäärän perusteella, ne ovat luultavasti stresser-palveluiden ilmaisia näytehyökkäyksiä.

Huhtikuussa palvelunestohyökkäysten tilauspalvelu webstresser.org suljettiin verkosta kansainvälisen poliisioperaation seurauksena. Kyseessä oli maailman suurin dos-palvelu, jonka alasajo vähensi hyökkäysten määrää kansainvälisesti. Silti verkossa on edelleen lukuisia palveluita, joista palvelunestohyökkäyksen voi tilata haluamaansa verkko-osoitteeseen.

Tyypillisesti palvelunestohyökkäykset kestävät niin kauan, kun niillä on vaikutusta kohteen toimintaan. Yleensä hyökkääjä lopettaa, kun palvelunestohyökkäys saadaan torjuttua ja palvelun toiminta palautuu. Usein hyökkääjä kuitenkin vain vaihtaa kohdetta, ja hyökkäys jatkuu johonkin toiseen saman kohdeorganisaation palveluun.

Suomessa nähtävät palvelunestohyökkäykset ovat tyypillisesti volyymeiltaan noin 1-10 Gbit/s. Näillä volyymeillä palvelun toimintaan voidaan yleensä vaikuttaa, ellei palvelunestohyökkäyksiin ole erikseen varauduttu. Yli 10 Gbit/s:n hyökkäyksiä nähdään Suomessa useita viikoittain. Vuonna 2018 suurin tietoomme tullut ja Suomeen suunnattu hyökkäys oli voimaltaan noin 90 Gbit/s, ja se kesti useita tunteja.

”noin 75 % kaikista Suomessa nähtävistä palvelunestohyökkäyksistä kestävät alle 15 minuuttia.

Hyökkäykset suomi.fi-tunnistamispalveluun olivat näkyvästi esillä

Kesän ja syksyn aikana suomi.fi-tunnistuspalveluun tehtiin useita palvelunestohyökkäyksiä, jotka heikensivät lukuisten valtion palveluiden toimintaa. Tunnistuspalvelu on keskeinen komponentti monien muiden palveluiden toiminnassa, joten se on houkutteleva kohde myös hyökkääjille.

Suomi.fi-hyökkäykset olivat ehkä näkyvin esimerkki palvelunestohyökkäyksistä, mutta ne eivät jääneet ainoiksi. Vuonna 2018 Suomessa tehtiin yhteensä useita tuhansia palvelunestohyökkäyksiä. Voidaankin sanoa, että palvelunestohyökkäykset ovat arkipäiväistyneet ja niitä tehdään jatkuvasti. Kaikilla hyökkäyksillä ei kuitenkaan ole näkyviä vaikutuksia palveluiden toimintaan, mistä voidaan kiittää organisaatioiden hyvää varautumista.

”Vuonna 2018 Suomessa tehtiin yhteensä useita tuhansia palvelunestohyökkäyksiä.

Hyökkäystekniikat ovat pysyneet lähes samoina

Palvelunestohyökkäysten toteutuksessa käytetään erilaisia tekniikoita, joista yleisimmät ovat reflektiohyökkäys sekä murretuilta päätelaitteilta lähetetty verkkoliikenne. Usein näitä tekniikoita myös yhdistellään. Reflektiohyökkäyksissä hyödynnetään internetissä olevia palvelimia, esimerkiksi nimipalvelimia tai CLDAP-hakemistopalveluita, hyökkäysliikenteen vahvistamiseksi. Vuonna 2018 reflektiohyökkäyksiä tehtiin entistä enemmän myös väärin asennettuja memcached-palvelimia hyödyntäen.

Hyökkäyksiltä ei voi suojautua ilman ennakointia ja suunnittelua

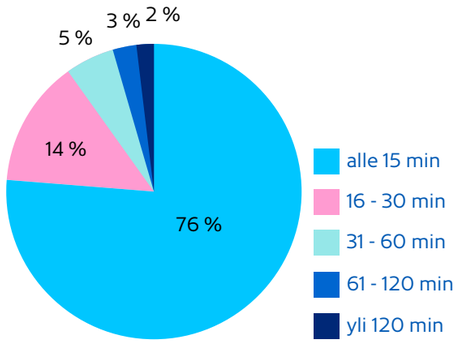
Palvelunestohyökkäykset tulee huomioida organisaation riskiarviossa. Jos esimerkiksi yrityksen palveluiden saatavuus internetissä on tärkeää, palvelunestohyökkäyksiltä suojautumista on suunniteltava, ja niihin on varauduttava hyvissä ajoin.

Erityyppisiltä hyökkäyksiltä on suojauduttava eri tavoin. Sovellustason hyökkäyksiä vastaan suojauduttaessa verkkopalvelu on suunniteltava siten, että sitä on vaikea kuormittaa yksittäisillä kyselyillä, kuten hankalilla tietokantahauilla. Lukuisia TCP-yhteyksiä luoviin hyökkäyksiin varauduttaessa verkkoarkkitehtuuri, kuormanjako ja sisällönvälitys on suunniteltava niin, ettei palvelu tukkeudu samanaikaisten istuntojen luomisesta. Teleyrityksiltä ostettavien palveluiden, esimerkiksi asiakaspalomuurin tai pakettipesureiden, avulla voidaan torjua volyymiin perustuvia hyökkäyksiä.

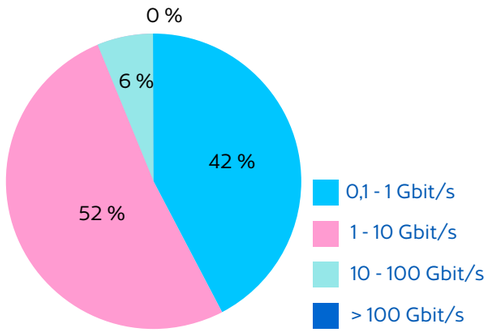
Yksittäistä ”hopealuotia” verkkopalvelun suojaamiseksi ei ole olemassa. Verkkopalvelun suunnittelun pitää kokonaisuudessaan tähdätä erilaisten hyökkäysten sietokykyyn ja nopeaan palautumiseen hyökkäysten jälkeen.

”Palvelunestohyökkäys on tietoturvauhkista hinta-laatusuhteeltaan näyttävin, mutta ei yleensä vakavin. Sitä voi verrata järjestäytyneeseen mielenilmaukseen toimistorakennuksen edustalla: se kerää huomiota ja estää asiakkaiden sisäänpääsyn. Pahimmillaan hyökkäys voi vaarantaa ihmishenkiä, jos se tukkii kriittiset palvelut.

Jarna Hartikainen
päällikkö
Traficom/Kyberturvallisuuskeskus



Suomeen kohdistuneiden palvelunestohyökkäysten ajalliset kestot vuonna 2018 (lähde: Telia).



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit vuonna 2018 (lähde: Telia).

Kotimaisten viestintäverkkojen toimintavarmuus

”Viime vuosina Kyberturvallisuuskeskuksen ja teleoperaattoreiden yhteistyö on parantunut merkittävästi ja muuttunut avoimempaan suuntaan. Operaattorit tapaavat toisiaan säännöllisesti muun muassa Liikenne- ja viestintäviraston eri työryhmissä, joissa käsitellään häiriötilanteiden hallintaa ja ennaltaehkäisyä. Tapaukset ja tilanteet, joissa yhteiskunnan toimivuuden kannalta on hyödyllistä tehdä yhteistyötä, löytyvät ryhmissä luontevasti. Näkökulma on laajempi kuin yksittäisen operaattorin.

Nopea toipuminen häiriöistä, yhteiskunnan kriittisten palveluiden toimivuus ja tilanteisiin varautuminen ovat kaikkien etu. Toimivat palvelut hyödyttävät meitä kaikkia, siksi - kilpailuasetelmasta huolimatta - operaattoreidenkin kannattaa tehdä yhteistyötä esimerkiksi laajoissa teknisissä häiriö- ja poikkeustilanteissa.

Tänään yhteistyössä ovat mukana myös sähköyhtiöt ja pelastuslaitokset. Nyt voimme paremmin huolehtia siitä, että kansalaisilla on mahdollisimman hyvin toimivat tietoliikennepalvelut käytettävissään.

Tomas Lång
DNA Oyj

Tilanne vain parantunut

Kotimaisten viestintäverkkojen merkittävät häiriöt ovat vähentyneet viime vuosina selvästi, sama trendi jatkui myös 2018. Sääolosuhteet aiheuttivat verkkoihin pitkäkestoisimmat häiriöt, mutta teleyritysten ja sähköyhtiöiden yhteistyöllä niiden vaikutukset pysyivät aiempiin vuosiin nähden maltillisina ja korjaustyöt etenivät tehokkaasti.

Saimme teleyrityksiltä ilmoitukset yhteensä lähes 70 merkittävästä toimivuushäiriöstä. Niistä vakavimpia ja laajimpia oli noin 14. Häiriöiden määrät ovat vähentyneet edellisvuoteen verrattuna noin kolmanneksella. A-vakavuusluokan häiriöitä oli kuitenkin enemmän kuin edellisenä vuonna. Vastaavasti B-vakavuusluokan häiriöitä oli yli puolet vähemmän kuin edellisvuonna.

Noin puolet A-vioista koskivat antenni-tv:n toimivuutta, ja useimmiten häiriön syynä olivat laiteviat. Myös teleyritysten verkon, laitteistojen ja ohjelmistojen muutostyöt aiheuttivat katkoja viestintäverkon palveluihin.

Puhelut ja internet toimivat, kriittisten järjestelmien toimintavarmuutta on parannettava

Vuoden 2018 alussa Kainuun alueella oli laajoja sähkökatkoksia, joiden kesto vaihteli muutamasta päivästä jopa yli viikkoon. Kainuun pelastuslaitos otti tilanteen yleisen johtovastuun itselleen, mikä kertoo häiriöiden laajuudesta ja vakavuudesta. Sähkökatkokset vaikuttivat myös viestintäpalvelujen toimivuuteen, mutta suurilta häiriöiltä vältyttiin. Esimerkiksi hätäpuhelut toimivat ja pelastustöihin osallistuneet pystyivät käyttämään tiedon jakamiseen matkapuhelinverkkoa.

Kotimaisten viestintäverkkojen toimivuus on parantunut viime vuosina. Yhtenä syynä ovat teleyritysten uudistamat verkkorakenteet, joissa yksittäisen linkin katkeaminen ei enää aiheuta laajaa häiriöitä. Verkkomuutosten positiiviset vaikutukset ovat nähtävissä vuoden 2018 tilastoissa merkittävien häiriömäärien vähentymisenä. Vuonna 2018 esiin ovatkin nousseet yksittäisten verkkojen häiriöt, jotka aiheuttivat katkoksia yhteiskunnalle tärkeisiin palveluihin. Esimerkiksi häiriöt sairaalan ja liikenteenohjausjärjestelmän tietoliikenneverkoissa estivät niihin liittyvien palvelujen käytön. Kriittisissä järjestelmissä katkoksiin ja häiriöihin tulisi varautua hyvissä ajoin, jo kilpailutus- ja sopimusvaiheessa.

Teleyritykset ilmoittavat tietoturvaloukkauksista yhä aktiivisemmin

Tietoturvaloukkausten tai -uhkien määrä vaihtelee vuosittain, mutta keskimäärin saamme merkittävistä tapauksista 1 tai 2 ilmoitusta kuukaudessa. Niin myös vuonna 2018. Suurin osa tapauksista koskee tietojärjestelmien tietomurtoja tai niiden luvatonta käyttöä, teleyritysten järjestelmien haavoittuvuuksia tai teleyritysten verkkojen kautta tehtyjä isoja palvelunestohyökkäyksiä.

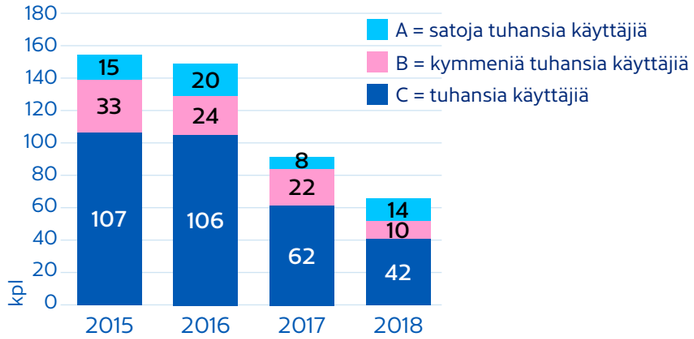
Viime vuosina vastaanottamamme henkilötietojen tietoturvaloukkausilmoitukset ovat lisääntyneet voimakkaasti. On epätodennäköistä, että henkilötietoloukkausten määrä sinänsä olisi kasvamassa. Pikemminkin teleyritykset tietävät nyt paremmin, millaisissa tilanteissa henkilötietojen tietoturvaa voidaan loukata ja että kaikista näistä tilanteista tulee tehdä ilmoitus.

Tavallisin henkilötietojen tietoturvaloukkaustapaustyyppi on asiakastietojen hallinnan virhe. Näissä tapauksissa teleyritys käsittelee asiakkaidensa henkilötietoja virheellisesti niin, että yhden asiakkaan henkilötiedot paljastuvatkin toiselle. Esimerkiksi uuden liittymätilauksen yhteydessä asiakas saakin vahingossa kopion häntä aiemmin palvellun asiakkaan liittymäsopimuksesta. Mahdollisia ovat myös tapaukset, joissa asiakas haluaa siirtää liittymälaskunsa eräpäivää ja ottaa yhteyttä teleyritykseen puhelimitse tai vaikkapa chat-kanavalla, mutta hänen yhteystietoihinsa tallennetaankin väärä puhelinnumero, jolloin vahvistustekstiviesti eräpäivän siirrosta lähetetään toiselle asiakkaalle.

Olemme keränneet tietoa teleyritysten merkittävistä viestintäverkkojen ja -palvelujen tietoturvaloukkauksista tai niiden uhista jo vuodesta 2002. Loukkaus tai uhka arvioidaan merkittäväksi erityisesti tilaajien ja käyttäjien oikeuksien suojan, palvelun käytettävyyden ja maantieteellisten vaikutusten perusteella.

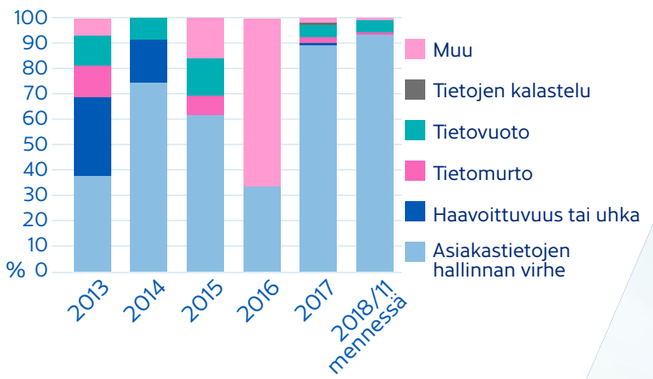
Vuodesta 2013 lähtien teleyritykset ovat ilmoittaneet nykyiselle Liikenne- ja viestintävirastolle myös henkilötietojen tietoturvaloukkauksista. Pääasiassa ilmoitukset liittyvät tapauksiin, joissa henkilötiedot tuhoutuvat, häviävät, muuttuvat tai niitä luovutetaan eteenpäin vahingossa tai luvattomasti.

Merkittävien toimivuushäiriöiden määrät eri vakavuusluokissa



Merkittävien häiriöiden (A-C) vuosittainen kokonaismäärä on pienentynyt jo vuodesta 2015 lähtien. Vuonna 2018 pienempiä C-vikoja oli vähemmän, kun taas A-vikoja enemmän kuin vuonna 2017.

Henkilötietoloukkausten tapaustyypit



”Verkkomuutosten positiiviset vaikutukset ovat nähtävissä vuoden 2018 tilastoissa merkittävien häiriömäärien vähentymisenä.

Esineiden internet

” Yksilön ongelmasta tulee yhteinen, kun turvattomia ja huonosti hallittuja laitteita kaapataan ja käytetään esimerkiksi palvelunestohyökkäyksiin.

Tietovuotoja, salakatseluja ja palvelunestohyökkäyksiä

Esineiden internet, Internet of Things (IoT), levittäytyi vuoden 2018 aikana yhä merkittävämmäksi osaksi kuluttajien arkea. Ympäristöään tarkkailevat ja siitä tietoa välittävät laitteet helpottavat kuluttajan elämää esimerkiksi ohjaamalla kodin valaistusta ja lämmitystä tai raportoimalla unen laadusta ja sykkeestä. Uusien IoT- innovaatioiden mukana levisivät valitettavasti myös laitteisiin liittyvät tietoturvaongelmat.

Kuluttajalaitteiden tietoturvallisuuspuutteet näkyivät muun muassa tietovuotoina ja yksityisyyden loukkauksina. Tapaukset osoittavat, että vain harva osaa arvioida ja hallita kodissa käytettävien, verkkoon kytkettyjen ja tietoa tallentavien laitteiden tietoturvallisuutta. Yksilön ongelmasta tulee yhteinen, kun turvattomia ja huonosti hallittuja laitteita kaapataan ja käytetään esimerkiksi palvelunestohyökkäyksiin. Kriittisten ja julkisten palvelujen digitalisoituessa IoT-laitteisiin kohdistetut hyökkäykset voivat heikentää koko yhteiskunnan toimintaa.

Toistaiseksi ei ole olemassa IoT-laitteita koskevia yleisesti tunnistettuja tai velvoittavia tietoturvavaatimuksia, siksi turvallisuuspuutteiden ehkäisy on vaikeaa. Teknologian nopea kehitys on vaikeuttanut laitteiden ja palveluiden riskien syvällistä ymmärtämistä. Myös lainsäädännön valmistelu on ollut hidasta, mutta tilanne näyttäisi vähitellen muuttuvan paremmaksi.

Puutteet kuriin sääntelyllä, turvallisille laitteille tietoturvaleima

Kalifornian osavaltio vahvisti syyskuussa 2018 tiettävästi maailman ensimmäisen esineiden internetiä koskevan tietoturvalain. Myös kansainväliset esineiden internetiä ja sen tietoturvaa koskevat standardit ovat valmistelussa. Kevyempiä periaatetason linjauksia on tehty vuoden aikana muun muassa Saksassa ja Isossa-Britanniassa.

Suomessa Liikenne- ja viestintävirasto Traficom on seurannut kansainvälistä sääntelyn kehitystä. IoT-laitteiden tietoturvaongelmat vaikuttavat lisääntyvän nopeammin kuin laitteita koskevat vaatimukset. Tämän vuoksi virastossa on alettu kehittää tietoturvallisuusleimaa, joka auttaisi kuluttajaa tunnistamaan tietoturvalliset laitteet ja tekemään turvallisia valintoja. Koska tietoturvaominaisuuksien lisääminen laitteisiin jälkikäteen on kallista ja usein vaikeaa, leiman on tarkoitus kannustaa myös valmistajia suunnittelemaan koko elinkaareltaan tietoturvallisia laitteita. Tätä kutsutaan secure by design -ajatteluksi. Kuluttajalaitteissa sitä on soveltanut jo esimerkiksi Ikea Trådfri-älyvalaisimissaan.

Tietoturvailmiöiden riskiarviot

Keskeiset tietoturvariskit yksityishenkilöille, organisaatioille ja valtionhallinnolle

Tässä arviomme keskeisiin kyberturvallisuusilmiöihin liittyvistä merkittävimmistä riskeistä vuonna 2018. Olemme nostaneet esiin esimerkkitapauksia, jollaisina riskit ovat voineet näyttäytyä yksityishenkilöille, yrityksille, kunnallisille organisaatioille tai valtionhallinnolle.

Nuolen suunta kertoo tilanteen kehityksestä vuoteen 2017 verrattuna. Näkemyksemme mukaan vuonna 2018 Suomen yleinen kyberturvallisuuden riskitaso pysyi lähes ennallaan vuoteen 2017 verrattuna. Tietyissä ilmiössä riskit ovat kasvaneet.

▶ Riski on pysynyt samana
▲ Riski on kohonnut

	YKSITYISHENKILÖT	ORGANISAATIOT	VALTIO
HUIJAUKSET JA KALASTELU	▲ Pankkitunnuksia ja luottokorttitietoja kalastellaan paljon. Huijaukset ja kiristykset hyvin yleisiä.	▲ Pilvipalveluiden käyttäjätilit ovat joutuneet lukuisten kalastelukampanjoiden kohteeksi.	▶ Toimitusjohtaja- ja laskutushuijaukset osuvat myös valtionhallintoon.
PALVELUNESTO-HYÖKKÄYKSET	▶ Murrettuja kotireitittimiä ja muita IoT-laitteita käytetään mm. palvelunestohyökkäysten tekemiseen.	▶ Palvelunestohyökkäykset ovat arkipäivää. Hyökkäysten torjuntaa suunniteltava, jotta organisaation verkkopalvelut pysyvät toiminnassa.	▶ Palvelunestohyökkäykset ovat arkipäivää. Sekä omat että palvelutoimittajalta ostetut verkkopalvelut suojattava.
HAITTAOHJELMAT JA HAAVOITTUVUUDET	▲ Haittaohjelmat tarttuvat nopeasti internetiin turvattomasti kytkettyihin IoT-laitteisiin.	▲ Internetiin turvattomasti kytkettyjä palvelimia etsitään ja murretaan. Haittaohjelmia levitetään sähköpostin liitteinä.	▶ Haittaohjelmia levitetään sähköpostin liitteinä.
VAKOILU	▶ Poliittisesti arkaluontoisia aiheita käsittelevät SOME-aktiivit voivat joutua kybervakoilun kohteeksi.	▲ Kriittisen infrastruktuurin yritysten vakoilu näyttää lisääntyneen.	▶ Valtionhallinto on edelleen merkittävä kybervakoilun kohde.
ESINEIDEN INTERNET, IOT	▶ Yksityisiä tietoja paljastuu verkkoon kytkettyjen, mutta suojaamattomien laitteiden kautta. Laitteita hyödynnetään myös bottiverkoissa.	▲ Verkkoresursseihin voi päästä käsiksi IoT-laitteiden turvallisuuspuutteita hyödyntämällä. Laite- ja käyttäjätietoja voi päätyä hyökkääjien käsiin myös julkisista lähteistä.	▲ IoT-laitteisiin liittyy erityisesti maineriski. Esimerkiksi älykellojen kautta on mahdollista seurata sotilaiden liikkeitä ja sijaintia.
VIESTINTÄVERKOT	▶ Digitaalisten palveluiden käyttö kasvaa, silti niiden toimivuudesta ei olla täysin riippuvaisia. Lyhyiden häiriöiden sietokyky on hyvä.	▲ Häiriöt vähenevät, mutta riippuvuus digitaalisista palveluista lisääntyy. Koska varautuminen häiriöihin on puutteellista, vaikutukset säteilevät kuluttajiinkin.	▲ Riippuvuus digitaalisista palveluista kasvaa. Varautuminen häiriöihin on vaihtelevaa.

KYBERTURVALLISUUS-KESKUS PALVELEE

Neuvontaa ja valvontaa tietoturvallisten ympäristöjen hyväksi

” Tietoturvaneuvonnan tarve on selvästi lisääntynyt.

Oppeja tietoturva-arvioinneista 2018

Arviointikohteissa oli vuoden aikana hurjia eroavaisuuksia, myös tietoturvaneuvonnan tarve oli selvä. Edellisvuosien tapaan tietojärjestelmäarvioinneissamme havaitsimme suojausten tason vaihtelevan merkittävästi. Myös arviointikohteiden skaala oli laaja.

Pienimuotoisin kohteemme oli muista ympäristöistä fyysisesti eriytetty erillistietokone. Tällaisissa tapauksissa keskityimme arvioimaan hallinnollisen ja fyysisen turvallisuuden lisäksi erityisesti hajasäteilyyn sekä tuotantoprosessiin liittyviä suojausmenetelmiä. Kun taas kyse oli useassa maassa ja useiden eri organisaation käyttämästä tietojärjestelmäkokonaisuudesta, arvioimme erityisesti turvallisuuden hallinnointia sekä toimitusketjujen turvallisuuteen liittyviä suojauksia.

Työssämme kävi selväksi, että tietoturvaneuvonnan tarve on selvästi lisääntynyt. Neuvoja kaivattiin sekä tietojärjestelmien tehokkaaseen suojaamiseen että koko yhteiskunnan kyberturvallisuuden varmistamiseen. Erityisesti tukea tarvittiin tietojärjestelmien suunnitteluun ja organisaatioihin kohdistuvien riskien tunnistamiseen.

Kohti parempaa yritysturvallisuutta

Tavoitteenamme on parantaa yritysturvallisuutta yhdessä tietoturvallisuuden arviointilaitosten kanssa. Yhteistoiminta on jo ottanut ensiaskelensa, ja hyväksi todettuja menetelmiä muodostuu vähitellen.

Yhteistoimintaa kehitetään suunnitelmallisesti muun muassa vuosikellon avulla. Sen tarkoituksena on tehdä organisaatioiden välisestä toiminnasta säännöllistä, lisätä tapaamisia, antaa koulutusta, yhtenäistää toimintatapoja – ehkä tärkeimpänä – luoda keskusteluyhteyksiä.

1 Resursoi ja huolehdi osaamisesta
Organisaatiot eivät resursoi tietoturvaa riittävästi. Ilman asiantuntemusta on lähes mahdotonta huolehtia toiminnan turvallisuudesta saati ylläpitää sitä. Erityisesti toimintaa tukevien järjestelmien tietoturvan suunnittelun tulisi olla asiantuntevissa käsissä, jotta vältytään ali- tai ylilyönneiltä.

2 Tunnista suojattavat kohteet ja kriittiset tiedot
Jos suojattavia tietoja ei tunnisteta tai määritellä, palveluiden toteutukseen liittyvät riskit ja kustannukset kasvavat. Pahimmillaan päädytään hallitsemattomiin arkkitehtuuriratkaisuihin. Tilanne on mahdollinen esimerkiksi silloin, jos suojattavaa kohdetta ei ole eriytetty riittävästi muista järjestelmistä.

3 Palveluita ei voi toteuttaa tietoturvallisesti, jos tarvittavaa osaamista ei itsellä ole
Palveluita ulkoistaessa on huomioitava, että palveluntarjoajan kanssa sovitut velvoitteet ja vastuut ovat tarkkaan määritellyt ja riittävät. Esimerkiksi poikkeamatilanteessa palveluntarjoaja ei toimitakaan tarvittavia tietoja tilanteen korjaamiseksi, päivityksiä voidaan laiminlyödä ja tietoturvattomia hallintayhteyksiä käyttää.

4 Oman verkon tapahtumia, poikkeamia ja lokeja pitää seurata
Vaikka järjestelmälokia pidettäisiinkin, lokit eivät välttämättä ole tarpeeksi kattavia. Niitä ei seurata tai ne voivat olla esimerkiksi aikaleimoiltaan niin ristiriitaisia, että tarvittavia tietoja ei pystytä selvittämään.

5 Todenna järjestelmien tietoturvallisuuden taso
Arviointia ei ole välttämättä tehty lainkaan, tai siitä vastaa kaupallisin perustein arviointipalvelua myyvä yritys. Tällöin arvioinnin riippumattomuus voidaan kyseenalaistaa. Kyberturvallisuuskeskuksen tai hyväksytyn arviointilaitoksen arvioinnit antavat riippumattoman kuvan järjestelmän turvallisuudesta.

Galileo sai suomalaiset satelliittiosaajat liikkeelle

Kulunut vuosi oli työntäyteinen erityisesti kyberturvallisuuden koordinaatiotyön parissa EU-yhteistyöelimissä. Puheenjohtajamaana muun muassa isännöimme syyskuussa EU-maiden PRS-viranomaisten yhteistapaamista Helsingissä.

Eurooppalaisten Galileo-satelliittien kattavuus on nyt maailmanlaajuinen. Tämä on lisännyt myös suomalaisten osaajien halukkuutta osallistua PRS-palvelun kansallisen osuuden rakentamiseen. Käsittelimme aihetta marraskuisessa työpajassa, johon osallistui yhteensä 80 edustajaa viranomaisista ja kriittisen infrastruktuurin yrityksistä.

Vuonna 2018 kotimaista PRS-yhteistyötä rakennettiin muun muassa Paikkatietokeskuksen ja puolustusvoimien kanssa. Yhteistyötä tiivistämässä oli myös virastomme taajuushallinto.

Suomessa EU:n oma Galileo-satelliittipaikannus saataneen käyttöön 2020-luvun alussa. Sen avulla voidaan nykyistä paremmin suojautua muun muassa gps-paikannuksen häirinnältä. Häirintä nousi esiin marraskuussa Lapissa, ja se yhdistettiin Naton suursotaharjoitukseen.

Ketterää ohjausta ja napakkaa valvontaa

Oikein käytettynä sääntely on hyvä työkalu, jolla yhteiskunnan kyberturvallisuutta ja häiriösietoisuutta voidaan parantaa.

Vuonna 2018 tietoturvallisuus ja varautuminen ovat näkyneet entistä enemmän lainsäädännön valmistelutyössä. Muutos on ollut havaittavissa etenkin säädännössä, joka koskee sähköisen asioinnin turvallisuutta tai tärkeän tiedon käsittelyä verkko- ja tietojärjestelmissä. Suuntaus on ilahduttanut, mutta myös työllistänyt keskustamme konsultointi- ja lausuntopyyntöinä.

Käsittelimme vuoden jälkimmäisellä vuosipuoliskolla 50 lausuntopyyntöä. Näistä jokaiseen liittyi jokin kyberturvallisuutta, tietoturvallisuutta tai varautumista koskenut näkökulma. Asiantuntijamme ovat olleet tuttuja vieraita niin työryhmissä kuin eduskunnan valiokunnissakin.

”Vuonna 2018 tietoturvallisuus ja varautuminen ovat näkyneet entistä enemmän lainsäädännön valmistelutyössä, käsittelimme syyskaudella 50 lausuntopyyntöä.

Kuvassa Galileo-satelliitti. PRS eli public regulated service on viranomaisille tarkoitettu satelliittipaikannuksen sijainti- ja aikapalvelu. Palvelun käyttäjiä hallinnoi ja avaintenjakelun toteutuksesta vastaa kussakin EU-maassa PRS-viranomainen, joka Suomessa on Liikenne- ja viestintävirasto, Traficom.

EU-sääntelyhankkeiden vaiheista on oltava perillä

Lainsäädännössä muutokset eivät tapahdu nopeasti. Työssä olennaista onkin erityisesti EU-säädäntömuutosten seuraaminen ja niihin varautuminen. Kuluneena vuonna olemme tiiviisti seuranneet muun muassa viimeksi 2009 muutetun sähköisen viestinnän direktiivipaketin kokonaisuudistusta (niin kutsuttu telekoodi), EU:n sähköisen viestinnän tietosuoja-asetuksen valmistelua (ePrivacy) ja EU:n kyberturvallisuusasetuksen etenemistä. Puhumattakaan vahvan sähköisen tunnistamisen luottamusverkostosääntelyn muutoksista, joiden kiireellisen valmistelun liikenne- ja viestintäministeriö käynnisti syksyllä.

Keväällä saatiin päätökseen tärkeä EU-hanke, kun NIS-direktiivinä tunnetun verkko- ja tietoturvallisuusdirektiivin vaatimukset tulivat voimaan. Direktiivi asettaa tietoturvan seurantaan ja raportointiin minimivelvoitteet yhteiskunnan kriittisille aloille ja sen perusteella saamme jatkossa laajemmin erialoilta tietoa tietoturvallisuuden tilanteesta. Tietoa voidaan tulevaisuudessa hyödyntää kyberturvallisuuden kehittämisessä.

Tietoturvallisuus- ja häiriöraportointivelvoitteet koskevat nyt myös digitaalisia palveluita eli pilvipalveluita, hakukoneita ja verkon markkinapaikkoja. NIS:in tietoturvavelvoitteita on noudatettava lisäksi energia-, liikenne-, finanssi-, ja terveydenhuoltotoimialalla sekä juomaveden jakelussa. Kutsuimme näiden alojen valvovat viranomaiset työryhmään, jossa ohjausta, osaamista ja valvontaa voidaan koordinoida. Direktiivin soveltamista tarkastellaan yhdessä myös muiden jäsenvaltioiden valvojien kanssa.

Sääntelyyn perustuva valvontamme koskee monenlaista toimintaa ja toimijaa.

Tähtäimessä luotettavat sähköiset palvelut

Sääntely ei ollut yhtä nopeaa kuin vaikkapa ohjelmistokehitys edes vuonna 2018, silti määräyksissämme ja muussa ohjauksessamme pyrimme toimimaan mahdollisimman ketterästi. Ennakoimme ja arvioimme, mitä säädetyt vaatimukset tarkoittavat valvomillemme yrityksille ja muille yhteisöille käytännössä. Tämä kaikki vie aikaa. Avoin yhteistyökin on ollut meille arvokasta mutta myös välttämätöntä, koska näin saadun tiedon avulla olemme pystyneet huomioimaan käytännön vaatimukset sääntelyn kehittämisessä ja tulkinnassa.

Kuuntelemme, otamme huomioon, mutta olemme myös vaativia. Säädettyjä vaatimuksia on kaikkien noudatettava, mutta laadimme määräyksiä sekä neuvomme säädösten tulkinnassa niin, että toimijat tietävät, mitä heiltä vaaditaan ja mitä he voisivat tehdä paremmin. Näin voimme olla mukana kehittämässä valvomiemme toimijoiden palveluiden luotettavuutta.

Valvontakeinoihin turvaudumme tarvittaessa. Loppuvuodesta patistelimme vielä viimeisiä vahvan sähköisen tunnistuksen tarjoajia lopettamaan TLS 1.0:n käyttöä. Kuluneena vuonna asiantuntijamme tapasivat myös useita seutuverkkotoimijoita, kun viestintäverkkojen varmistusten määräyksenmukaisuutta tarkastettiin.

Yhteistyötä ja tiedonjakoa

Tiedonvaihtoryhmissä saadaan parhaat opit

Yhteistyö ja tiedonvaihto valtionhallinnon ja huoltovarmuuskriittisten yritysten kanssa on keskeinen osa Kyberturvallisuuskeskuksen toimintaa. Etenkin tiedonvaihtoryhmissä, eli ISACeissa (Information Sharing and Analysis Centre), joiden toimintaa koordinoimme, yhteistyö on tiiveimmillään.

Yhteiskunnan toiminnan kannalta merkittävillä toimialoilla on omat ISAC-ryhmänsä, joissa etsitään alaan liittyviä tietoturvaratkaisuja sekä jaetaan tietoa ajankohtaisista kyberuhkista ja -ilmiöistä. Yhteistyöstä hyötyvät ryhmissä mukana olevat organisaatiot, viranomaiset ja ennen kaikkea kansalaiset. Tuemme organisaatioita, jotka toteuttavat yhteiskunnalle kriittisiä ja kansalaisille tärkeitä palveluja pitämään huolta tietoturvallisuuden ylläpidosta ja kehittämisestä liiketoiminnallisissa ratkaisuissaan.

Ryhmiä eri toimi aloilta valtionhallinnosta mediaan on tällä hetkellä 13. Uusin tiedonvaihtoryhmä on syksyllä perustettu VESI-ISAC. Energia-alan tiedonvaihtoryhmän, entisen E-CIPin nykyisen E-ISACin, toiminta on pitkäikäisintä. Ryhmien toiminnan kehittämiseen on panostettu merkittävästi myös vuonna 2018. Työhön olemme saaneet lisäresursseja Kyber 2020 -ohjelmasta.

Toimialakohtaisissa ryhmissä on mahdollista keskittyä juuri toimialalle ominaisiin haasteisiin ja uhkiin. Vuoden 2018 aikana eri ryhmissä on käsitelty muun muassa vaalivarautumista, palvelunestohyökkäyksiltä suojautumista, reitittimien tietoturvaa ja automaatioympäristöjen etäyhteyksien tietoturvan varmistamista sekä harjoiteltu tiedonvaihtoa häiriötilanteissa.

Vaikka ryhmissä on eroavaisuuksia, suuri osa aiheista on kaikille yhteisiä. Harmaita hiuksia aiheuttavat muun muassa pilviratkaisujen tietoturvan varmistaminen ja henkilöstön kouluttamiseen liittyvät kysymykset. Nopeasti muuttuvan teknologiaympäristön ja kustannustehokkuuden nimissä yhä useamman organisaation on ulkoistettava tietoturvapalveluitaan. Toimiakseen ulkoistukset sopimuksineen vaativat erityisosaamista.

Energia-alan tiedonvaihtoryhmä palkittiin ansiokkaasta yhteistyöstä

Energiatoimiala on paljon vartijana yhteiskunnan toiminnan turvaajana. Tämä on ymmärretty hyvin toimialan osaajien parissa, jotka toimivat aktiivisesti yhteistyössä alansa kyberturvallisuuden kehittämiseksi. Palkitsimme E-ISACin Tietoturvan suunnannäyttäjä -palkinnolla esimerkillisen yhteistyön ansiosta keväällä 2018.

Vuoden 2018 aikana energiatoimialalla korostui ongelmiin etukäteen varautumisen, yhteistoiminnan ja omien toimintojen kehittämisen ja niiden harjoittelun tärkeys.

Syyskuussa Olkiluodon ydinvoimalassa järjestettiin TURVA18-harjoitus. Lokakuussa TIETO18:ssa energia-alan toimijat olivat muiden yritysten ja viranomaisten kanssa harjoittelemassa laajojen kyberturvahäiriöiden varalta. Marraskuisessa Black Screen II –harjoituksessa keskityttiin kyberuhkien hallintaan yhdessä pohjoismaisten kantaverkkoyhtiöiden ja alan viranomaisten kesken. Puolestaan Kyber-ENE2-projektissa parannettiin kriittisiä energiatuotteita ja -palveluja tuottavien alan toimijoiden kyberturvallisuutta. Erilaisia kyberturvallisuuteen liittyviä työpajoja ja harjoituksia tullaan järjestämään myös vuoden 2019 aikana.

Microsoft Office 365 -huijauskampanja väritti vuotta 2018. Kesällä saimme tietoomme lukuisia onnistuneita ja läheltä piti -huijauksia ISAC-ryhmiemme kautta. Tietojen perusteella arvioimme tilanteen Suomessa vakavaksi ja julkaisimme huijauskampanjasta kriittisen varoituksen. Varoitus auttoi suomalaisia organisaatioita suojautumaan huijaukselta ja sen aiheuttamilta vahingoilta. ISACeilta on myös saatu merkittävää apua ja ohjeistusta Office 365 -huijauksilta suojautumiseksi.

ISAC-toimialojen 2018 kuulumiset

TOIMIALA	ERITYISPIIRTEET	AJANKOHTAISTA
VALTIONHALLINTO	Runsaasti lakisääteisiä ja kansainvälisistä velvoitteista johtuvia tietoturvavaatimuksia. Tarve pohtia tarkasti esimerkiksi tiedon maantieteelliseen säilyttämiseen liittyviä kysymyksiä.	Tulossa keväällä useat vaalit ja syksyllä Suomen EU-puheenjohtajuuskausi.
FINANSSI	Varauduttu hyvin ”uudeksi normaaliksi” muodostuneisiin palvelunestohyökkäyksiin. Pankkien haasteena kalasteluviestit.	Yhteistyön kansainvälistyminen ja erityisesti pohjoismainen yhteistyö. NIS-velvoitteiden käyttöönoton seuranta.
VESIHUOLTO	Voimakas riippuvuus automaatiojärjestelmistä, joten niiden suojaaminen tärkeä yhteistyökohde.	Aloittanut ISAC-yhteistyötoiminnan vuonna 2018. NIS-velvoitteiden käyttöönoton seuranta. HVK:n Kyber-vesi -hanke toi työkaluja vesihuollon kyberturvallisuuden kehittämiseen.
TELEYRITYKSET (ISP)	Ratkaisut tehokkaaseen tiedonvaihtoon kyberuhkista niin häiriötilanteisiin varautumisessa kuin operatiivisissa häiriötilanteissa.	Teleoperaattoreiden yhteinen harjoitus laajoihin häiriötilanteisiin varautumiseksi.
SOTE	Terveydenhuollon asiakastietojen tietoturvallisen jakamisen menetelmät.	HVK:n Kyber-Terveys-hanke kehittää laajasti alan kyberturvallisuutta. STM:n SOTE-palveluntarjoajien varautumisohjeita päivitetty huomioiden kyberturvallisuus. NIS-velvoitteiden käyttöönoton seuranta.
ENERGIA	Runsaasti yhteistä harjoitustoimintaa. Ennalta varautuminen korostuu toiminnassa.	Meneillään Kyber-ENE2-projekti. Harjoituksia (esim. Olkiluodon ydinvoimalan TURVA18-harjoitus, TIETO18-harjoitus, Black Screen II –harjoitus). NIS-velvoitteiden käyttöönoton seuranta.
KEMIA JA METSÄTEOLLISUUS	Toiminta riippuvaista automaatiojärjestelmistä ja tuotantoa useassa maassa. Edellyttää tietoturvan toteuttamista erilaisissa työkulttuureissa ja lainsäädäntöympäristöissä.	IoT:n hyödyntämisen voimakas lisääntyminen sekä ulkoistamiseen liittyvät näkökulmat.
ELINTARVIKE JA KAUPANJAKELU	Toiminnan digitalisointi voimakasta, siirrytään automatisaatioon ja robotisaatioon.	Sähköpostiturvallisuuteen liittyvät kysymykset.
LIIKENNE	Liikenteen automatisaatio ja voimakas verkottuminen tulevaisuuden haasteita. Ala voimakkaassa muutoksessa.	ISAC aloittaa toimintansa 2019 alussa. NIS-velvoitteiden käyttöönoton seuranta.
MEDIA	Mediaorganisaatioiden tuotantojärjestelmien verkottuminen. Toimitusten ja toimittajien tietoturva.	Pilvipalvelujen asianmukainen suojaus. Vaalien tietoturvakysymykset mediaorganisaatioiden kannalta.

Kyberharjoitusten tukea ja suunnittelua

”Yhdessä tekemällä ja verkostoitumalla saadaan onnistumisia, jotka ovat osiensa summaa suurempia.

Oppimismahdollisuuksia ja parempaa kybervarautumista harjoittelemalla

Harjoitustoiminnan tavoitteena on parantaa organisaatioiden toiminta- ja toipumiskykyä vakavien tietoturvaloukkaustilanteiden varalta. Harjoituksessa simuloidaan kriisitilanne, jonka ratkaisemisesta harjoituksen osallistujat voivat saada arvokkaita oppeja.

Harjoituspalvelumme ovat osa Huoltovarmuuskeskuksen Kyber 2020 -hanketta, ja ne ovat huoltovarmuuskriittisten organisaatioiden käytettävissä. Autamme muun muassa sopivan yhteistyökumppanin löytämisessä, harjoitusskenaarion laatimisessa ja sopivan harjoitustavan valinnassa. Palvelujamme on myös hyödynnetty yhteisharjoitusten TIETO, KYHA ja TAISTO suunnittelussa ja järjestämisessä.

Harjoittelun avulla yhteistyön edut esiin

Huoltovarmuuskeskuksen syksyllä järjestämä TIETO18-harjoitus kokosi yhteen yli 120 yritysten ja viranomaisten edustajaa harjoittelemaan haastavien tietoturvatapahtumien ratkomista yhteistyöverkostojen avulla. Harjoitus järjestettiin kolmessa osassa, joista viimeinen vaihe tulosten purkuineen kesti 3 päivää.

Harjoitusta varten luotiin kuvitteellisia organisaatioita, jotka yhteistyössä torjuivat lukuisia tietoturvauhkia. Viranomaiset olivat mukana ratkomassa ongelmia ja rakentamassa toimintamalleja uhkatilanteista selviytymiseksi. Harjoitukseen toi oman mausteensa YLE, joka järjesti oman valmiusharjoituksensa samanaikaisesti. Osallistujat pääsivät antamaan haastatteluja oikeille toimittajille, ja paikan päältä lähetettiin myös harjoitusuutisia toisen harjoituspäivän ajan.

Viranomaistoimintakin hyötyy verkostoitumisesta

Turvallisuusviranomaisten oma KYHA-harjoitus Jyväskylässä asetti viranomaiset tosipaikan eteen. Harjoitusympäristöön oli luotu tietojärjestelmiä, joita vastaan harjoituksen järjestäjien kokoama ”punainen tiimi” hyökkäsi.

Myös KYHA-harjoituksessa keskityimme luomaan tiedonvaihtoverkostoja ja muodostamaan tilannekuvaa, jonka perusteella olisi mahdollista tehdä oikea-aikaisia ja perusteltuja ratkaisuja.

Suuret KYHA- ja TIETO18-harjoitukset olivat hyviä esimerkkejä kyberyhteistyöstä, jossa yhdessä tekemällä ja verkostoitumalla saadaan onnistumisia, jotka ovat osiensa summaa suurempia.

Yhteisharjoitukset täydentävät erinomaisesti yritysten ja muiden organisaatioiden itsenäistä harjoittelua, jossa pelitilanteet rajoittuvat usein omien seinien sisään.

Harjoituksia, joiden suunnittelussa / toteutuksessa olemme olleet mukana.

2016: **10** kpl
2017: **9** kpl
2018: **20** kpl

”Erityisesti suunnitteluvaiheessa tuli hyviä kommentteja todentuntuisista skenaarioista ja mitä [tietoturvaloukkauksia] Kyberturvallisuuskeskus on nähnyt todellisessa elämässä.”
– Huoltovarmuuskriittinen organisaatio omasta harjoituksestaan

”Kyberturvallisuuskeskuksen toimiminen harjoituksen keskiössä oli keskeinen ja onnistunut osuus. Panos oli harjoituksen kannalta erittäin tärkeä.”
– Yhteisharjoituksen järjestäjä

Tulevaisuustyö ja toiminnan kehittäminen

Tulevaisuuteen valmistaudutaan yhteisvoimin

Virastoomme on muodostettu viestintäalan tulevaisuuden näkymiin ja kehitykseen keskittyvä asiantuntijaryhmä. Ryhmän tarkoituksena on tunnistaa uusia viestinnän ja kyberturvallisuuden ilmiöitä sekä teknologioita, jotka tulevat muuttamaan viranomaistoimintaamme, yhteiskuntaamme ja arkeamme.

Vuonna 2018 ryhmässä on keskitytty 5G-verkkoihin, kuluttajien IoT-tuotteisiin ja tähdätty myös pilvipalveluiden parempaan tietoturvallisuuteen. Olemme myös perehtyneet 5G- ja IoT-ekosysteemien toimintaan sekä satelliittiteknologian yhteiskunnallisiin vaikutuksiin.

Selvitys 5G-verkkojen kyberturvallisuudesta

Selvitimme, millaisia kyberturvallisuusriskejä kuluttajiin, yrityksiin ja viranomaisiin voi kohdistua, kun 5G-teknologia ja esimerkiksi yritysten liiketoiminnan kannalta kriittinen infrastruktuuri sulautuvat ja leviävät yhteiskunnan toimintojen jaetuksi tietojenkäsittelyalustaksi.

Selvitys antaa eväitä virastomme ennakoivalle ja ajantasaiselle sääntelytyölle. Näin 5G-teknologian käyttöönottoa harkitsevat toimijat pystyvät tekemään turvallisia ratkaisuja.

Työ on edistynyt hyvin ja aikataulussa, keskeiset riskit on tunnistettu ja tunnemme nyt paremmin erityisesti 5G:n sekä aiempien mobiiliteknologioiden väliset erot.

Erityistä huomiota vaativiksi uusiksi osa-alueiksi hankkeessa tunnistettiin

Tietojen välittämisestä käsittelyyn:
Tietojen välittämiseen keskittyneestä infrastruktuurista ollaan siirrytty kokonaiseen tietojenkäsittelyyn keskittyneeseen infrastruktuuriin pilvipalveluineen. Tämä on keskeisimpiä 5G-verkkoihin liittyviä muutoksia. Tietojen käsittely siirtyy yhä lähemmäksi loppukäyttäjiä, siten myös verkosta tulee monimutkaisempi ja keskinäisriippuvaisempi. Muutos vaikuttaa perinteisiin riskienhallinta- ja turvallisuusarkkitehtuurimalleihin, joiden kehittämisessä haluamme olla mukana kansallisesti ja kansainvälisesti.

Operaattorista käsittelyalustan tarjoaja:
5G-verkon arkkitehtuuri haastaa vanhan mallin, jossa teleoperaattorin on vain viestin välittäjä. 5G-teknologian reunalaskentatoiminnallisuuksien vuoksi operaattorin rooli muuttuu viestin välittäjästä myös tiedon käsittelyalustan tarjoajaksi. Samalla verkon ydin ja reuna lähestyvät toisiaan, ja teleoperaattorilla on entistä suurempi rooli loppukäyttäjätoimijoiden tietojen turvaamisessa.

Virtualisointi:
Virtualisointiin perustuvan reunalaskentakapasiteetin tarjoaminen loppukäyttäjille haastaa teleoperaattoreita ja verkkolaitevalmistajia uusin tavoin. Verkko muuttuu suljetusta avoimemmaksi ja sen tietoturvapäivityksiin on kiinnitettävä aiempaa enemmän huomiota. Virtualisointi on kustannustehokas tapa skaalata resursseja, mutta samalla siihen liittyvien riskien tunnistaminen ja hallinta ovat tentistä tärkeämmässä roolissa.

Viipalointi:
Verkon viipalointi ja verkkotoimintojen virtualisointi tuo loppukäyttäjien saataville entistä parempaa suorituskykyä tarjoavia palveluluokkia, joten 5G houkuttelee kriittisiäkin toimintoja tarjoavia toimijoita siirtämään verkkoliikenteensä mobiiliverkon päälle. Nämä migraatiot vaativat tarkan riskianalyysin, jossa huomioidaan myös fyysiseen turvallisuuden uhkien muutokset.

Vuoden 2019 alkupuolella järjestämme 5G-hackathonin, jossa koetellaan 5G-verkon ja siihen keskeisesti liittyvien IoT-laitteiden häiriönsietoa ja turvallisuutta oikeissa käyttötilanteissa. Hackathoniin osallistuu kansainvälisiä tutkijoita virastomme haavoittuvuustutkijaverkostosta.

Tietoturvallinen-konsepti

Hyviä IoT-laitteiden ja pilvipalveluiden kyberturvallisuusperiaatteita on tarvittu jo jonkin aikaa. Tärkeänä on myös pidetty, että esimerkiksi kuluttajat voisivat tunnistaa tietoturvalliset laitteet ja palvelut niitä hankkiessaan.

Näihin tarpeisiin vastaamme Tietoturvallinen-konseptilla, johon kuuluvat vapaaehtoisuuteen perustuvat turvallisuusvaatimukset ja -periaatteet sekä Tietoturvallinen-leima. Leiman voi saada valmistaja, joka huomioi tietoturvan jo tuotteidensa tai palveluidensa suunnitteluvaiheessa.

Kokonaiskonseptia ja periaatteita viimeistellään. Lisäksi on aloitettu keskustelut sidosryhmien kanssa, jotta saisimme konseptista palautetta ja kehitysehdotuksia ennen käyttöönottoa. Yhteistyö digitaalisten palveluiden ja IoT-laitteiden valmistajien sekä jälleenmyyjien kanssa on ollut rakentavaa ja tuonut hyviä jatkokehitysideoita.

Selvitys satelliitti-teknologiasta

Mikä on todellinen satelliittiteknologian yhteiskunnallinen rooli? Kuinka tunnistaa toimijat, joilla on satelliitteihin ja avaruuteen liittyvää liiketoimintaa? Entä kuinka ennakoida liiketoimintaa tulevaisuudessa? Näihin kysymyksiin haluamme selvityksellämme vastata kuin myös löytää ne tavat, joilla suomalaisia toimijoita voitaisiin parhaiten tukea. Kuinka esimerkiksi tietoturvasta voitaisiin luoda kilpailuetu?

Satelliittiteknologian yleistymisessä voi jo nähdä teknologisen vallankumouksen aineksia. Ilmiö on verrattavissa esimerkiksi internetin arkipäiväistymiseen.

Seuraavaksi selvitämme, kuinka luoda otollisimmat olosuhteet satelliittiviestinnän tietoturvaan liittyville innovaatioille ja liiketoiminnan kasvulle.

Kyberturvallisuuden kehittämisohjelma KYBER 2020

Huoltovarmuuskeskuksen kyberturvallisuuden kehittämisohjelma, KYBER 2020, on ollut keskeinen tekijä toimintamme kehittämisessä jo vuodesta 2017. Ohjelman keskeisenä tavoitteena on turvata huoltovarmuuskriittisten yritysten toiminnan jatkuvuus kaikissa olosuhteissa. KYBER 2020 -ohjelman tukemana on käynnistetty ja tullaan käynnistämään useita kehittämishankkeita vuosina 2017 – 2020.

Keskuksemme toimintaa kehitetään tällä hetkellä kolmessa eri hankkeessa, joita ovat HAVARO 2.0, ISAC-tiedonvaihtoryhmät ja harjoitustoiminta. Hankkeiden avulla haluamme muun muassa parantaa kansallista havainnointikykyämme, kehittää harjoitustoimintaamme ja sujuvoittaa tiedonvaihtoa sekä yhteistyötä verkostoissamme. Lisäksi osallistumme kehityshankkeisiin, joissa keskitytään esimerkiksi energia- ja SOTE-alan kyberturvallisuuskysymyksiin.

HAVARO 2.0 -palvelulla parempaa suojaa vakavilta tietoturvauhkilta

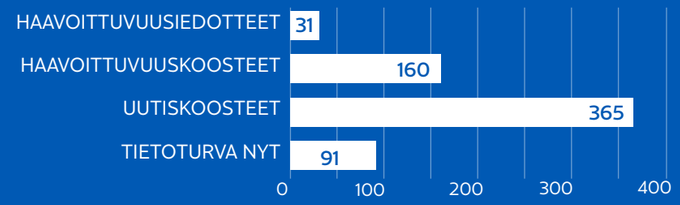
HAVARO-palvelumme on rakennettu organisaatioiden käyttöön vakavien tietoturvauhkien havainnoinnin avuksi. Nyt palvelu on kehitysvaiheessa versioon Havaro 2.0, jossa viranomaispalvelusta ollaan siirtymässä kaupallisten toimijoiden ja Kyberturvallisuuskeskuksen yhdessä tuottamaan palveluun.

HAVARO 2.0 -hankkeen tavoitteena on luoda luottamusverkosto, jossa jäsenet voivat keskenään vaihtaa tietoa entistä paremmin. Nopean ja luotettavan tiedonvaihdon avulla HAVARO-palvelua voidaan ylläpitää ja kehittää vastaamaan kyberuhkien määrällistä ja laadullista kehitystä, kuitenkin kohtuullisin resurssein. Toiminnan perustana tulee olemaan Havaro 2.0- järjestelmä, jonka ohjelmistokehitystyöstä tehtiin sopimus Reaktor Oy:n kanssa syyskuussa.

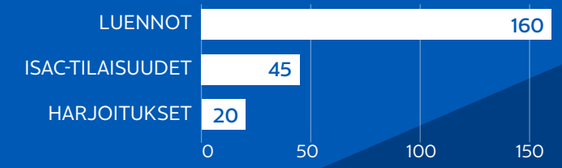
Toimintamme tunnuslukuja

Erityisesti viestintämme, harjoitustoimintamme sekä toimialayhteistyömme lisääntyivät vuonna 2018. Työtä kyberturvallisuuden edistämiseksi riittää, koska esimerkiksi Autoreporter-järjestelmä havaitsi Suomesta lähtöisin olevaa liikennettä huomattavasti enemmän kuin edellisvuonna.

Viestintä ja tiedotteet



Tilaisuudet ja harjoitukset



KATKEAMATON PÄIVYSTYS
2 4 / 7 / 3 6 5

VAROITUKSET **2**

KÄSITELLYT TAPAUKSET (”TIKETIT”) **6 100**

HÄIRIÖMÄÄRÄT: VAKAVIA **41** MERKITTÄVIÄ YHTEENSÄ **67**

HAAVOITTUVUUSKOORDINAATION KÄSITTELEMÄT TAPAUKSET **35**

HAITALLISTEN SIVUSTOJEN ALASAJOT **500**

FACEBOOK-SEURAAJAT **5 135**

TWITTER-SEURAAJAT **8 356**

MEDIAYHTEYDENOTOT **187**

AUTOREPORTER **154 000**

TILANNEKUVATUOTTEISIIMME OLLAAN TYYTYVÄISIÄ

Toteutimme vuoden aikana kolme asiakaskyselyä, jossa selvitimme asiakasorganisaatioidemme tyytyväisyyttä tilannekuvatuotteisiimme. Kyselyidemme arviointiskaala oli huonosta (1) kiitettävään (5).

OIKEA-AIKAISUUS:
4,1

SISÄLTÖ:
4,1

MERKITYKSELLISYYS:
4,1

KYSELY TOIMIALOJEN TIEDONVAIHTORYHMILLE:

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

ARVOSANA:
4,1

HAASTATTELUTUTKIMUS SIDOSRYHMILLE:

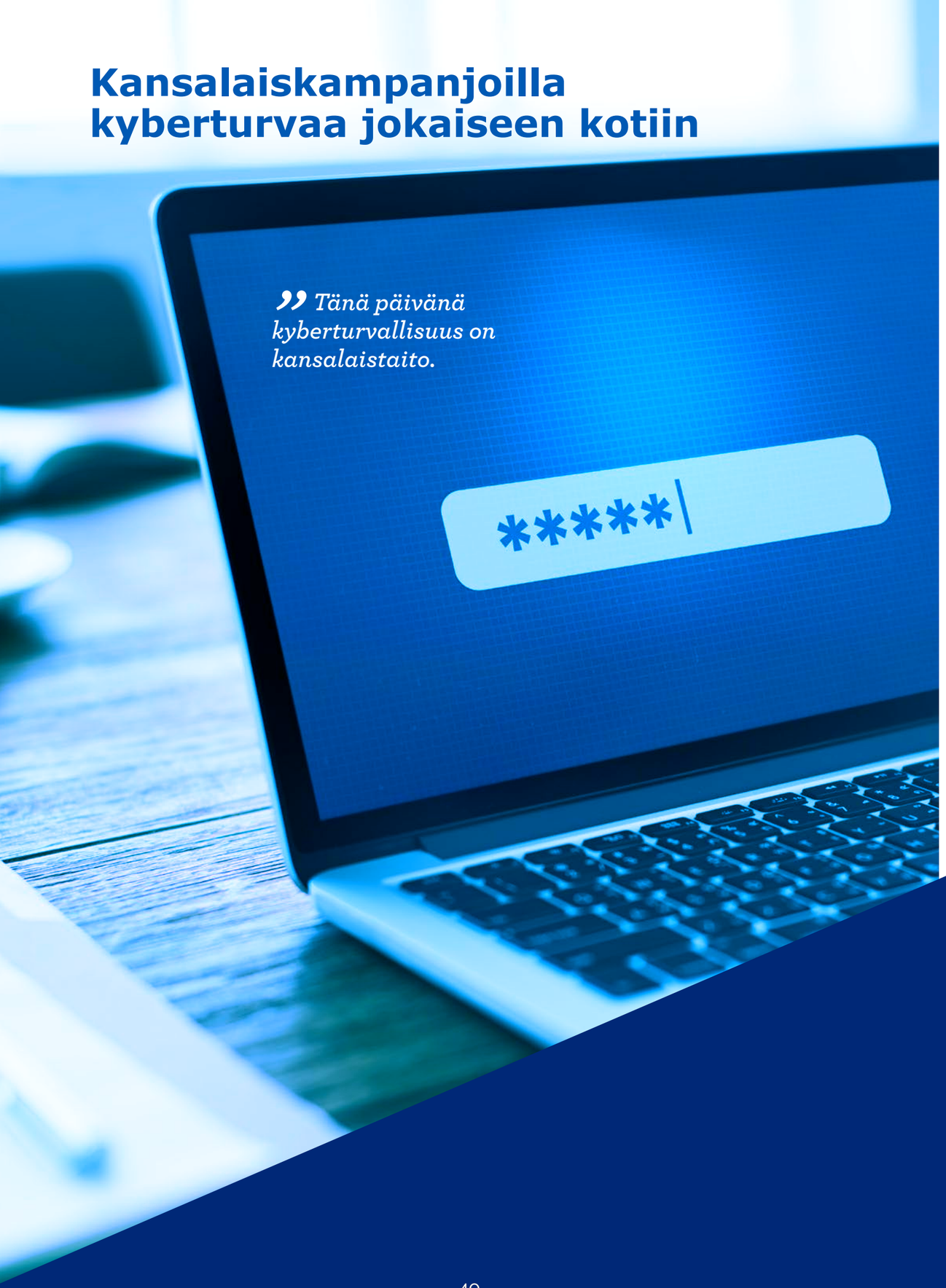
Tietoturvauhkiin liittyvän koordinoinnin ja avunannon onnistuminen.

ARVOSANA:
4,2

Kyselyyn vastaajista palvelujamme hyödyntää säännöllisesti, toisin sanoen päivittäin/viikoittain.

66 %

Kansalaiskampanjoilla kyberturvaa jokaiseen kotiin



Tunnetko Pidempi parempi -salasanalingon ja turvalisti Teijon?

Halusimme tuoda tietoturvan mahdollisimman monen lähelle ja kampanjoimme kyberturvallisuuden perustaitojen puolesta loppuvuodesta 2018. Pidempi parempi -salasanalinko ja turvalisti Teijo antoivat käytännöllisiä tietoturvavinkkejä.

Vinkkien lisäksi Teijo jakeli seuraajilleen turvalismeja eli tietoturva-aforismeja Turvalistit -somekanavilla ja verkkosivulla turvalistit.fi. Teijon pysäyttäviä tietoturvainterventioita voi seurata myös videoilla.

Arkemme sujuu, kun puhelimet ja tietokoneet toimivat ja pystymme esimerkiksi asioimaan verkkopankissa turvallisin mielin. Viranomaiset, sähköyhtiöt ja teleyritykset tekevät osansa, mutta vastuu kuuluu myös jokaiseen kotiin. Tänä päivänä kyberturvallisuus on kansalaistaito.

Pidempiparempi.fi-salasanalinko heittää esimerkin, jonka avulla luot itse omat salasanasi. Hyvä salasana on pitkä, ja sen tiedät vain sinä.

Muistathan nämä perusasiat

1. Luo pitkä ja ainutlaatuinen salasana jokaiseen käyttämääsi palveluun.
2. Päivitä laitteesi ohjelmistoineen säännöllisesti.
3. Varmuuskopioi tärkeät tietosi ja kuvasi.

KYBERSÄÄ 2018
JA KATSE KYBERVUOTEEN 2019

10 + 1 tietoturvanäkymää vuodelle 2019

1 Inhimillisen tietoturvan merkitys kasvaa

Tietoturvasuojausten kehittyessä ihmisten heikkouksien hyväksikäyttö nousee entistä voimakkaammin teknisten tietoturvauhkien rinnalle. Tekniikkaa tarvitaan edelleen, mutta lisäksi tarvitaan ihmisten osaamiseen ja käyttäytymiseen perustuvia suojautumisratkaisuja.

2 Internetiin liitettävien kuluttajalaitteiden tietoturvan merkitys korostuu

Heikko tietoturva aiheuttaa harmia niin IoT-laitteiden käyttäjille kuin muille internetissä asioiville. Tilannetta pyritään parantamaan yhä enemmän sääntelyllä, kansainvälisellä yhteistyöllä ja standardoinnilla. Onneksi kuluttajat ovat yhä kiinnostuneempia laitteidensa tietoturvasta ja -suojasta. Laitteen tietoturvasta kertova merkki tulee helpottamaan kuluttajien päätöksentekoa.

3 Riippuvuudet digitaalisista palveluista luovat yllättäviä tilanteita

Palveluiden, tuotteiden ja prosessien digitalisointi tuo merkittäviä tehokkuushyötyjä. Samalla syntyy uusia ketjumaisia riippuvuuksia ja kokonaisriskien näkyvyys voi pienentyä. Paine tehdä digitaalisuuteen nojaavia liiketoimintamuutoksia ja kokeiluja on kuitenkin suuri. Riskienhallinnalla on kova työ pysyä muutoksessa mukana.

4 Vähäisiksi arvioidut tutut uhkat pahenevat hiljalleen

Laajaa huomiota herättämättä tutut ja vähäisiksi arvioidut uhkat kasvavat massiivisiksi. Erityisesti tietojenkalastelu on yhä hankalampi vitsaus, ja tietojen urkinnasta tulee yhä kohdistetumpaa. Hyödyntämisyritykset vaihtelevat verkon pikkurikollisuudesta valtiolliseen toimintaan. Verkkorikolliset tavoittelevat erityisesti taloudellista hyötyä ja uhrilleen elintärkeitä tietoja.

5 Uudet teknologiat määrittävät 2020-luvun tietoturvahaasteet

Esimerkiksi koneoppiminen, robotiikka, 5G ja tekoäly ovat lähitulevaisuuden käyttöön otettavaa uutta teknologiaa. Niiden kehitykseenkin investoidaan paljon. Kuinka kehityksessä ja käyttöönotossa huomioidaan tietoturva, näyttää millaisten tietoturvahaasteiden kanssa painimme 2020-luvulla.

6 Pilvi tulee voimalla, ja muutos riemastuttaa ja huolestuttaa

Tietoturva edellyttää kykyä mukauttaa perinteisiin suojausratkaisuihin nojaava tietoturva ja pilvimaailma yhdeksi kokonaisuudeksi. Kysyntä uudelle ajattelulle ja innovatiivisille ratkaisuille kasvaa.

7 Tietoturvan ulkoistaminen lisääntyy

Erityisesti erilaiset tietoturvavalvomot ja SOC-palvelut lisääntyvät. Myös muita ulkoisia tietoturvapalveluja hankitaan yhä enemmän oman osaamisen tueksi.

8 Valtiollisten toimijoiden kyberhyökkäykset ja niistä uutisointi jatkuu

Kybertoimintaympäristössä toteutettavat hyökkäykset ovat tehokkaita, ja suora kiinnijäämisen pelko on pieni. Eri maat nostavat arvioitaan tekijöistä yhä voimakkaammin esiin.

9 Organisaatioiden tietoturvan perusasioissa on yhä parannettavaa

Esimerkiksi päivityksistä, varmuuskopioinneista ja salasanoista ei edelleenkään pidetä riittävästi huolta. Erityisesti palveluntarjoajien ja kumppanien kanssa tehtävissä sopimuksissa on tietoturvan kannalta paljon parannettavaa.

10 Tietoturva nousee osaksi liiketoiminta-lähtöistä riskienhallintaa

Tietoturva nousee yhä paremmin IT-osaston uumenista organisaatioiden kokonaisvaltaisen riskienhallinnan agendalle. Riskien omistajuus on annettava riskeihin liittyvien päätösten tekijöille. Tämä on ainoa tehokas keino taistella lisääntyviä kyberturvallisuusuhkia vastaan.

+1 Mobiililaitteisiin kohdistettuja haitta-ohjelmaepidemioita ei tulla näkemään

Olemme ennustaneet mobiilihaittaohjelmien esiinmarssia jo useana vuonna, mutta näin ei ole vielä koskaan käynyt.

Kybersää 2018

Vuoden merkittävimmät tietoturvapoikkeamat tammi-joulukuussa 2018

Tammi

Laskutushuijaus virastomme pääjohtajan nimissä

Havaintopiikki: Tilausansoja tekstiviestein

Meltdown- ja Spectre- hyökkäykset nousivat esiin

Tykkylumi häiritsi verkkojen toimintaa Kainuussa

Helmi

Memcached, historian voimakkain hyökkäys (1,7 Tbit/s)

Poikkeuksellisen paljon palvelunestohyökkäyksiä Suomessa

WannaMine tarttui useiden organisaatioiden palvelimiin Päijät-Hämeessä

Hyökkäyksiä olympialaisten tietojärjestelmiin

Maalis

Tapaus Cambridge Analytica

Huhti

Suomalaisten selväkielisiä salasanoja paljastunut liiketoimintasuunnitelma.com -sivustolta

Kaapattuja O365-sähköpostitilejä käytetään aktiivisesti huijauksiin

Kansainvälinen poliisioperaatio sulki webstresser.org-palvelun verkosta

Touko

Office 365 -sähköpostitilejä varastetaan

Runsaasti kotireitittimien haittaohjelmatartuntoja

VPNFilter-haittaohjelma levisi pienyritysreitittimiin ja verkkotallennuslaitteisiin maailmalla

Hide and seek -haittaohjelma leviää IoT-laitteisiin

VPNFilter-bottiverkko yhdistetty APT28-ryhmään

Kesä

Office 365 -tunnuksia kalastellaan aktiivisesti

IoT-laitteisiin tarttuvien louhintahaittaohjelmien esiinmarssi

Magecart-hyökkäys Ticketmaster-verkkokauppaan

Heinä

Office 365 -tunnuksia kalastellaan aktiivisesti

Pornokiristyskampanja: Tiedän salasanasi!

Urheilukellovalmistajien järjestelmistä tietovuotoja

Elo

Office-sähköposti-tunnuksia kalastellaan ja kaapattuja tilejä käytetään edelleen huijauksiin

Suomi.fi-verkkopalveluun palvelunestohyökkäys

Magecart-hyökkäys British Airwaysin verkkokauppaan

Haavoittuvuuksia faksien laiteohjelmistoissa, myös 3D-tulostimia suojaamattomina verkossa

SÄPO: Ruotsin parlamenttivaaleihin yritetään kybervaikuttaa

Syys

Office 365 -tunnuksia kalastellaan aktiivisesti, nyt myös väärennetyillä turvaposti-ilmoituksilla

OmaVeron nimissä kalastellaan maksukorttitietoja

suomi.fi taas hyökkäyksen kohteena

Vuoden 2018 suurin palvelunestohyökkäys Suomessa, volyymi 90 Gbit/s

Noin 50 miljoonan käyttäjätiedon vuoto Facebookista

Magecart-hyökkäys Newegg-verkkokauppaan

Satori-bottiverkon tekijäksi epäilty pidätettiin

Loka

Office 365 -tunnuksia kalastellaan aktiivisesti

Pornokirityshuijauksesta suomenkielinen versio

Kovter- ja Emotet-haittaohjelmahavainnot lisääntyvät

Port Smash -haavoittuvuus julki

Löydetty haavoittuvuuksia SSD-kiintoleivyistä

Marras

Office 365 -tunnuksia kalastellaan aktiivisesti

Marriot-tietomurto

Yandex-sovellus vuotaa tietoja

Saksan viranomaisten (BSI) kotireitittimien tietoturvallisuuskriteeristö

Joulu

Office 365 -tunnuksia kalastellaan aktiivisesti

Eu:n diplomaattiviestintää vakoiltu vuosien ajan tietojenkalastelua

Yhdysvaltain syyttäjä: APT10-ryhmän vakoilu ulottui myös Suomeen

= Kansainvälinen uutisnosto

Miten vuoden 2018 tietoturvanäkymät toteutuivat?

Arviomme kuluneen vuoden tietoturvailmiöstä osuivat oikeaan melko hyvin. Puolet näkymistämme toteutui, kaksi meni täysin metsään ja kolme luokittelimme rajatapauksiksi.

Oikein! Kyllä

Vuonna 2018 GDPR ja NIS saivat organisaatiot panostamaan tietoturvaan. Kun suurin osa Suomessa havaitsemistamme haittaohjelmatartunnoista johtui suojaamattomista ja päivittämättömistä IoT-laitteista, ennusteemme verkkoon hylätyistä IoT-laitteistakin piti paikkansa. Tietoturvaosaajista ei ollut liikaa tarjontaa; bug bountyt ja hackathonit lisäsivät avoimuutta sekä tietoturvatietoutta. Lisäksi ulkoistettuja toimitusketjuja hyödynnettiin tietomurroissa, ennusteemme mukaisesti.

Väärin meni! Ei

Päivitysketjuja ei käytetty hyväksi haittaohjelmien levityksessä odottamallamme tavalla. Ja hyvä niin. Rikolliset eivät myöskään hyökänneet yrityksiin sosiaalisen median kautta, vaan käyttivät lähinnä sähköpostia huijausten ja haittaohjelmien levitykseen. Rikollisten somehyökkäyksistä kärsivät eniten yksityishenkilöt.

Tavallaan kyllä, tavallaan ei... –

Vuonna 2018 innovatiivisten tietoturvatuotteiden ja tekoälyn liitto ei noussut ilmiöksi, vaikka teknisissä ratkaisuissa edistyttiin ja uusia kehitellään jatkuvasti. Automatiikkaa ja koneoppimista hyödynnetään jo runsaasti, valitettavasti myös kyberrikollisuudessa. Tekoälyä rikollisetkaan eivät näkyvästi hyödyntäneet. Kauppaa tehtiin enemmänkin palvelunestohyökkäyksillä, jotka saivat voimansa IoT-laitteista muodostuvista bottiverkoista. Murrettuja IoT-laitteita käytettiin myös kryptovaluutan louhintaan. IoT-haittaohjelmiakin havaitsimme, mutta epidemioilta vältyttiin.

1. Kyllä **GDPR ja NIS saavat organisaatiot panostamaan tietoturvaan**
2. Kyllä **Verkkoon kuolevat IoT-laitteet riesana**
3. Kyllä **Tietoturvaosaajien kysyntä työmarkkinoilla jatkuu**
4. – **Innovatiiviset tietoturvatuotteet hyödyntävät tekoälyä**
5. – **IoT houkuttelee rikollisia ja kiristyshaittaohjelmia**
6. Kyllä **Avoimuus lisääntyy (bug bounty, hackathon)**
7. – **Rikolliset tehostavat hyökkäyksiään tekoälyllä**
8. Ei **Päivitysten turvallisuutta horjutetaan**
9. Kyllä **Ulkoistettuja toimitusketjuja hyödynnetään tietomurroissa**
10. Ei **Some hyökkäysväylänä yrityksiin**

Uutiskoonti vuoden merkittävimmistä tapauksista

Huijaukset ja tietojenkalastelu

- **Office 365 -varoitus: Office 365 -tunnuksia kalastellaan aktiivisesti.**
  https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota
- **Huijarin pokka pitää – laskuhuijari esiintyy Viestintäviraston pääjohtajana:**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/01/ttn201801231206.html
- **Pornokiristyshuijaus:**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/07/ttn201807171603.html
  https://www.is.fi/digitoday/tietoturva/art-2000005848028.html
- **Huijauksia tekstiviestein:**
  https://www.mtvuutiset.fi/artikkeli/poliisi-varoittaa-huijausviesteista-ala-avaa-linkkia-ja-sulje-viesti/6747364#gs.bMJpkrtC
- **OmaVero:**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/09/ttn201809111520.html

Haavoittuvuudet ja haittaohjelmat

- **Meltdown & Spectre:**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/01/ttn201801041615.html
- **Wannamine:**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/02/ttn201802161123.html
- **VPNFilter:**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/05/ttn201805241306.html
  https://www.thedailybeast.com/exclusive-fbi-seizes-control-of-russian-botnet
- **Hide and seek -haittaohjelma leviää IoT-laitteisiin:**
  https://www.bleepingcomputer.com/news/security/hide-and-seek-becomes-first-iot-botnet-capable-of-surviving-device-reboots/
- **Kovter, mainoksia klikkaava haittaohjelma:**
  https://www.proofpoint.com/us/threat-insight/post/kovter-group-malvertising-campaign-exposes-millions-potential-ad-fraud-malware
- **Emotet, pankkihaittaohjelma:**
  http://blog.trendmicro.com/trendlabs-security-intelligence/new-malicious-macro-evasion-tactics-exposed-ursnif-spam-mail/
- **Port Smash -haavoittuvuus:**
  https://www.io-tech.fi/uutinen/intelin-prosessoreista-lo-ytyi-uusi-portsmash-sivukanavahaavoittuvuus/
- **SSD-kiintolevyjen haavoittuvuudet:**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/11/ttn201811081513.html

Tietovuodot ja -murrot

- **Cambridge Analytica & Facebook:**
  https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
  https://yle.fi/uutiset/3-10121765
- **Magecart-hyökkäykset**
  - **Ticketmaster**
    https://www.securityweek.com/ticketmaster-breach-tip-iceberg-major-ongoing-magecart-attacks
  - **British Airways**
    https://www.bleepingcomputer.com/news/security/british-airways-fell-victim-to-card-scraping-attack/
  - **Newegg**
    https://www.bleepingcomputer.com/news/security/newegg-credit-card-info-stolen-for-a-month-by-injected-magecart-script/
- **50 miljoonan käyttäjätiedon vuoto Facebookista:**
  https://yle.fi/uutiset/3-10430506
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/10/ttn201810011357.html
- **Urheilukellot:**
  https://www.mtvuutiset.fi/artikkeli/viestintavirasto-sijaintitieto-ja-maailmalla-levittaneesta-sovelluksesta-voi-tulla-yllatyksena-etta-tiedot-menevat-kaikille/6987790#gs.kQinniCY
- **Marriot-hotelliketjun tietomurto:**
  https://yle.fi/uutiset/3-10534789
- **Yandex-sovellus vuotaa tietoja:**
  https://www.mtvuutiset.fi/artikkeli/asiantuntija-yandex-kohusta-kyberturvallisuuskeskuksella-ei-ole-resursseja-tutkia-yksittaisten-sovellusten-tietoturvaa/7162778#gs.PZV5cZwA

Vakoilu

- **Olympialaisten tietojärjestelmiä yritettiin tuhota:**
  http://blog.talosintelligence.com/2018/02/olympic-destroyer.html
- **Ruotsin parlamenttivaalit & kybervaikuttaminen:**
  https://yle.fi/uutiset/3-10366498
- **Belgialaisoperaattori Belgacomin vakoilu:**
  https://www.theguardian.com/uk-news/2018/oct/25/uk-refusal-cooperate-belgian-hacking-inquiry-condemned-gchq-belgacom
  https://www.theregister.co.uk/2018/10/26/belgium_finds_evidence_gchq_belgacom_hack_proximus/
- **Hyökkäykset toimitusketjujen kautta:**
  https://www.tekniikkatalous.fi/talous_uutiset/yritykset/sahkoposti-harrastuskerhon-vetajalta-kyberrosvot-valmistautuvat-jo-todella-hyvin-keikkoihinsa-pystyy-jopa-tappamaan-6746737

Palvelunestohyökkäykset

- **webstresser.org-palvelun alasajo:**
  https://www.bleepingcomputer.com/news/security/europol-shuts-down-worlds-largest-ddos-for-hire-service/
- **suomi.fi-tunnistuspalveluun hyökkäys:**
  https://valtori.fi/artikkeli/-/asset_publisher/sunnuntain-12-8-palvelunestohyokkayksen-yksityiskohtia-selvitetaan
  https://yle.fi/uutiset/3-10349357?origin=rss
  https://vrk.fi/artikkeli/-/asset_publisher/suomi-fi-tunnistuksessa-on-kohdistetusta-palvelunestohyokkayksesta-johtuva-hairio
  https://legacy.viestintavirasto.fi/viestintavirasto/blogit/2018/ddosinternetinraksyttavarakkikoiraeisaaaikaanhaavaa.html
- **Memcached, historian voimakkain hyökkäys (1,7 Tbit/s):**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/02/ttn201802281537.html
- **Satori-bottiverkko:**
  https://portswigger.net/daily-swig/hacker-arrested-over-satori-botnet-malware

Viestintäverkkojen toimivuus

- **Kainuun sähkökatkot:**
  https://twitter.com/CERTFI/status/956127257755635712
  https://erveuutiset.erillisverkot.fi/blog/2018/01/24/sahkot-poikki-kainuussa/
- **Yksittäisten verkkojen häiriöt aiheuttivat katkoksia yhteiskunnalle tärkeisiin palveluihin:**
  https://yle.fi/uutiset/3-10207164
- **GPS-paikannuksen häirintä Lapissa:**
  https://yle.fi/uutiset/3-10498891

IoT

- **IoT-laitteisiin tarttuvat louhintahaittaohjelmat:**
  https://www.bleepingcomputer.com/news/security/prowli-malware-operation-infected-over-40-000-servers-modems-and-iot-devices/
  https://www.fortinet.com/blog/threat-research/pyromineiot--nsa-exploit--monero-xmr--miner---iot-device-scanne.html
- **Faksit ja 3D-tulostimet:**
  https://blog.checkpoint.com/2018/08/12/faxploit-hp-printer-fax-exploit/
  https://isc.sans.edu/diary/rss/24044
- **Saksan viranomaiset (BSI) & kotireitittimien tietoturvallisuuskriteeristö:**
  https://www.zdnet.com/article/germany-proposes-router-security-guidelines/

TRAFICOM
Kyberturvallisuuskeskus

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

YHTEYSTIEDOT
Kyberturvallisuuskeskus
Liikenne- ja viestintävirasto
Traficom
PL 320
00059 TRAFICOM