TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Marraskuu 2020

#kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Tämä tuote on ensisijaisesti suunnattu tietoturvasta vastaaville henkilöille. Lukija saa nopean kokonaiskuvan siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. Tilanne voi olla:

rauhallinen huolestuttava vakava

Kybersää marraskuu 2020

Tietomurrot ja -vuodot

- Useaan ministeriöön kohdistunut tietovuoto Virossa.
- Office 365 –tietomurrot jatkuvat, murrettuja sähköpostilaatikoita hyödynnetään kalasteluviestien lähettämiseen.

Huijaukset ja kalastelut

- Huijauspuhelut, Posti-teemaiset SMS-huijaukset ja O365-teemainen kalastelu jatkuvat vilkkaina.
- Häläripuhelut (wangiri) alkoivat jälleen lisääntyä, nyt suunnasta +212.
- Tietojenkalastelu on tärkeä työkalu myös kohdennettuja tietomurtoja tekeville rikollisille.

Haittaohjelmat ja haavoittuvuudet

- Emotet-tapausten määrä on vähentynyt, siitä tehty varoitus on poistettu.
- Fortinet VPN-laitteiden vanhoja haavoja on hyödynnetty.
- Pankkien nimissä tulevien turvapostien kautta on levitetty haittaohjelmia.

Automaatio ja IoT

- AWS:n häiriöt haittasivat mm. robotti-imureiden toimintaa ympäri maailman.
- Rikolliset käyttivät Suomessa sijaitsevia IoT-laitteita luottokorttipetosten verkkoliikenteen reitittämisen.
- Gitpaste-haittaohjelma tarttuu myös IoT-laitteisiin.

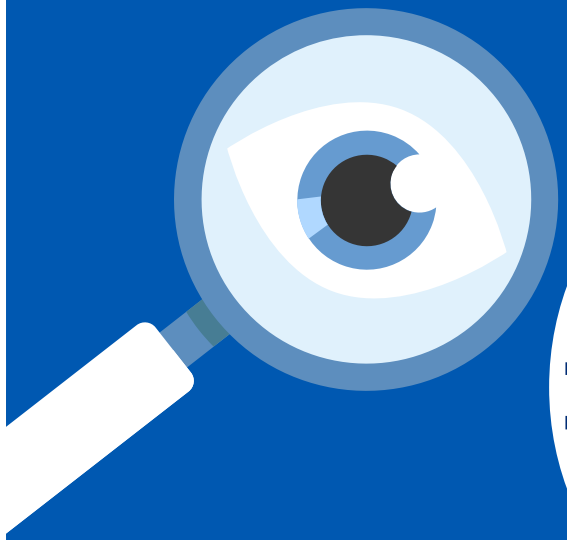
Verkkojen toimivuus

- Hieman keskimääräistä enemmän verkkojen häiriöitä.
- Saimme ilmoituksia palvelunestohyökkäyksistä, joilla oli myös laajoja vaikutuksia palveluiden toimintaan.
- Palvelunestohyökkäyksiin liittyviä kiristysviestejä ilmoitettu Kyberturvallisuuskeskukselle.

Vakoilu

- Tietoturvayritys FireEye joutui valtiollisen toimijan tietomurron kohteeksi, jonka tavoitteena oli saada valtiollisiin asiakkuuksiin liittyviä tietoja.
- COVID-rokotteita kehittäviä organisaatioita kybervakoillaan, taustalla useita toimijoita.
- Kohteena mm. Euroopan lääkevirasto.

Kuukauden tunnuslukuja



100 GBPS

ORGANISAATIOON KOHDISTETUN PALVELUNESTOHYÖKKÄYKSEN VOLYYMI. HYÖKKÄYS TEHTIIN OSANA ORGANISAATIOLLE TOIMITETTUA KIRISTYSVIESTIÄ VOIMAKKAAMMISTA HYÖKKÄYKSISTÄ.

KIRISTÄJIEN UHKAAMIA 2 TBPS HYÖKKÄYKSIÄ EI OLE KUITENKAAN NÄHTY.

12 000 €

SUURIN TEKNISEN TUEN HUIJAUKSESSA YHDELLÄ KERTAA MENETETTY RAHAMÄÄRÄ MARRASKUUSSA. SUMMA MAKSETTIIN TILISIIRTONA RIKOLLISTEN KÄYTTÄMÄLLE MUULITILILLE.

MARRASKUUN AIKANA MIKROTUKIHUIJAUKSILLA VARASTETTIIN 500 – 12 000 EURON SUMMIA.

4,41

KUINKA HYÖDYLLISIKSI KYBERTURVALLISUUSKESKUKSEN TILANNEKUVATUOTTEET KOETTIIN VUODEN 2020 AIKANA ASTEIKOLLA 1-5 (5 MAKSIMIARVO).

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Eri kyberhyökkäysmenetelmien käyttö kiristämiseen yleistyy ja uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

2

Tietojenkalastelu on erittäin yleistä, ja viestin vastaanottajan voi olla vaikea havaita huijausta. Tätä hyödynnetään myös kohdennetuissa hyökkäyksissä ja vakoilussa.

3

Haavoittuvuuksien hyväksikäyttö on nopeaa, mikä edellyttää nopeita päivityksiä. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja suojaustoimet sekä ylläpito ovat puutteellisia.

kohonnut

laskenut

ennallaan

Keltainen = uutta/ päivitettyä*

4

Heikko kyberriskienhallinta ja palveluidenhallinnan epäselvä vastuunjako. Kyberuhkien vaikutuksia ei osata ennakoida ja epäselvyydet palveluiden hallinnan vastuunjaossa heikentävät tietoturvaa.

5

Lokitietojen puutteellisuus on riski monessa organisaatiossa. Puutteellisen lokitietojen keruun, seuraamisen ja säilyttämisen takia poikkeamatilanteita ei kyetä havainnoimaan tai selvittämään.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

1

Eri kyberhyökkäysmenetelmien käyttö kiristämiseen yleistyy ja uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

- Tapauksia myös Suomessa. Suurin osa organisaatioista valikoituu kohteeksi heikon tietoturvan takia.
- Kyberrikolliset etsivät jatkuvasti verkosta haavoittuvia palveluita ja huonoja salasanoja sekä levittävät haittaohjelmia sähköpostitse.
- Uusia ilmoituksia laajoista kiristyshaittaohjelmatartunnoista tulee kansainvälisesti viikoittain. Lisäksi uusia rikollistoimijoita tulee jatkuvasti.
- Kiristyshyökkäysten uutena ilmiönä kohdetta kiristetään myös hyökkääjän haltuun saamien tietojen myymisellä, vuotamisella tai julkaisemisella lunnasvaatimuksen tehostamiseksi.
- Myös palvelunestohyökkäyksiä käytetään hyödyksi ja niillä uhkaillaan sekä kiristetään organisaatioita.

CASE

UUSI

Yhdysvaltain kriittisen infrastruktuurin ja kyberturvallisuuden virasto CISA ja FBI julkaisivat 28.10. varoituksen terveydenhuoltoon kohdistetuista kiristyshaittaohjelmahyökkäyksistä. Varoituksessa kerrottiin, että viranomaisilla oli tietoa välittömästä uhasta USA:n sairaaloita ja terveydenhuoltolaitoksia kohtaan tehtävistä koordinoiduista ja laajoista kyberhyökkäyksistä.

Julkisten lähteiden tietojen mukaan, varoitus tehtiin sen jälkeen kun viranomaiset olivat seuranneet rikollisten käymää keskustelua, jossa suunniteltiin ainakin 400 terveydenhuoltolaitokseen hyökkäämistä Ryuk haittaohjelmalla.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

2

Tietojenkalastelu ja muu käyttäjien manipulointi (social engineering) on erittäin yleistä, ja viestin vastaanottajan voi olla vaikea havaita huijausta. Tätä hyödynnetään myös kohdistetuissa hyökkäyksissä ja vakoilussa.

- Tietojenkalastelu on ollut hyvin yleistä pidemmän aikavälin tarkastelulla. Tyypillisesti rikolliset kalastelevat suomalaisilta Office 365 –tuotteiden ja sähköpostin käyttäjätunnuksia ja salasanoja.
- Uutena tapana on lähettää kokouskutsuja, jotka ovat kalastelulinkkejä
- Typosquatting / domainsquatting liittyvät myös ilmiöön: kirjoitusvirheillä höystetyillä verkkotunnuksilla voidaan tehostaa huijauksen vaikuttavuutta.
- Henkilökunnan koulutuksella on suuri merkitys. Tutkimusten mukaan tietojenkalastelua ja käyttäjän manipulaatiota opitaan tunnistamaan koulutuksen avulla, jolloin tietojenkalastelu jää vain yritykseksi.

CASE

Rikollinen onnistui tunkeutumaan yrityksen toimipisteen yhteisosoitteeseen Office 365 –tietojenkalastelun avulla. Sähköpostitililtä lähetettiin 800 kalasteluviestiä uusille uhreille. Lisäksi rikollinen oli luonut uusia käyttäjätilejä yrityksen ympäristöön murretun yhteistilin laajojen oikeuksien kautta.
Office 365 –kalastelua tapahtuu edelleen aktiivisesti. Monivaiheinen tunnistautuminen on tärkein keino suojautua sähköpostin tietomurrolta, vaikka tunnukset olisikin syötetty tietojenkalastelusivulle.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

3

Haavoittuvuuksien hyväksikäyttö on nopeaa, mikä edellyttää nopeita päivityksiä tai muita toimenpiteitä. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja joiden suojaustoimet ja ylläpito ovat puutteellisia.

- Rikolliset kehittävät hyväksikäyttömenetelmiä nopeasti heti ohjelmistopäivitysten ilmestyttyä ja tunnistavat kohteet, joita ei ole päivitetty. Erityisesti tietoturvatuotteissa olevat haavoittuvuudet ovat vakavia, sillä ne on yleensä sijoitettu muutenkin hyökkäyksille alttiisiin tietojärjestelmien kohtiin.
- Valtiolliset toimijat ovat tyypillisesti ensimmäisten joukossa hyödyntämässä uusia haavoittuvuuksia kybervakoiluun ja vaikuttamiseen. Valtiollisilla toimijoilla on myös riittävät resurssit päivitysten takaisinmallintamista varten uusien hyökkäysten mahdollistamiseksi kriittisissä ohjelmistoissa.
- Mitä pidempään haavoittuvuuden korjaamisessa kestää tai korjausta siirretään myöhemmäksi, sitä korkeammaksi hyväksikäyttämisen riski kasvaa.

CASE

UUSI

Marraskuussa hakkeriryhmä julkaisi 50000:n haavoittuvan VPN-laitteen tiedot verkossa. Haavoittuvuus oli tullut julki jo vuonna 2018 ja siihen oli ollut olemassa korjaava päivitys siitä asti.

Organisaatiot, jotka eivät olleet päivittäneet laitteitaan ajan tasalle joutuivat listalle. VPN-tunnukset mahdollistavat hyökkääjälle organisaation verkon haltuunoton ja esimerkiksi haittaohjelman asentamisen. On ensisijaisen tärkeää päivittää laitteet ajallaan, kuten tämäkin esimerkki opettaa.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

4

Heikko kyberriskienhallinta ja palveluidenhallinnan epäselvä vastuunjako. Kyberuhkien vaikutuksia toimintaan ei osata ennakoida, minkä vuoksi riskit aliarvioidaan. Epäselvyydet palveluntoimittajan, alihankkijoiden ja tilaajan vastuiden välillä heikentävät organisaation tietoturvan hallintaa.

- Tietoturvaloukkauksiin vastaamista tai niistä toipumista ei usein suunnitella riittävästi ennakkoon. Häiriön iskiessä siitä palautumisen monimutkaisuus ja työläys yllättävät.
- Tehdyt suunnitelmat tulee testata ja niitä pitää harjoitella.
- Epäselvä vastuunjako ICT-palveluiden hankinnassa ja tuotannossa heikentää tietoturvan hallintaa. Tämä pätee myös organisaatioiden sisällä jos tietoturvariskien omistajuus ja tietoturvavastuut eivät ole selkeästi määriteltyjä. Vastuut tulisi tehdä selväksi viimeistään hankinnan sopimusvaiheessa.

CASE

Organisaatio käyttää pilvipohjaista sovellusta (Software as a Service, SaaS) raporttien tekoon kumppaneidensa kanssa. Erään raportin julkaisussa tapahtuneiden epäselvyyksien johdosta pilvipalveluntarjoajaa pyydetään toimittamaan lokitiedot kyseisen raportin käsittelystä. Palveluntarjoaja vastaa, etteivät he voi luovuttaa lokitietoja, sillä heidän jaettuja resursseja käyttävät palvelut eivät erottele eri asiakkaiden lokitietoja. Tältä tilanteelta oltaisiin voitu välttyä, jos tämä vastuunjakoon liittyvä asia olisi sovittu jo sopimuksentekovaiheessa.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

5

Lokitietojen puutteellisuus on riski monessa organisaatiossa.
Poikkeamatilanteita ei kyetä havainnoimaan ja selvittämään mikäli oikeiden järjestelmien tai sovellusten lokitietoja
ei kerätä, seurata ja säilytetä riittävän kauan.

- Kattavan lokienhallinnan avulla tietomurto on mahdollista havaita jo alkuvaiheessa. Pahimmillaan joissain tapauksissa ei lokitietojen riittämättömyydestä johtuen koskaan saada selville milloin, miten ja kuinka laajalti ympäristöön on tunkeuduttu.
- Organisaatioiden on tunnistettava mitkä ovat heille keskeiset järjestelmät ja sovellukset tietoturvaloukkausten havainnoinnissa ja selvittämisessä sekä huolehdittava riittävästä lokitietojen keräämisestä ja niiden riittävän pitkästä varastoinnista.
- Tietoturvaloukkauksen selvitykseen tarvittavia lokitietoja olisi hyvä säilyttää vähintään vuoden ajan.

CASE

Yrityksen etäkäyttöpalvelussa on havaittu kirjautumiseen viittaavaa liikennettä epäilyttävästä lähteestä. Palvelusta ei kuitenkaan kerätä kirjautumislokeja, joten tapausta ei voida selvittää tämän pidemmälle.

Organisaation Windows-ympäristössä vain epäonnistuneista kirjautumisyrityksistä tehdään lokimerkintä. Tunkeutujan anastamilla tai itse luomilla tunnuksilla tehdyt kirjautumiset jäävät piiloon eikä tunkeutumisen laajuutta pystytä selvittämään.

Tietomurrot ja -vuodot

Tietomurroissa ja -vuodoissa käsitellään suojauskeinoja sekä tietoomme tulleita trendejä tietomurroista ja –vuodoista. Onnistuneilla tietomurroilla voidaan aiheuttaa kohdeorganisaatiolle esimerkiksi merkittäviä taloudellisia tappioita sekä mainetappioita.

Tietomurrot ja -vuodot

- Viron tietojärjestelmäviranomainen (RIA) tiedotti 1.12. kolmeen Viron ministeriöön kohdistuneesta tietomurrosta, joista on aiheuttanut merkittäviä henkilötietojen menetyksiä.
  - Hyökkäyksen kohteiksi joutuneet ministeriöt ovat Viron ulkoministeriö, sosiaaliministeriö sekä talouden- ja viestinnänministeriö
  - Tietomurtojen yhteydessä on anastettu henkilötietoja ja mm. tarttuvien tautien hallintaan liittyviä tietoja
    - Sosiaaliministeriöltä varastettu tieto sisälsi tarttuvien tautien hallintaan liittyviä tietoja, jotka koskivat 9158 henkilöä
    - Hyökkäyksellä oli myös vaikutuksia useisiin talouden- ja viestinnänministeriön käyttämiin palvelimiin, mutta niillä ei raportoidusti ollut vaikutuksia ministeriön tarjoamiin palveluihin.

ANALYYSI

- Kenen tahansa tiedot saattavat joutua tietovuodon kohteeksi
- Omien tietojen antamista tulee aina harkita tarkkaan ja pyytää poistamaan omat tiedot palveluista, joita ei enää käytä
- Olemme koonneet suomalaisten tietovuototapausten uhreille neuvoja ja ohjeita yhdelle sivulle https://www.tietovuotoapu.fi/fi/neuvoja-ja-ohjeita-tietovuodon-uhreille

Tietomurrot ja -vuodot

- Saamme edelleen paljon ilmoituksia Office 365-tietomurroista
  - Ilmoituksia onnistuneista tietomurroista ja niiden yrityksistä tulee tasaisella tahdilla
- Uhrin sähköpostitietoihin käsiksi päässyt rikollinen on jossain tapauksissa käyttänyt kaikkia viesteistä löytyneitä osoitteita hyväkseen uusien kalasteluviestien lähetyksessä
  - Harkitse, onko viestin vastaanottajien tarpeen nähdä toistensa sähköpostiosoitteet, vai olisiko parempi lähettää viesti piilokopiona (Bcc)
  - Tällöin et myöskään turhaan levitä muiden henkilötietoja ulkopuolisille ja suojaat samalla vastaanottajien yksityisyyttä

ANALYYSI

- Office 365 –tapauksissa monivaiheisen tunnistautumisen käyttäminen suojaa tehokkaasti tietomurrolta
- Tietomurron jälkeen luottamuksellista tietoa voi paljastua ja päätyä rikollisten käsiin
- Tiliä ja sieltä saatuja tietoja voidaan käyttää rikolliseen toimintaan kuten laskutuspetoksiin, tietojen kalasteluun ja haittaohjelmien levitykseen

Tietojenkalastelu – yleisin yrityksiin osuva verkkorikos Office365 huijauksen vaiheet:

Huijaukset ja kalastelut

Huijauksiin ja tietojenkalasteluun sisältyy käyttäjätunnusten ja salasanojen kalastelua, laskutuspetoksia, yrityshuijauksia, kiristyksiä ja muita vastaavia huijauksia. Lisäksi organisaatioihin voi kohdistua pankkitunnus- ja maksukorttikalastelua ja muita geneerisiä yksittäisten uhrien huijauksia.

Huijaukset ja kalastelut

- Marraskuuta ovat synkistäneet edelleen jatkuvat huijauspuhelut, posti-aiheiset tekstiviestihuijaukset ja entisestään lisääntynyt Office 365 -sähköpostipalvelun tunnusten kalastelu.
- Joulusesongin lähestyminen näkyy lisääntyneinä pakettiaiheisina huijauksina. Tekstiviesteissä kerrotaan saapuvasta lähetyksestä, joka on muka jäänyt odottamaan vastaanottajan toimenpiteitä. Viestin linkki johtaa kuitenkin huijarin sivulle, jossa kalastellaan luottokorttinumeroita.
- Marraskuun lopussa olemme nähneet aiemmin jo hiipuneiden hälärihuijausten lisääntyneen uudelleen. Uusia hälärihuijauksia on soitettu Marokon suuntanumerosta +212. Numeroon ei kannata soittaa takaisin.

ANALYYSI

- Joulusesonki näkyy pakettiaiheisina huijausviesteinä
  - Tekstiviesteinä lähetetään paljon Postin, DHL:n, UPS:n ja muiden kuriiriyritysten saapumisilmoituksiksi väärennettyjä viestejä. Huijauksissa voidaan väittää, että paketti on pysäytetty jakelukeskukseen, koska jokin maksu puuttuu.
  - Tekstiviestin linkki johtaa tietojenkalastelusivulle. Muutaman euron maksun varjolla uhrilta kalastellaan luottokortin numero. Ole yhteydessä pankkiisi, jos erehdyit syöttämään luottokorttisi numeron huijaussivulle.
  - Samalla pakettiteemalla tehdään paljon myös tilausansoja ja muita huijauksia.

Teknisen tuen nimissä soittelu jatkuu

- Sekä ulkomaisista että suomalaisista puhelinnumeroista soitetaan edelleen paljon puheluita, joissa yritetään huijata Microsoftin teknisen tuen nimissä.
- Tuntemattomaan numeroon vastaaminen ei ole vaarallista eikä siitä koidu kuluja. Soittajalle ei kuitenkaan pidä kertoa pankkitunnuksia, salasanoja eikä henkilötietoja.
  - Yhteistä tapauksille on soittajan halu saada ”asiakkaan” koneelle etähallintayhteys, jolla uhrin tietoihin pääsee käsiksi. Etäyhteyteen käytetään TeamVieweria tai muuta vastaavaa etähallintasovellusta.

ANALYYSI

- Valvomaton pääsy organisaation työasemalle määrittämättömäksi ajaksi on merkittävä tietoturvariski.
- Yrityksen tulee varmistaa keinot selvittää tapaus jälkikäteen. Uhri harvoin pystyy kertomaan tarkasti, mitä etäyhteyden kautta tehtiin teknisen selvittämisen mahdollistamiseksi.
- On tärkeä varmistaa lokituksen toimivuus, jotta mahdollinen onnistunut huijaus ja koneelle pääsy voidaan jälkikäteen selvittää niiden avulla.
- Turvallisuuskulttuurin merkitys korostuu: jos oviakaan ei avata tuntemattomalle, miksi tietokoneelle pitäisi päästä tuntematon taho?
- Yksityishenkilön ei ole tarpeen säilyttää käyttämätöntä etähallintaohjelmaa asennettuna laitteella.

Ammattirikolliset kalastelevat tietoja

- Tietojenkalastelu on keskeinen väline ammattirikollisten työkalupakissa. Sillä saa kerättyä tietomurtoihin tarvittavia tietoja, pankkitunnuksia, organisaatiorakenteita, henkilötietoja, käyttäjätunnuksia ja salasanoja.
- Pankkitietoja kalastellaan lähettämällä huijaussähköpostia, jossa pyydetään linkin kautta kirjautumaan sivustolle.
- Lue Tietoturva Nyt! -artikkelimme Neuvoja epäilyttävien sivujen tunnistamiseksi: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-epailyttavien-sivujen-tunnistamiseksi

ANALYYSI

- Siinä missä sähköpostihuijauksia voi tehdä vain lähettelemällä sähköpostia, onnistunut tietojenkalastelu vaatii laajempaa valmistelua ja huijaussivustojen laatimista.
- Monet näistä huijaussivustoista näyttävät hyvin uskottavilta. Sivut on tehty taitavasti ja niitä voi olla mahdoton tunnistaa nopealla katselulla. Takana voi olla kansainvälinen ammattirikollisryhmä.
- On tärkeä pohtia, mitä kautta sivulle surffaa ja välttää esimerkiksi sähköpostin kautta tulleita linkkejä ja kirjautua sivulle aina palveluntarjoajan osoitteen kautta.

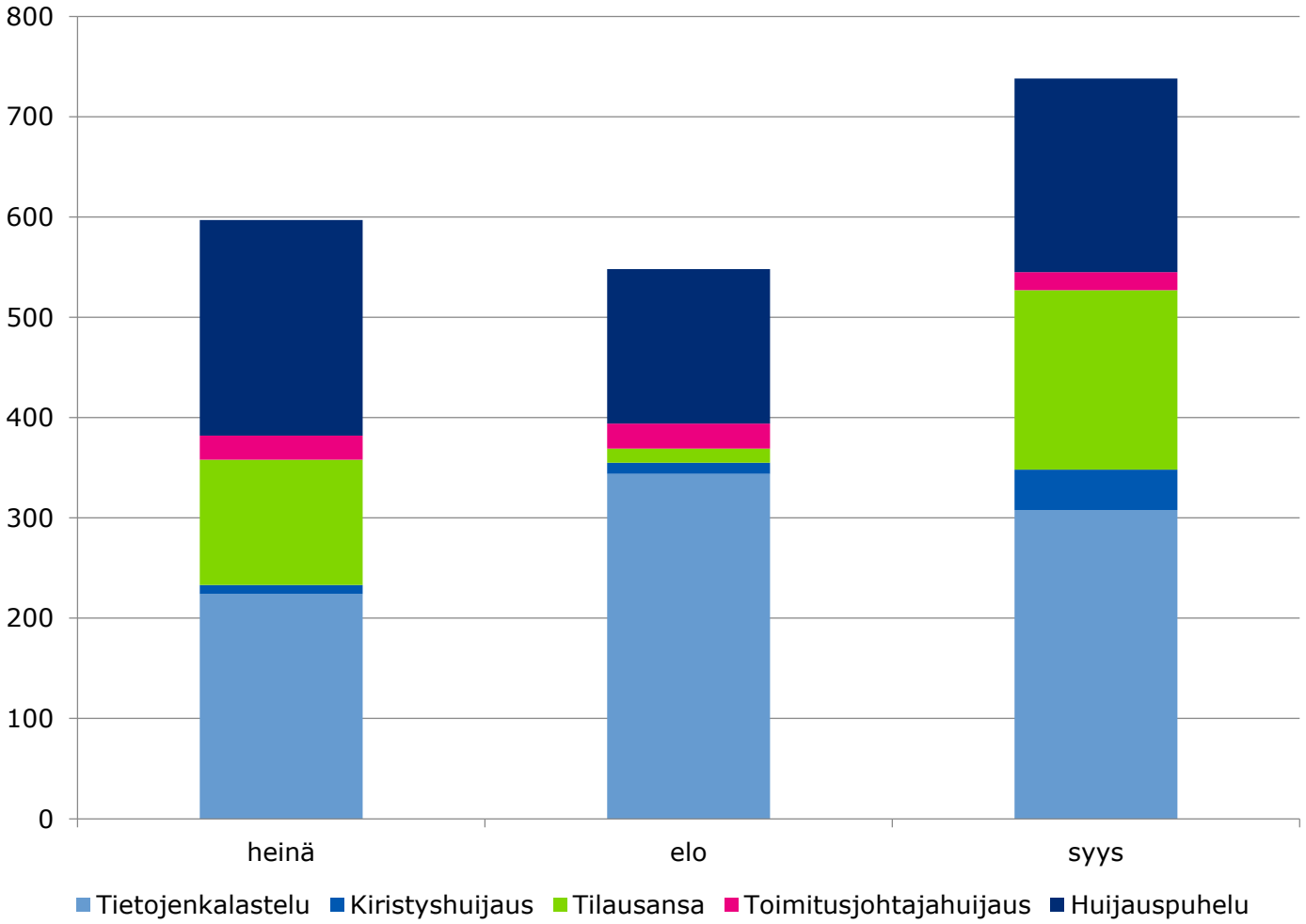
Office 365 -tietojenkalastelu

- Office 365 -tietojenkalastelu on edelleen yleistä. Uusimpana kalastelulinkkien jakelukanavana on käytetty Box-tiedostonjakopalvelua.
  - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kalastelusivujen-anatomiaa-box-tiedostonjakopalvelua-jaljitteleva-kampanja
- Lokakuussa 2020 alkanut laadukas Office 365 -tunnuksien kalastelu hyvin uskottavilla väärennetyillä Zoom-kokouskutsuilla jatkui edelleen marraskuussa. Kansainvälisen kalastelukampanjan uhriksi jäi kymmeniä suomalaisiakin kohteita.

ANALYYSI

- Mikäli yritys on joutunut onnistuneen kalastelun kohteeksi, tulisi sillä olla keinot jäljittää tapausta.
- Uusimmissa tapauksissa ongelmana on ollut se, että olemassa olevat mekanismit, kuten sähköpostisuodattimet, eivät tunnista haitallista liitettä. Näiden lisäksi tulisi olla käytössä myös muita keinoja.
  - Lokitietojen merkitys on tärkeä, jotta tiedon lähteelle päästään jälkikäteen.
  - Tunnusten hyödyntämistä voidaan osin estää käyttämällä monivaiheista tunnistautumista.
- Onnistuneen tietojenkalastelun seurauksena kalastelu voi levitä myös uhrilta seuraavalle. Tällöin vaikutuksia on myös moniin muihin. **Mikäli joudut tietojenkalastelun uhriksi, ilmoita siitä myös Kyberturvallisuuskeskukselle.**

Käsiteltyjä huijaustapauksia Q3/2020



- Kolmannen neljänneksen 2020 näkyvimmät trendit ovat olleet:
  - Jatkuvat Postin nimissä tehdyt huijaukset, jotka johtavat tilausansoihin, tai puhelimen haittaohjelmaan.
  - Teknisen tuen huijauspuhelut jatkuivat edelleen.
- Tietojenkalastelut ovat tavallisin tapa murtautua yrityksen verkkoon: Kalastellaan tunnuksia ja salasanoja järjestelmäpääsyn toivossa.

Haittaohjelmat ja haavoittuvuudet

Haittaohjelmissa ja haavoittuvuuksissa käsitellään aihealueen merkittävimmät julkaisut ja havainnot sekä annetaan toimenpidesuosituksia ja linkkejä lisätietoihin.

Haittaohjelmat

- Emotet-haittaohjelmasta kertova keltainen varoitus passivoitiin 18.11.
  - Kyberturvallisuuskeskukselle saapuneet Emotet-ilmoitusmäärät ovat laskeneet, joten aktiivinen ilmoitus on päätetty passivoida
    - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/emotet-haittaohjelmaa-koskenut-keltainen-varoitus-poistettiin
- Turvapostiteemalla pankkien nimissä sekä Zoom videokonferessi-kutsujen kautta on levitetty haittaohjelmia
  - Sähköpostin liitteenä tai tekstiviestitse saapuvia linkkejä ei pidä klikkailla harkitsemattomasti

ANALYYSI

- Emotet toimii kausittaisesti, jolloin pitkää passiivisuutta voi seurata aktiivisempi haittaohjelman levityskausi
- Sähköposti on edelleen yleisin haittaohjelmien levitykseen käytettävä kanava

Haavoittuvuudet

- Suomessa on tunnistettu n. 60 haavoittuvaa Fortinet VPN-laitetta
  - Laitteet ovat löytyneet n. 50 000 haavoittuvan Fortinet VPN-laitteen osoitelistalta
    - Oletusarvoisesti yksi osoite on yhden organisaation laite
  - Alkuperäiset haavoittuvuudet ovat vuodelta 2018
- Haavoittuvuus mahdollistaa hyökkääjälle mahdollisuuden onkia VPN-tunnukset SSL VPN –käyttöliittymästä.
- Tunnusten avulla hyökkääjälle on mahdollista saada organisaation verkko haltuunsa esimerkiksi haittaohjelman levittämiseksi. Ensisijainen ohjeistus on ollut vaihtaa käyttäjätunnus ja salasana heti laitteille päivitystä unohtamatta.

ANALYYSI

- Verkkoon näkyviä palveluita ei pidä unohtaa käytön lopettamisen jälkeen internettiin
- Seuraa internettiin näkyviä omia palveluita ja poista tarpeettomat käytöstä
- Kannattaa varmistaa, että kriittisetkin palvelut pystytään päivittämään
- Vanhatkin päivitykset pitää huomioida ja tiedostaa, että rikolliset käyttävät niitä myös mahdollisuuksien mukaan hyväkseen

Marraskuun haavoittuvuusjulkaisut

- Google julkaisi korjaavia päivityksiä Chrome-selainten kriittisiin haavoittuvuuksiin (34/2020)
- Apple julkaisi korjaavia kriittisiä päivityksiä iOS-laitteiden 0-päivähaavoihin (35/2020)
- VMware julkaisi korjaavan päivityksen kriittiseen haavoittuvuuteen (36/2020)

- Kyberturvallisuuskeskus on tehnyt haavoittuvuuksia käsittelevää neliosaista juttusarjaa, joiden ensimmäiset kolme juttua pääset lukemaan täältä:
  - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/paivitykset-laastaria-alylaitteen-haavoihin
  - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-miten-niista-ilmoitetaan-oikein
  - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuuksien-hallinta-ohjelmistoyrityksessa

ANALYYSI

- Päivitykset tulee asentaa viipymättä, haavoittuvuuksien hyväksikäyttö on todella nopeaa
- Päivityssyklien ulkopuoliset päivitykset tulee myös huomioida, muutoin järjestelmään voi jäädä kriittisiä haavoittuvuuksia pitkäksikin aikaa

Automaatio ja IoT

Automaatio-osiossa ilmiöseurantaryhmä seuraa alan uutisia ja ilmiöitä maailmalla ja kotimaassa. Automaatiojärjestelmiä käytetään ohjaamaan ja monitoroimaan esimerkiksi erilaisia yksittäisiä tehtaan tai vastaavan tuotantolaitoksen palveluita tai laitteita.

Automaatio ja IoT

- Dragos on julkaissut raportin, jonka mukaan kyberriskit valmistavassa teollisuudessa kasvavat seuraavin tavoin:
  - Toimitusketjujen varmuus heikkenee
  - Tuotantoprosessien häirintä lisääntyy
  - Prosessitietojen varastaminen yleistyy
  - ICS-järjestelmiä vastaan tehtyihin hyökkäyksiin erikoistuneiden toimijoiden määrä kasvaa
  - https://www.dragos.com/blog/industry-news/manufacturing-sector-cyber-threats/

ANALYYSI

- Häiriöt valmistavan teollisuuden organisaatioissa voivat vaikuttaa laajasti kriittisiin toimijoihin mm. vaikeuttamalla varaosien saamista
- Jatkuvuudenhallinnassa tulisi ottaa huomioon millaiset varastot on kriittisiä, usein tarvittavia komponentteja ja onko toimitusketjuissa valmistavaan teollisuuteen liittyviä yksittäisiä riskitekijöitä, jotka voivat toteutuessaan pysäyttää koko toiminnan

Automaatio ja IoT

- Amazonin Yhdysvaltojen Pohjois-Virginiassa sijaitsevat verkkopalvelut kärsivät toimintahäiriöstä
  - Häiriö vaikutti mm. verkkoon kytkettyjen kodin älyratkaisujen kuten ovikellojen ja robotti-imurien toimintaan
  - Lisätietoja: https://www.datacenterdynamics.com/en/news/aws-us-east-1-region-suffers-errors-and-outages-impacting-its-status-page/

ANALYYSI

- Ilmiö on tunnettu jo pitkään, mutta tilanne ei ole parantunut ajan mittaan
- Laitteiden toiminta perustuu usein oletukseen katkeamattomasta verkkoyhteydestä. On hyvä tiedostaa, että laitteen tila verkkoyhteyden katketessa voi vaikuttaa siihen, onko se paikallisesti hallittavissa sen jälkeen.
- IoT-ekosysteemi vaikuttaa kokonaisuudessaan IoT-laitteiden ja -palveluiden käytettävyyteen ja turvallisuuteen. Tämä on hyvä ottaa huomioon esimerkiksi hankinnoissa
  - Hankinnoissa huomioon otettavia asioita voi kartoittaa esimerkiksi Kyberturvallisuuskeskuksen SOTE-alan mallin mukaisesti: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/sosiaali-ja-terveydenhuollon-hankintojen-tietoturva-ja

IoT

- Suomessa olevia IoT-laitteita käytettiin liikenteen alkuperän peittämiseen verkossa tehtyjen luottokorttipetosten yhteydessä
- Mobiilireitittimeen murtauduttu ja liittymällä tehty ostoksia
  - Mobiililiittymien käyttö rikollisessa toiminnassa tavallista
  - Vaatii ymmärrystä paikallisesta markkinasta.
- Automaattinen Gitpaste-haittaohjelma on murtautunut IoT-laitteisiin(kin)

ANALYYSI

- IoT-laitteiden haavoittuvuuksia käytetään aktiivisesti hyväksi
- Rikolliset etsivät jatkuvasti uusia tapoja taloudellisen hyödyn saamiseen haavoittuvuuksia hyväksi käyttäen
- IoT-laitteet ovat rikollisille houkutteleva murtautumiskohde ja väline muiden rikosten tekemiseen: niissä on usein tunnettuja haavoittuvuuksia ja käyttäjät eivät yleensä valvo niiden toimintaa tai eivät kykene tunnistamaan, että niihin on murtauduttu.

Verkkojen toimivuus

Verkkojen toimivuus -osassa käsitellään yleisten viestintäpalveluiden merkittäviä toimivuushäiriöitä Suomessa, muiden ICT-palveluiden huomattavia häiriöitä Suomessa ja maailmalla, sekä palvelunestohyökkäyksiä Suomessa ja maailmalla.

Verkkojen toimivuus

- Marraskuussa oli kahdeksan merkittävää toimivuushäiriötä
  - Niistä viisi johtui sähkökatkoista.
  - Kolme häiriötä johtui Liisa-myrskyn aiheuttamista sähkökatkoista.
- Vuoden 2020 häiriömäärä oli tammikuun ja marraskuun välisenä aikana 66 kappaletta.
  - Vuonna 2019 merkittäviä häiriöitä oli kaikkiaan 68 kappaletta.

ANALYYSI

- Marraskuussa oli hieman keskimääräistä kuukautta enemmän häiriöitä. Kuukausittaiset satunnaiset vaihtelut ovat kuitenkin suuria.
- Vuosittainen merkittävien häiriöiden määrä näyttää kääntyneen hienoiseen kasvuun vuoden 2018 jälkeen.

Palvelunestohyökkäykset

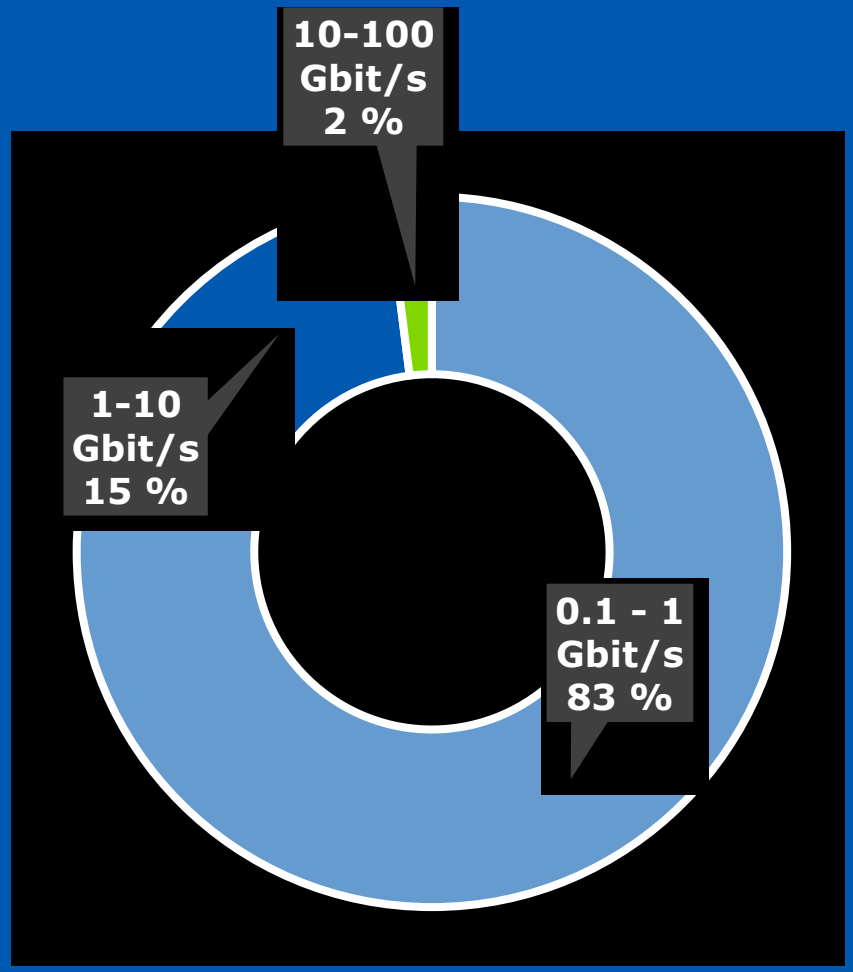
- Marraskuussakin Kyberturvallisuuskeskus sai ilmoituksia palvelunestohyökkäyksistä, joilla oli myös laajoja vaikutuksia palveluiden toimintaan.
- Palvelunestohyökkäyksillä uhkailu ja lunnasrahojen vaatiminen ovat yleistyneet maailmalla ja ilmiö on rantautunut myös Suomeen.
  - Uutena ilmiönä palvelunestohyökkäyksiä käytetään tehostamaan kiristyshaittaohjelmahyökkäysten lunnasvaatimuksia.
  - Kyberturvallisuuskeskukselle on ilmoitettu kiristysviesteistä ja niiden tehostamiseksi tulleista palvelunestohyökkäyksistä. Vaikka lyhyitä hyökkäyksiä on raportoitu, uhattuja laajoja hyökkäyksiä ei ole tapahtunut.
- Olemme saaneet ilmoituksia ilkivaltaisista palvelunestohyökkäyksistä.
  - Hyökkäysten motiivina on ollut tietyn palvelun häirintä.
  - Tämän tyyppisillä hyökkäyksillä voi olla myös vaikutuksia muihin palveluihin kuin hyökkäyksen kohteeseen.

ANALYYSI

- Jos organisaatio on etukäteen varautunut hyökkäyksiin, palvelunestohyökkäyksillä ei yleensä ole vaikutuksia palveluiden toimivuuteen. Kiristysviestien yhteydessä on havaittu yli 100 Gbps-hyökkäyksiä, joilla voi olla vaikutuksia pk-yrityksen toimintaan.
- Hyökkäyksiin varautumisessa tulisi huomioida sekä volumetriset että sovellustason hyökkäykset.

Palvelunestohyökkäysten tunnuslukuja

- 63 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q3/2020.
- Noin 78% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



SUOMEEN KOHDISTUNEIDEN PALVELUNESTOHYÖKKÄYSTEN VOLYYMIT (Q3/2020 - TILASTO PÄIVITETÄÄN KVARTAALEITTAIN.)

Vakoilu

Vakoiluosiossa käsitellään valtiollisten toimijoiden tai niihin liitettyjen ryhmien harjoittamaa kybervakoilua ja -vaikuttamista. Tavoitteena voi olla poliittinen tiedonhankinta, yritysvakoilu tai esimerkiksi tietojärjestelmien tuhoaminen.

Vakoilu

- Norja syyttää Venäjän sotilastiedusteluorganisaatiota GRU:ta elokuussa havaitusta tietomurrosta, joka kohdistui maan parlamenttiin eli Suurkäräjiin.
  - Norjan mukaan murto on ollut osa laajempaa kansainvälistä kampanjaa, joka on jatkunut vuodesta 2019.
  - https://pst.no/alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/

- Tietoturvayritys FireEye on joutunut valtiollisen toimijan tekemän tietomurron kohteeksi. FireEyen mukaan murto on tavoitellut tiettyihin valtiollisiin asiakkuuksiin liittyviä tietoja, mutta hyökkääjät saivat saaliiksi tiettävästi vain FireEyen tekemiä hyökkäystyökaluja.
  - New York Timesin tietojen mukaan hyökkäyksestä epäillään Venäjän tiedustelupalveluita
  - https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html

ANALYYSI

- FireEyen murto osoittaa miten myös tietoturvataloja hyödynnetään osana kybervakoilua. Tietoturvataloilta saa kriittistä tietoa asiakkaiden tietoturvajärjestelyistä sekä teknisiä tietoja siitä miten yritys havaitsee hyökkääjiä.

Vakoilu

- COVID-rokotteita kehittävät tahot usean valtiollisen toimijan kohteina
  - Euroopan lääkevirasto EMA kertoi 9.12. joutuneensa vakoilun kohteeksi ja että rokotetietoihin on päästy luvattomasti katselemaan
    - EMA:n on todennut, että kyberhyökkäyksellä ei tule olemaan vaikutusta sen suorittamalle koronavirusrokotteen tarkastelulle ja hyväksynnälle. Hyökkäyksen tekijä tai miten hyökkäys on tehty ei ole vielä tiedossa.
  - Rokotetta kehittävä AstraZeneca on Reutersin mukaan ollut Pohjois-Koreaan liitetyn toimijan kohteena
    - https://www.reuters.com/article/healthcare-coronavirus-astrazeneca-north/exclusive-suspected-north-korean-hackers-targeted-covid-vaccine-maker-astrazeneca-sources-idUSL8N2IC2QU
  - Microsoft raportoi myös kolmen kybervakoilutoimijan hyökänneen rokotevalmistajia ja tutkimuslaitoksia vastaan. Havaintojen mukaan hyökkäysten taustalla on ollut kaksi Pohjois-Korealaista toimijaa sekä Venäjään liitetty APT28.
  - https://threatpost.com/russia-north-korea-attacking-covid-19-vaccine-makers/161205/

ANALYYSI

- Useat valtiot voivat pyrkiä edistämään intressejään kybervakoilun keinoin. Kybervakoilulla voidaan pyrkiä saamaan esimerkiksi tietoa päätöksenteosta tai hyötymään muiden tekemästä teknologisesta kehittämisestä tai innovoinnista.
- Toimiva COVID-rokote on strategisesti erittäin merkittävä kohde valtiolliselle kybervakoilulle.

Tietoturva-alan kehitys

Tietoturva-alan kehitys -osiossa kerromme keskeisistä uudistuksista esimerkiksi alaa koskevan lainsäädännön tai asetusten päivityksiin liittyen. Kerromme kaikille tärkeää kyberturvallisuustietoa ja Kyberturvallisuuskeskuksen ajankohtaisista asioista.

Oikeudelliset asiat

- Traficomin suositus tiettyihin tietoliikenneportteihin suuntautuvan liikenteen tietoturvaperusteinen suodattaminen teleyritysten verkoissa (312/2020)

TIIVISTELMÄ

- Suositus tuli voimaan 30.11.2020 ja korvaa Viestintäviraston suosituksen 312 A/2016
- Suosituksen uudessa versiossa ei enää suositella Mirai-bottiverkkoon liittyvän portin suodattamista, jota koskeva suositus annettiin vuonna 2016.
- Suositus ja lisätietoja: https://www.kyberturvallisuuskeskus.fi/fi/saadokset-ohjeistukset-suositukset?limit=20&offset=0&query=&sort=created&toggle=Tiettyihin%20tietoliikenneportteihin%20suuntautuvan%20liikenteen%20tietoturvaperusteinen%20suodattaminen%20teleyritysten%20verkoissa%20

Oikeudelliset asiat

- Hallituksen esitys eduskunnalle laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi

  - Eduskunta on hyväksynyt esityksen liikenne- ja viestintävaliokunnan mietinnön mukaisesti muutettuna 7.12.2020.
  - Ehdotuksella pannaan täytäntöön sähköisen viestinnän verkkoja ja palveluja koskeva niin sanottu ”teledirektiivi” sekä televisio- ja radiotoimintaa ja muita audiovisuaalisia sisältöjä koskeva niin sanottu ”AVMS-direktiivi”. Direktiivien täytäntöönpanon yhteydessä ehdotetaan myös yksittäisiä muista EU:n säädöksistä sekä kansallisista tarpeista johtuvia muutoksia lainsäädäntöön. Lait on tarkoitettu tulemaan voimaan pääosin 21.12.2020.
  - Ks. asian käsittelytiedot ja annetut lausunnot: https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_98+2020.aspx

Oikeudelliset asiat

HE (237/2020) laeiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta sekä vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta ja väliaikaisesta muuttamisesta annetun lain voimaantulosäännöksen muuttamisesta

- Hallituksen esitys eteni eduskunnan käsittelyyn pitkälti samassa muodossa kuin se oli lausuttavana. Lausunnoissa esitettiin tarkennuksia lähinnä esityksen perusteluihin.
- Esityksellä jatkettaisiin ensitunnistamisen ketjuttamisen enimmäishintasääntelyä kahdella vuodella. Hinta olisi jatkossakin korkeintaan 0,03 euroa.
- Liikenne- ja viestintävirastolle esitetään uutta tehtävää kerätä ja muodostaa tilastotietoa vahvan sähköisen tunnistamisen markkinasta ja tarjonnasta sääntelyn vaikutusten seuraamista, sähköisen tunnistamisen markkinoiden ohjaamista ja lainsäädännön kehittämistä varten.
- Ks. https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_237+2020.aspx

Oikeudelliset asiat

Komissio ehdottaa toimenpiteitä datan yhteiskäytön tehostamiseksi ja eurooppalaisten data-avaruuksien kehittämiseksi

- Komission 25.11.2020 ehdottama datanhallintaa koskeva asetus on EU:n datastrategian ensimmäinen konkreettinen tulos. Sillä luodaan datastrategian mukaisesti uudelle eurooppalaiselle datanhallinnalle perusta, joka noudattaa EU:n arvoja ja periaatteita, joihin kuuluvat muun muassa henkilötietojen suoja, kuluttajansuoja ja kilpailusäännöt.
- Asetuksella säädetään muun muassa toimenpiteistä, joilla lisätään luottamusta datan yhteiskäyttöön, koska luottamuksen puute on tällä hetkellä merkittävä este ja johtaa korkeisiin kustannuksiin.
- Lisäksi asetuksella säädetään toimenpiteistä, joilla helpotetaan julkisen sektorin hallussa olevan tietynlaisen datan uudelleenkäyttöä. Esimerkiksi terveysdatan uudelleenkäyttö voisi auttaa edistämään tutkimusta harvinaisten tai kroonisten sairauksien hoitokeinojen löytämiseksi. Asetuksessa esitetään myös keinot, joilla voidaan antaa eurooppalaisille mahdollisuus valvoa tuottamansa datan käyttöä ja luovutusta.
- Lisätietoja: https://ec.europa.eu/finland/news/data_201125_fi ja https://ec.europa.eu/commission/presscorner/detail/fi/ip_20_2102

Arjen kyberturvallisuus – marraskuu

Väärennettyjä puheluita teknisen tuen nimissä

- Organisaatioille ja yksityisille henkilöille tulee edelleen runsaasti puheluita teknisen tuen nimissä. Huijari voi myös esiintyä esimerkiksi yrityksen, kotimaisen operaattorin taikka oman organisaation IT-tuen nimissä
- Jos olet vastannut epämääräiseen puheluun, lyö luuri rohkeasti soittajan korvaan. Rikolliselle ei tarvitse olla kohtelias.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vaarennettyja-puheluita-teknisen-tuen-nimissa

Traficom myönsi Koronavilkulle ja Philips Hue –älyvaloratkaisulle Tietoturvamerkin

- Tietoturvamerkki takaa kuluttajalle, että laitteen tai sovelluksen tietoturvan perusominaisuudet ovat kunnossa.
- Marraskuussa vuoden täyttänyt Tietoturvamerkki on myönnetty tähän mennessä yhteensä 9 tuotteelle.
- Lisätietoa Tietoturvamerkistä ja merkin saaneista tuotteista ja palveluista. https://tietoturvamerkki.fi/

Saitko tekstiviestin Postin nimissä? Varothan, viesti voi olla huijaus

- Loppuvuoden verkkokauppaan uumoillaan kaikkien aikojen sesonkia.
- Varaudu huijaustekstiviesteihin, joissa ilmoitetaan esim. saapuneesta postipaketista. Älä avaa mitään linkkejä harkitsematta, koska vastaan voi tulla haittaohjelmia, kalastelua ja muita huijauksia.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/saitko-tekstiviestin-postin-nimissa-varothan-viesti-voi-olla-huijaus

Kyberrikoksista kannattaa tehdä rikosilmoitus

- Kansalliseen rikosuhritutkimukseen (2018) osallistuneista 55 % kertoi joutuneensa elämänsä aikana kyberrikoksen uhriksi. Heistä vain noin 3% teki asiasta rikosilmoituksen poliisille.
- Rikosilmoitusta tehdessäsi, ota myös yhteyttä Kyberturvallisuuskeskukseen. Ilmoitusten avulla voimme jakaa tietoa ja neuvoja tietoturvaan liittyvistä ilmiöistä.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/toimi-nain-jos-havaitset-tietoturvapoikkeaman

Ajankohtaista Kyberturvallisuuskeskuksesta

Digitaalinen ja fyysinen turvallisuus paiskaavat kättä Fortumissa

- Kyberturvallisuuden johtaminen edellyttää kokonaisvaltaista tietoa liiketoimintaan liittyvistä fyysiseen ja digitaaliseen turvallisuuteen liittyvistä uhkista.
- Fortumin Senior Vice Presidentin Arto Rädyn mukaan: "Koska kyberriskit läpileikkaavat organisaation eri toimintoja, ne tulee ottaa huomioon läpi organisaation, ei vain tietohallinnossa, vaan myös johtamisessa".
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/digitaalinen-ja-fyysinen-turvallisuus-paiskaavat-katta-fortumissa

HAVARO-palvelu uudistuu

- HAVARO on Liikenne- ja viestintävirasto Traficomin tuottama palvelu, joka havainnoi suomalaisiin yrityksiin kohdistuvia vakavia tietoturvauhkia ja varoittaa niistä.
- Vuosien 2020-2021 aikana palvelumallissa siirrytään kaupallisten toimijoiden ja Traficomin Kyberturvallisuuskeskuksen yhdessä tuottamaan palveluun.
- Ota yhteyttä osoitteeseen info@havaro.fi niin kerromme tarkemmin miten pilottiin pääsee mukaan.
- Lisätietoa HAVARO:sta löydätte täältä: https://havaro.fi/fi/

Lausuntopyyntö SRD-laitteiden, 5G:n ja satelliittijärjestelmien käyttöönotosta

- Traficom pyytää lausuntoja SRD-laitteiden eli lyhyen kantaman radiolähettimien käytöstä tulevaisuudessa, 5G-käytöstä taajuusalueella 66-71 GHz sekä satelliittijärjestelmien käyttöönotosta.
- Suomen hallinnon kannanoton muodostamiseksi Traficom pyytää kommentteja edellä mainituista raportti- ja päätösluonnoksista 4.1.2021 mennessä.
- Lue lisää: https://www.traficom.fi/fi/ajankohtaista/lausuntopyynto-euroopan-komission-lyhyen-kantaman-radiolahettimien-paatoksen-paivitys

Epäiletkö tietoturvaloukkausta?

Jos teihin on kohdistunut tai epäilette teihin kohdistuneen tietoturvaloukkauksen, olkaa yhteydessä meihin.

- Sähköinen lomake: https://www.kyberturvallisuuskeskus.fi/fi/ilmoita
- Sähköposti: cert@traficom.fi
- Puhelin: 0295 345 630 (arkisin klo 9-15)

- Muissa asioissa voitte olla meihin yhteydessä osoitteessa kyberturvallisuuskeskus@traficom.fi
- Kyberturvallisuuskeskuksen eri toimintojen ja hankkeiden yhteystiedot löydät keskitetysti täältä: https://www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot