TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Tammikuu 2021

#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 tammikuu 2021

Tietomurrot ja -vuodot

- Työnvälitysyhtiö Eilakaislaan on kohdistunut tietomurto ja kiristyshaittaohjelma
- Vastaamon potilastietoja on tullut jälleen tammikuussa jakoon useampaan paikkaan

Huijaukset ja kalastelut

- Pankkitietoja kalastellaan väärien hakukonetulosten avulla.
- Suomenkielinen pornokiristyskampanja aktivoitui jälleen. Kiristysviestejä lähetetään edelleen myös englanniksi.

Haittaohjelmat ja haavoittuvuudet

- Emotet bottiverkko on ajettu alas kansainvälisessä viranomaisyhteistyössä
- OmaPosti-teemainen tekstiviestitse leviävä laaja mobiilihaittaohjelmien levityskampanja on ollut hyvin aktiivinen

Automaatio ja IoT

- NAT Slipstreaming v2.0: Uusi hyökkäystapa voi altistaa kaikki sisäverkon laitteet internetille
- Kyberturvallisuuskeskus kannustaa SBOMin käyttöön blogikirjoituksella

Verkkojen toimivuus

- Kuusi merkittävää häiriötä yleisissä viestintäpalveluissa
- Maailmanlaajuinen häiriö tiimiviestintäpalvelu Slackissa.
- Palvelunestohyökkäyksillä on ollut vaikutuksia tammikuussakin Suomessa. Kiitämme kaikista saamistamme ilmoituksista!

Vakoilu

- Tietoturva- ja haavoittuvuustutkijat kiinnostavat valtiollisia toimijoita.
- Euroopan lääkeviraston tietomurron yhteydessä vietyjä tietoja vuodettiin verkkoon muunneltuina.
- Saksa varoittaa APT31-ryhmän kartoittavan mahdollisuuksiaan tunkeutua länsimaisiin poliittisiin organisaatioihin.

Kuukauden tunnuslukuja

1268

ILMOITUSTA
KYBERTURVALLISUUSKESKUKSELLE
TAMMIKUUN AIKANA

YLI 30

PANKKIASIAKKAAN PANKKITILIT
TYHJENNETTY HAKUKONEISIIN
UJUTETTUJEN VÄÄRIEN
VERKKOPANKKILINKKIEN AVULLA

8500

HAITALLISTA SIVUA POISTETTU
VUODEN 2020 AIKANA
KYBERTURVALLISUUSKESKUKSEN
PYYNNÖSTÄ

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1 ↑

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

2 ↓

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

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

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.
- Linkki kalastelusivulle voi olla piilotettu kokouskutsuun, naamioitu turvapostiksi, tai väärennetty postin tai pankin tekstiviestiksi.
- Hakukoneiden hakutuloksiin on ujutettu myös vääriä huijaussivuja, joilla kalastellaan tietoja. Varsinkin väärin kirjoitettu hakusana johtaa helposti rikollisten rakentamaan ansaan (typosquatting).
- Henkilökunnan koulutuksella on suuri merkitys. Tutkimusten mukaan tietojenkalastelua ja käyttäjän manipulaatiota opitaan tunnistamaan koulutuksen avulla, jolloin tietojenkalastelu jää vain yritykseksi.

CASE

UUSI

Verkkopankin asiakkaiden pankkitilejä tyhjennettiin ja rahaa varastettiin lyhyessä ajassa suuria summia.

Epäiltiin uutta tehokasta haittaohjelmaa, mutta syyllinen olikin hakukoneiden tietokannan manipulointi tai verkkomainonta. Rikollinen onnistui nostamaan omia sivujaan tuloksissa oikeiden verkkopankkien edelle ja kymmenet käyttäjät erehtyivät tietojenkalastelusivulle. Pankkitietojen avulla rikollinen pääsi verkkopankkiin ja tyhjensi uhrien tilit.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

2

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

Palvelunestohyökkäyksillä kiristäminen nousi maailmalla ilmiönä loppu-vuodesta 2020 ja ilmiö rantautui myös Suomeen. Kyberturvallisuuskeskus on saanut ilmoituksia myös vuonna 2021 aiheeseen liittyen.

Yleisesti organisaatio vastaanottaa kiristysviestin sähköpostitse, joka on allekirjoitettu näennäisesti tunnettujen haitallisten toimijoiden nimissä. Kiristysviestin lähettämisen aikoihin on joissain tapauksissa tehty myös palvelunestohyökkäys viestin tehostamiseksi. Viestissä kerrotaan organisaation kohtaavan suuren palvelunestohyökkäyksen, mikäli lunnaita ei makseta. Ohjeemme on ja pysyy: älä maksa kiristäjille.

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

Marraskuussa hakkeriryhmä julkaisi 50 000: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

- Työvälitysyhtiö Eilakaislaan kohdistunut tietomurto ja kiristystapaus
  - Yritys tiedotti sunnuntaina 10.1., että kiristyshaittaohjelman vuoksi Eilakaislan palvelin lakkasi toimimasta edeltävänä perjantaiaamuna
  - Hyökkäyksen yhteydessä saatiin lyhyt englanninkielinen uhkausviesti, jossa uhattiin Eilakaislaa liiketoiminnan lakkauttamisella
  - Hyökkääjät pyysivät Eilakaislaa olemaan yhteydessä muutamaan sähköpostiosoitteeseen, jotta järjestelmiin päästäisiin takaisin. Rahasummaa ei kuitenkaan täsmennetty eikä Eilakaisla ole ollut yhteydessä rikollisiin

ANALYYSI

- Lunnaiden maksaminen ei ole suotavaa, sillä tietojen takaisinsaamisesta ei ole mitään takeita eikä mikään takaa, että tiedot eivät maksusta huolimatta päätyisi julkisuuteen
- Ajantasaiset varmuuskopiot varmistavat, että toimintaa kyetään jatkamaan nopeasti

Tietomurrot ja -vuodot

- Vastaamon potilastietoja jälleen julki
  - Tammikuun lopulla julkaistiin Tor-verkossa ja sen jälkeen myös julkisessa verkossa 30 000 potilastietoa, jotka vaikuttavat olevan peräisin Vastaamon tietovuodosta
  - Poliisin tietojen mukaan kyseessä on nyt syksyn tapahtumien jälkeen ensimmäinen kerta, kun Vastaamon potilaiden tietoja on jaettu laajamittaisesti
  - Julkisuudessa olleiden tietojen mukaan tiedot julkaistiin pienemmässä tiedostossa, jossa oli ilmeisesti pelkästään tekstimuotoisia potilaskertomuksia

- Tietovuotoapu-sivusto auttaa edelleen tietovuotojen uhreja: https://tietovuotoapu.fi/

ANALYYSI

- Tietovuodossa julkisuuteen päätyneitä tietoja ei pidä ladata itselleen, levittää eteenpäin tai käydä katsomassa mitä tiedosto sisältää
- Tietojen lataaja, levittäjä tai katselija saattaa syyllistyä rikokseen näin toimiessaan

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

- Kuukauden aikana kalasteltiin runsaasti pankkitunnuksia, luottokorttitietoja, ja eri palveluiden käyttäjätunnuksia. Huijarit käyttivät kalastelemiaan henkilötietoja mm. pikavippien nostamiseen.
- Kalasteltuja Office 365 -tunnuksia käytettiin säännöllisesti tietomurtoihin. Murtojen avulla verkkosivuille pystytettiin kryptovaluuttasijoitushuijauksia, joihin taas houkuteltiin uhreja murretuilta sähköpostitileiltä lähetellyillä viesteillä.
- Erilaisilla lahjakorttivoittoroskaposteilla houkuteltiin tilausansoihin. Huijausviestejä tehtailtiin eri tuotemerkkien nimissä, kuten Tokmanni, Prisma, Elisa, Finnair ja HBO Nordic.
- Myös Postin ja monien kuriiriyritysten nimissä lähetettiin tekaistuja saapumisilmoituksia, jotka johtivat tilausansoihin.

ANALYYSI

- Omaposti-teemaiset tekstiviestihuijaukset
  - Omaposti-viesteiksi naamioiduissa tekstiviesteissä houkuteltiin taas huijaussivustolle, jolla tarjottiin Android-puhelimille FakeCop/FakeSpy-haittaohjelmaa.
  - Haittaohjelma lähettää puhelimesta tuhansittain tekstiviestejä liittymän laskuun.
  - Apple-puhelimilta kalasteltiin käyttäjätunnuksia tai yritettiin saada lupaa maksaa maksuja.
  - Huijaussivu piileskeli .top- ja .xyz-päätteisten verkkotunnusten suojissa ja vaihtoi paikkaa aina kun edellinen saatiin poistettua.

Huijauksia ja petoksia

- Toimitusjohtajan nimissä yritettiin jälleen kymmeniä laskutuspetoksia. Ainakin yhdessä tapauksessa menetettiin 8000 euroa, kun ulkomaisen yrityksen murrettua sähköpostitiliä käytettiin laskutustietojen väärentämiseen.
- Koronavirusteemaa käytettiin luottokorttitietojen kalasteluun. Sähköpostitse lupailtiin pääsyä rokotusjonojen ohitse, mutta sitä varten piti antaa luottokortin numero ja huijaustahan sekin kaikki valitettavasti on.

VANHAN ILMIÖN UUDET METKUT

- Sähköpostitse lähetetyt pornokiristysviestit lähtivät jyrkkään nousuun tammikuun puolivälissä, kun uusi suomenkielinen huijausaalto käynnistyi.
- Alkukuun englanninkieliset huijaukset "I got you" ja " I recorded you" vaihtuivat suomenkieliseen "Liiketoimintaehdotus"-huijaukseen. Kyberturvallisuuskeskus sai huijauksesta yli sata ilmoitusta.
- Kiristyshuijauksissa vaadittiin lunnassummaa kryptovaluuttana, jottei kiristäjä levittäisi uhrista muka ottamaansa intiimiä videota.
- Huijausviestissä väitettiin myös, että hyökkääjällä olisi pääsy myös uhrin puhelimeen ja neuvottiin nollaamaan puhelin ja vaihtamaan kaikki salasanat. Turvallisuuspäivitysten säännöllinen asentaminen on hyvä neuvo, mutta kaikki muu hyökkääjän väittämä on silkkaa huijausta.

Teknisen tuen nimissä soittelu jatkuu

- Joulun aikaan hiljentyneet huijauspuhelut lisääntyivät uudestaan tammikuussa. Kyberturvallisuuskeskukselle tehdyt ilmoitukset teknisen tuen huijauspuheluista lähes kaksinkertaistuivat joulukuusta.
- 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.

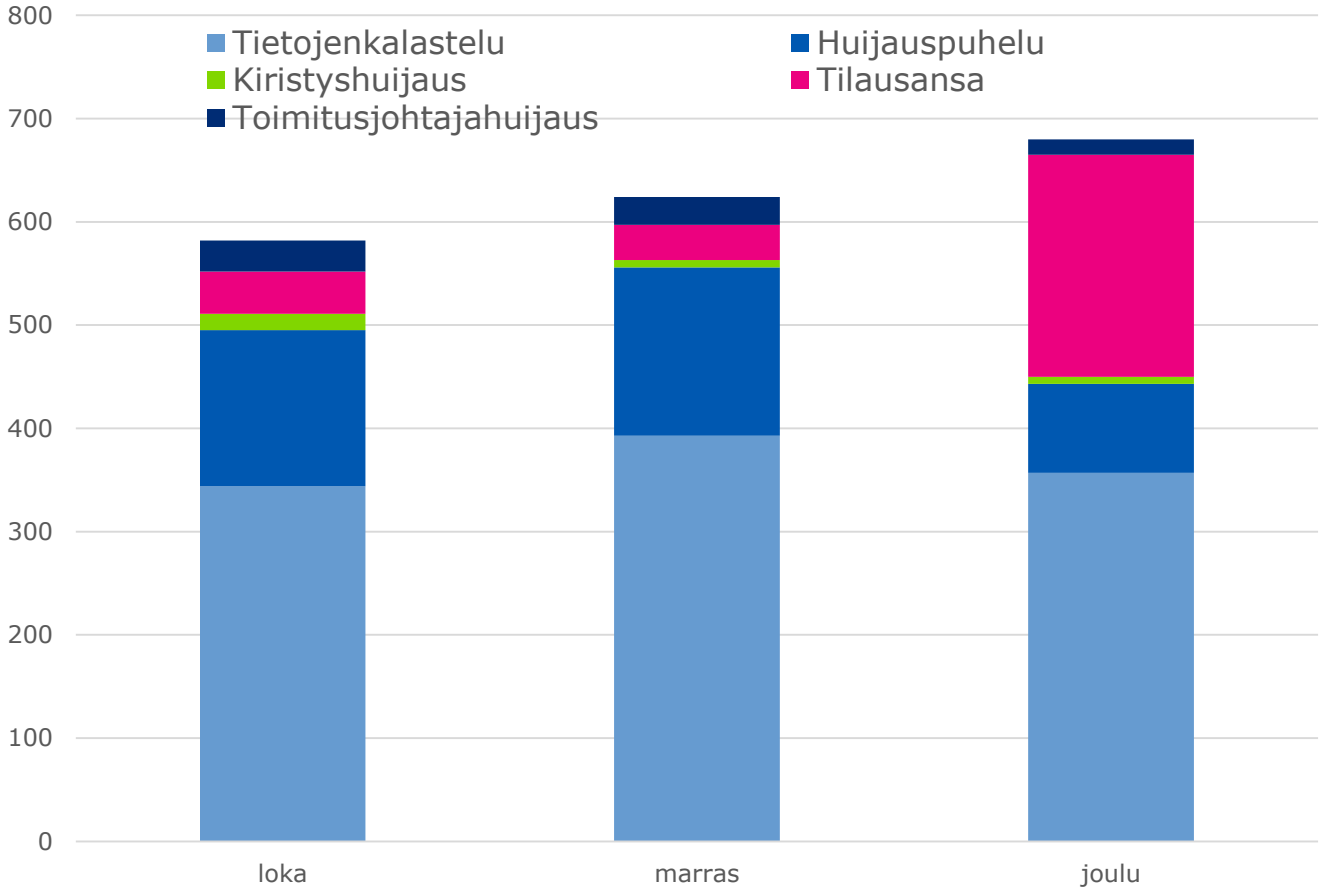
Kymmenittäin verkkopankkihuijauksia

- Verkkopankkien käyttäjiltä on viety rahaa varastetuilla pankkitunnuksilla. Väärät hakukonetulokset ovat vieneet oikean verkkopankin sijasta rikollisten kalastelusivulle.
- Verkkopankkien varmistusviesteissä on syytä olla tarkkana siitä, onko maksettava rahasumma oikea ja kohdetili oikea.

ANALYYSI

- Joidenkin hakukoneiden tuloksiin on saatu ujutettua joko optimoimalla tai mainontaa ostamalla haitallisia pankkitunnusten kalastelusivuja.
- Selaimen osoiteriville vajavaisesti kirjoitettu nettiosoite toimiikin syötteenä hakukoneelle. Selain kertoo hakukonetuloksia, joiden joukossa voi olla myös huonoja tuloksia.
- Normaalisti hakukone tarjoaa hakutuloksena ensimmäisenä pankin oikean osoitteen, mutta tässä tapauksessa ensimmäisenä tuloksena on voinut tulla rikollisen syöttämä tietojenkalastelusivu.
- Asiakas luulee kirjautuvansa verkkopankkiin, mutta syöttääkin tunnuksensa rikollisen huijaussivulle, joilla rikollinen kirjautuu oikeaan verkkopankkiin. Oikea käyttäjä saa kirjautumisesta varmistuspyynnön, jonka hän pahaa aavistamatta tekee.
- Tällainen väliintulohyökkäys (man-in-the-middle) onnistuu, jos asiakas luulee olevansa kirjautuneena oikeaan verkkopankkiin. Samalla hyökkääjä pääsee myös asiakkaan tekemien tilisiirtojen ja laskujen maksamisen väliin ja vaihtaa rahan siirtokohteeksi omat tilinsä, jotka voivat olla erilaisia muulitilejä.

Käsiteltyjä huijaustapauksia Q4/2020



- Viimeisen neljänneksen 2020 näkyvimmät trendit ovat olleet:
  - Jatkuvat Postin nimissä tehdyt huijaukset, jotka johtavat tilausansoihin, pikavippeihin, tai puhelimen haittaohjelmaan.
  - Teknisen tuen huijauspuhelut jatkuivat, mutta laantuivat loppuvuonna.
- 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-bottiverkko poliisin haltuun
  - Tietoja varastanut Emotet-bottiverkko suljettiin kansainvälisessä poliisioperaatiossa
  - Emotet-haittaohjelman kautta on levitetty muitakin haittaohjelmia, kuten Trickbot ja Ryuk
  - Vaikka Emotet ei tällä hetkellä leviä, sen uhrina olleiden organisaatioiden on syytä varmistaa, ettei mahdollisia muita haittaohjelmatartuntoja ole
  - Emotet levitysyrityksiä alkoi näkyä Suomessa joulukuussa lyhyen tauon jälkeen, levittämistä yritettiin sähköpostien liitetiedostojen, .zip-pakettien ja sähköpostissa olevien linkkien kautta
  - Kyberturvallisuuskeskus on välittänyt teleoperaattoreiden kautta Suomessa olevista saastuneista laitteista tietoa uhreille, tartuntoja ei ole Suomessa ollut lukumääräisesti paljon

ANALYYSI

- Tietoja varastava haittaohjelma Emotet on ollut yksi yleisimmistä ja vaarallisimmista haittaohjelmista
- Emotet ei itse varsinaisesti aiheuta vahinkoa järjestelmille, mutta aktivoiduttuaan se tarjoaa muille haittaohjelmia levittäville rikollisille pääsyn koneisiin jotta niihin voidaan asentaa esim. kiristyshaittaohjelmia

Haittaohjelmat

- OmaPostin nimissä lähetetty tekstiviesti tarjoilee Android-haittaohjelmaa
  - Fakecop-haittaohjelmaa levitetään tekstiviestin välityksellä Android-käyttäjille OmaPostin nimissä haittaohjelmalla saastuneista puhelimista
  - Asennettaessa haittaohjelmalla on laajat käyttöoikeudet, haittaohjelma varastaa puhelimeen tallennetut yhteystiedot sekä kykenee varastamaan käyttäjätunnuksia ja salasanoja puhelimesta
  - Postin nimissä levitetyt huijausviestit ovat johtaneet haittaohjelmasivustolle
  - Huijaussivulta asennettu haittaohjelma on saanut puhelimen lähettämään tekstiviestejä tuhansilla euroilla
    - Lisää tietoa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/saitko-tekstiviestin-postin-nimissa-varothan-viesti-voi-olla-huijaus

ANALYYSI

- Sovellukselle annettavia käyttöoikeuksia pitäisi aina miettiä ja pohtia haluaako sovellukselle antaa kaikki sen pyytämät oikeudet
- Tekstiviestitse saapuvia linkkejä ei pidä klikkailla harkitsemattomasti, koska linkkien avulla levitetään myös haittaohjelmia

Tammikuun haavoittuvuusjulkaisut

- Microsoft Defender -tietoturvaohjelmistossa haavoittuvuus (1/2021)
- DNSpooq-haavoittuvuusjoukko laajalti käytössä olevassa dnsmasq-ohjelmistossa (2/2021)
- Kriittinen haavoittuvuus SonicWall VPN-ohjelmistoissa (3/2021)
- Apple korjasi iOS 14.4 päivityksellä vakavia haavoittuvuuksia (4/2021)
- Sudon haavoittuvuus mahdollistaa Unix-järjestelmissä käyttöoikeuksien korottamisen (5/2021)

- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

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

- Kyberturvallisuuskeskus on julkaissut Software Bill of Materialsin (SBOM) käyttöön kannustavan blogikirjoituksen
  - SBOM auttaa havaitsemaan ja hallitsemaan haavoittuvat tuotteet ja päivittämään ne ajoissa
  - Linkki blogikirjoitukseen: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-hallintaan-sbommin-varmasti
- Singaporen kansallinen kyberviranomainen on laajentanut IoT-laitteiden kyberturvasertifikaatin koskemaan kaikkia kuluttajille myytäviä IoT-laitteita
  - Traficomin Tietoturvamerkkiä vastaavan Singaporen Cybersecurity Labeling Scheme on laajentanut sovellusalaa reitittimistä ja älykotijärjestelmistä kaikkiin kuluttajien IoT-tuotteisiin. Merkinnän käyttö pysyy edelleen valmistajille ja myyjille vapaaehtoisena.
  - Lisää tietoa: https://www.zdnet.com/article/singapore-widens-security-labelling-to-include-all-consumer-iot-devices/

ANALYYSI

- Ainesosalista on nykyään itsestäänselvyys muun muassa elintarvikkeissa ja kemikaaleissa, mutta ei ohjelmistoja sisältävissä tuotteissa. Asia kaipaa keskustelua, jotta se tulisi laajasti tunnetuksi.
- Useissa maissa on huomattu IoT-laitteiden tietoturvastandardien puuttuminen ja tehty nopeasti vapaaehtoiseen arviointiin perustuvia järjestelmiä, jotta kuluttajat voisivat tehdä järkeviä päätöksiä IoT-laitteita ostaessaan. Singaporen järjestelmä on yksi pisimmälle kehittyneistä.

Automaatio ja IoT

- NAT Slipstreaming v2.0: Uusi hyökkäystapa voi altistaa kaikki sisäverkon laitteet internetille
  - Periaatteessa hyökkäystapa toimii mitä tahansa laitetta tai järjestelmää vastaan, jota ulkoverkon palomuurin ajatellaan suojelevan. Hyökkäyksellä voidaan ohittaa palomuuri kokonaan, kunhan joku sisäverkossa saadaan klikkaamaan hyökkääjän antamaa linkkiä.
  - Automaatio- ja IoT-laitteiden suojaukset rakennetaan erityisen usein verkkotason tarjoamaan suojan varaan, joten hyökkäystapa on erityisen vaarallinen niille.
  - Lisää tietoa: https://www.armis.com/resources/iot-security-blog/nat-slipstreaming-v2-0-new-attack-variant-can-expose-all-internal-network-devices-to-the-internet/
- Tietoturvayritys Claroty on löytänyt kriittisiä haavoja OPC-protokollan toteutuksista
  - Automaatiojärjestelmien sisäisessä viestiliikenteessä yleisesti käytetyn OPC-protokollan useista toteutuksista löydettiin vakavia haavoittuvuuksia. Haavoittuvia protokollatoteutuksia uskotaan käytettävän hyvin laajasti. Haavoittuvuuden korjaavia ohjelmistopäivityksiä on saatavilla. Haavoittuvuudet löytänyt tietoturvayritys Claroty uskoo, että OPC-toteutuksissa on lisää vastaavia vakavia haavoittuvuuksia.
  - Lisää tietoa: https://www.claroty.com/2021/01/25/blog-research-critical-flaws-in-opc-protocol/

ANALYYSI

- NAT Slipstreaming v2.0 -haavoittuvuus korostaa monikerroksisen suojauksen tärkeyttä: sisäverkossakin pitäisi käyttää kunnollista pääsynhallintaa verkkosegmenttien välillä.
- Monikerroksisen suojauksen merkitys kasvaa jatkuvasti monimutkaisuuden ja järjestelmien ja laitteiden välisten riippuvuuksien lisääntyessä

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

- Tammikuussa tapahtui 6 merkittävää toimivuushäiriötä.
  - Viisi häiriötä vaikutti kiinteän verkon internetyhteyspalveluihin.
  - Häiriöt vaikuttivat kerrallaan muutamiin tuhansiin käyttäjiin.
- Tiimiviestintäpalvelu Slackissa oli maailmanlaajuinen häiriö 4.1.
  - Häiriö johtui viasta palvelun ylläpidon automatiikassa (palvelinten provisiointi).

ANALYYSI

- Yleisten viestintäpalveluiden merkittävien häiriöiden määrä oli lähellä kuukausittaista keskiarvoa ja vaikutukset suhteellisen pieniä. Tätä voi pitää häiriöiden minimitasona, johon jokaisen tulisi varautua (tehdä sopeutumistoimenpiteitä tai tietoisesti hyväksyä riski).
- Slackin häiriö on tyypillinen esimerkki suosittujen internetpalveluiden isoista toimivuushäiriöistä. Palvelut toimivat tavallisesti niin hyvin, että häiriötilanteiden mahdollisuus unohtuu helposti käyttäjiltä.

Palvelunestohyökkäykset

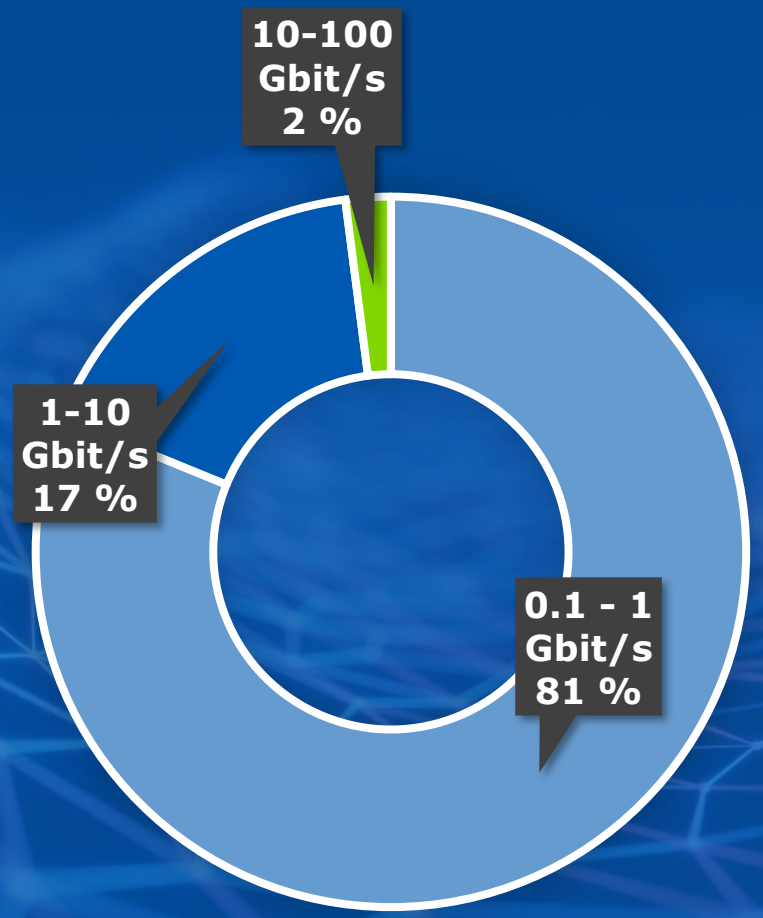
- Tammikuussakin Kyberturvallisuuskeskus sai ilmoituksia palvelunestohyökkäyksistä, joilla oli laajoja vaikutuksia palveluiden toimintaan.
  - Olemme saaneet viime aikoina ilmoituksia palvelunestohyökkäyksistä ja toivomme edelleen, että ilmoitatte meille organisaatioihinne kohdistuneista tietoturvaloukkauksista. Yhteystiedot ilmoittamiseen löytyvät kybersään viimeiseltä sivulta.
- Palvelunestohyökkäysten kohteena ovat olleet esimerkiksi palveluntarjoajat ja VPN-ratkaisut.
  - Suosittelemme varautumaan palvelunestohyökkäyksiin esimerkiksi erilaisten mitigointipalveluiden avulla.
  - Nimipalveluiden toiminnan suojaamiseksi suosittelemme ottamaan käyttöön maksuttoman toissijaisen hajautetun nimipalvelumme FI-verkkotunnuksille: https://www.traficom.fi/fi/hajautettu-nimipalvelu-valittajien-kayttoon
- Palvelunestohyökkäyksillä on jälleen kiristetty organisaatioita. Kiristäminen on osa laajempaa kansainvälistä ilmiötä, joka näkyy myös Suomessa.

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

- 61 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q4/2020.
- Noin 73% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



SUOMEEN KOHDISTUNEIDEN PALVELUNESTOHYÖKKÄYSTEN VOLYYMIT (Q4/2020 - 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

- Tietoturva- ja haavoittuvuustutkijat ovat olleet Pohjois-Koreaan yhdistetyn vakoilukampanjan kohteena.
  - Googlen ja Microsoftin tietoturvatutkijoiden mukaan haavoittuvuuksien tutkimisen sekä organisaatioiden ja järjestelmien tietoturvatestauksen parissa työskenteleviä oli muun muassa lähestytty erilaisilla sosiaalisen median alustoilla haitallisten tiedostojen jakamiseksi tai tutkijoille lähettämiseksi.
  - Lisäksi hyökkääjien verkkoblogissa oli viitteiden perusteella syötetty valikoiduille vierailijoille haitallista sisältöä mahdollisesti hyödyntäen Chromen nollapäivähaavoittuvuutta.
- Tammikuussa uutisoitiin myös Pohjois-Koreaan liitettyjen hakkereiden pyrkimyksistä vakoilla sijoitussovelluksen käyttäjiä. Siitä, oliko kampanjan tavoitteena vaikuttaa markkinoihin vai hankkia tietoa, ei ole tarkempaa tietoa.

ANALYYSI

- Haavoittuvuustutkijoiden ja tietoturvatestaajien mahdollisesti löytämät uudet haavoittuvuudet ovat valtiollisille toimijoille houkuttelevia tietoja. Tunkeutuminen kybervakoilun ensisijaisiin kohteisiin voi onnistua niitä käyttäen helpommin tai huomaamattomammin.
- Tutkijoiden ja tietoturvatestaajien on hyvä tiedostaa voivansa olla kybervakoilun kohteena työnsä vuoksi ja ottaa tämä huomioon esimerkiksi siinä, millä laitteilla ja virtuaalikoneilla mitäkin asioita tehdään.

Vakoilu

- Loppuvuodesta Euroopan lääkevirasto EMA:sta vietyjä tietoja on vuodettu verkkoon.
  - Vuodettujen tietojen joukossa oli muun muassa sähköposteja ja asiakirjoja.
- Tietoja jaettiin siten muunneltuina, että vuodetut tiedot herättäisivät epäilyjä Pfizerin ja BioNTechin rokotteen luotettavuudesta.
- EMA antoi kyseiselle rokotteelle hyväksyntänsä joulukuussa hieman tietomurron jälkeen.

ANALYYSI

- Muunneltujen tietojen vuotamisen tarkoituksena on arvioitu olevan vaikuttaminen ihmisten rokotushalukkuuteen ja epäilysten herättäminen rokotteiden turvallisuudesta.
- Tietomurtoihin varauduttaessa on hyvä miettiä mahdollista toimintasuunnitelmaa ja viestintää tilanteessa, jossa tietomurron yhteydessä vietyjä tietoja hyödynnetään vaikuttamistarkoituksessa esimerkiksi siten, että tietoja irrotetaan asiayhteydestään tai muunnellaan.

Vakoilu

- Saksan kotimaan turvallisuuspalvelu (Bundesamt für Verfassungsschutz, BfV) varoittaa APT31-ryhmittymän kartoittavan mahdollisuuksiaan tunkeutua poliittisiin kohteisiin länsimaissa.
  - BfV varoittaa saksalaisia organisaatioita siitä, että ne ovat olleet sekä kartoitustoiminnan että hyökkäyksen valmisteluun tähtäävien toimenpiteiden kohteena.
  - BfV:n mukaan kartoitus- ja valmistelutoimenpiteisiin kuuluu muun muassa seurantasähköpostien lähettämistä ja kohdeorganisaatioiden verkkoinfrastruktuurin kartoitusta.
  - Julkisuudessa APT31 on yhdistetty Kiinaan. Se tunnetaan myös nimellä ZIRCONIUM.
  - Aiemmin viime vuonna ryhmittymä oli uutisissa mm. Joe Bidenin kampanjaan kohdistuneiden vakoiluepäilyjen vuoksi.

ANALYYSI

- BfV pitää todennäköisimpinä tunkeutumistapoina tunnettuihin haavoittuvuuksiin olevien julkisten hyökkäyskoodien ja -työkalujen hyödyntämistä internetistä käsin saavutettavissa olevia palveluita vastaan tai käyttäjien salasanojen koneellista arvaamista (nk. bruteforcing- ja password spray -hyökkäykset).

Vakoilu

- Jälkipyykki joulukuussa tietoturvamaailmaa ravisuttaneen, SolarWinds Orion -hallintatyökaluun kohdistuneen toimitusketjuhyökkäyksen ympärillä jatkuu.
  - Esimerkiksi sähköpostin tietoturvaan keskittyvä Mimecast kertoi tammikuun alussa julki tulleen, siihen kohdistuneen tietomurron juontavan juurensa SolarWinds-tuotteeseen ja olevan saman hyökkääjän tekosia.
  - Reuters uutisoi, että myös kiinalaisiksi epäillyt hakkerit olisivat hyödyntäneet SolarWindsin tuotteessa ollutta haavoittuvuutta, joka on kuitenkin ollut eri kuin SUNBURST-haittaohjelman kohdalla. Reutersin mukaan tämä olisi tapahtunut samoihin aikoihin, kun venäläisiksi epäillyt toimijat käyttivät SolarWinds Orioniin ujuttamaansa takaovea valitsemiinsa kohteisiin tunkeutumiseksi.
- Kyberturvallisuuskeskuksen tämänhetkisen käsityksen valossa vaikuttaa edelleen siltä, että myös suomalaisissa organisaatioissa käytössä ollutta hallintatyökalun takaovellista versiota ei käytetty Suomessa pidemmälle edenneisiin tietomurtoihin.

ANALYYSI

- Erilaiset ylläpito- ja hallintatyökalut, verkon toteutukseen ja turvalliseen yhteydenmuodostukseen liittyvät järjestelmät sekä tietoturvaratkaisut ovat erityisen houkuttelevia järjestelmiä toimitusketjuhyökkäykselle.

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

- Liikenne- ja viestintäministeriö asetti ajalle 9.11.2020 – 31.1.2021 työryhmän selvittämään tietoturvan ja tietosuojan parantamista yhteiskunnan kriittisillä toimialoilla (TiTuKri). Loppuraportti julkaistiin 1.2.2021.
- Työryhmä teki ehdotukset poliittisiksi linjauksiksi kriittisten toimialojen tietoturvan ja tietosuojan parantamiseksi sekä määritteli vastuutahot ja aikataulut toimenpiteiden toteuttamiseksi. Kehitettäviä kohteita on useita ja raportissa todetaan myös lisäresurssien tarve.
- Linjausehdotukset perustuvat seitsemään vaatimukseen, joiden tulisi toteutua, jotta toiminnan tietoturva ja tietosuoja ovat riittäviä, näitä olivat esimerkiksi:
  - Toimijoilla on oltava riittävä tietämys ja osaaminen velvoitteiden noudattamisessa.
  - Jokainen toimija kantaa vastuun toimintansa tietoturvasta ja tietosuojasta.
  - Eri toimialoilla käytössä olleet yleisluontoiset huolellisuusvelvoitteet eivät ole riittäviä, tietoturvallisuuden ja tietosuojan tason varmistamiseksi vaatimusten tulee perustua velvoittaviin määräyksiin ja säännölliseen valvontaan
- Linkki tiedotteeseen: https://www.lvm.fi/-/tyoryhman-loppuraportti-toimiva-digitaalinen-yhteiskunta-edellyttaa-panostuksia-tietoturvaan-1254566
- Linkki loppuraporttiin: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162783/LVM_2021_1.pdf?sequence=1&isAllowed=y

Oikeudelliset asiat

- Lausuntopyyntö hallituksen esityksen luonnoksesta eduskunnalle laeiksi sähköisen viestinnän palveluista annetun lain ja tietoyhteiskuntakaaren muuttamisesta ja väliaikaisesta muuttamisesta annetun lain muuttamisesta
- Esityksessä ehdotetaan kahden nykyisin voimassa olevan määräaikaisen sääntelyn voimassaolon jatkamista kolmella vuodella:
  - Matkapuhelinliittymien puhelinmarkkinoinnin kieltoa kuluttajien suojaamiseksi häiriöllisiltä markkinointimenettelyiltä ja markkinoilla tapahtuvien häiriöiden ehkäisemiseksi
  - Radioviestinnän luottamuksellisuuden osalta on laajennettu oikeutta käsitellä ja hyödyntää radioviestinnän anonymisoituja välitystietoja. Sääntelyn tarkoituksena on hallitusti ja kokeiluluontoisesti tehdä mahdolliseksi uudenlaista liiketoimintaa yksityisyyden suojaa vaarantamatta.
- Hallituksen esityksen luonnos on lausuttavana 16.2.2021 asti ja lakien voimaantulo 21.6.2021 ja 2.7.2021
- https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=27a7b9ab-e186-4700-aae2-b482729e01f4

ISO 27002 ohjeistus kommentoitavana

- Tietoturvan hallintajärjestelmästandardi ISO 27001:n vaatimuksia tarkentava ohjeistus ISO 27002 on uusittavana. Standardiluonnos on nyt kansainvälisellä lausuntokierroksella, ja siihen voi tutustua ja ottaa kantaa maksutta. Lausuntoaika päättyy 1.4.2021.

- Standardiluonnokseen pääsee tutustumaan täältä, palveluun tulee rekisteröityä: https://lausunto.sfs.fi/Home/Details/1282

Arjen kyberturvallisuus – tammikuu

Rikolliset kalastelevat verkkopankkitunnuksia hakutulosten avulla

- Uudessa huijaustavassa henkilö ohjataan verkon hakukoneen tuloksen kautta väärennetylle sivustolle, joka muistuttaa aitoa verkkopankkia. Verkkopankkitunnusten kalastelu tapahtuu tällä sivustolla.
- Tee omalle verkkopankin osoitteelle selaimeesi kirjanmerkki, äläkä mene verkkopankkiin sähköpostilinkeistä tai tekstiviestistä
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/rikolliset-kalastelevat-verkkopankkitunnuksia-hakutulosten-avulla

Digivinkkejä kaikenikäisille Mediataitoviikolla

- Kyberturvallisuuskeskus on mukana Mediataitoviikolla 8. - 14.2.2021 vahvistamassa lasten ja aikuisten tietoturvataitoja
- Tutustu meidän ja muiden Mediataitoviikon kumppaneiden materiaaleihin alla olevan linkin kautta.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/digivinkkeja-kaikenikaisille-mediataitoviikolla

Saitko tekstiviestin Postin nimissä? Varothan, viesti voi olla huijaus

- Postin nimissä lähetetään runsaasti huijauksia tekstiviestien välityksellä.
- Älä avaa viesteissä tulevia linkkejä harkitsematta, koska vastaan voi tulla haittaohjelmia, tietojenkalastelua ja tilausansoja.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/saitko-tekstiviestin-postin-nimissa-varothan-viesti-voi-olla-huijaus

Tietoturva 2021: 3 uhkaa ja 3 ratkaisua jokaiselle

- Vuoden 2021 TOP 3 -tietoturvavinkkimme liittyvät yleisimpiin arkeamme tai organisaatioita uhkaaviin ilmiöihin, jotka eivät juurikaan muutu.
- Lue alla olevasta linkistä tiivistys yksityishenkilöiden ja organisaatioiden kolmesta merkittävimmästä tietoturvauhasta ja -ratkaisusta.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturva-2021-3-uhkaa-ja-3-ratkaisua-jokaiselle

Ajankohtaista Kyberturvallisuuskeskuksesta

Kyberturvallisuuskeskuksen CERT-toiminnon PGP-avaimet vaihtuvat

- Kyberturvallisuuskeskuksen CERT-toiminnon yleinen avain (NCSC-FI Incident Response), tiedotteiden allekirjoittamiseen käytetty avain (NCSC-FI Advisory Signing Key) ja uutiskoosteen allekirjoittamiseen käytetty avain (NCSC-FI Newsfeed Signing Key) vaihtuvat.
- Uudet avaimet ovat saatavilla keskuksen www-sivuilla ja yleisillä avainpalvelimilla.
- Lisätietoja ja uusien PGP-avainten tunnisteet ja sormenjäljet löydät täältä: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/cert-toiminnon-pgp-2021

Kyberharjoitusskenaariot 2021 - uusia ideoita kyberharjoituksiin

- Uusi Kyberharjoitusskenaariot 2021 -julkaisumme sisältää todentuntuisia kyberuhkia maksujärjestelmän tietovuodosta laajamittaiseen epidemiaan.
- Kokoelma on laadittu yhteistyössä kumppaniyritysten asiantuntijoiden kanssa. Skenaariot perustuvat tosielämän kyberturvallisuus-poikkeamiin.
- Skenaariot käsittelevät monipuolisesti erilaisia tietoturvaa ja tietosuojaa koskevia uhkatilanteita, joita yhdistelemällä voidaan rakentaa monimutkaisia ja haastavia koko organisaation toiminnan kattavia harjoituksia.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberharjoitusskenaariot-2021-uusia-ideoita-kyberharjoituksiin

Toisiolain mukaisten käyttöympäristöjen arviointien määräaika lähestyy

- Traficom on määritellyt, millä edellytyksillä sen hyväksymä tietoturvallisuuden arviointilaitos voi tehdä sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain mukaisen käyttöympäristön tietoturvallisuuden arvioinnin ja antaa vaatimusten täyttymistä koskevan todistuksen.
- Tietoturvallisten käyttöympäristöjen palveluntarjoajat voivat olla suoraan yhteydessä arviointilaitoksiin, mikäli haluavat teettää käyttöympäristölleen kyseisen arvioinnin ja saada siitä todistuksen.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/toisiolain-mukaisten-kayttoymparistojen-arviointien-maaraaika-lahestyy-kahdella

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