TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Joulukuu 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 joulukuu 2020

Tietomurrot ja -vuodot

- SolarWinds hallintatyökalun takaoven sisältävää versiota on käytössä myös Suomessa.
- Office 365 -tilit ovat edelleen aktiivisten tunkeutumisyritysten kohteena..

Huijaukset ja kalastelut

- Tekstiviesteillä levitetään runsaasti huijauksia, jotka johtavat tilausansoihin, tietojenkalasteluun ja haittaohjelmiin.
- Saapumisilmoitukset ovat johtaneet tietojenkalasteluun, jonka avulla tehtaillaan pikavippejä uhrien laskuun.

Haittaohjelmat ja haavoittuvuudet

- SolarWinds-hallintatyökalusta löydettin takaovi, joka mahdollisti vakoilun ja tietomurrot.
- Emotet-havainnot ovat yleistyneet Suomessa kuukauden passiivisen ajanjakson jälkeen.

Automaatio ja IoT

- Gitpaste-haittaohjelmasta on ilmennytenemmän hyökkäys- ja leviämistapoja
- Automaatiojärjestelmissä havaittujen haavoittuvuuksien päivittämisessä puutteita – pitkät toimitusketjut hidastavat reagointia ja vaikeuttavat tunnistamista

Verkkojen toimivuus

- Vain kaksi merkittävää häiriötä yleisissä viestintäpalveluissa
- Maailmanlaajuinen häiriö Googlen palveluissa esti työnteon monilta. Monet IoT-laitteet eivät toimineet.
- Palvelunestohyökkäysten kohteena ovat olleet esimerkiksi palveluntarjoajat ja VPN-ratkaisut.

Vakoilu

- Suomen eduskuntaan kohdistui syksyllä kyberhyökkäys, jossa joitakin eduskunnan sähköpostitilejä vaarantui – joukossa oli myös kansanedustajien tilejä.
- Yhdysvalloissa ministeriöihin, virastoihin ja teknologiayhtiöihin tunkeuduttiin SolarWinds Orion -hallintatyökaluun lisätyllä takaovella.

Kuukauden tunnuslukuja

215

TILAUSANSOJA ON VIRITETTY JOULUKUUSSA POIKKEUKSELLISEN PALJON. SEKÄ SÄHKÖPOSTILLA ETTÄ TEKSTIVIESTEILLÄ LÄHETETTIIN ERI TEEMOILLA RUNSAASTI HUIJAUSVIESTEJÄ, JOTKA JOHTAVAT TILAUSANSOIHIN.

1

EDUSKUNTAAN KOHDISTUI VIIME SYKSYNÄ KYBERHYÖKKÄYS, JOTA KESKUSRIKOSPOLIISI (KRP) TUTKII EPÄILTYINÄ TÖRKEÄNÄ TIETOMURTONA JA VAKOILUNA. EDUSKUNTA TIEDOTTI ASIASTA JOULUKUUN LOPULLA.

16.12.2020

EU:N UUSI KYBERTURVALLISUUSSTRATEGIA JULKAISTIIN (THE EU'S CYBERSECURITY STRATEGY FOR THE DIGITAL DECADE)

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

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

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

- SolarWinds hallintatyökalun tietomurtotapaukset Suomessa
  - Hyökkäyksen kohteena ovat olleet ainakin suuret organisaatiot sekä Yhdysvaltain valtionhallinto.
    - Lisää aiheesta tämän Kybersään osioissa Vakoilu sekä Haittaohjelmat ja haavoittuvuudet
  - Suomessa on organisaatiota, joissa käytetään takaoven sisältänyttä SolarWinds hallintatyökalun versiota. Kyberturvallisuuskeskuksen tiedossa ei ole, että takaovea olisi hyödynnetty Suomessa tietomurroissa
- Julkaisimme: Opas tietomurtojen havaitsemiseen
  - Ohjeessa keskitytään erityisesti tietomurron havaitsemiseen lokitietojen avulla. Esimerkkeinä käytetään Windows Event Log -tapahtumalokeja tai muita Windows-käyttöjärjestelmän lokitapahtumia
    - https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/opas-tietomurtojen-havaitsemiseen

ANALYYSI

- Kyberhyökkäykset ovat kohdennettuja tai sattumanvaraisia, joten kohteena voi olla, mikä tahansa toimija tai organisaatio
- Hyvä havainnointikyky, tiedon, tietoverkon, päätelaitteiden ja käyttöoikeuksien hallinta ovat avainasemassa tietomurtojen torjunnassa

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

- Tilausansoja on viritetty joulukuussa poikkeuksellisen paljon. Sekä sähköpostilla että tekstiviesteillä on lähetetty eri teemoilla runsaasti huijausviestejä, jotka johtavat tilausansoihin. Verukkeena voi olla paketin saapumisilmoitus, arpajaisvoitto, arvontaan osallistuminen, tai kauppojen lahjakortteja.
- Postin saapumisilmoituksien tekstiviestejä on väärennetty moniin eri huijauksiin. Tilausansojen ja Android-haittaohjelman levityksen lisäksi saapumisilmoituksen valelinkki on johtanut tietojenkalasteluun ja sitä kautta pikavippihuijauksiin.
- Jolusesonki on lisännyt myös yrityksiin kohdistuvia laskutushuijauksia ja palkanmaksuhuijauksia.

ANALYYSI

- Pikavippejä tekstiviestikalasteluiden tiedoilla
  - Tekstiviesteinä lähetetään paljon Postin, DHL:n, UPS:n ja muiden kuriiriyritysten saapumisilmoituksiksi väärennettyjä viestejä. Huijauksissa kerrotaan saapuneesta lähetyksestä, tai väitetään, että paketti on pysäytetty jakelukeskukseen, koska jokin maksu puuttuu.
  - Tekstiviestin linkki johtaa tietojenkalastelusivulle, jossa uhrilta kysytään kirjautumistiedot. Kirjautumistiedoilla nostetaan pikavippejä uhrin laskuun.
  - Jos olet joutunut huijauksen uhriksi, tee rikosilmoitus poliisille. Kerro myös Kyberturvallisuuskeskukselle, niin saamme kalastelusivun poistettua verkosta.

Teknisen tuen nimissä soittelu jatkuu

- Sekä ulkomaisista että suomalaisista puhelinnumeroista soitetaan edelleen paljon puheluita, joissa yritetään huijata Microsoftin teknisen tuen nimissä.
- Myös hälärihuijaukset aktivoituivat jälleen joulukuussa. Marokon suuntanumerosta +212 soitettiin paljon huijauspuheluita.
- 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

- Joulukuussa kalasteltiin runsaasti pankkitunnuksia kaikkien pankkien asiakkailta. Turvapostiksi väärennetty huijausviesti väitti, että tuntematon laite on liitetty tiliisi, klikkaa tästä lisätietoja.
- Myös eri palveluiden kirjautumistunnuksia kalastellaan paljon: Netflix, Amazon, Paypal, jne.
- Tietojenkalastelu on keskeinen väline ammattirikollisten työkalupakissa. Sillä saa kerättyä tietomurtoihin tarvittavia tietoja, pankkitunnuksia, organisaatiorakenteita, henkilötietoja, käyttäjätunnuksia ja salasanoja.
- 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.

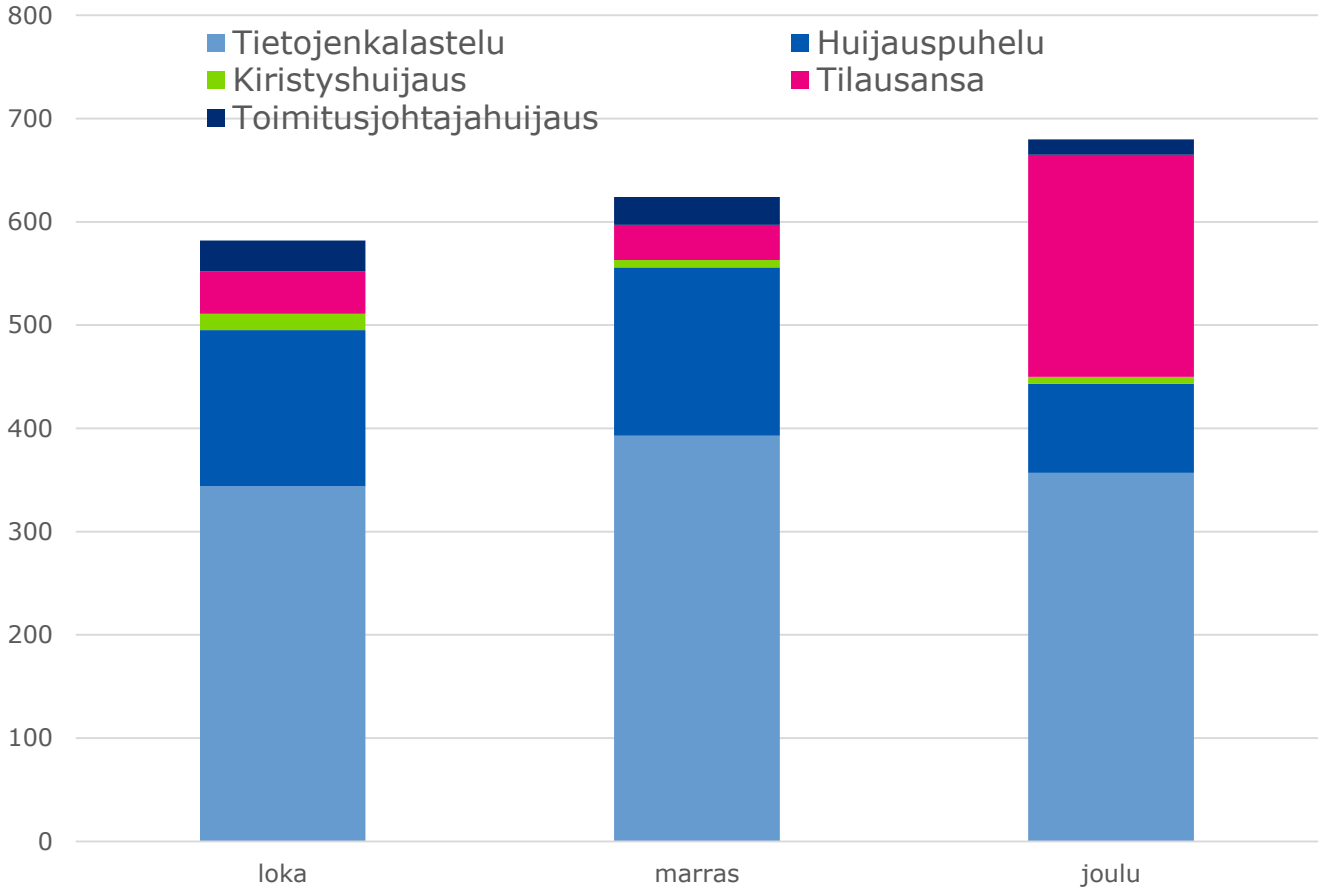
Office 365 -tietojenkalastelu

- 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 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

- Emotetin levitysyrityksiä havaittu jälleen Suomessa
  - Ajan tasalla olevat tietoturvatuotteet pienentävät tartuntariskiä ja estävät haitallisen liitetiedoston päätymisen sähköpostiin
  - Olemme saaneet myös kansainvälisiltä kollegoilta tietoa uudesta aktiivisemmasta Emotetin levityksestä
  - Antamamme Keltainen varoitus on poistettu 18.11. eikä sitä ole toistaiseksi muutettu aktiiviseksi
    - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/emotet-haittaohjelmaa-koskenut-keltainen-varoitus-poistettiin

ANALYYSI

- Emotet toimii kausittaisesti, jolloin pitkää passiivisuutta voi seurata aktiivisempi haittaohjelman levityskausi
- Yritysten havainnointikyky ja ajantasaiset tietoturvatuotteet vähentävät tietoturvariskiä

Haavoittuvuudet

- Hallintatyökaluista löydetty vakavia haavoittuvuuksia.
  - IT-infrastruktuurin keskitettyyn valvontaan ja hallintaan käytetyn SolarWinds Orion Platformin takaovi mahdollisti vakoilun ja tietomurtoja
    - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/solarwinds-orion-platformin-takaovi-mahdollisti-vakoilun-ja-tietomurtoja
    - Lisätietoja aiheesta on myös tämän Kybersään Vakoilu-osiossa
  - HPE palvelinten hallintaan tarkoitettu hallintatyökalu sisälsi kriittisen nollapäivähaavoittuvuuden, kirjoitimme aiheesta haavoittuvuustiedotteen
- Päivitimme SolarWinds-tiedotteeseen 28.12. tarkempaa tietoa myös haittaohjelma Supernovasta
  - Toisen löydetyn haavoittuvuuden avulla on asennettu hallintatyökaluun haittaohjelma Supernova, joka mahdollistaa ohjelmointirajapinnan tunnistautumisen ohittamisen

ANALYYSI

- SolarWinds kehoittaa asiakkaitaan päivittämään Orion Platform -työkalun versioon 2020.2.1 HF 2 mahdollisimman pian, sillä päivitys korjaa vaarantuneen komponentin sekä myöhemmin löydetyn haavoittuvuuden
- Palvelimilta kannattaa sallia vain tarvittavat yhteydet ulospäin. Näin SolarWindsin takaovikaan ei saa yhteyttä komentopalvelimeensa

Joulukuun haavoittuvuusjulkaisut

- ABB on julkaissut Arctic wireless gateway -tuotteeseen liittyvän haavoittuvuuden (37/2020)
- SolarWinds Orion Platform -hallintatyökalusta löydetty takaovi (38/2020)
- Kriittinen nollapäivähaavoittuvuus HPE Systems Insight Manager –ohjelmistossa (39/2020)
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

- Julkaisimme myös Tietoturva Nyt! –artikkelin SolarWinds –hallintatyökalusta
  - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/solarwinds-orion-platformin-takaovi-mahdollisti-vakoilun-ja-tietomurtoja

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

- Automaatiojärjestelmissä havaittu haavoittuvuuksia ja päivitysten asentamisessa viivettä
  - Forescout on löytänyt IoT- ja automaatiolaitteissa käytetyistä TCP/IP-pinoista kriittisiä haavoittuvuuksia, jotka koskevat miljoonialaitteita yli 150 valmistajalta.
    - https://www.forescout.com/research-labs/amnesia33/
  - Tietoturvayritys Armis löysi aikaisemmin 11 kriittistä haavoittuvuutta laajasti käytetystä VxWorks-käyttöjärjestelmästä. Joulukuun tarkastelussa 97 % näistä haavoittuvuuksista on edelleen paikkaamatta saatavilla olevista päivityksistä huolimatta
    - https://www.armis.com/urgent11/

ANALYYSI

- Tunnistamattomat haavoittuvuudet tai niiden päivitysten viivästyminen vaarantavat organisaation tietoturvallisuuden
- Haavoittuvuuksien hallinta edellyttää omien toimitusketjujen ja ohjelmisto-omaisuuden tunnistamista
  - Software bill of materialsin (SBOM) käyttö on yksi hyvä tapa pitää ajantasaista tilannekuvaa
- Vastuu päivityksistä on hyvä määrittää sopimuksissa palveluntarjoajan kanssa

Automaatio ja IoT

- Kyberturvallisuuskeskuksen vuosittaisen avoimien automaatiolaitteiden kartoituksen tulokset vuodelta 2020 on koostettu
  - Yhteensä havaittiin noin 1000 laitetta, Kokonaismäärä pysyi edellisvuoden tasolla
  - Havaittujen suojaamattomien teollisuuden ohjausjärjestelmien sekä rakennusautomaatiojärjestelmien määrät ovat pienentyneet, mutta yksittäiset suojaamattomat automaatiolaitteet ovat lisääntyneet vuodesta 2019
  - Lisäksi havaittiin verkkoon liitettyjä IoT-laitteita, joita ovat esimerkiksi kotireitittimet, laajakaistamodeemit, tulostimet ja verkkokamerat. Näitä on verkoissa on kuin esimerkiksi rakennusautomaatiolaitteita.
    - Tilastokeskuksen mukaan Esineiden internet on käytössä 40 prosentilla yrityksistä*

ANALYYSI

- Laitteet voidaan jättää suojaamatta, jotta niiden käyttäminen olisi mahdollisimman helppoa eri sidosryhmille.
  - Mieti, mitä järjestelmiä sinulla on hallussasi ja miten ne on suojattu. Testaa mitä tietoa löydät omista järjestelmistäsi käyttäen eri työkaluja. Ota tarvittaessa yhteyttä laitteen valmistajaan tai myyjään tarkempien ohjeiden saamiseksi.
  - Selvitä ja testaa, että palomuurien asetukset toimivat oikein, jotta laitteet ja niiden palvelut eivät näy avoimena julkiverkkoon.
  - Päivitä internetiin kytketyt laitteet uusimpiin versioihin. Mikäli omistat laitteet, mutta et voi tehdä päivitystä itse, ota yhteyttä ensisijaisesti järjestelmän toimittaneeseen yritykseen tai järjestelmän ylläpidosta vastaavaan yritykseen.
  - Vaihda etenkin etäyhteyksien päässä olevien automaatiolaitteiden oletussalasanat.

Automaatio ja IoT

- GitPaste-haittaohjelmasta on ilmennyt entistä enemmän hyökkäys- ja leviämistapoja, jotka uhkaavat Linux-pohjaisia järjestelmiä sekä verkkosovelluksia, -kameroita ja reitittimiä
  - https://thehackernews.com/2020/12/wormable-gitpaste-12-botnet-returns-to.html
- Hollantilainen tietoturvayritys EYE havaitsi Zyxelin reitittimissä ylimääräisen käyttäjätilin, jossa on kovakoodattu oletussalasana
  - Päivitys on julkaistu, mutta verkossa on edelleen suuri määrä päivittämättömiä haavoittuvia laitteita
  - https://www.eyecontrol.nl/blog/undocumented-user-account-in-zyxel-products.html

ANALYYSI

- Päivitysten laiminlyönti mahdollistaa haittaohjelmien leviämisen ja niiden aiheuttamien ongelmien kasvun
- Reitittimien tietoturvapuutteet altistavat myös sen kautta verkkoon yhteydessä olevat laitteet ja järjestelmät tietoturvahyökkäyksille
  - Reitittimien tietoturvapäivitykset tulisi asentaa välittömästi niiden tullessa saataville
  - Päivitysten olisi hyvä asentua oletusarvona automaattisesti ilman että käyttäjältä vaaditaan toimenpiteitä

Automaatio ja IoT

- Googlen verkkopalvelut kärsivät joulukuussa käyttökatkosta, jolla oli merkittävä vaikutus käyttäjiin
- Katko johtui ongelmista autentikaatiopalvelussa
- Katko vaikutti Googlen älykotijärjestelmiin mm. valaistukseen, ääniohjaukseen, lämmitysjärjestelmän säätöön ja palovaroittimiin
- https://www.theguardian.com/technology/2020/dec/14/google-suffers-worldwide-outage-with-gmail-youtube-and-other-services-down

ANALYYSI

- Voimakas keskitetty riippuvuus palveluntarjoajan järjestelmistä voi johtaa yllättäviin ja yllättävän laajavaikutteisiin ongelmiin jokapäiväisessä toiminnassa
- Käyttäjän tulisi tunnistaa olemassa olevat riippuvuudet, arvioida niiden vaikutukset ja tarvittaessa varautua ongelmatilanteisiin

IoT

- Eurooppa-neuvosto on julkaissut yhteenvedon verkkoon liitettävien laitteiden kyberturvallisuudesta
  - https://www.consilium.europa.eu/en/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/
- Yhdysvaltojen hallinto asetti joulukuussa tietoturvavaatimukset IoT-laitteiden hankinnoille, ja NIST on julkaissut vaatimusten toteuttamisen ohjeistuksen
  - https://www.congress.gov/bill/116th-congress/house-bill/1668
  - https://www.nist.gov/news-events/news/2020/12/nist-releases-draft-guidance-internet-things-device-cybersecurity
- OWASP (Open Web Application Security Project) on asettanut IoT:n tietoturvan todentamisstandardin kommentoitavaksi
  - https://owasp.org/www-project-iot-security-verification-standard/

ANALYYSI

- IoT-laitteiden tietoturvaa koskevien vaatimusten ja todentamisen määrittely lisääntyy kiihtyvällä tahdilla
- Vaatimusten ja todentamismenettelyiden käyttö on toistaiseksi perustunut vapaaehtoisuuteen, nyt nähtävissä myös pakottavaan sääntelyyn siirtymistä
- Organisaatioiden on hyvä varautua pakottavien tietoturvavaatimusten käyttöönottoon ja todentamiseen mahdollisimman aikaisessa vaiheessa

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

- Joulukuussa vain kaksi merkittävää häiriötä yleisissä viestintäpalveluissa
  - Kiinteän internetyhteyspalvelun häiriö Oulussa ja kaapeli-TV:n ja kaapelilaajakaistan häiriö Kuopiossa
- Vuonna 2020 merkittäviä toimivuushäiriöitä oli kaikkiaan 67.
- Googlen pilvipalveluissa oli 14.12. vajaan tunnin katkos.
  - Kirjautumista vaativia Googlen sovelluksia ei voinut käyttää.
  - Monien IoT-laitteiden toiminnassa oli häiriöitä: esimerkiksi Googlen omistaman Nestin turvakameroita ja termostaatteja ei voinut säätää häiriön aikana.

ANALYYSI

- Vuosittainen merkittävien toimivuushäiriöiden määrä jäi lopulta yhden pienemmäksi kuin vuonna 2019. Laajimpien häiriöiden määrä väheni edellisvuodesta.
- Pilvipalveluiden häiriöt vaikuttavat kerralla suureen käyttäjäjoukkoon, mutta yksittäisen käyttäjän kannalta pilvipalvelut todennäköisesti kasvattavat toimintavarmuutta. Toimintahäiriöihin varautuminen on silti tärkeää. Esimerkiksi IoT-laitteet pitäisi suunnitella siten, että ne suoriutuvat ainakin joistakin perustehtävistään myös ilman verkkoyhteyttä.

Palvelunestohyökkäykset

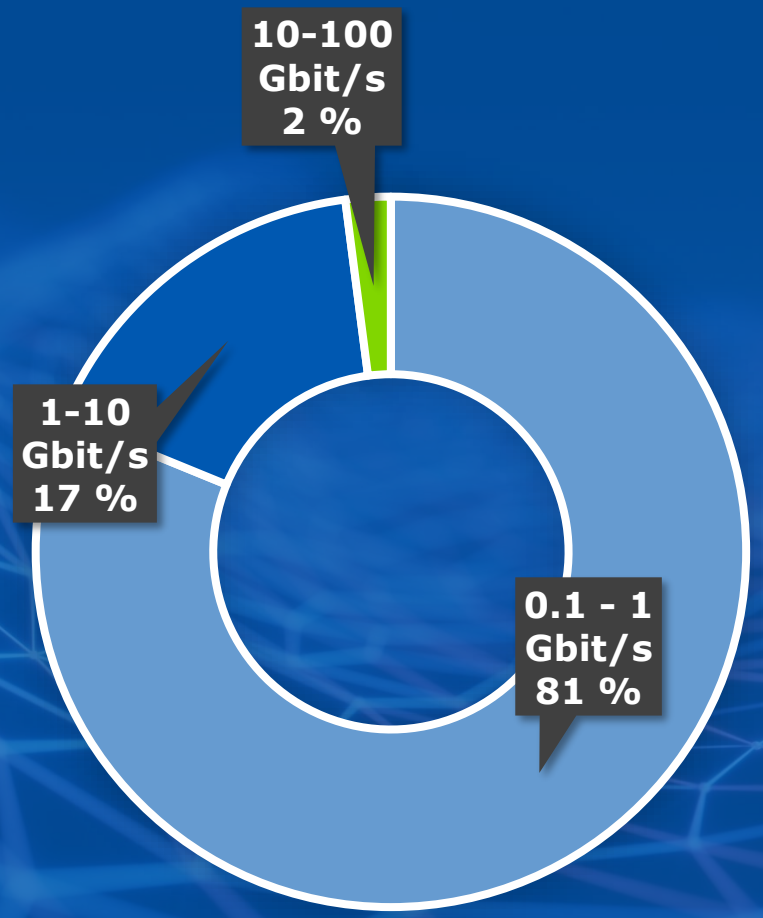
- Joulukuussa Kyberturvallisuuskeskus sai ilmoituksia palvelunestohyökkäyksistä, joilla oli laajoja vaikutuksia palveluiden toimintaan.
- Palvelunestohyökkäysten kohteena ovat olleet esimerkiksi palveluntarjoajat ja VPN-ratkaisut.
  - Suosittelemme varautumaan palvelunestohyökkäyksiin esimerkiksi erilaisten mitigointipalveluiden avulla.
  - Nimipalveluiden toiminnan suojaamiseksi suosittelemme ottamaan käyttöön maksuttoman toissijaisen hajautetun nimipalvelumme FI-verkkotunnuksille: https://www.traficom.fi/fi/hajautettu-nimipalvelu-valittajien-kayttoon
- Loppusyksystä nähtyjä kiristystapauksia ei enää joulukuussa nähty.
- Tietoturvatestaaminenkin voi aiheuttaa häiriöitä, jos testaamisesta ei etukäteen tiedoteta. Testaamisen suunnittelussa kannattaa ottaa huomioon mahdolliset välilliset vaikutukset.

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

- Eduskuntaan kohdistui viime syksynä kyberhyökkäys, jota Keskusrikospoliisi (KRP) tutkii epäiltyinä törkeänä tietomurtona ja vakoiluna. Eduskunta tiedotti asiasta joulukuun lopulla.
  - Eduskunnan mukaan jotkut eduskunnan sähköpostitilit vaarantuivat kyberhyökkäyksen seurauksena. Näiden tilien joukossa oli myös kansanedustajien sähköpostitilejä. Hyökkäys oli havaittu eduskunnan sisäisessä teknisessä valvonnassa.
  - KRP on aloittanut esitutkinnan asiasta. Selvityksessä on sekä tietomurron tekotapa että se, kuka tai ketkä murron ovat tehneet.
  - KRP on kertonut, että hyökkäys ei ollut sattumanvarainen tai vahinko, ja sen mukaan on mahdollista, että hyökkäyksellä pyrittiin hankkimaan tietoa vieraan valtion hyväksi tai Suomen vahingoksi.
- Vuoden 2020 aikana myös ulkomaiset valtionhallinnon toimijat ovat tiedottaneet kyberhyökkäyksistä.
  - Esimerkiksi Norjan parlamentti eli Suurkäräjät kertoi sen sähköpostitilien vaarantumisesta kyberhyökkäyksen seurauksena, mutta tiedossa ei ole, liittyvätkö tapaukset toisiinsa.

ANALYYSI

- Poliittinen päätöksenteko on perinteinen mutta edelleen ajankohtainen kybervakoilun kohde. Valtionhallinnon organisaatiot ja päätöksentekoelimet joutuvat varautumaan kehittyneisiin kyberhyökkäyksiin, joiden toteuttajana voi olla kyvykäs ja määrätietoinen hyökkääjä.

Vakoilu

- SolarWindsin Orion-hallintatyökalun ohjelmakoodiin lisätyn takaoven avulla tunkeuduttiin lukuisaan joukkoon merkittäviä kohteita. SUNBURST-haittaohjelmalla pyrittiin tiettävästi vakoilemaan poliittisia sekä kansalliseen turvallisuuteen liittyviä kohteita Yhdysvalloissa sekä murtauduttiin tietoturva- ja IT-alan toimijoiden järjestelmiin.
  - Yhdysvaltojen valtionhallinnossa haavoittuvuus vaikutti tiettävästi muun muassa kotimaan turvallisuusvirastoon (DHS) sekä valtiovarain-, energia- ja kauppaministeriöihin. Yhdysvaltojen turvallisuusvirastot ovat yhteisessä julkilausumassaan pitäneet tietomurtojen todennäköisimpänä syypäänä venäläistä APT-ryhmää. Tiedot tietomurtojen vaikutuksista tarkentuvat edelleen.
  - Tietoturvayhtiö FireEye ja IT-jätti Microsoft kertoivat SolarWinds-liitännäisistä tietomurroista. Microsoftin mukaan hyökkääjä pääsi tarkastelemaan ohjelmakoodia mutta ei muuttamaan sitä. FireEye puolestaan raportoi, että hyökkääjä onnistui saamaan käsiinsä yhtiön tietoturvatestauksessa käyttämiä työkaluja. Yhtiö on julkaissut ohjeet niiden luvattoman käytön havaitsemiseksi.
  - Myös Suomessa on ollut organisaatioita, joihin takaovella varustettu versio tuotteesta on asennettu. Kyberturvallisuuskeskuksen tiedossa ei ole tapauksia, joissa hyökkääjä olisi hyödyntänyt mahdollisuuttaan suomalaisorganisaatioihin tunkeutumiseen.
  - Tarkemmin ohjelmistoon lisätystä takaovesta osioissa Haittaohjelmat ja haavoittuvuudet sekä Tietomurrot ja -vuodot.

ANALYYSI

- Erilaiset toimitus- ja alihankintaketjut voivat mahdollistaa hyökkääjille keinon päästä huomaamattomammin varsinaiseen kohteeseensa tai saamaan samalla kertaa pääsyn laajaan kohdejoukkoon.
- Erityisen houkuttelevia järjestelmiä tämänkaltaiselle tunkeutumiselle ovat mm. erilaiset ylläpito- ja hallintatyökalut, verkon toteutukseen ja turvalliseen yhteydenmuodostukseen liittyvät järjestelmät sekä tietoturvaratkaisut.

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

- Euroopan komissio ja unionin korkea edustaja esittelivät EU:n uuden kyberturvallisuusstrategian
  - EU:n uusi kyberturvallisuusstrategia julkaistiin 16.12.2020 (The EU's Cybersecurity Strategy for the Digital Decade)
  - Strategia rakentuu kolmelle päätavoitteelle, jotka ovat
    1. häiriönsietokyky, teknologinen riippumattomuus ja johtajuus
    2. operatiivisten valmiuksien kehittäminen uhkien ehkäisemiseksi, torjumiseksi ja niihin vastaamiseksi
    3. maailmanlaajuisen ja avoimen kybertoimintaympäristön edistäminen
  - Keskiössä avoimen, turvallisen ja kansalaisten perusoikeuksien kunnioittamiselle perustuvan Internetin turvaaminen.
  - Tärkeässä roolissa myös investoinnit EU:n digitalisaatioon sekä kyberosaamisen kehittäminen ja yhteisen tilannekuvan luominen. Eurooppalaisten pk-yritysten kybervarautumisessa todetaan olevan paljon kehitettävää.
  - Lisätietoja: https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy

Oikeudelliset asiat

- Euroopan komission ehdotus uudeksi NIS-direktiiviksi
  - Euroopan komissio antoi 16.12.2020 ehdotuksensa verkko- ja tietoturvadirektiivin uudistamiseksi (ns. NIS-direktiivi), jolla on tarkoitus kumota kokonaan edellinen NIS-direktiivi ja säätää uudesta direktiivistä kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella.
  - Muutosehdotus on kattava ja soveltamisalaa laajennetaan monille uusille toimialoille ja toimijoille, lisäksi soveltamisalan piirissä olevat toimialat jaettaisiin yhteiskunnan toiminnan kannalta välttämättömiin ja tärkeisiin toimialoihin. Soveltamisalan piiriin tulisivat automaattisesti kaikki keskisuuret ja suuret toimijat ko. toimialoilla.
  - Riskienhallintavelvoitteita tarkennetaan, toimijoille ja valvoville viranomaisille säädetään uusia velvollisuuksia.
  - Yritysten häiriöraportointivelvoitteita täsmennetään ja tiukennetaan. Lisäksi tietoturvavelvollisuuksien rikkomisesta ehdotetaan säädettäväksi rahamääräinen sanktio, joka olisi enintään 10M€ tai 2% yrityksen globaalista liikevaihdosta.
  - Direktiiviehdotus siirtyy seuraavaksi Euroopan unionin neuvoston ja parlamentin käsiteltäväksi.
  - Lisätietoja: https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union

Oikeudelliset asiat

- Sähköisen viestinnän palveluista annetun lain muutos voimaan
  - Tasavallan presidentti on vahvistanut sähköisen viestinnän palvelulakiin tehdyt muutokset. Lakimuutokset tulivat voimaan 1.1.2021
  - Lakimuutoksella 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.
  - Kuluttajien turvaa ja palveluja parannetaan, verkkotoimilupiin muutoksia ja tukiasemien rakentaminen helpottuu, verkkojen ja sisältöjen turvallisuuteen entistä enemmän huomiota
  - LVM:n tiedote: https://www.lvm.fi/-/sahkoisen-viestinnan-palvelulaki-voimaan-1-1-2021-1249001
  - Ks. asian käsittelytiedot ja annetut lausunnot: https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_98+2020.aspx

Arjen kyberturvallisuus – joulukuu

Tutustu Traficomin uusiin tietoturvalähettiläisiin

- Tietoturva on oleellinen osa kodin älylaitteiden turvallista käyttöä ja sujuvaa toimivuutta. Uudet tietoturvalähettiläämme - turvalistit - pohtivat uusilla videoilla tavallisia kodin tietoturvakysymyksiä ja ratkaisevat niitä yhdessä perheen ja ystävien kanssa.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tutustu-traficomin-uusiin-tietoturvalahettilaisiin

Kirjauduthan palveluun monivaiheista tunnistautumista hyödyntäen, jos se on mahdollista?

- Eri palveluiden, kuten some, peli ja sähköposti, tileille yritetään murtautua aktiivisesti usein eri keinoin.
- Ottamalla käyttöön kaksi- tai monivaiheisen tunnistautumisen (MFA, multi-factor authentication) sähköpostissasi ja sosiaalisen median tileissäsi teet tiliesi varastamisesta huomattavasti vaikeampaa.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-yksityishenkiloille

Ajankohtaista Kyberturvallisuuskeskuksesta

Tarjoa asiakkaillesi parasta: vahva sähköinen tunnistus

- Asiakkaiden vahvan sähköisen tunnistuksen hankkiminen on helpottunut tunnistuspalveluiden luottamusverkoston sääntelyn ansiosta.
- Pankkitunnistuksella, mobiilivarmenteella tai poliisin myöntämässä henkilökortissa olevalla kansalaisvarmenteella voit tunnistautua verkkopalveluihin turvallisesti.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tarjoa-asiakkaillesi-parasta-vahva-sahkoinen-tunnistus

ENISA julkaisi 5G uhkaraportin

- Ensimmäisen kerran uhkaraportti on julkaistu 2019 ja nyt julkaistu raportti päivittää tätä.
- Raportti kuvaa 5G-arkkitehtuurin kehitystä ja tiivistää 5G:hen liittyvät standardointiasiakirjoissa olevat tiedot.
- Raportissa löydetyt haavoittuvuus- ja uhka-arviot tuovat merkittävän edistyksen edelliseen painokseen tarjoamalla kattavampaa tietoa.
- https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

Muuttuva maailma tarvitsee uusia ketteriä menetelmiä kyberturvallisuuden parantamiseksi - yritysten tietoturvaa voi parantaa helposti!

- Yritykselle suojattavien kohteiden tunnistaminen on tärkeää. Se on myös yksi tehokkaan suojautumisen mahdollistaja. Monimutkaisten eristettyjen verkkojen eristys ei aina ole niin hyvällä tasolla kuin on suunniteltu.
- Toteutettavuustutkimus testasi ja kehitti menestyksekkäästi uusia ketteriä ja skaalautuvia menetelmiä näiden osa-alueiden parantamiseksi.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/toteutettavuustutkimus

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