TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Maaliskuu 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 maaliskuu 2020

Tietomurrot ja -vuodot

- Ilmoitettujen Office 365 – tietomurtojen määrä lievässä laskussa.
- Kanta-asiakasjärjestelmiin kohdistunut useampi tietovuoto, joihin liittyen myös suomalaisten tietoja päätyi vääriin käsiin.

Huijaukset ja kalastelut

- Korona-aiheisissa huijauksissa on kaupiteltu olemattomia suojaimia ja testauskittejä.
- Teknisen tuen huijauspuhelut loppuivat kokonaan 24.3.

Haittaohjelmat ja haavoittuvuudet

- Huolehdi, että etätyön mahdollistavat toimenpiteet eivät vaaranna yritysverkon tietoturvaa.
- COVID-19 teemalla levitetään paljon haitallista sisältöä

Automaatio

- Internetiin avoinna olevien automaatioympäristöjen määrä on kasvussa. Etähallintayhteyksien avaaminen tulee tehdä vasta huolellisen tarkastelun jälkeen.

Verkkojen toimivuus

- Viestintäverkot ovat kestäneet hyvin siirtymisen konttoreilta ja koulutusta kotona työskentelyyn.
- Osalla palvelunestohyökkäyksistä välillisiä vaikutuksia myös mm. etäyhteyksien toimivuuteen.

Vakoilu

- Koronavirusteemaa hyödynnetään myös kybervakoilussa.
- Päivittämättömät järjestelmät ovat houkutteleva kohde myös APT-ryhmille.

Kuukauden tunnuslukuja

24.3.

PUHELINHUIJAUKSET LOPPUIVAT.

HELMIKUUSSA NÄIDEN SOITTOJEN MÄÄRÄ NÄKYI MERKITTÄVÄSTI YHTEYDENOTTOJEN MÄÄRÄSSÄ KYBERTURVALLISUUSKESKUKSELLA.

0

MAALISKUUSSA EI OLLUT YHTÄÄN VAKAVAA VERKKOJEN TOIMIVUUSHÄIRIÖTÄ.

SUOMEN VIESTINTÄVERKOT KESTIVÄT HYVIN SIIRTYMISEN ETÄTYÖHÖN JA –OPISKELUUN.

161 GBIT/S

ENSIMMÄISEN KVARTAALIN AIKANA HAVAITTIIN SUOMESSA SUURI PALVELUNESTOHYÖKKÄYS

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

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

2

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

3

Laajavaikutteiset kiristyshyökkäykset uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

4

Epäselvä vastuunjako palvelutoimittajan, alihankkijoiden ja tilaajan välillä heikentää tietoturvan hallintaa. Puutteet lokien tarkkailussa vaikeuttavat uhkien havaitsemista.

5

Organisaatiot eivät osaa hallita kyberriskejään. Uhkien vaikutuksia toimintaan ei osata ennakoida, minkä vuoksi riskit aliarvioidaan. Palautumissuunnitelmissa on puutteita.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

1

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

- Rikolliset kehittävät hyväksikäyttömenetelmiä nopeasti heti ohjelmistopäivitysten ilmestyttyä ja iskevät kohteisiin, joita ei ole päivitetty. Erityisesti tietoturvatuotteissa olevat haavoittuvuudet ovat vakavia, sillä ne on yleensä sijoitettu muutenkin hyökkäyksille alttiisiin tietojärjestelmien kohtiin.
- Hyökkäyksissä käytetyt järjestelmähaavoittuvuudet ovat usein olleet 2-6 kk vanhoja haavoittuvuuksia, joihin on ollut saatavilla korjaus jo pitkään, mutta syystä tai toisesta haavoittuvuutta ei ole korjattu.
- Mitä pidempään haavoittuvuuden korjaamisessa kestää tai korjausta siirretään myöhemmäksi, sitä korkeammaksi hyväksikäyttämisen riski kasvaa.

CASE

Microsoft Exchange-sähköpostipalvelimiin julkaistiin helmikuussa 2020 kriittinen korjauspäivitys. Julkinen hyväksikäyttökeino oli saatavilla helmikuun loppuun mennessä. Maaliskuussa uutisoitiin useiden valtiollisten toimijoiden tekemistä hyökkäyksistä. Odotettavissa on, että haavoittuvuutta hyödynnetään seuraavaksi kiristyshaittaohjelmien levitykseen.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

2

Tietojenkalastelu 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.
- Typosquatting / domainsquatting liittyvät myös ilmiöön: kirjoitusvirheillä höystetyillä verkkotunnuksilla voidaan tehostaa huijauksen vaikuttavuutta.
- Henkilökunnan koulutuksella on suuri merkitys. Tutkimusten mukaan tietojenkalastelua opitaan tunnistamaan koulutuksen avulla ja tämä auttaa siihen, että tietojenkalastelu jää vain yritykseksi.

CASE

Vakavia laskutuspetoksia valikoituihin kohteisiin

Helmikuussa julkisten EU-kilpailutusten tietoja ja lakitoimistoihin tehtyjä tietomurtoja käytettiin laskutuspetoksiin. Petoksissa yritettiin huijata satoja tuhansia tai miljoonia euroja kerrallaan.

Kohteelle räätälöity sähköpostiviesti sisälsi oikeita tietoja, mutta vääriä tilinumeroita. Yksi huijaus paljastui vasta, kun oikea maksunsaaja otti yhteyttä maksajaan.

Lakitoimistojen ja Finanssivalvonnan nimissä on lähetetty huijausviestejä, joilla tähdätään satojen tuhansien eurojen laskutuspetoksiin.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

3

Laajavaikutteiset kiristyshyökkäykset (Big Game Hunting) uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

- Tapauksia myös Suomessa. Suurin osa organisaatioista valikoituu kohteeksi heikon tietoturvan seurauksena.
- Kyberrikolliset etsivät jatkuvasti verkosta haavoittuvia palveluita ja huonoja salasanoja. Jos rikolliset havaitsevat huonosti suojatun ympäristön kiristämisen arvoiseksi, siihen saatetaan kohdistaa Big Game Hunting –toimintaa.
- Uusia ilmoituksia laajoista kiristyshaittaohjelmatartunnoista tulee kansainvälisesti viikoittain. Lisäksi uusia toimijoita tulee jatkuvasti. Esimerkkinä tästä on ICS-toimijoihin kohdistuva EKANS.
- Kiristyshyökkäysten uutena ilmiönä uhataan julkaista hyökkääjän haltuun saamia tietoja lunnasvaatimuksen tehostamiseksi.

CASE

Norjassa Norsk Hydroon kohdennettu kiristyshaittaohjelma pääsi leviämään tuotantojärjestelmään asti. Toimintahäiriöt kestivät kuukausia ja koskettivat yrityksen useita eri toimipisteitä.

Norsk Hydro arvioi omilla sivuillaan kiristyshaittaohjelman kokonaiskustannukseksi noin kuusikymmentä miljoonaa euroa.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

4

Epäselvä vastuunjako palvelutoimittajan, alihankkijoiden ja tilaajan välillä heikentää tietoturvan hallintaa. Puutteet lokien tarkkailussa vaikeuttavat uhkien havaitsemista.

- Epäselvä vastuunjako ICT-palveluiden hankinnassa ja tuotannossa heikentää tietoturvan hallintaa. Tämä pätee myös organisaatioiden sisällä, jos tietoturvariskien omistajuus ja tietoturvavastuut eivät ole selkeästi määriteltyjä.
- Yleinen puute on jättää keräämättä ja tarkkailematta tietoturvalokeja. Lokien jatkuvan tarkkailun avulla tietojärjestelmän omistaja voi havaita lievät tietoturvaloukkaukset ja järjestelmän heikkoudet ennen kuin kukaan ehtii käyttää niitä suurempaan vahingontekoon. Lokeja tarvitaan myös loukkausten selvittämiseen jälkikäteen.
- Lisäksi käytöstä poistuvien palveluiden alasajo tulee tehdä huolella. Jos alasajotoimenpiteitä ei tehdä johdonmukaisesti loppuun asti, voi taustalle jäädä pyörimään käyttämättömiä palveluita, jotka voivat aiheuttaa merkittäviä tietoturvariskejä organisaatiolle.

CASE

Korona-aikana epäselvän vastuunjaon lisäksi nousee esille resurssien riittävyys sekä erilaisten varautumissuunnitelmien tärkeys. Pandemian aikana henkilöstöllä on keskeinen rooli, jotta toiminnot saadaan pidettyä yllä ja resurssien tulee olla riittävät kaikissa tilanteissa. Vaikutuksia saattaa olla myös tuotantoketjuissa, jolloin normaalisti saatava tuote jääkin tulematta ja tällä on vaikutuksia toimintaan.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

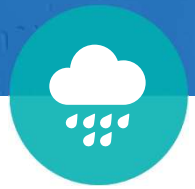
5

Organisaatiot eivät osaa hallita kyberriskejään. Uhkien vaikutuksia toimintaan ei osata ennakoida, minkä vuoksi riskit aliarvioidaan. Palautumissuunnitelmissa on puutteita.

- Tietoturvaloukkauksista toipumista ei usein suunnitella huolellisesti ennakkoon. Suunnitelmat ovat vain luokkaa "palautetaan tiedot varmuuskopioista". Palautumisen tärkeysjärjestyksiä, resursseja ja aikajänteitä ei mietitä ennakkoon.
- Häiriön iskiessä palautumisen monimutkaisuus ja työläys yllättävät. Jos palautuminen olisi suunniteltu ennakolta paremmin, myös varautuminen häiriöihin ja niiden ennaltaehkäisyyn olisi parempaa.
- Kyberturvallisuuskeskus on julkaissut yritysten hallituksille suunnatun kyberturvallisuutta käsittelevän oppaan. Kyberturvallisuus ja yrityksen hallituksen vastuu -opas antaa työkaluja ja tukea organisaation kyberturvallisuuden parantamiseen.
  - Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuus-ja-yrityksen-hallituksen-vastuu-opas

CASE

Organisaatioiden kyvyssä hallita kyberriskejään on selviä puutteita. Tyypillisesti organisaatiot eivät osaa ennalta arvioida kyberuhkien toteutumisen vaikutuksia niiden päivittäiseen toimintaan, tai arvioivat vaikutukset selvästi todellista lievemmiksi. Tämän seurauksena on, että kyberriskit aliarvioidaan eikä niiden hallintaan osoiteta riittävästi resursseja.



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

- Kyberturvallisuuskeskukseen ilmoitettujen Office 365 -tietomurtojen määrässä lievää laskua
  - Ilmoituksia Offfice 365 –tietomurtoja ilmoitetaan edelleen liki päivittäin, mutta määrässä on pitkän aikavälin arviona lievää laskua. Valitettavasti ilmiöstä on tullut ”uusi normaali”.
  - Kyberturvallisuuskeskus on julkaissut ohjeen Office 365 –ympäristön koventamisesta. Se on saatavilla suomen-, englannin- ja ensi viikosta alkaen myös ruotsinkielisenä.
  - Ohje löytyy osoitteesta: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/organisaatio-torju-office-365-tunnusten-kalastelu-oppaamme-avulla

ANALYYSI

- Tietomurron kohteeksi joutuminen voi aiheuttaa taloudellisten menetysten lisäksi myös merkittävän mainehaitan. Useissa tapauksissa murrettua sähköpostitiliä on käytetty uusien huijausviestien lähettämiseen.
- Monivaiheisella tunnistautumisella voitaisiin estää suurin osa tietomurroista.

Tietomurrot ja vuodot

- Maaliskuussa Suomessa ja ulkomailla kanta-asiakasjärjestelmiin kohdistui tietovuotoja
  - Tietovuodot ovat aiheuttaneet myös suomalaisten tietojen päätymisen vääriin käsiin. Tiedossa ei ole, että luottokortti- tai muita kriittisiä tietoja olisi vuodettujen tietojen joukossa.
  - Suomalaisen logistiikka-alan yrityksen kanta-asiakkaiden tunnuksia saatiin murrettua brute force –menetelmällä. Murroilla rikollinen sai haltuunsa kanta-asiakkaiden tietoja.
  - Suuri määrä kansainvälisen hotelliketjun asiakastietoja päätyi vääriin käsiin.

ANALYYSI

- Tietovuodoilla haltuun saatavat tiedot ovat verkkorikollisille kauppatavaraa, joita pyritään hyödyntämään taloudellisen hyödyn saamiseksi.
- Tietovuotojen vahinkojen minimoimiseksi on tärkeää käyttää eri verkkopalveluissa eri salasanaa. Lisäksi verkossa on olemassa palveluita, joilla tunnusten vuotamisen voi tarkastaa. Tarkastustyökalut ovat suuntaa antavia, eivät kaikki vuodot kattavia.

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

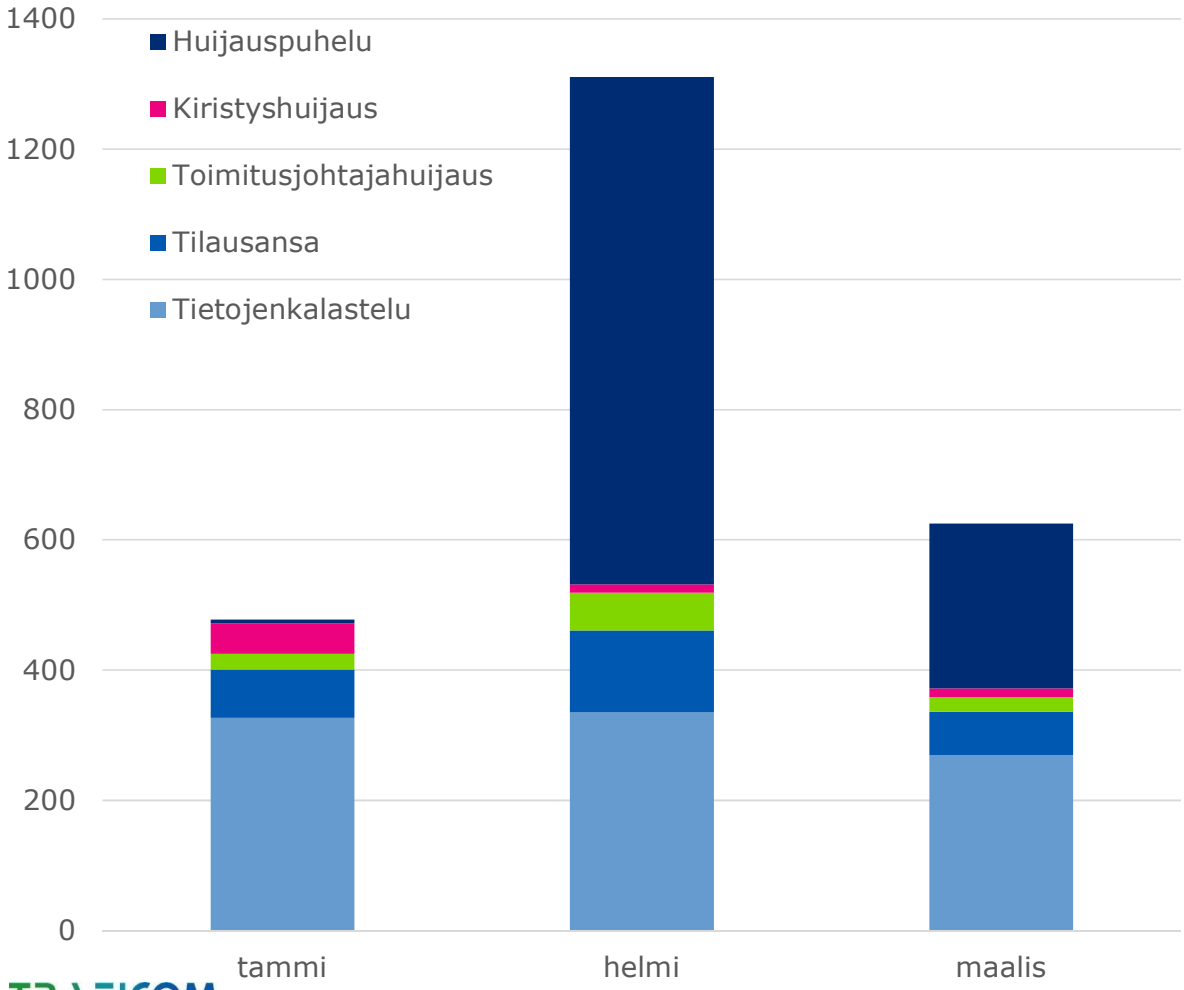
- Teknisen tuen huijaukset jatkuivat vielä maaliskuussa
  - Organisaatiolle ja yksityisille tulleet teknisen tuen huijaussoitot hiljenivät maaliskuun lopulla.
  - Huijarit halusivat etähallintayhteyden uhrin tietokoneeseen, minkä jälkeen uhrilta vietiin henkilötietoja, pankkitunnuksia, luottokorttitietoja jne.
- Valeuutisointia suomalaisten poliitikkojen nimissä
  - Intialainen huijaritoimittaja rekisteröi Valtioneuvoston nimeä muistuttavan verkkotunnuksen ja levitti sen avulla intialaiseen mediaan tekaistuja uutisia suomalaisten ministerien lausunnoista.

ANALYYSI

- Rikolliset kalastelevat tunnettujen pilvipalveluiden tunnuksia ja salasanoja huijausviesteillä. Huijausviestit tulevat useimmiten väärennetystä osoitteesta, kaapatulta tililtä, tekaistusta verkkotunnuksesta, tai muusta epäilyttävästä lähteestä. Viestissä oleva linkki johtaa kalastelusivulle. Tarkista aina, mihin olet syöttämässä tunnuksiasi, salasanojasi ja henkilötietojasi!
- Kaksivaiheisen tunnistautumisen koodeja yritetään myös kalastella mm. Whatsapp-viesteillä ja -puheluillla.

Tietojenkalastelu – yleisin yrityksiin osuva verkkorikos – Office365 huijauksen vaiheet:

Käsiteltyjä huijaustapauksia 2020



- Vuoden 2020 näkyvin trendi on ollut huijauspuhelut
  - Helpdesk-huijari yrittää saada uhrin tietokoneen haltuunsa ja varastaa siten tietoja ja rahaa.
  - Hälärihuijauksissa uhri yritetään saada soittamaan takaisin kalliiseen ulkomaan numeroon tai satelliittipalveluun.
- Kiristyshuijaukset ovat sähköposteja, joissa huijari uhkailee jollain, tai väittää saaneensa uhrin koneen haltuunsa ja vaatii lunnaita.
- Toimitusjohtajahuijaukset kohdistuvat yrityksiin ja organisaatioihin. Väärennetyt viestit tähtäävät laskutuspetokseen.
- Tilausansoja suunnataan kaikille kuluttajille esiintyen mm. Postin, Gigantin, tai muiden tuotemerkkien nimissä. Useimmat tekstiviestihuijaukset johtavat tilausansaan.
- Tietojenkalastelut ovat tavallisin tapa murtautua yrityksen verkkoon: kalastellaan tunnuksia ja salasanoja, joilla järjestelmiin pääsee.

Tilasto päivitetään kvartaaleittain

Haittaohjelmat ja haavoittuvuudet

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

Haittaohjelmat ja haavoittuvuudet

- Sähköpostitse levitetään eri teemoilla haittaohjelmia
  - Useat rikollisryhmät ovat ottaneet COVID-19 –teeman käyttöön haitallisissa viesteissään.
- Lähettämiseen käytetään murrettuja tilejä tai väärennettyjä lähettäjätietoja
  - Maaliskuussa nähty mm. Airbusin nimissä levitettyjä viestejä, jossa linkkejä haitallisiin tiedostoihin.
- TTN! Korona-aiheisia huijauksia on liikkeellä - mieti mitä klikkaat https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/korona-aiheisia-huijauksia-liikkeella-mieti-mita-klikkaat

ANALYYSI

- Haitallisten tiedostojen levittämiseen käytetään ajankohtaisia teemoja, koska ne ovat tehokkaita.
- COVID-19 teemalla on julkaistu paljon haitallista sisältöä levittäviä sivustoja. Näistä esimerkkinä on havainnot useista Johns Hopkinsin yliopiston COVID-19 levinneisyyskarttaa matkivista sivuista.

Haittaohjelmat ja haavoittuvuudet

- Laitteiden internetiin avoimet etäyhteyspalvelut altistavat organisaatiot tietomurroille.
  - Yritysten tulisi arvioida etätyön mahdollistavat ratkaisut tietoturvan näkökulmasta. Huolehdi, ettei etätyöjärjestelyt vaaranna yrityksen tietoturvaa.
  - Ylimääräinen, ei töihin liittyvä liikenne, pois yritysverkoista
  - Poikkeusratkaisut muistettava purkaa normaalioloihin palattaessa

ANALYYSI

- Kyberturvallisuuskeskus havainnut merkittävää kasvua internetiin avointen palveluiden määrässä.
  - Avoimien etäyhteyspalvelujen, kuten esimerkiksi avoimien etätyöpöytäyhteyksien ja tiedostonjakopalvelujen (esim. RDP, VNC ja SMB), määrä on kasvanut maaliskuussa neljänneksen verrattuna tammi-helmikuuhun.
- Lisätietoa ja ohjeita: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suojattomien-etatyopoyta-ja-verkkoyhteyspalveluiden-maara-kasvoi-maaliskuussa

Haittaohjelmat ja haavoittuvuudet

- Kriittinen haavoittuvuus Microsoftin verkkolevyprotokollassa (SMBv3) (Haavoittuvuus 7/2020)
  - Mahdollisesti haavoittuvia palveluita avattu etätyötarpeiden vuoksi lisää internetiin.
- Windows-työasemissa havaittu Adoben type manager haavoittuvuus (sandbox w10). Päivitystä ei ole julkaistu. Saatavilla ohjeita hyökkäyksen estämiseksi. (Haavoittuvuus 8/2020)

ANALYYSI

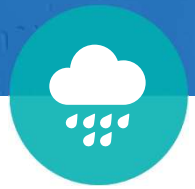
- Vanhat Windows-versiot eivät välttämättä saa enää päivityksiä kriittisiinkään haavoittuvuuksiin.
- Adoben haavoittuvuutta käytetty myös kohdistetuissa hyökkäyksissä.
- Lisätietoja SMBv3: https://www.kyberturvallisuuskeskus.fi/fi/kriittinen-haavoittuvuus-microsoftin-smbv3-toteutuksessa
- Lisätietoja Adobe: https://www.kyberturvallisuuskeskus.fi/fi/korjaamaton-haavoittuvuus-ms-windows-adobe-type-manager-fonttikirjastossa

Haittaohjelmat ja haavoittuvuudet

- HPE julkaisi tiettyjä SSD-levyjä koskevan haavoittuvuuden (Haavoittuvuus 9/2020)
  - Ohjelmistovirhe aiheuttaa tiettyjen levyjen rikkoontumisen 40 000 käyttötunnin jälkeen.
  - Ohjelmistovirheeseen on olemassa korjaava päivitys.

ANALYYSI

- Suosittelemme päivityksen välitöntä asentamista. Päivittämättömiä levyjä alkaa rikkoutua lokakuusta 2020 lähtien.
- Lisätietoja haavoittuvuustiedotteessa: https://www.kyberturvallisuuskeskus.fi/fi/kriittisia-ohjelmointivirheita-loydetty-ja-korjattu-hpen-ssd-levyjen-laiteohjelmistoista
- Voit lisäksi tilata KTK:n eri tilannekuvatuotteet, kuten haavoittuvuustiedoteet, itsellesi https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen



Automaatio

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

- Suojaamattomien, internetiin avointen etäyhteyspalveluiden määrä on ollut myös automaatioverkkojen osalta kasvussa.
- Automaatiolaitteiden useista kriittisistä haavoittuvuuksista esimerkkinä Moxan teollisuuskäyttöön tarkoitetussa langattomassa tukiasemassa oleva haavoittuvuus. (icsa-20-063-04)
- Lisätietoa, Shodan: https://blog.shodan.io/trends-in-internet-exposure/
  - Shodan käy läpi koko internetin IP-avaruuden päivittäin ja saatuja hakutuloksia on mahdollista selata palvelun avulla. Shodan näyttää tietoja kohteesta.

ANALYYSI

- Etähallintayhteyksien avaaminen tulee tehdä huolellisen riskiarvion pohjalta
- Tilapäisratkaisut muistettava purkaa normaalioloihin palattaessa

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

- Yleisissä viestintäpalveluissa maaliskuussa neljä merkittävää häiriötä
  - Käyttäjävaikutuksiltaan kaikkein merkittävimmiltä häiriöiltä kuitenkin vältyttiin.
  - Poikkeusoloista huolimatta häiriöt kyettiin korjaamaan normaalisti kohtuullisessa ajassa.
  - Kolme häiriöistä kohdistui matkaviestinverkon palveluihin, ja yksi kiinteään verkkoon.

ANALYYSI

- Toimivuushäiriö osuu melko harvoin yksittäisen käyttäjän kohdalle. Tällaisen tilanteen tullessa kohdalle käyttäjä voi ottaa mahdolliset ennalta valmistelemansa viestinnän varakeinot käyttöön tai sietää tilannetta, kunnes teleyritys saa häiriön poistettua.
- Kannattaa arvioida ennakolta, miten pitkiä viestintäpalveluiden katkoja organisaation keskeiset toiminnot sietävät.
- Häiriöihin voi varautua mm. eri teleyrityksiltä hankituilla liittymillä. Huoltovarmuuskriittiset yritykset voivat käyttää VIRVEä.

Verkkojen toimivuus

- Useiden ICT- ja internetpalveluiden toimivuus ja kapasiteetti ovat olleet koetuksella etätyöskentelyn lisäännyttyä ympäri maailmaa koronaviruspandemian johdosta.
  - Suomessa Valtorin Kauko-VPN-palvelun kapasiteetti loppui kesken maaliskuun puolivälissä. https://www.is.fi/digitoday/tietoturva/art-2000006437777.html
  - Pilvipalveluiden käyttö kasvoi maaliskuussa maailmanlaajuisesti moninkertaiseksi, mikä on ajoittain heikentänyt niiden toimivuutta. https://azure.microsoft.com/en-au/blog/update-2-on-microsoft-cloud-services-continuity/

ANALYYSI

- Euroopassa yleisten viestintäpalveluiden kapasiteetti on riittänyt hyvin, mutta jotkin niiden kautta käytetyt sovellukset ovat olleet kovilla.
- Palveluntarjoajat ja käyttäjät ovat sopeutuneet tilanteeseen suhteellisen ketterästi. VPN-palveluiden käyttäjät voivat esimerkiksi harkita liikenteen jakamista päätelaitteista suoraan tiettyihin luotettuihin pilvipalveluihin.

Verkkojen toimivuus

- Yli miljoona Let’s Encrypt -palvelun myöntämää verkkosivuvarmennetta peruttiin 4.–5.3.
  - Let’s Encrypt käsitteli varmenteiden allekirjoituspyyntöjä väärin, mikä loi väärinkäytösten mahdollisuuden.
  - Let’s Encrypt perui varmenteita, joita se oli allekirjoittanut väärän käsittelyn perusteella. Peruminen saattoi aiheuttaa joidenkin verkkosivustojen toimimattomuutta.
  - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/lets-encrypt-perui-tietyt-verkkosivujen-varmenteet-4-532020

ANALYYSI

- Varmenteiden käsittelyssä voi tapahtua virheitä kelle tahansa käyttäjälle tai myöntäjälle.
- Varmenteiden käyttäjien kannattaa varautua siihen, että sen internetpalveluissaan käyttämät varmenteet voivat muuttua epäkelvoiksi lyhyellä varoitusajalla. Oleellista on seurata varmenteiden myöntäjien tiedotteita ja dokumentoida oma varmenteiden käsittelyprosessi huolellisesti.

Palvelunestohyökkäykset

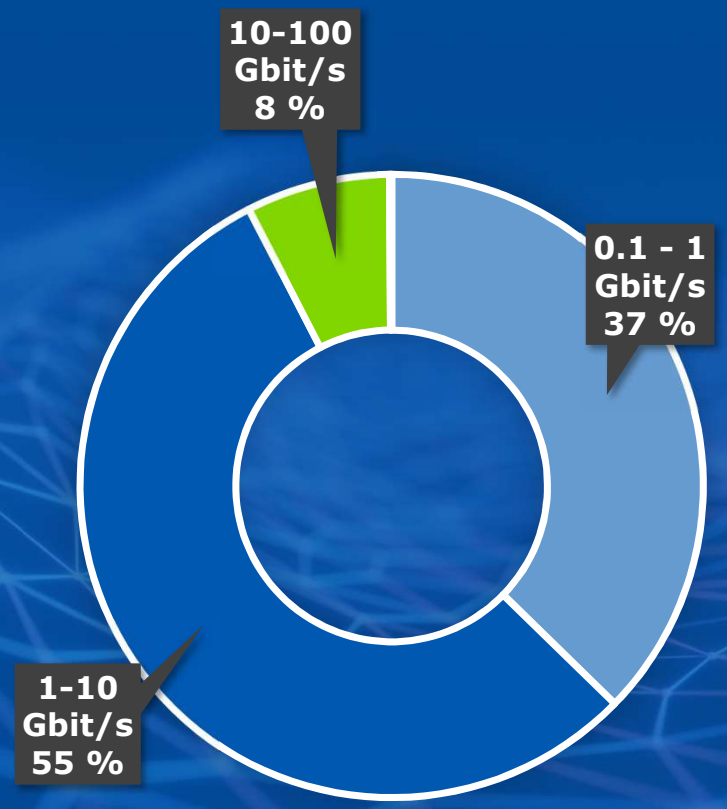
- Maaliskuussa nähtiin kirjava joukko palvelunestohyökkäyksiä eri toimijoita kohtaan.
  - Hyökkäyksillä ei yhtenäistä tekotapaa tai kohderyhmää. Osalla hyökkäyksistä oli vaikutuksia myös organisaation sisäisten palveluiden kuten VPN:n ja Skypen toimivuuteen.
  - Korona ja etäkoulu nosti myös erään koulun ja kodin välisen viestintäkanavan palvelunestohyökkäysten kohteeksi
- Raportoiduissa hyökkäyksissä on käytetty vanhoja tuttuja TCP SYN- ja UDP-reflektiotekniikoita. UDP-puolella mm. LDAP-, CLDAP- ja NTP-palvelimet ovat suosittuja vahvistuksen lähteitä.

ANALYYSI

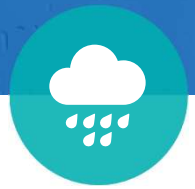
- Koronan seurauksena vallitsevissa poikkeusoloissa tehdään paljon etätöitä, jolloin esimerkiksi VPN-palvelun toimivuus on kriittistä. Osa tässä kuussa nähdyistä palvelunestohyökkäyksistä on sivuvaikutuksena vaikuttanut myös etäyhteyksien toimintaan kuormittamalla yhteisiä verkkokomponentteja.
- Jos organisaatio on etukäteen varautunut hyökkäyksiin, palvelunestohyökkäyksillä ei tyypillisesti ole vaikutuksia palveluiden toimivuuteen.

Palvelunestohyökkäysten tunnuslukuja

- 161 Gbit/s suurin Suomessa nähty palvelunestohyökkäys vuonna 2020
- Noin 80 % hyökkäyksistä on pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja



SUOMEEN KOHDISTUNEIDEN PALVELUNESTO-HYÖKKÄYSTEN VOLYYMIT (Q1/2020)



Vakoilu

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

Vakoilu

- Myös valtiolliset tahot hyödyntävät koronavirus- ja COVID-19-aiheita tietomurtojen valmistelussa ja toteuttamisessa.
  - Ulkomailla valtiollisiin toimijoihin liitetyissä kampanjoissa koronavirusteemalla on mm. kalasteltu käyttäjätunnuksia ja salasanoja ja jaettu haittaohjelmia.
  - Ainakin Kiinaan, Pohjois-Koreaan ja Venäjään liitettyjen ryhmien on uutisoitu hyödyntäneen koronavirusteemaa tavalla tai toisella.

ANALYYSI

- Organisaatioiden on hyvä ohjeistaa työntekijöitään erityiseen tarkkaavaisuuteen tilanteissa, joissa vastaanotetaan materiaalia tai viestejä uuteen, runsaasti huomiota herättävään aiheeseen liittyen.
- Ilmiö itsessään ei ole uusi, vaan kertoo pikemminkin siitä, että sekä kybervakoilussa että -rikollisuudessa hyökkäyksiä tehostetaan ajankohtaisilla ja kiinnostavilla teemoilla harhauttamalla.

Vakoilu

- Myös perinteiset menetelmät kybervakoilun toteuttamiseksi jatkuvat.
  - FireEye kertoi Kiinaan liitetyn APT41-ryhmän pyrkineen tunkeutumaan organisaatioiden VPN-ratkaisuihin alkuvuoden ajan. Kohteita etsittiin myös Suomesta: https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html
  - Useiden ryhmien kerrottiin myös pyrkineen hyödyntämään esimerkiksi Microsoft Exchange-sähköpostipalvelimen haavoittuvuutta.

ANALYYSI

- Haavoittuvia laitteita ja järjestelmiä etsitään verkosta aktiivisesti, ja niitä yritetään murtaa. Tämä pätee myös kybervakoiluun.
- Haavoittuvuuksien löytämisestä ja niiden hyödyntämisen alkamisen välisen aikaikkunan lyhentymisestä johtuen julkisesta internetistä saavutettavissa olevat järjestelmät pitäisi pystyä päivittämään mieluiten vuorokaudessa.

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.

Arjen kyberturvallisuus – melkoinen maaliskuu

Ohjeita etätyöhön

- Moni siirtyi maaliskuun aikana etätyön ja opiskelun pariin. Etätyöhän ja opiskeluun oli tarjolla erilaisia ohjeita. Myös Kyberturvallisuuskeskus antoi ohjeita etätyön tekemiseen
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vaarennettyja-puheluita-teknisen-tuen-nimissa

Korona-teemaa hyödynnetään myös huijauksissa

- Kyberturvallisuuskeskus on koonnut erilaisia huijausviestejä käsittelevän uutisen sivuilleen.
- Verkkohuijaukset ei ilmiönä ole uusi asia, mutta rikolliset pyrkivät hyödyntämään ajankohtaista teemaa huijauksissa
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/korona-aiheisia-huijauksia-liikkeella-mieti-mita-klikkaat

Spoofy-peli valittiin yleisön suosiksiksi vuoden 2020 parhaana digitaalisen oppimisratkaisun eEemeli-kilpailussa

- Spoofy on viihteellinen oppimispeli, joka tutustuttaa lapset kyberturvallisuuden sanastoihin ja ilmiöihin. Kyberturvallisuuskeskus oli mukana kehittämässä CGI:n toteuttamaa kyberpeliä.
- Pääset tutustumaan Spoofy-peliin https://spoofy.fi

Lasten ja nuorten turvallisuus verkossa on tärkeää

- Eri tahot ovat nostaneet lasten ja nuorten verkkoturvallisuuden esille, kun siellä vietetään nyt enemmän aikaa. Eri toimijat ovat koonneet tietoa ja materiaalia lasten verkkoturvallisuuteen liittyen. Keskusrikospoliisi on koonnut eri sivuja oman tiedotteensa yhteyteen.
- https://www.poliisi.fi/keskusrikospoliisi/tiedotteet/1/0/lasten_riski_joutua_seksuaalisen_hyvaksikayton_uhreiksi_verkossa_kasvaa_koronakriisin_aikana_89248

Ajankohtaista Kyberturvallisuuskeskuksesta

Poikkeusolo-sivustot yrityksille ja yksityishenkilöille

- Kyberturvallisuuskeskus kokosi yrityksille ja yksityishenkilöille omat sivustot, joihin on koottu ajankohtaisia uutisia ja ohjeita, joita saatetaan poikkeusolojen aikana tarvita.
- Sivujen tarkoituksena on helpottaa tiedon löytymistä ja niille päivitetään Kyberturvallisuuskeskuksen julkaisemat uutiset, jotka löytyy myös muista sivu-osioista.
- https://www.kyberturvallisuuskeskus.fi/fi/tukea-poikkeusolojen-tietoturvaan

Muista laitteiden, ohjelmistojen ja sovellusten päivittäminen!

- Hyökkäyksissä käytetyt haavoittuvuudet ovat usein olleet tiedossa jo useita kuukausia. Korjauksetkin ovat olleet saatavilla jo pitkään, mutta syystä tai toisesta haavoittuvuuksia ei ole korjattu. Vaarana on, että poikkeusaikoina päivitykset jäävät tekemättä entistä helpommin. Päivitysten tekemättä jättäminen tarjoaa rikollisille reitin järjestelmiisi ja tietoihisi.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/muista-laitteiden-ohjelmistojen-ja-sovellusten-paivittaminen

Valitse videoneuvotteluratkaisu käyttötarpeen ja tiedon luottamuksellisuuden mukaan

- Siirtyminen etäyhteyksien käyttöön on herättänyt myös keskustelun erilaisten videoneuvotteluyhteyksien käytöstä ja niiden tietoturvasta.
- Kokouksen järjestäjän kannattaa myös etukäteen huolehtia siitä, että kokoukseen voivat osallistua vain halutut henkilöt ja että videoneuvotteluun liittyvillä on vain tarvittavat käyttöoikeudet.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/valitse-videoneuvotteluratkaisu-kayttotarpeen-ja-tiedon-luottamuksellisuuden-mukaan

Korona-extra

Kyberturvallisuuskeskus on koonnut maaliskuun osalta myös erillisen korona-kybersään, jossa tehdään vielä erityisesti nostot korona-teemaan liittyen. Korona-kybersää julkaistaan osana kybersäätä, mutta se ei ole pysyvä osio.

Korona-Kybersää maaliskuu 2020

Tietomurrot ja -vuodot

- Mahdollisesti viivästyvät päivitykset altistavat tietomurroille ja vuodoille.
- Sosiaali- ja terveydenhuoltoala on maailmanlaajuisesti yksi rikollisten kohde, koska se on kriittinen toimija pandemian aikana

Huijaukset ja kalastelut

- KTK saanut toistaiseksi melko vähän ilmoituksia koronaa hyväksikäyttävistä huijauksista ja tietojenkalastelusta.
- Erilisia korona-teemaisia viestejä lähetetään sekä yksityishenkilöille roskapostina, mutta myös yrityksille

Haittaohjelmat ja haavoittuvuudet

- Maailmalla raportoitu kiristyshaittaohjelmia sairaaloissa ja laboratorioissa
- Myös muut yhteiskunnan kriittiset toimijat voivat olla kiinnostavia kohteita rikollisille

Automaatio

- Viivästyneet päivitykset ja muutostyöt voivat altistaa tietomurroille ja haittaohjelmien leviämiselle.
- Automaatiossa on myös huomioitava tarvittavan oman tai kumppaneiden henkilöstön saatavuus esim. asennusten tai päivitysten osalta.

Verkkojen toimivuus

- Vaikka kotona työskentely on lisääntynyt, Suomen viestintäverkoissa on tilaa verkkoasioinnille ja etätyölle.

Vakoilu

- Vakoiluun erikoistuneet tahot käyttävät myös koronateemaa hyökkäyksissään.
- Maailman terveysjärjestö WHO on ollut usean eri edistyneen kyberkampanjan kohteena.

Top 5 korona-kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Haavoittuvuuksia ei kyetä päivittämään tarpeeksi nopeasti, mikäli palvelutoimittajien tai organisaatioiden resurssitilanne heikentyy. KTK:n havaintona on ollut jo pidemmän aikaa että rikolliset hyväksikäyttävät haavoittuvuuksia entistä nopeammin.

2

Koronateemaa hyväksikäyttävä tietojenkalastelu ja huijaukset tulevat todennäköisesti lisääntymään ja saamaan uusia muotoja epidemian levitessä myös Suomessa. Henkilöstön ohjeistaminen on tärkeää uhan torjumiseksi.

3

Laajavaikutteiset kiristyshyökkäykset ovat merkittävä uhka, etenkin kriittisille toimijoille. Rikolliset todennäköisesti kokevat, että virusepidemia lisää organisaatioiden halua ja kykyä maksaa heille lunnaat.

4

Henkilöstövajetta saattaa ilmetä tulevien viikkojen aikana virustartuntojen lisääntyessä. Nyt tulisi viimeistään miettiä miten turvataan osaavan henkilöstön saatavuus – niin etätöissä kuin paikan päällä.

5

Palvelunestohyökkäykset. Ennestään vilkkaasti liikennöidyt internetsivut ovat helppoja kohteita rikollisille. Mikäli tietoa ei ole saatavilla virallisten lähteiden kautta, osa ihmisistä voi etsiä tietoa muualta internetistä tai sosiaalisesta mediasta, jolloin mahdollisuus langeta huijauksiin ja disinformaatioon voi kasvaa.

Mitä voi tehdä parantaakseen omaa kyberturvallisuutta

1

Pidä laitteet ajan tasalla ja päivitettynä. Tietokone tai muu laite yleensä muistuttaa saatavilla olevista päivityksistä työpöytäilmoituksella. Älä lykkää tarjottujen päivitysten asentamista.

2

Käytä eri salalauseita eri järjestelmissä. Työpaikan järjestelmiin ja käyttäjätileihin ei kannata käyttää samoja tunnuksia, joita käytät esimerkiksi verkkokauppaan tai vapaa-ajan sähköpostiisi kirjautuessasi.

3

Tarkista, mitä palveluita ja sovelluksia sinulla on käytössä. Jos et käytä sovellusta, voit hyvin poistaa sen. Huolehdi myös some-tiliesi yksityisyysasetuksista.

4

Käytä luotettuja ja suojattuja verkkoja. Jos käytät etätöissä langatonta lähiverkkoa eli WLANia tai WiFiä, katsothan että se on suojattu salasanalla. Vieraan verkon sijaan kannattaa käyttää esimerkiksi oman puhelimen verkkoyhteyttä. Etätyössä suosi Wlania, jotta puhelinverkko ei ruuhkaudu.

5

Ota varmuuskopiot. Välillä on hyvä siirtää laitteelta tietoja toiseen tallennuspaikkaan. Mikäli laite vioittuu, on tiedot tallessa ja palautettavissa. Näin esimerkiksi valokuvat säilyy, jos puhelin menee rikki.

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)