TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Helmikuu 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 helmikuu 2020

Tietomurrot ja -vuodot

- Ilmoitettujen Office 365 – tietomurtojen määrä kasvaa edelleen.
- Helmikuussa esille tullutta Exchange-palvelimen haavoittuvuutta käytetään hyväksi tietomurroissa.

Huijaukset ja kalastelut

- Suomalaisille soitettu satoja tuhansia teknisen tuen puhelinhuijauksia.
- Office 365 -tunnusten kalastelu jatkuu edelleen ja johtaa tietomurtoihin lähes päivittäin.

Haittaohjelmat ja haavoittuvuudet

- Kriittisten päivitysten laiminlyönti vaarantaa yritystoiminnan jatkuvuuden.
- Kannettavien tietokoneiden mobiiliyhteydet yritysten sokea piste?

Automaatio

- EKANS-kiristyshaittaohjelmaa havaittu maailmalla. Mahdollinen yhteys aiempaan MEGACORTEX-kiristyshaittaohjelmaan tunnistettu.

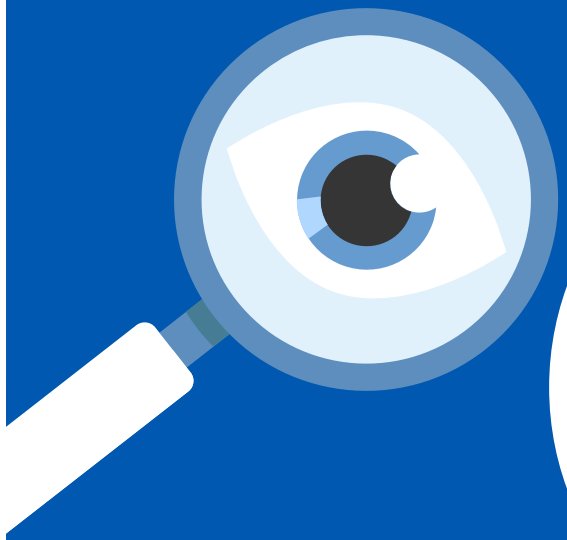
Verkkojen toimivuus

- Palvelunestohyökkäyksiä on raportoitu runsaasti, mutta niillä ei ole ollut merkittäviä vaikutuksia palveluiden toimintaan.
- Helmikuussa kuusi merkittävää toimivuushäiriötä.
- Laaja häiriö Microsoft Teamsissa; Microsoft unohti uusia varmenteen.

Vakoilu

- Lokienhallinta ei yleensä ole riittävällä tasolla tietomurtojen selvittämiseksi.

Kuukauden tunnuslukuja



83 %

ZSCALERIN TUTKIMUKSEN MUKAAN 83 % IOT-LAITTEISTA LÄHETTI DATAA SALAAMATTOMANA

VARJO-IOT:STA VOI TULLA YRITYKSELLE MERKITTÄVÄ RISKI

256 %

KASVUA TILANNEKESKUKSEN KÄSITTELEMISSÄ TAPAUKSISSA VERRATTUNA VUODEN 2019 HUIPPUUN

SUURIN KASVU AIHEUTUI PUHELINHUIJAUKSIEN HYÖKYAALLOSTA

yli 1 M€

YHTEISTYÖLLÄ JA TIEDONVAIHDOLLA ESTETTYJÄ LASKUTUSPETOKSIA

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.

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kaytosta-poistuvien-palveluiden-alasajo-tulee-tehda-huolella

OHJE

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

- Office 365 -tietomurtojen määrässä edelleen kasvua
  - Lukuisista varoituksista ja ohjeistuksesta huolimatta Office 365 –tietomurtojen määrässä ei näy laskua. Valitettavasti ilmiöstä on tullut ”uusi normaali”.
  - Kyberturvallisuuskeskus on julkaissut ohjeen Office 365 –ympäristön koventamisesta. Se on saatavilla suomen-, englannin- ja kohta 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

- Exchange-sähköpostipalvelimien haavoittuvuutta käytetään hyväksi tietomurroissa
  - Helmikuussa ilmi tullut haavoittuvuus mahdollistaa hyökkääjän oman koodin suorittamisen palvelimessa korotetuin oikeuksin, mikäli hyökkääjä on saanut haltuunsa yksittäisen sähköpostipalvelimen käyttäjän tunnukset.
  - Haavoittuvuuteen on olemassa korjaava päivitys.

ANALYYSI

- Microsoft korjasi sähköpostin Exchange-palvelimiin liittyvän haavoittuvuuden helmikuun päivityksissä.
- Haavoittuvuutta ryhdyttiin käyttämään hyväksi varsin laajamittaisesti muutama viikko haavoittuvuuden julkitulon jälkeen.
- Kansainvälisten arvioiden mukaan haavoittuvuutta ovat käyttäneet hyväksi myös valtioiden tukemat toimijat: https://threatpost.com/microsoft-exchange-server-flaw-exploited-in-apt-attacks/153527/

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 huijauksia väärennetyistä puhelinnumeroista
  - Organisaatiolle ja yksityisille on tullut tuhansittain englanninkielisiä puheluita, joissa huijari esiintyy teknisenä tukena. Huijarit haluavat etähallintayhteyden uhrin tietokoneeseen, minkä jälkeen uhrilta varastetaan henkilötietoja, pankkitunnuksia, luottokorttitietoja jne.
  - Puhelut tulevat väärennetyistä puhelinnumeroista, jotka viittaavat suomalaisiin matkapuhelin- tai telealuenumeroihin.
- Laskutuspetoksia Finanssivalvonnan ja lakiasiaintoimistojen nimissä
  - Väärennetyissä viesteissä yritetään suuria laskutuspetoksia suomalaisiin yrityksiin.

ANALYYSI

- Puhelinhuijausten määrä on helmikuussa lisääntynyt räjähdysmäisesti usean eri huijauskampanjan myötä. Lue lisää täältä: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vaarennettyja-puheluita-teknisen-tuen-nimissa
- Office 365 -tunnuksia kalastellaan edelleen paljon. Tunnusten kalastelu saattaa johtaa tietomurtoihin.

Tietojenkalastelu – yleisin yrityksiin osuva verkkorikos – Office365 huijauksen vaiheet:

Haittaohjelmat ja haavoittuvuudet

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

Haittaohjelmat ja haavoittuvuudet

- Julkiverkkoon avoimissa palveluissa olevia haavoittuvuuksia hyödynnetään aktiivisesti tietomurroissa haittaohjelmien levittämiseen ja Big Game Hunting -toimintaan
  - Helmikuussa oli merkittäviä haavoittuvuuksia esimerkiksi Tomcat-, Jboss- ja Exchange-tuotteissa.
  - Kyberturvallisuuskeskuksen tiedossa on tietomurtoja, joissa kannettavan tietokoneen 4G-yhteyden kautta on päästy yritysverkkoon. 4G-yhteyttä ei oltu suojattu käyttöjärjestelmän palomuurilla, joten RDP-palvelu oli 4G-yhteyden kautta avoinna julkiseen verkkoon.

ANALYYSI

- Huomioikaa 4G-yhteyksien asianmukainen suojaaminen mm. palomuurilla, ettei sitä kautta ole suoraa pääsyä yrityksen sisäverkkoon.
- Tomcat ja JBoss ovat yrityskäytössä yleisiä sovellusalustoja, jotka jäävät helposti päivittämättä, koska niiden olemassaoloa ei usein tiedosteta.
- Lisätietoja Tomcatista: https://www.kyberturvallisuuskeskus.fi/fi/vakava-haavoittuvuus-tomcat-sovellusalustassa-cve-2020-1938-ghostcat

Haittaohjelmat ja haavoittuvuudet

- Kyberturvallisuuskeskuksella on useita havaintoja kansainvälisestä haittaohjelman levityskampanjasta.
  - Levitetään laajamittaisesti suomenkielisten sähköpostien välityksellä.
  - Agent Teslalla pystytään esimerkiksi varastamaan salasanoja ja ottamaan yhteys uhrin laitteeseen.

ANALYYSI

- Agent Tesla on myynnissä oleva haittaohjelma, joka tarjoaa hyökkääjälle esimerkiksi etäyhteyden kohteeseen ja mahdollisuuden tietojen keräämiseen. Pelkästään haittaohjelman perusteella ei siis pysty tekemään tarkkoja päätelmiä hyökkääjän motiivista.
- Kyberturvallisuuskeskuksen havainnot haittaohjelmasta ovat yhteneviä kolmannen osapuolen tekemän artikkelin kanssa: https://blog.360totalsecurity.com/en/large-scale-phishing-attack-on-western-europe/

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

- EKANS-kiristyshaittaohjelma on kehitetty automaatioprosesseja ja -sovelluksia vastaan.
  - Teollisuusautomaation kriittisyyden vuoksi siihen kohdistetut uhat ovat vakavia.
  - EKANS-kiristyshaittaohjelman uskotaan olevan uudempi versio MEGACORTEX-kiristyshaittaohjelmasta.
  - Lue lisää: https://dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

ANALYYSI

- Kiristyshaittaohjelma voi vaikuttaa tuotantoon ja pahimmillaan lamauttaa sen. Vaikutukset voivat olla rahallisten menetysten lisäksi yhteiskunnallisesti huomattavia.
- Tieto omista järjestelmistä, sovelluksista ja prosesseista on hyvä olla ajan tasalla.
- Torjunta on perusperiaatteiltaan sama kuin muissakin haittaohjelmatapauksissa.

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 helmikuussa kuusi merkittävää häiriötä
  - Kukin häiriö vaikutti tyypillisesti muutaman kunnan alueella ja muutaman tunnin ajan yhden teleyrityksen matkaviestinpalveluihin kerrallaan. Myös yksi kiinteän verkon häiriö.
  - Yksi häiriö vaikutti 50 minuutin ajan Telian mobiiliviestintäpalveluihin koko Suomessa.

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

- Microsoftin Teams -palvelussa oli laajoja häiriöitä ympäri maailman 3.2.2020
  - Microsoft oli unohtunut uusia yhden palvelussa käytetyn varmenteen. Teamsin käyttäjät eivät voineet tehdä tilanteelle mitään.
  - Lue lisää: https://www.theverge.com/2020/2/3/21120248/microsoft-teams-down-outage-certificate-issue-status

ANALYYSI

- Pilvipalveluiden käytön helppouden kääntöpuoli on, että palvelun jatkuvuus ei ole käyttäjän hallinnassa. Käyttäjät voivat varautua häiriöihin vain järjestämällä itselleen vaihtoehtoisia viestintävälineitä.
- Katso myös Kyberturvallisuuskeskuksen ”Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille” https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohjeita_pilvipalvelujen_turvallisuudesta_123-2019.pdf

Palvelunestohyökkäykset

- Helmikuussa yhden toimialan useille eri organisaatioille on kohdistunut poikkeuksellisen paljon palvelunestohyökkäyksiä. Hyökkäysten taustalla olevista motiiveista ei ole tietoa.
- Muuten helmikuu on ollut kohtuullisen rauhallinen.
- Raportoiduissa hyökkäyksissä on käytetty vanhoja tuttuja TCP SYN- ja UDP-reflektiotekniikoita. UDP-puolella mm. LDAP-, CLDAP- ja NTP-palvelimet ovat suosittuja vahvistuksen lähteitä.

ANALYYSI

- Pahimmillaan yksittäiseen palveluun kohdistunut palvelunestohyökkäys voi sivuvaikutuksena esimerkiksi kaataa palomuurin tai muun verkkolaitteen ja siten estää myös yrityksen koko verkkoliikenteen.
- Jos organisaatio on etukäteen varautunut hyökkäyksiin, palvelunestohyökkäyksillä ei tyypillisesti ole vaikutuksia palveluiden toimivuuteen.
- Volymetristen hyökkäysten lisäksi kannattaa varautua myös sovellustason hyökkäyksiin.

Palvelunestohyökkäysten tunnuslukuja

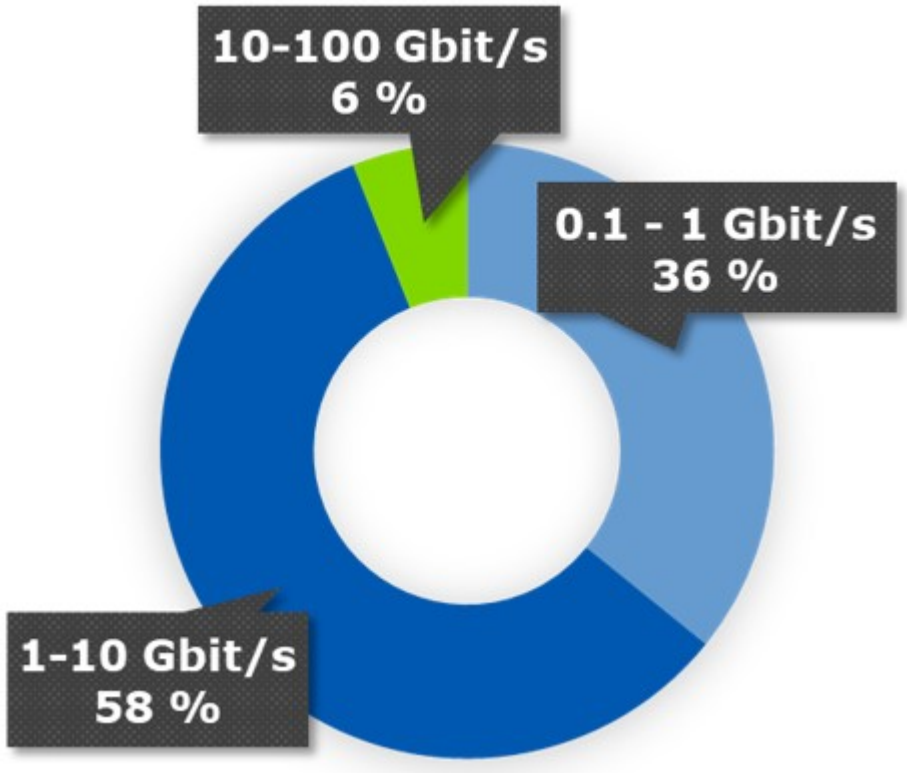
162 Gbit/s

VUONNA 2019 SUURIN SUOMESSA NÄHTY PALVELUNESTOHYÖKKÄYS

85 %

HYÖKKÄYKSISTÄ ON PITUUDELTAAN ALLE 15 MINUUTTIA.

VARAUTUMISESSA KANNATTAA ARVIOIDA LYHYENKIN PALVELUKATKOKSEN TOIMINNALLE MAHDOLLISESTI AIHEUTTAMIA HAITTOJA.



SUOMEEN KOHDISTUNEIDEN PALVELUNESTO-HYÖKKÄYSTEN VOLYYMIT (Q4/2019)

Tilasto päivitetään kvartaaleittain.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Vakoilu

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

Vakoilu

- Valtiolliseen kybervakoiluun liittyviä tapauksia tutkittaessa huomataan säännönmukaisesti, että lokienhallinta ei ole riittävällä tasolla.
  - Tehokkaan lokienhallinnan toteuttamiseksi organisaation on osoitettava siihen riittävät resurssit.
  - Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

ANALYYSI

- Koska tietomurto havaitaan tyypillisesti vasta viikkoja tai kuukausia myöhemmin, tutkinnan edellytyksenä on lokitietojen riittävän pitkäaikainen säilytys.
- Yleisimmin tarvittavat lokityypit ovat tietoliikenne- ja kirjautumislokit, esimerkiksi välityspalvelimen lokit sekä etäkäyttöpalvelujen, työasemien ja palvelinten kirjautumislokit.

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

- Hallitus on 13.2.2020 antanut eduskunnalle esityksen (HE 8/2020) laeiksi ydinenergialain, turvallisuusselvityslain 21 §:n ja kaivoslain muuttamisesta.

- Esityksessä muillekin kuin viranomaisille annettaisiin mahdollisuus puuttua miehittämättömien ilma-alusten (drone) kulkuun.
- Ydinenergialakiin ehdotetaan muutosta, jonka perusteella ydinvoimalaitoksen turvahenkilöllä on ydin- tai säteilyturvallisuuden turvaamiseksi oikeus ottaa miehittämätön ilma-alus teknistä laitetta tai voimakeinoa käyttäen tilapäisesti haltuun, estää sen käyttö tai muutoin puuttua sen kulkuun, jos miehittämätön ilma-alus saapuu oikeudetta luvanhaltijan pysyvässä olevalle alueelle.
- Aikaisemmin samankaltaisista oikeuksista on säädetty poliisille, puolustusvoimille, Rajavartiolaitokselle ja Rikosseuraamuslaitokselle.
- Linkki eduskunnan sivuille: https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_8+2020.aspx

Oikeudelliset asiat

- Apulaistietosuojavaltuutettu on 20.2.2020 antanut päätöksen, jonka mukaan puheluiden tallentamisesta on ilmoitettava asiakkaille ennen nauhoittamisen aloittamista ja rekisteröidyllä on oikeus saada puhelutallenteet.

- Viestinnän osapuolella on sähköisen viestinnän palveluista annetun lain 136 §:n perusteella mahdollista tallentaa puhelut. Viestinnän osapuolella tarkoitetaan viestin lähettäjää ja sitä, jolle viesti on tarkoitettu. Osapuolia ovat esimerkiksi luonnolliset henkilöt, yritykset ja työnantajat.
- Asiassa on lisäksi kyse myös henkilötietojen käsittelystä, jolloin asiakkaille on ilmoitettava asiasta ennen nauhoittamisen aloittamista ja rekisteröidyllä on oikeus saada puhelutallenteet.
- Linkki tietosuojavaltuutetun tiedotteeseen: https://tietosuoja.fi/artikkeli/-/asset_publisher/apulaistietosuojavaltuutettu-puheluiden-tallentamisesta-on-ilmoitettava-asiakkaille-ennen-nauhoittamisen-aloittamista

Arjen kyberturvallisuus – huijausten helmikuu

Väärennettyjä puheluita teknisen tuen nimissä

- Huijari soittaa uhrille ja esiintyy Microsoftin teknisenä tukena. Puhelussa pyydetään tekemään tietokoneelle päivitys, asentamaan etäkäyttöohjelma tai antamaan henkilötodistuksen tai maksuvälineen tietoja.
- Puhelut näyttivät tulevan suomalaisesta puhelinnumerosta, mutta huijarit puhuivat usein englantia.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vaarennettyja-puheluita-teknisen-tuen-nimissa

Varo hälärihuijauksia oudoista ulkomaan numeroista

- Puhelin soi kerran tai pari ja sen jälkeen puhelu katkeaa. Soittajan tarkoituksena on saada uhri soittamaan takaisin ulkomaiseen tai satelliittipalveluntarjoajan numeroon, johon soittaminen maksaa kymmeniä euroja minuutilta.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/varo-halarihuijauksia-oudoista-ulkomaan-numeroista

Näin suojaudut nettihuijaukselta

- Verkon huijarit houkuttelevat sinulta rahaa tai henkilötietoja. Älä usko epämääräisiin sijoitusmainoksiin. Huijausviestejä satelee sähköpostitse, tekstiviestitse ja puhelimitse useilla eri teemoilla.
- Maltti on valttia ja kiirettä klikata linkkejä tai aukaista liitetiedostoja on syytä välttää. Varmista miksi kyseinen taho sinua lähestyy.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-nettihuijaukselta

Netiketti - Verkossa liikkujan työkalupakki

- Annamme vinkkejä ja perusohjeistusta, kuinka voit toimia turvallisesti ja vastuullisesti netissä. Voit käyttää neuvojamme myös muistilistana. Pidä huolta fiksusta verkkojäljestäsi ja -identiteetistäsi, muista lähdekritiikki ja päivitykset. Näillä periaatteilla olet jo hyvällä tietoturvapolulla.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/netiketti-verkossa-liikkujan-tyokalupakki

Uutisia Kyberturvallisuuskeskuksesta

Tietoturvan vuosi 2019 sisälsi iloa, murhetta ja muutoksia

- Vuosi 2019 sisälsi useita tietoturva-alan positiivisia saavutuksia ja mielenkiintoisia ilmiöitä.
- Järjestämämme 5G ja Galileo -hakkeritapahtumat saivat kansainvälistäkin huomiota.
- Harjoitusoppaamme antoi organisaatioille eväitä kyberharjoitteluun ja Tietoturvamerkki kuluttajille mahdollisuuden fiksuihin älylaitehankintoihin.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvan-vuosi-2019-sisalsi-iloa-murhetta-ja-muutoksia

Mediataitoviikolla huomio lasten ja vanhempien tietoturvataitoihin

- Mediataitoviikko (10.-16.2.2020) on mediakasvatuksen teemaviikko, jonka tavoitteena on kehittää lasten ja nuorten mediataitoja sekä vahvistaa aikuisten valmiuksia mediakasvatukseen.
- Tietoturvaosaaminen on nykyarkemme kansalaistaitoja. Tietojen ja taitojen omaksuminen alkaa älylaitteen ensikosketuksesta, ja kehitys jatkuu läpi elämän.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/mediataitoviikolla-huomio-lasten-ja-vanhempien-tietoturvataitoihin

Valtion kyberturvallisuus-johtajaksi valittu Rauli Paananen

- Paananen siirtyy tehtävään Kyberturvallisuuskeskuksen poikkeamienhallintaosaston johtajan työstä.
- Paananen aloittaa tehtävässä huhtikuun alussa. Ensimmäisenä hän alkaa valmistella kyberturvallisuuden kehittämisohjelmaa.
- Kolme vuotta sitten valtioneuvoston kanslian raportissa arvioitiin, että Suomi ei ole edelläkävijä kyberuhkiin varautumisessa, mutta yltää silti varsin hyvään joukkoon.
  - Ihan kärkeen ei ylletty, mutta kärkijoukossa ollaan edelleen, Paananen arvioi.
- https://yle.fi/uutiset/3-11230455

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)