TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Lokakuu 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 lokakuu 2020

Tietomurrot ja -vuodot

- Office 365 –tapauksista edelleen ilmoituksia
- Psykoterapiakeskus Vastaamoa ja sen asiakkaita kiristettiin tietovuodon uhalla. Potilas- sekä henkilötietoja vuodettiin
- https://tietovuotoapu.fi –sivustolle on koottu neuvoja.

Huijaukset ja kalastelut

- Office 365 -tunnuksia on kalasteltu erittäin uskottavilla Zoom-kokouskutsuilla.
- COVID19-teema on palannut pornokiristyksiin, lahjoitushuijauksiin, nigerialaiskirjeisiin ja monenlaisiin tietojenkalastelukampanjoihin.

Haittaohjelmat ja haavoittuvuudet

- Kiristyshaittaohjelmia on kohdennettu terveydenhuoltosektoriin
- Postin nimissä levitetään Android-haittaohjelmaa

Automaatio ja IoT

- Nokian julkaisemassa uhkaraportissa kolmasosa kaikista haittaohjelmahavainnoista kohdistui IoT-laitteisiin.
- Osuus nousi vuoden takaisesta 17 prosenttiyksiköllä, mikä kertoo IoT-laitteiden heikosta tietoturvatasosta ja määrän lisääntymisestä.

Verkkojen toimivuus

- Vain kolme merkittävää häiriötä kotimaisissa viestintäpalveluissa
- Microsoftin ja Slackin palveluissa maailmanlaajuisia häiriöitä
- Kyberturvallisuuskeskus sai ilmoituksia palvelunestohyökkäyksistä, joilla oli myös laajoja vaikutuksia palveluiden toimintaan.

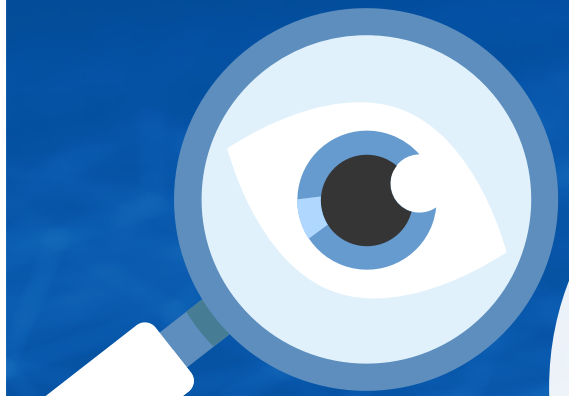
Vakoilu

- Norja syyttää Venäjää maansa parlamenttiin aiemmin syksyllä kohdistuneesta kyberhyökkäyksestä.
- Suojelupoliisin mukaan koronaviruspandemia on kasvattanut kybervakoilun roolia suhteessa muuhun vakoiluun. Supon mukaan Suomi on erityisesti Venäjän ja Kiinan kiinnostuksenkohteena.

Varoitus 1/2020 Emotet-haittaohjelmaa levitetään aktiivisesti Suomessa

- Elokuussa 2020 julkaistu Emotet varoitus on edelleen voimassa
- Haittaohjelmaa levitetään sähköpostitse suomalaisten organisaatioiden nimissä.
- Keltainen varoituksemme kertoo tilanteesta, jossa käyttäjien ja ylläpitäjien on noudatettava yleistä varovaisuutta tai valmistauduttava mahdollisiin korjaaviin toimiin.
- Lue koko varoitus: https://www.kyberturvallisuuskeskus.fi/fi/emotet-haittaohjelmaa-levitetaan-aktiivisesti-suomessa

Kuukauden tunnuslukuja



31

LOKAKUUSSA VIETETTIIN KYBERTURVALLISUUSKUUKAUTTA. ERI ORGANISAATIOT TOIVATKIN USEANA PÄIVÄNÄ ERILAISIA NEUVOJA JA VINKKEJÄ, JOILLA TIETOTURVAA VOI PARANTAA.

~25 000

RIKOSILMOITUSTA POLIISILLE TÄHÄN MENNESSÄ KOSKIEN PSYKOTERAPIAKESKUKSEN TIETOMURTOA. TAPAUS KOSKETTI NOIN 40 000 YKSILÖÄ. VIRANOMAISET, YKSITYINEN SEKTORI JA JÄRJESTÖT OVAT TYÖSKENNELLEET YHDESSÄ. UHRIEN AUTTAMISEKSI

1

LOKAKUUSSA JULKISTETTIIN JÄLLEEN UUSI TIETOTURVAMERKKI. KULUTTAJALLE TIETOTURVAMERKKI ON TAE SIITÄ, ETTÄ TUOTTEESEEN JA PALVELUUN LIITTYVIIN TIETOTURVA-ASIOIHIN ON KIINNITETTY HUOMIOTA

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

Universal Health Services (UHS) sairaalaketjuun kohdistui syyskuussa kiristyshaittaohjelmahyökkäys. Raporttien mukaan haittaohjelma käynnistyi viikonlopun aikana ja sen vaikutukset kestivät noin viikon ajan. Tuona aikana hoitolaitokset ovat raportoidusti toimineet ilman sisäisiä IT-järjestelmiään. Lisäksi raportoitiin, että joitain potilaita on käännytetty pois taikka ohjattu toisiin sairaaloihin. UHS on varmistanut, että kiristyshaittaohjelmalla oli vaikutuksia kaikkiin heidän Yhdysvalloissa oleviin hoitolaitoksiinsa. UHS:lla on yhteensä 400 hoitolaitosta Yhdysvalloissa ja Iso-Britanniassa.

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

Windowsiin kohdistuva Zerologon-haavoittuvuus ja sen korjaava päivitys julkaistiin elokuussa 2020. Hyväksikäyttömenetelmä tuli syyskuussa julki ja aktiivista hyväksikäyttöä havaittiin nopeasti. Mikäli haavaa ei viipymättä päivitetty heti elokuussa, hyökkääjälle mahdollistui käyttöoikeuksien laajentaminen ja toimialueen ohjauskoneen (domain controller) murtaminen ilman mitään tunnuksia.

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

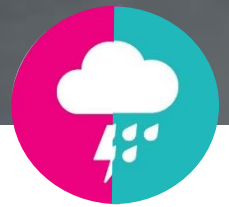
Lokitietojen puutteellisuus on riski monessa organisaatiossa.
Poikkeamatilanteita ei kyetä havainnoimaan ja selvittämään mikäli oikeiden järjestelmien tai sovellusten lokitietoja
ei kerätä, seurata ja säilytetä riittävän kauan.

- 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

- Suomalaisen psykoterapiakeskuksen tietovuototapaus
  - Yritystä ja sen asiakkaita kiristettiin tietovuodon uhalla, potilastietoja myös julkaistiin
    - 40 000 henkilön tiedot vaarantuneet, 300 henkilön tiedot julkaistu kiristäjän toimesta
    - 25 000 tehtyä rikosilmoitusta ja ~800 ilmoitusta Kyberturvallisuuskeskukselle
  - Kyberturvallisuuskeskus tarjoaa apua kiristyksen ja tietovuodon uhreille
    - Laajan yhteistyön tuloksena koottu https://tietovuotoapu.fi/ -sivusto, jossa toimintaohjeet ja neuvot ovat samassa paikassa

ANALYYSI

- Vastaamon-tapaus toi yhteen viranomaisia ja toimijoita eri sektoreilta tarjoamaan apua kansalaisille. Tämän tapauksen hoitamisessa laaja yhteistyö osoittautui hyvin tuottoisaksi.
- Suomessa poikkeuksellinen tapaus sai laajaa mediahuomiota
- Omaa ympäristöä sekä siellä olevia tietoja tulee ymmärtää ja suojata asianmukaisesti
- Organisaation on syytä varautua myös tietovuodolla kiristämiseen ainakin valmiiden toimenpiteiden ja viestintäsuunnitelman osalta

Tietomurrot ja –vuodot

- Saamme edelleen paljon ilmoituksia Office 365-tietomurroista
  - Ilmoituksia onnistuneista tietomurroista ja niiden yrityksistä tulee tasaisella tahdilla

ANALYYSI

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

Tietojenkalastelu – yleisin yrityksiin osuva verkkorikos Office365 huijauksen vaiheet:

Huijaukset ja kalastelut

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

Huijaukset ja kalastelut

- Lokakuu on ollut vilkas kaikilla huijausrintamilla. Erityisesti Netflix-tunnuksia on kalasteltu kömpelöillä huijausviesteillä. Myös pankkitunnuksia, LinkedIn-, Steam- ja Paypal-tunnuksia kalastellaan paljon.
- Posti-teemaiset tekstiviestihuijaukset ovat jatkuneet sitkeästi lokakuussa. Huijausviestien linkit johtavat tilausansoihin, mutta linkkien takaa tarjoillaan myös Apple ID -kalastelua ja Android-haittaohjelmaa.
  - Haittaohjelma lähettää tuhansia tekstiviestejä ulkomaille, mistä aiheutuu liittymälle iso lasku.
  - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/saitko-tekstiviestin-postin-nimissa-varothan-viesti-voi-olla-huijaus

ANALYYSI

- Kyberturvallisuuskeskukselle ilmoitettiin lokakuussa kymmeniä toimitusjohtajahuijausten yrityksiä, mutta onneksi niistä ei yksikään johtanut menetyksiin. Huijausyrityksissä kokeiltiin monia erilaisia teemoja, kuten lahjakorttien maksamista tai palkkatilin vaihtamista huijarin tiliksi.
- COVID19-teema näkyi lokakuussa monenlaisissa huijauksissa.
  - Pornokiristäjä pyytää anteeksi kiristystään, mutta poikkeustilanteen vuoksi hänen täytyy turvautua tällaiseen.
  - Poikkeustilan varjolla on sekä uhkailtu palkan leikkauksella että luvattu avuksi lisää rahaa, mutta oikeasti vain kalasteltu käyttäjätunnuksia.

Teknisen tuen nimissä soittelu jatkuu

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

ANALYYSI

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

Ammattirikolliset kalastelevat tietoja

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

ANALYYSI

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

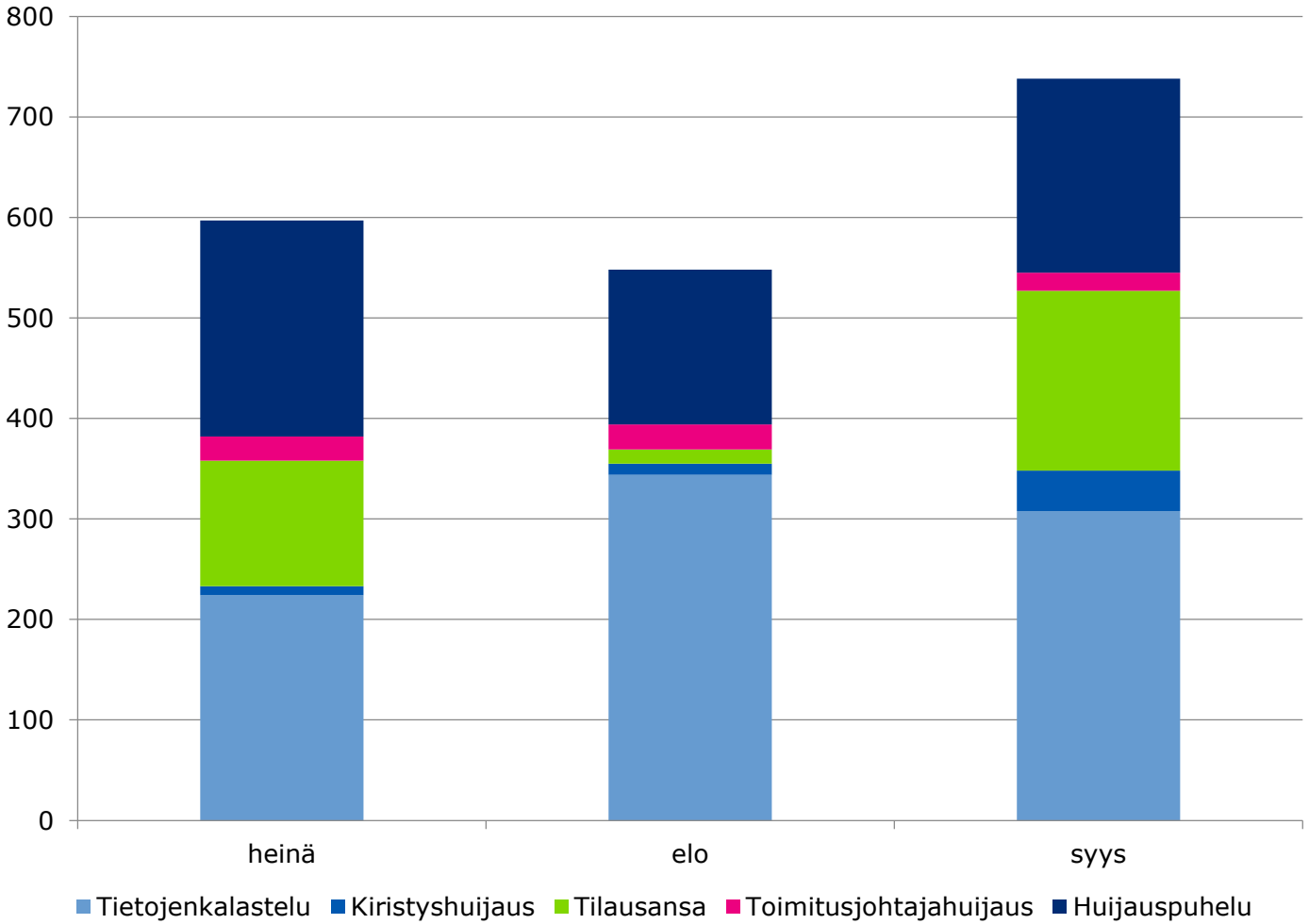
Office 365 -tietojenkalastelu

- Office 365 -tietojenkalastelu on edelleen yleistä. Kalasteluaalto rauhoittui hetkeksi, mutta on jälleen aktivoitunut loka-marraskuussa 2020.
- Lokakuussa 2020 alkoi laadukas Office 365 -tunnuksien kalastelu hyvin uskottavilla väärennetyillä Zoom-kokouskutsuilla. Kansainvälisen kalastelukampanjan uhriksi jäi kymmeniä suomalaisiakin kohteita.
- Jossain tapauksessa tietomurto ja sähköpostin vakoilu on voinut jatkua kuukausia ilman että uhri huomaa sitä.

ANALYYSI

- Mikäli yritys on joutunut onnistuneen kalastelun kohteeksi, tulisi sillä olla keinot jäljittää tapausta.
- Uusimissa 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 siis olet joutunut tietojenkalastelun uhriksi, tee siitä ilmoitus myös Kyberturvallisuuskeskukselle.**

Käsiteltyjä huijaustapauksia Q3/2020



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

Haittaohjelmat ja haavoittuvuudet

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

Haavoittuvuudet ja haittaohjelmat

- Kiristyshaittaohjelmat aiheuttavat harmia Suomessakin
  - Yhdysvalloissa terveydenhuoltosektorilla on ollut paljon Trickbot ja Ryuk –haittaohjelmahavaintoja
    - Seuraukset toiminnan keskeytyksestä ovat terveydenhuoltosektorilla erityisen vakavat, joten kynnys maksaa lunnaat on pienempi
  - Osuessaan kohdalle kiristyshaittaohjelma voi halvaannuttaa yrityksen koko toiminnan pitkäksi aikaa
- Terveydenhuoltoalan palveluiden haavoittuvuuksia tutkittu Suomessa
  - Vapaaehtoiset tietoturvatutkijat ovat yhdistäneet voimiaan ja kartoittaneet haavoittuvuuksia terveydenhuoltoalan järjestelmistä

ANALYYSI

- Varmuuskopiot on pidettävä erillisessä verkossa päivittäin käytettävän verkon sijaan, palautumista ja palauttamista tulee myös harjoitella
- Verkko on segmentoitava, jotta mahdollisia haittaohjelman vaikutuksia voidaan rajoittaa

Haittaohjelmat

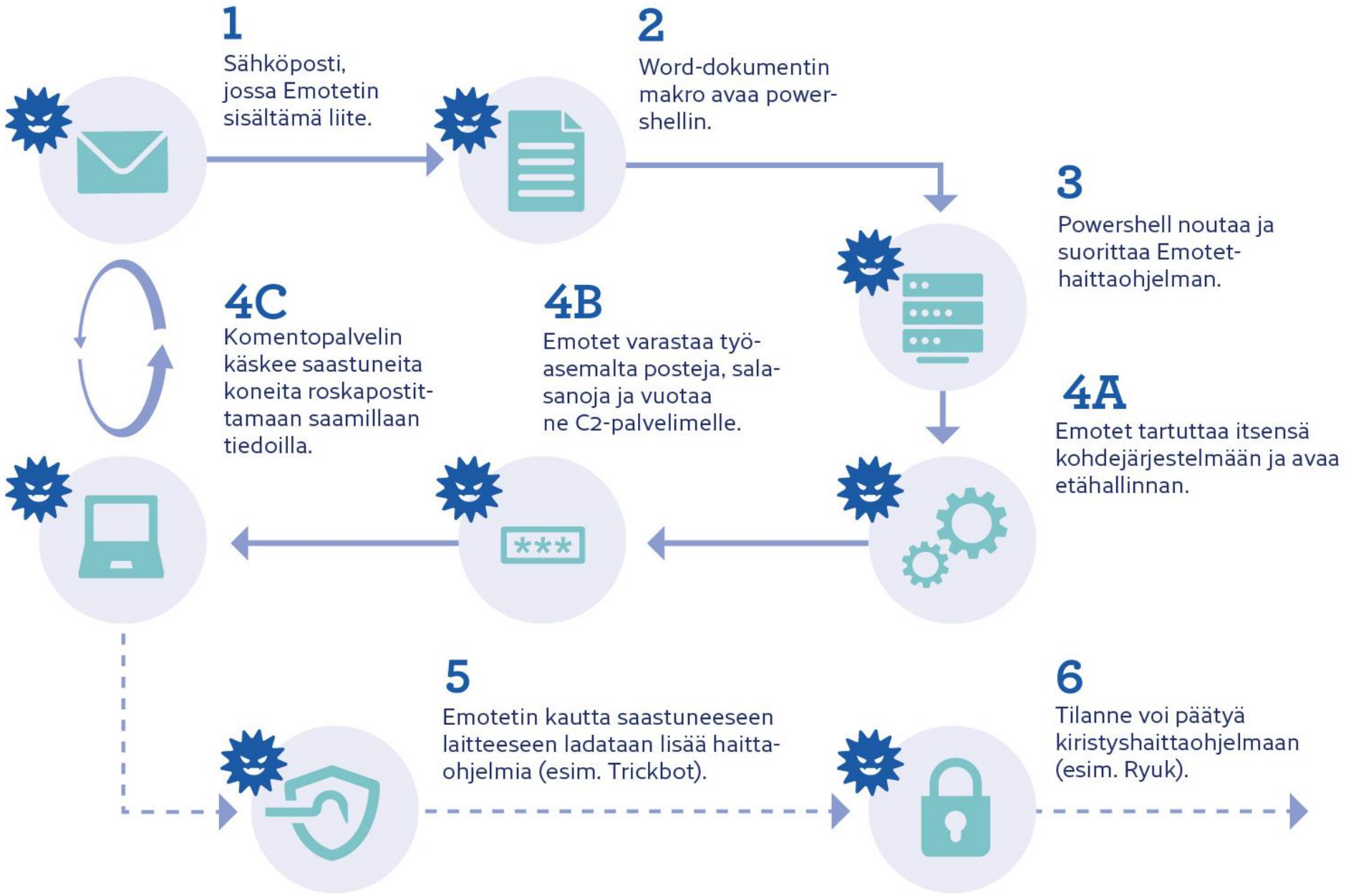
- Emotet-haittaohjelma leviää edelleen ja elokuussa 2020 julkaistu varoitus on yhä voimassa
  - Sähköpostisuodattimet ja virustorjuntatyökalut ovat tunnistaneet Emotet-haittaohjelman hyvin
  - Uusilta tartunnoilta on pääosin vältytty

- Posti-aiheiset huijausviestit johtavat Android-haittaohjelmaan
  - Tekstiviestit tarjoavat ”maksa tästä” –linkin jotta paketin saa itselleen
  - Linkkiä klikkaamalla tarjoutuu ”mahdollisuus” asentaa haittaohjelma
  - Haittaohjelma lähettää puhelimesta tuhansittain tekstiviestejä, minkä vuoksi liittymälle generoituu isoja laskuja

ANALYYSI

- Sähköposti on edelleen yleisin levitysvektori haittaohjelmille
- Virustorjuntatyökalujen päivityksetkin tulee pitää ajan tasalla

Emotet-haittaohjelmatartunnan eteneminen



Haavoittuvuudet

- Windowsin IPv6-reitityksen toteutuksesta on löydetty kriittinen haavoittuvuus
  - Haavoittuvuus mahdollistaa mielivaltaisen koodin suorittamisen haitallisten pakettien avulla

ANALYYSI

- Vaikka Windows ja Chrome päivittyvät automaattisesti voi haavoittuvuuksien julkaisun ja päivityksien asentamisen välille jäädä haavoittuvuusikkuna, jossa haavoittuvuudet voivat tulle hyväksikäytetyksi
- Windowsista löydettiin paikallinen käyttöoikeuksien laajentaminen (privesc) haavoittuvuus, Chromesta on löydetty myös kriittisiä haavoittuvuuksia. Hyökkääjät voivat mahdollisesti yhdistää näitä haavoja, järjestelmien päivityssyklien aikaeron välillä.

Lokakuun haavoittuvuusjulkaisut

- Kriittinen haavoittuvuus SonicWall VPN-laitteissa (31/2020)
- Havaittu aktiivista Oracle WebLogic palvelimen hyväksikäyttöä (32/2020)
- Havaittu Oracle Solaris-käyttöjärjestelmän todentamisrajapinnan (PAM) todennuksen ohittamista (33/2020)

- Näiden lisäksi myös edellisellä kalvolla mainittu Windows IPv6-reitityksen haavoittuvuus on yksi lokakuun haavoittuvuustiedotteista (30/2020).
- Lue lisää: www.kyberturvallisuuskeskus.fi/haavottuvuudet

ANALYYSI

- Lokakuun päivitystiistaina julkaistiin lukuisia kriittisiä korjauksia haavoittuvuuksiin monissa eri järjestelmissä
- Päivitykset tulee asentaa viipymättä, haavoittuvuuksien hyväksikäyttö on todella nopeaa
- Päivityssyklien ulkopuoliset päivitykset tulee myös huomioida, muutoin järjestelmään voi jäädä kriittisiä haavoittuvuuksia pitkäksikin aikaa

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 ja IoT

- Nokian Threat Intelligence Report on julkaistu lokakuussa
  - Raportin mukaan noin 33 % kaikista haittaohjelmahavainnoista on tehty IoT-laitteissa
  - Nousua prosenttiosuudessa viime vuoteen verrattuna 17 %
  - Latauslinkki https://www.nokia.com/about-us/news/releases/2020/10/22/nokia-threat-intelligence-report-warns-of-rising-cyberattacks-on-internet-connected-devices/

ANALYYSI

- IoT-laitteiden määrä kasvaa jatkuvasti, mutta tietoturvataso ei ole parantunut oleellisesti kasvun myötä
- Laitemäärän kasvu yhdistettynä heikkoon tietoturvatasoon johtaa siihen, että yhä suurempi osa kaikista haittaohjelmatartunnoista kohdistuu IoT-laitteisiin
- Verkkojen ja käyttäjien turvaaminen edellyttää IoT-laitteiden tietoturvan parantamista. IoT-laitteiden heikkotasoinen tietoturva vaarantaa sekä kansalaisten että organisaatioiden tiedot, toiminnan ja turvallisuuden.

Automaatio ja IoT

- Singaporen kyberturvallisuusviranomainen on julkaissut kansallisen kyberturvallisuussertifikaatin IoT-kuluttajalaitteille
  - Sertifiointi kohdistuu alkuvaiheessaan reitittimiin ja älykotikeskuksiin (smart hub)
  - Singaporen IoT-kuluttajalaitteiden tietoturvaskeema on Suomen jälkeen toinen kansallinen maailmassa ja ensimmäinen Kauko-Idässä
  - Lisätietoja: https://www.csa.gov.sg/programmes/cybersecurity-labelling/about-cls
- Australian kyberturvallisuusviranomainen on julkaissut ohjeet IoT-tietoturvallisuuteen kuluttajille ja laitevalmistajille

ANALYYSI

- Kansallisten viranomaisten tietoisuus IoT-laitteiden tietoturvallisuuden tasosta ja merkityksestä heijastuu erilaisten ohjeistusten ja tietoturvasertifikaattien kehitystyönä
- Myös EU:n kyberturvallisuusasetuksen puitteissa valmistellaan kuluttajien IoT-laitesertifiointia
- Vapaaehtoiset sertifioinnit luovat pohjaa myös IoT-laitteiden tietoturvan pakottavalle regulaatiolle

Automaatio

- Yhdysvallat on asettanut sanktioita venäläisille, joiden epäillään olevan syyllisiä Triton-haittaohjelmaan.
  - Haittaohjelma on kehitetty erityisesti automaatiojärjestelmien turvajärjestelmiin hyökkäämiseen ja vakavien tuhojen aiheuttamiseen laitteille ja niiden käyttäjille
  - Ensimmäinen tunnettu hyökkäys haittaohjelmaa käyttäen elokuussa 2017

ANALYYSI

- Yhdysvallat on ryhtynyt järjestelmällisiin toimiin vieraisiin valtoihin kytkeytyvien tietoturvaloukkauksien käsittelyssä
- Epäilyjen nostaminen julkisuuteen tuo ilmi ilmiön vakavuuden, ja auttaa organisaatioita ymmärtämään mahdollisia seurauksia aikaisempaa paremmin
- Korkean tason haittaohjelmatartunnoilta välttyminen on äärimmäisen vaikeaa, mikä korostaa havaitsemiskyvyn tärkeyttä ja havaitsemisen jälkeisen valvonta- ja reaktiokyvyn merkitystä

Automaatio

- Automaatiojärjestelmien verkkorajapintojen kriittisiin haavoittuvuuksiin on julkaistu lokakuussa korjauksia
  - Pepperl+Fuchs Comtrol -tuotteet https://sec-consult.com/en/blog/advisories/multiple-critical-vulnerabilities-in-rocketlinx-series/
  - Bosch Rexroth -teollisuus-PC:t https://psirt.bosch.com/security-advisories/bosch-sa-856281.html

ANALYYSI

- Verkkolaitteissa olevat haavoittuvuudet vaarantavat kaiken niiden välityksellä kulkevan liikenteen sekä altistavat päätelaitteet verkosta tuleville uhille
- Automaatiojärjestelmien päätelaitteet eivät tyypillisesti tarkasta verkkoliikenteen eheyttä, mikä korostaa verkkolaitteiden merkitystä koko automaatiojärjestelmän tietoturvan portinvartijoina.

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

- Lokakuussa oli vain kolme merkittävää toimivuushäiriötä yleisissä viestintäpalveluissa
  - Häiriöt vaikuttivat kukin vain yhden tai kahden kunnan alueella.
  - Häiriöt koskivat puhelinpalvelua ja internetpalvelua kiinteässä verkossa sekä puhelinpalvelua ja internetpalvelua matkaviestinverkossa.
  - Häiriöiden syinä olivat huoltotöiden sivuvaikutukset, laitevika ja ohjelmistovika.

ANALYYSI

- Merkittäviä häiriöitä oli vähemmän kuin keskimäärin kuukaudessa ja tapahtuneet häiriöt olivat melko lyhyitä ja rajautuivat pienille maantieteellisille alueille.
- Lokakuussa ei ollut isoja myrskyjä, mikä osaltaan piti häiriöiden määrän alhaisena.

ICT-palveluiden toimivuus

- Microsoftin Office 365 -palveluissa oli maailmanlaajuisia häiriöitä maanantaina 28.9. ja uudelleen 1.10.
  - Häiriöt johtuivat Microsoftin tekemistä muutoksista käyttäjien tunnistamisen palveluihin. Microsoft joutui perumaan muutokset häiriöiden korjaamiseksi.
  - https://www.forbes.com/sites/daveywinder/2020/10/01/new-worldwide-microsoft-outage-confirmed-heres-what-we-know/
- Ryhmäviestintäpalvelu Slackissa oli maailmanlaajuisia häiriöitä 5.10.
  - Ensimmäiset Slackin tekemät korjaukset vain pahensivat ongelmaa.
  - https://status.slack.com/2020-10/e8c094cc99aabf64
- HUS:n koronabotti-palvelu ei ollut saatavissa 5.10. tietoliikennehäiriön vuoksi
  - https://yle.fi/uutiset/3-11579085

ANALYYSI

- Pilvipalvelut toimivat yleensä häiriöttömästi, mutta häiriöiden tullessa käyttäjäorganisaatiot eivät voi muuta, kuin käyttää jotakin muuta korvaavaa palvelua. Korvaavaa palvelua ei kuitenkaan voida noin vain ottaa käyttöön, jos käyttöönottoon ei ole varauduttu ja sitä harjoiteltu. Oleellisten sisäisten ja ulkoisten sidosryhmien olisi esimerkiksi tiedettävä, milloin korvaavaa viestintäpalvelua käytetään.

Palvelunestohyökkäykset

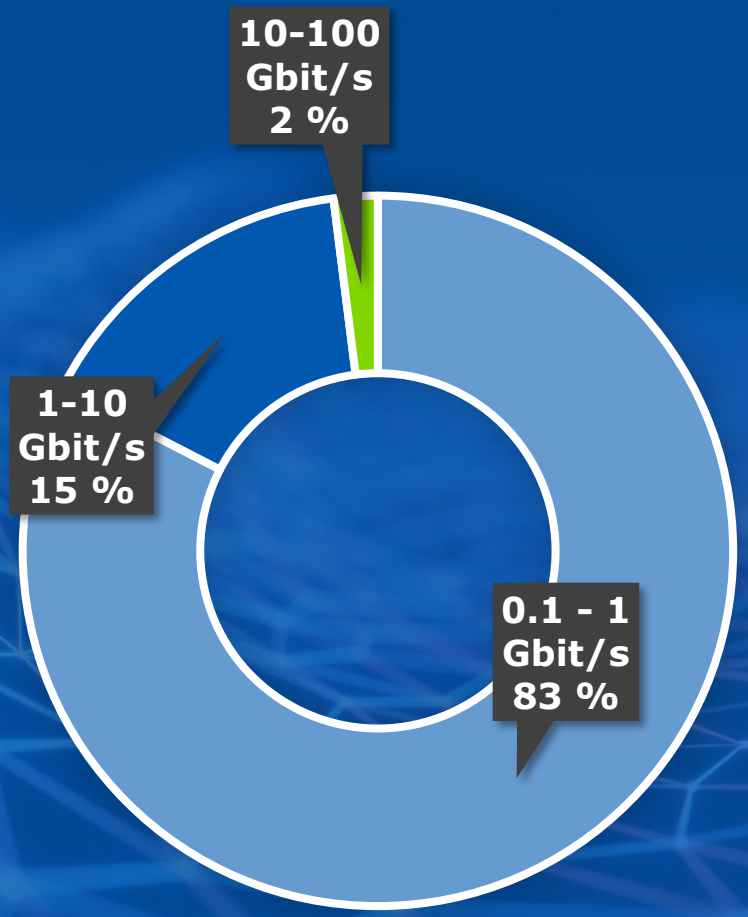
- Lokakuussa Kyberturvallisuuskeskus sai ilmoituksia palvelunestohyökkäyksistä, joilla oli myös laajoja vaikutuksia palveluiden toimintaan.
- Palvelunestohyökkäyksillä uhkailu ja lunnasrahojen vaatiminen ovat yleistyneet maailmalla ja ilmiö on rantautunut myös Suomeen.
  - Uutena ilmiönä palvelunestohyökkäyksiä käytetään tehostamaan kiristyshaittaohjelmahyökkäysten lunnasvaatimuksia.
  - Varsinaisia hyökkäyksiä uhkauksiin liittyen ei kuitenkaan ole ilmoitettu Kyberturvallisuuskeskukselle.
- Olemme saaneet ilmoituksia ilkivaltaisista palvelunestohyökkäyksistä.
  - Hyökkäysten motiivina on ollut tietyn palvelun häirintä.
  - Tämän tyyppisillä hyökkäyksillä voi olla myös vaikutuksia muihin palveluihin kuin hyökkäyksen kohteeseen.

ANALYYSI

- Jos organisaatio on etukäteen varautunut hyökkäyksiin, palvelunestohyökkäyksillä ei yleensä ole vaikutuksia palveluiden toimivuuteen.
- Hyökkäyksiin varautumisessa tulisi huomioida sekä volumetriset että sovellustason hyökkäykset.

Palvelunestohyökkäysten tunnuslukuja

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



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

Vakoilu

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

Vakoilu

- Venäjään liitettyjen APT-ryhmien toiminta oli lokakuussa esillä runsaasti. Useat syytökset liittyivät julkishallintoon tai poliittisiin kohteisiin tunkeutumiseen tai tunkeutumisyrityksiin.
  - Norja syyttää Venäjää kuluvan vuoden elokuussa havaitusta tietomurrosta, joka kohdistui maan parlamenttiin eli Suurkäräjiin.
  - Yhdysvallat julkaisi tietoja syyskuussa alkaneesta hyökkäyksestä, jossa kohteena on ollut Yhdysvaltojen osavaltio- ja aluehallintoa sekä ilmailusektorin verkkoja. Hyökkääjä oli pyrkinyt saamaan käsiinsä esimerkiksi tietoja verkkoratkaisujen toteutuksesta ja suojauksista sekä tietoja laite- tai järjestelmätoimittajista ja -hankinnoista. Yhdysvaltojen mukaan hyökkäyksen takana on ollut Venäjään yhdistetty Berserk Bear -ryhmä.
  - Syyskuussa Yhdysvaltojen liittovaltioon kohdistuneen tietomurron tekijöiksi puolestaan arvellaan Fancy Bear -ryhmää. Yhdysvallat kertoi tietomurrosta mutta ei yksilöinyt tekijöitä. Tietoturvayhtiöt pitävät kuitenkin kerrottujen yksityiskohtien valossa Fancy Bear -ryhmää todennäköisenä tekijänä.
  - Suojelupoliisi on niin ikään varoittanut kansallisen turvallisuuden katsauksessaan, että Venäjä kohdistaa kybervakoilua myös Suomeen. Toisena tällaisena maana Supo nosti katsauksessaan esiin Kiinan.

LISÄTIETOJA

- https://supo.fi/documents/38197657/39761269/FI+Kansallisen+turvallisuuden+katsaus_2020.pdf/

Vakoilu

- Myös Venäjään liitettyjen ryhmien aiemmat teot ja käyttämät haittaohjelmat saivat lokakuussa jälleen huomiota:
  - Euroopan Unioni asetti lokakuussa pakotteita venäläisille tiedustelu-upseereille liittyen Saksan liittovaltion parlamenttiin kohdistuneeseen tietomurtoon vuodelta 2015.
  - Venäjään yhdistetystä Turla-ryhmästä puolestaan saatiin lisätietoja, kun Yhdysvallat julkaisi analyysin ryhmän käyttämästä ComRAT-haittaohjelmasta.
    - Yhdysvaltojen kriittisen infrastruktuurin turvallisuusviranomaisen CISA:n raportti aiheesta: https://us-cert.cisa.gov/ncas/analysis-reports/ar20-303a

ANALYYSI

- Useat valtiot voivat pyrkiä edistämään intressejään kybervakoilun keinoin. Kybervakoilulla voidaan pyrkiä saamaan esimerkiksi tietoa päätöksenteosta tai hyötymään muiden tekemästä teknologisesta kehittämisestä tai innovoinnista.
- Myös Suomen julkishallinto ja päätöksentekoelimet sekä suomalaiset organisaatiot voivat olla kybervakoilun kohteina eri syistä.

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

- KRP takavarikoi lokitietoja F-Securen hallusta, kaksi oikeusastetta kumosi takavarikon ja määräsi tiedot tuhottaviksi.
- Helsingin käräjäoikeuden päätös 10.5.2019 ja Helsingin hovioikeuden päätös 21.10.2020. Ratkaisut ovat julkisia.

TIIVISTELMÄ

- Kyseessä lokitiedot, jotka syntyvät kun käyttäjä tunnistautuu F-Securen Freedome-palveluun. F-Secure on kerännyt palvelua tarjotessaan IP-osoitteita, tietoja yhteyden kestosta sekä yhteyden ajankohdasta.
- Keskeisin kysymys on, ovatko lokitiedot takavarikoimiskiellon alaisia välitystietoja vai takavarikoitavia asiakastietoja.
- Käräjäoikeus sekä hovioikeus katsoivat, että Freedome-palveluun tunnistautumisen yhteydessä tallentuvat lokitiedot ovat luottamuksellisen viestinnän suojan piiriin kuuluvia viestinnän välitystietoja. Tietojen hankinta olisi ollut mahdollista vain pakkokeinolaissa säädetyllä menettelyllä, ei poliisilain mukaisella takavarikolla.

Arjen kyberturvallisuus – luottavainen lokakuu

Lokakuussa vietettiin Euroopan kyberturvallisuuskuukautta

- Arjen kyberturvallisuustaitoja on hyvä ylläpitää myös lokakuun jälkeen.
- Tämän vuoden kyberturvallisuuskuukauden pääteemat ovat kyberhuijaukset ja kybertaidot.
- Tutustu kampanjaan tältä sivulta: https://www.kyberturvallisuuskeskus.fi/fi/euroopan-kyberturvallisuuskuukausi-european-cyber-security-month

RuuviTag sai Tietoturvamerkki

- RuuviTag mittaa ilman lämpötilaa, kosteutta, painetta sekä liikettä ja lähettää nämä tiedot majakkana lähialueen vastaanottimille.
- Tietoturvamerkki kertoo siitä, että merkillä varustettu tuote tai palvelu on suunniteltu tietoturvalliseksi.
- https://tietoturvamerkki.fi/fi/tuote-ruuvitag/

Tietovuotoapu.fi sivusto

- Liikenne- ja viestintävirasto Traficom on tehnyt viranomaisten ja muiden organisaatioiden kanssa yhteisen Tietovuotoapu.fi-sivuston, jonne kootaan oleellinen tieto psykoterapiakeskus Vastaamon tietomurron uhrien auttamiseksi.
- Sivustolla on tarjolla tietomurron uhreille toimintaohjeita ja auttavien organisaatioiden yhteystiedot.
- https://tietovuotoapu.fi/fi/tietovuotoapu

Vieraskynä: Nettihuijaukset ovat kaikkien asia

- Tämän vuoden kyberturvallisuuskuukauden pääteemat ovat kyberhuijaukset ja kybertaidot.
- Huijari kuriin! –hankkeella pyritään auttamaan uhreja ja lisäämään tietoisuutta.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vieraskyna-nettihuijaukset-ovat-kaikkien-asia

Ajankohtaista Kyberturvallisuuskeskuksesta

Uusi työkalu johdolle kyberuhkien hallintaan

- Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen kehittämä Kybermittari auttaa yritysjohtoa saamaan kyberriskit kattavammin hallintaan ja turvaamaan liiketoiminnan jatkuvuuden.
- Kybermittarin avulla saa näkymän toiminnalle tärkeiden kyberkyvykkyyksien kypsyystasoon osa-alueittain ja tavoitteittain.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uusi-tyokalu-johdolle-kyberuhkien-hallintaan

Tietoturvan suunnannäyttäjät

- 3.11. järjestetyssä seminaarissa jaettiin Vuoden tietoturvan suunnannäyttäjä –palkinto.
- Palkittavat tekevät tärkeää ja pyyteetöntä työtä, joka on oleellista kansallisen tilannekuvan muodostamisessa ja joka on yhteiskunnallisesti merkittävää.
- Tunnustuksen saivat Jouko Katainen (Ilmarinen), Jussi Törhönen (Enfo), Tomi Vehkasalo (Aditro) ja Jani Räty (Aditro).
- https://www.traficom.fi/fi/ajankohtaista/tietoturvan-suunnannayttaja-tunnustuksen-voittajat-tekevat-korvaamatonta-tyota

KONEella kyberharjoittelu on tulevaisuuden tietoturvan kehitystyön tukena

- ONE on kokenut valmiusharjoittelija myös kyberturvallisuuden saralla. Tällä kertaa kyberharjoittelun vaatimustasoa haluttiin nostaa tuomalla perinteiseen työpöytäharjoitukseen mukaan toiminnallisia elementtejä.
- Tavoitteena oli, että KONEella organisaationa on paremmat valmiudet ennakoida ja kohdata kyberturvallisuutta vaarantavia häiriötilanteita sekä selviytyä niistä nopeammin ja tehokkaammin.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/koneella-kyberharjoittelu-tulevaisuuden-tietoturvan-kehitystyon-tukena

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