TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Kesäkuu 2020

Kybersää Kesäkuu 2020

Tietomurrot ja -vuodot

- Sähköposteihin kohdistuvia laajoja tietomurtokampanjoita myös Suomessa.
- Yritysten kanta-asiakasjärjestelmiä kohtaan tietomurtoja ja niiden yrityksiä.

Huijaukset ja kalastelut

- Teknisen tuen nimissä soitetaan taas aktiivisesti.
- Toimitusjohtajahuijaukset ja muut laskutuspetokset lisääntyvät taas lomakauden aikana.

Haittaohjelmat ja haavoittuvuudet

- Useita kriittisiä haavoittuvuuksia, jotka vaikuttavat mm. Palo Alto Networksin ja F5:n VPN-ratkaisuihin sekä Citrixin Application Delivery Controller (ADC), Citrix Gateway sekä Citrix SD-WAN WANOP –tuotteisiin.

Automaatio

- EKANS-haittaohjelmahyökkäykset kohdistettiin Hondaan ja ENEL Groupiin.
- Kesäkuussa julkaistiin pari merkittävää tutkimusta automaatio- ja IoT-aiheista.

Verkkojen toimivuus

- 12 merkittävää toimivuushäiriötä, joista 3 johtui Päivö-myrskystä.
- Vuosia jatkunut merkittävien häiriöiden määrän lasku näyttää kääntyneen hienoiseen nousuun.
- Kesäkuu oli palvelunestohyökkäysten osalta Suomessa rauhallinen.

Vakoilu

- Myös sosiaalisen median palveluita voidaan hyödyntää haitallisten viestien ja liitteiden välittämisessä.
- Organisaation verkon toteutukseen liittyvät järjestelmät ja turvalliset yhteysratkaisut ovat kiinnostavia tunkeutumiskohteita tietoa tai jalansijaa havittelevalle hyökkääjälle.

Kuukauden tunnuslukuja

3

MERKITTÄVÄÄ VERKKOJEN TOIMIVUUSHÄIRIÖTÄ KESÄKUUN LOPUN PÄIVÖ-MYRSKYN TAKIA

1

UUSI TIETOTURVAMERKKI LÄHITAPIOLAN ELÄMÄNTURVASOVELLUKSELLE

63%

KASVU KYBERTURVALLISUUSKESKUKSEN TIETOON TULLEISSA PUHELU- JA SÄHKÖPOSTIHUIJAUKSISSA VERRATTUNA TOUKOKUUHUN

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

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

2

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

3

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

kohonnut

laskenut

ennallaan

Keltainen = uutta/ päivitettyä*

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

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

UUSI

Kyberturvallisuuskeskus on saanut runsaasti ilmoituksia tietojenkalastelusta ja huijausten yrityksistä kesällä. Toimitusjohtaja- ja laskutushuijauksissa rikollinen pyrkii usein hyödyntämään loma-ajan vähentyneitä henkilöstöresursseja ja kokemattomia sijaisia, joille laskutusten hoitaminen ja muut organisaation prosessit eivät välttämättä ole tuttuja. Tärkeä keino huijausten ja kalastelun ehkäisyyn on työntekijöiden perusteellinen perehdytys. Työntekijöiden tulee myös tietää keneltä he voivat varmistaa laskun maksamisen. Varmistus ennen maksamista on hyvä tehdä esihenkilöltä, kollegalta tai laskun lähettäjältä.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

2

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 kohdetta kiristetään myös hyökkääjän haltuun saamien tietojen myymisellä, vuotamisella tai julkaisemisella lunnasvaatimuksen tehostamiseksi.*

CASE

Amerikkalainen ICT-palveluntarjoaja Cognizant joutui Maze-kiristyshaittaohjelman uhriksi. Tapaus ei koskettanut vain yritystä itseään vaan kiristyshaittaohjelman vaikutukset ulottuivat asiakkaisiin saakka. Yritys on arvioinut, että se käyttää 50-70 miljoonaa dollaria seuraavan kolmen kuukauden aikana hyökkäyksen aiheuttamien vahinkojen korjaamiseksi. Tämän lisäksi kuluja kertynee juridisista, konsultoinnista ja hyökkäyksen selvittämiseen liittyvistä kuluista. Maze paitsi lukitsee uhrin koneiden tiedostot, se myös ottaa niistä kopiot hyökkääjälle.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

3

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 tunnistavat kohteet, 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

Palvelinten ylläpitoon käytetystä Saltstack Salt -hallintakehikosta korjattiin kriittisiä haavoittuvuuksia huhtikuun lopulla. Ensimmäiset automatisoidut hyökkäykset havaittiin vain pari päivää myöhemmin, myös Suomessa. Hyökkääjä asensi virtuaalivaluuttaa louhivan haittaohjelman kaikkiin hallinnan piirissä oleviin palvelimiin. Verkkoon auki olevia palveluita löytyi yli 6000.

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

UUSI

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 organisaatiolle, että he eivät voi luovuttaa lokitietoja, sillä heidän jaettuja resursseja käyttävät palvelut eivät erottele eri asiakkaiden lokitietoja. Tältä tilanteelta oltaisiin mahdollisesti voitu välttyä, jos tämä vastuunjakoon liittyvä asia olisi selvitetty ja sovittu jo sopimuksentekovaiheessa.

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

UUSI

Korona-aikana etätyö lisääntyi ja osaavan henkilöstön saatavuus heikentyi. Tietoteknisiin ympäristöihin on jouduttu tekemään muutoksia ja tietoturvapäivitykset ovat monin paikoin harventuneet. Tämä on lisännyt järjestelmien päivitys- ja korjausvelkaa, mikä nostaa niiden alttiutta tietomurroille ja muita kyberturvallisuusriskejä. Organisaatioiden on nyt syytä kiriä korjausvelkaa umpeen ja varmistaa järjestelmien päivitykset, ajantasaisuus ja toimivuus.

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

- Sähköposteihin kohdistuvia laajoja tietomurtokampanjoita myös Suomessa.
  - Suomessa oli kesäkuussa laajasti liikkeellä ainakin kaksi erillistä kalasteluketjua. Kalastelut liittyvät isompaan kansainväliseen kampanjaan.
  - Kyberturvallisuuskeskuksen tiedossa on kymmenien organisaatioiden edustajia Suomessa, joiden sähköpostitunnukset ovat päätyneet vääriin käsiin.
  - Murtojen uhreja on tavoiteltu, mutta lomakausi vaikeuttaa heidän tavoittamistaan.
  - Osassa tapauksista tileille on tunkeuduttu sisään ilman, että asiaa olisi organisaatiossa havaittu.

ANALYYSI

- Kansainväliset kampanjat osuvat myös Suomeen. Osa kampanjoista räätälöidään maakohtaisesti, joten valitettavasti hyvä suomen kieli ei ole enää takuu viestin aitoudesta.
- Monivaiheinen tunnistautuminen suojaisi liki poikkeuksetta myös sähköposteihin kohdistuvilta tietomurroilta.

Tietomurrot ja vuodot

- Yritysten kanta-asiakasjärjestelmiin tehtiin kesäkuussa tietomurtoja ja niiden yrityksiä.
  - Tunkeutumisyritykset kohdistuivat käyttäjien tileihin eivätkä varsinaiseen järjestelmään.
  - Tunkeutumisissa käytettiin toisista palveluista vuotaneita käyttäjätunnuksia ja salasanoja, kalasteltiin tunnuksia käyttäjiltä sekä kokeiltiin yleisimpiä tunnuksia ja salasanoja.
  - Ylläpidon nopeat toimenpiteet estivät vahingolliset tapahtumat jokaisessa tietomurrossa.

ANALYYSI

- Asiakastiedot sekä järjestelmien tunnukset ovat kauppatavaraa. Käytä eri palveluissa eri salasanaa. Ohjeemme hyvistä salasanoista löytyy osoitteesta: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan
- Salasanojen hallintaan on syytä harkita salasanojen hallintajärjestelmää.

Tietomurrot ja vuodot

- Verkkokauppa-alusta Magento muistuttaa, että Magento 1- alustan tuki on päättynyt kesäkuussa 2020.
  - Tuen loppumisen jälkeen tuotteeseen ei enää ole saatavilla uusia päivityksiä. Tämän takia palvelun käytön tietoturvariski kasvaa.
  - Magento 1:n on laajasti käytetty maailmalla ja se on edelleen käytössä myös joillakin tunnetuilla suomalaisilla verkkokaupoilla.
- Hakkeriryhmittymä Magecart hyödyntää verkkokauppa-alustojen haavoittuvuuksia ja tekee niin kutsuttuja toimitusketju-hyökkäyksiä.
  - Kohteena ovat kokoaikaisia työntekijöitä useimmiten heikommin turvatut alihankkijat ja toimittajat.

ANALYYSI

- Verkkokauppa-alustojen turvaaminen on tärkeää, koska niillä käsitellään asiakas- ja maksutietoja, jotka vääriin käsiin päätyessään vaarantavat asiakkaan tietoturvan.
- Toimitusketjun turvallisuus tulisi huomioida kokonaisvaltaisesti ja varmistaa liiketoiminnan kannalta kriittisten järjestelmien tietoturvapäivitykset ja tuen ajantasaisuus.

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.

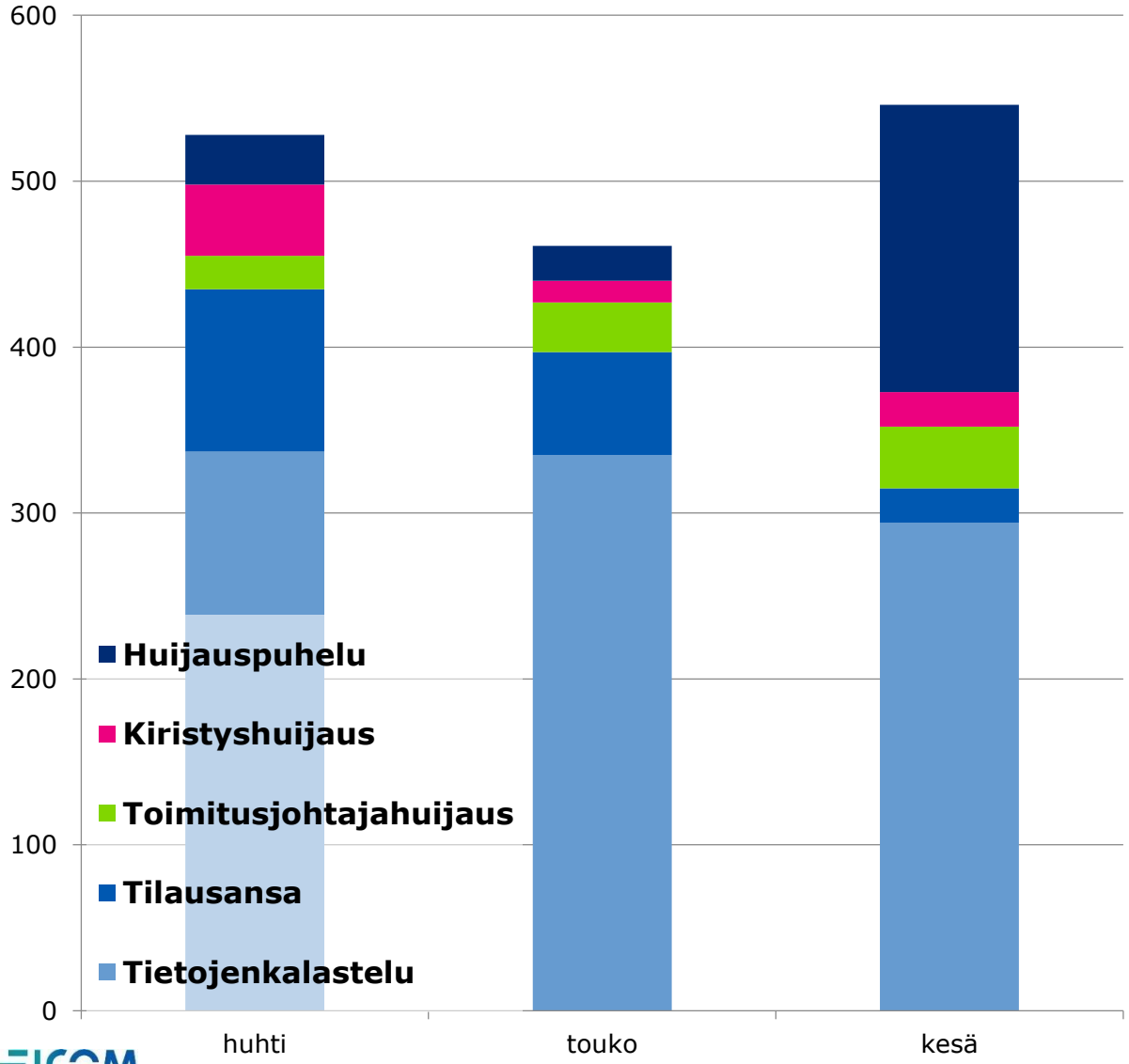
Huijaukset ja kalastelut

- Kesäkuussa 2020 oli enemmän KTK:lle ilmoitettuja tapauksia kuin 2019 kesäkuussa.
  - Huhti-kesäkuun tapahtumien tilasto löytyy seuraavalta sivulta.
- Kuten toukokuussa ennustimme, erilaiset laskutuspetokset ja toimitusjohtajahuijaukset yleistyvät kesäkuun aikana.
- Toimitusjohtajahuijauksia ja muita laskutuspetoksia on tehostettu oikean näköisillä mutta vähän väärin kirjoitetuilla verkkotunnuksilla (typosquat).
  - Toimitusjohtajahuijauksissa tiedustellaan alkuun tilin saldoa ja maksuvalmiutta tai yleisemmin sitä, onko kohde käytettävissä ja voiko hän tehdä palveluksen.
  - Laskutuspetoksissa hyödynnetään murrettuja sähköpostiosoitteita, jolloin sähköpostitililtä on saatu maksutietoja, joita rikolliset muuttavat.

ANALYYSI

- Kyberturvallisuuskeskus sai kesäkuun aikana ilmoituksia toimitusjohtajahuijausyrityksistä, mutta onnistuneista tapauksista ei tullut ilmoituksia.
  - Arvioimme, että tietoisuus eri huijauksista on lisääntynyt, koska niistä on ollut eri kanavissa tietoa ja yritykset myös itse tiedottavat tärkeästä asiasta organisaatiossa. Näin on vältytty onnistuneilta huijauksilta.
- On tärkeää, että tietoisuutta ilmiöstä pidetään yllä. Kesän aikana tulee huolehtia siitä, että työntekijät tietävät keneltä he voivat tarkistaa mahdollisen maksun oikeuden mikäli he epäilevät asiaa.

Käsiteltyjä huijaustapauksia Q2/2020



- Toisen neljänneksen 2020 näkyvimmät trendit ovat olleet:
  - Teknisen tuen huijauspuhelut
  - Huijaukset Postin nimissä (kts. lisää aiheesta Toukokuun kybersää)
- Toimitusjohtajahuijaukset kohdistuvat yrityksiin ja organisaatioihin. Väärennetyt viestit tähtäävät laskutuspetokseen. Huijausyritysten määrä on kohonnut kesälomakaudella, mutta valveutuneisuus on estänyt niiden onnistumisen.
- Tietojenkalastelut ovat tavallisin tapa murtautua yrityksen verkkoon: Kalastellaan tunnuksia ja salasanoja järjestelmäpääsyn toivossa.
- Tilausansoja suunnataan kaikille kuluttajille esiintyen mm. Postin, Gigantin, tai muiden tuotemerkkien nimissä. Niiden määrä on vähentynyt seurantajaksolla (Q2)

Q2/2020 - tilasto päivitetään kvartaaleittain

Teknisen tuen nimissä soitetaan jälleen

- Kyberturvallisuuskeskus on saanut jälleen enenevissä määrin ilmoituksia yrityksiltä ja yksityishenkilöiltä teknisen tuen soitoista. Puheluita soitetaan sekä kotimaisista numeroista että ulkomaan suuntanumeroista.
  - Yhteistä tapauksille on soittajan halu päästä ”asiakkaan” koneelle etäyhteyden kautta suorittamaan tarvittavia toimenpiteitä. Etäyhteys on tavallisimmin otettu TeamViewer –sovellusta hyödyntäen.
  - Helmikuuta riivanneet huijauspuhelut loppuivat maaliskuun lopussa ja alkoivat pitkän tauon jälkeen uudelleen toukokuussa.

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.

Kesä ja kalastelut

- Pankkien nimissä on tehty aktiivisesti tietojen kalastelua kesäkuun aikana
- Kalastelua on tapahtunut Handelsbankenin, Osuuspankin, Säästöpankin sekä S-Pankin nimissä
- Pankkitietoja kalastellaan lähettämällä huijaussähköpostia, jossa pyydetään linkin kautta kirjautumaan sivustolle.
- Katso Tietoturva Nyt! –artikkelimme Neuvoja epäilyttävien sivujen tunnistamiseksi https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-epailyttavien-sivujen-tunnistamiseksi

ANALYYSI

- Pankkitunnusten kalastelua on nähty jo pidemmän aikaa ja kalasteluissa hyödynnetään eri pankkeja. Rikolliset haluavat pankkitunnukset, joiden avulla he voivat siirtää itselleen rahaa.
- Monet näistä huijaussivustoista ovat uskotavan näköisiä. Sivut on tehty taitavasti ja niiden tunnistaminen nopealla katselulla voi olla jopa mahdotonta.
- 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. Alkuvuodesta näytti siltä, että tietojenkalastelu olisi rauhoittunut hieman, mutta tämä oli vain hetkellistä.
- Uutena havaintona on, että tietojenkalasteluviestit sisältävät liitteen, jonka lähdekoodi on sumutettu (muutettu symboliseen konekieliseen muotoon)
- Sähköpostin liitteenä olleita tiedostoja ei ole aluksi havaittu haitallisiksi erilaisten sähköpostisuodattimien avullakaan

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 tässä tärkeää, 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.**

Haittaohjelmat ja haavoittuvuudet

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

Haittaohjelmat ja haavoittuvuudet

- IoT-laitteissa käytetyssä Treck-nimisen valmistajan TCP/IP-verkkototeutuksesta on löytynyt useita haavoittuvuuksia, jotka voivat mahdollistaa laitteen kaappaamisen. Haavoittuvuuksista keskustellaan myös nimellä Ripple20. (Haavoittuvuus 20/2020)
  - Haavoittuvuuden uskotaan vaikuttavan satoihin miljooniin IoT-laitteisiin.
- PaloAlton verkkolaitteista on löydetty kriittinen haavoittuvuus, joka mahdollistaa tunnistautumisen ohittamisen. Haavoittuvuus koskee SAML (Security Assertion Markup Language) –menetelmää käyttäviä konfiguraatioita. (Haavoittuvuus 21/2020)
  - Haavoittuvuus on erityisen kriittinen GlobalProtect VPN -tuotteissa, koska se mahdollistaa hyökkääjien pääsyn suojattavaan verkkoon. Katso lisätietoa myös vakoilu-osiosta.
- Citrix Application Delivery Controller (ADC), Citrix Gateway sekä Citrix SD-WAN WANOP -tuotteista on löydetty 11 haavoittuvuutta, joista vakavimmat haavoittuvuudet voivat mahdollistaa palvelunestotilan tai ohittaa palvelun hallintakäyttöliittymän kirjautumisen. (Haavoittuvuus 22/2020)

ANALYYSI

- TCP/IP-verkkototeutuksen haavoittuvuuksien vakavuutta lisää se, että haavoittuva komponentti voi olla laitteissa, joihin valmistaja ei enää tarjoa päivityksiä tai sellaisissa laitteissa, joiden päivittäminen on vaikeaa. Lisäksi on haastavaa selvittää mikä ohjelmakomponentti on käytössä missäkin laitteessa.

Haittaohjelmat ja haavoittuvuudet

- Kiristyshaittaohjelmia levitetään edelleen aktiivisesti
  - Kansainvälisesti useita merkittäviä kiristyhaittaohjelmahavaintoja
  - Ekans –kiristyshaittaohjelman epäillään murtautuneen Hondan tietojärjestelmiin ja aiheuttaneen merkittäviä häiriöitä autojen valmistukseen: https://threatpost.com/snake-ransomware-honda-energy/156462/
- Useat kiristyshaittaohjelmia käyttävät ryhmät uhkaavat varastettujen tietojen vuotamisella tiedostojen salaamisen lisäksi
  - Maze kiristyshaittaohjelman vuotosivulla julkaistiin myös toisen toimijan varastamia tietoja https://www.bleepingcomputer.com/news/security/ransomware-gangs-team-up-to-form-extortion-cartel/

ANALYYSI

- Kiristyshaittaohjelmaryhmät tekevät yhteistyötä ja niiden toiminta kehittyy jatkuvasti. Tietojen varastaminen on yleistynyt ja hyökkääjät voivat jäädä pitkäksi aikaa ympäristöön etsimään uusia hyödyntämiskeinoja.
- Etenkin Yhdysvalloissa yleistyneet kiristyshaittaohjelmatapaukset saattavat ennakoida tapausmäärien kasvua myös Suomessa.

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-haittaohjelmahyökkäyksiä kohdistui Hondaan ja ENEL Groupiin.
- Laajassa honeypoteilla toteutetussa automaatioverkkojen tutkimuksessa suurin osa verkkoliikenteestä oli skannauksia, mutta ohessa paljastui useita täysin uusia haavoittuvuuksia. Haavoittuvuudet, jotka eivät ole yleisesti tiedossa, ovat erityisen hyödyllisiä kohdistettujen hyökkäysten tekijöille.
  - https://ccdcoe.org/uploads/2020/05/CyCon_2020_15_Dodson_Beresford_Vingaard.pdf
  - https://www.zdnet.com/article/security-four-zero-day-attacks-spotted-in-attacks-against-honeypot-systems/
- Fraunhofer-instituutti on julkaissut lähinnä kotireitittimien tietoturvaa käsittelevän tutkimuksen, jossa saatuja tuloksia ja havaintoja kannattaa tarkastella myös laajemmin IoT-näkökulmasta.
  - https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf

ANALYYSI

- Automaatiojärjestelmien yhteiskunnallinen merkitys on lisääntynyt ja niiden kyberturvallisuutta kehitetään ja ohjeistetaan.
- Automaatiojärjestelmistä etsitään ja ilmoitetaan haavoittuvuuksia verrattain vähän, mutta se ei tarkoita, etteikö niitä käytettäisi hyökkäyksissä.

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 oli kesäkuussa 12 merkittävää häiriötä
  - Useimmat häiriöt kestivät alle 3 tuntia ja vaikuttivat kukin alle 10000 käyttäjään.
- Päivö-myrsky 30.6.-1.7. aiheutti kolme merkittävää toimivuushäiriötä
  - Myrskyn katkaisemat sähköt vaikuttivat lähinnä matkaviestinverkkojen palveluihin Itä-Suomessa. Sähköjä katkesi myös radio- ja TV-verkon täytelähettimiltä, mutta sen vaikutukset palveluihin jäivät vähäisiksi.
- Tammikuusta kesäkuuhun häiriöitä on ollut 37. Vuonna 2019 vastaavana aikana oli 32 häiriötä

ANALYYSI

- Merkittävien häiriöiden määrän pitkäaikainen lasku näyttää loppuneen.
- Päivö-myrskystä selvittiin suhteellisen hyvin. Keskeistä myrskyn aiheuttamien häiriöiden poistamiselle on tiivis yhteistyö teleyritysten, sähköverkkoyhtiöiden ja pelastuslaitosten välillä.
- Varavoiman syöttäminen tukiasemille ja telelaitetiloihin ei vieläkään ole kaikissa tilanteissa sujuvaa. Esimerkiksi osa liittimistä ei sovi yhteen.

Verkkojen toimivuus

- IBM:n pilvipalveluissa oli saatavuuden häiriöitä ympäri maailmaa 9.6.2020
  - Syyksi osoittautui reititysvirhe, joka aiheutti valtavan liikennekuorman IBM:n pilvipalvelimille.
  - IBM Cloud global outage caused by "incorrect" BGP routing (11.6.2020) https://www.bleepingcomputer.com/news/technology/ibm-cloud-global-outage-caused-by-incorrect-bgp-routing/
- Yhdysvalloissa T-Mobilen palveluissa oli laaja häiriö 16.6.2020
  - Häiriö vaikutti myös hätäpuheluiden soittamiseen. T-Mobile on Yhdysvaltain kolmanneksi suurin teleoperaattori.
  - T-Mobile confirms nationwide outage impacting millions of customers (16.6.2020) https://abc13.com/tmobile-outage-is-out-t-mobile-down/6248980

ANALYYSI

- Pienet reititysvirheet ovat Internetin arkipäivää. Ne kuitenkin harvoin johtavat suurten internetpalveluiden saatavuusongelmiin.
- T-Mobilen häiriö herätti heti suurta huomiota myös valvovassa viranomaisessa (FCC), joka ilmoitti vaativansa häiriön perusteellista selvittämistä.

Palvelunestohyökkäykset

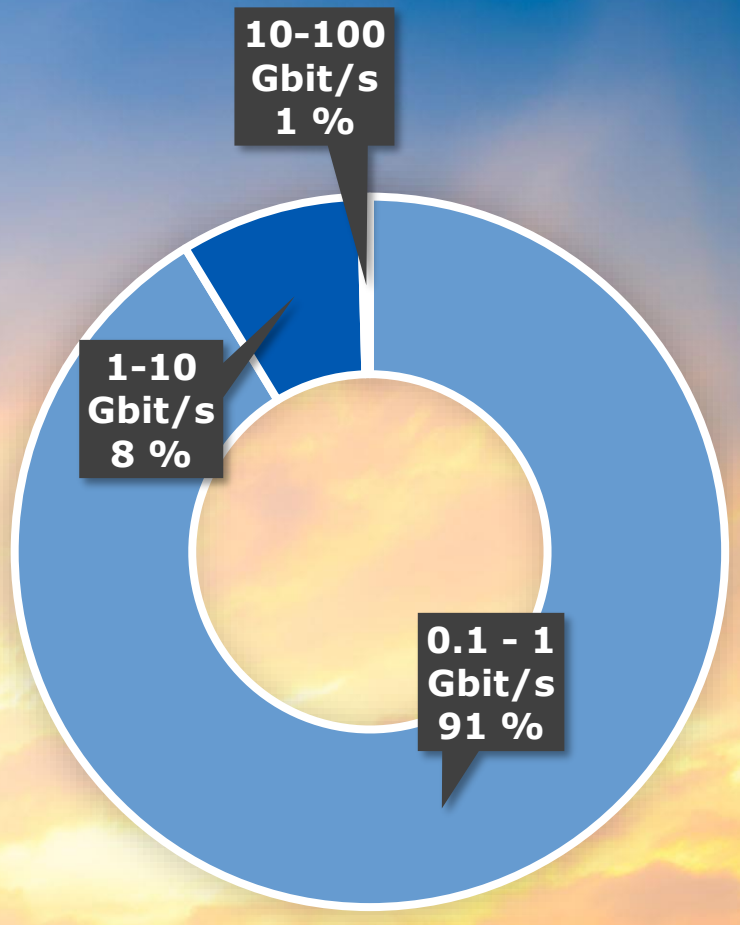
- Kesäkuu oli palvelunestohyökkäysten osalta Suomessa rauhallinen. Raportoiduilla hyökkäyksillä ei pääasiassa ollut vaikutuksia palveluiden toimintaan.
- Suomeen kohdistuneiden palvelunestohyökkäysten määrä ja volyymit ovat kuitenkin olleet lievässä nousussa.
- Eurooppalaista pankkia vastaan tehtiin kesäkuussa verkkoliikenteen pakettimäärällä mitaten historian suurin palvelunestohyökkäys. Tehokkaat suojaukset kuitenkin estivät vahingot.
  - https://blogs.akamai.com/2020/06/largest-ever-recorded-packet-per-secondbased-ddos-attack-mitigated-by-akamai.html

ANALYYSI

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

Palvelunestohyökkäysten tunnuslukuja

- 59 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q2 aikana 2020.
- Noin 54% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



SUOMEEN KOHDISTUNEIDEN PALVELUNESTO-HYÖKKÄYSTEN VOLYYMIT (Q2/2020 - 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

- Keskeiset verkkolaitteet ja organisaation verkon tietoturvaratkaisut ovat houkuttelevia tunkeutumiskohteita hyökkääjälle, jota kiinnostaa organisaation kriittinen tieto tai jalansijan saaminen verkkoon.
  - Esimerkiksi hiljattain on julkistettu haavoittuvuuksia muun muassa Palo Alto Networksin palomuuri- ja VPN-ratkaisuissa ja F5:n VPN-ratkaisuissa. Lisäksi tietoturvayhtiö Fox-IT kertoi, että vuodenvaihteessa julkaistu Citrix Netscaler/ADC -haavoittuvuus on kevään aikana johtanut lukuisiin tietomurtoihin.
  - Esimerkiksi Yhdysvaltojen tietoturvaviranomainen CISA varoitti Palo Alto Networksin tuotteiden haavoittuvuuksiin liittyen, että APT-ryhmät yrittävät todennäköisesti nopeasti hyödyntää niitä.

ANALYYSI

- Julkisesta internetistä saavutettavissa olevat järjestelmät pitäisi pystyä päivittämään tai muutoin suojaamaan mieluiten vuorokauden kuluessa haavoittuvuuden julkaisusta johtuen siitä, että aikaikkuna haavoittuvuuksien julkistamisesta niiden hyödyntämiseen on lyhentynyt.
- Tilanteissa, joissa haavoittuvuutta on voitu ehtiä hyödyntämään, ei pelkkä järjestelmän päivittäminen riitä, vaan organisaation tulisi muilla keinoin varmistua siitä, että järjestelmään ei ole ehditty murtautua.

Vakoilu

- Sosiaalisen median hyödyntäminen sopivien uhrien tai valikoitujen kohteiden lähestymisessä oli kesäkuussa esillä, kun tietoturvayhtiö ESET kertoi joihinkin ilmailu- ja avaruusteknologiasektorin ja puolustusteollisuuden organisaatioihin kohdistetusta kampanjasta.
  - Operaatiossa kohteita lähestyttiin liike-elämään ja työnhakuun keskittyvässä yhteisöpalvelussa LinkedInissä.
  - Kohdeorganisaatioiden työntekijöille lähestyttiin tekaistuilta profiileilta valheellisen työtarjouksen turvin, jonka avulla uhri saatiin avaamaan joko suoraan LinkedInissä tai sähköpostitse lähetetty haitallinen liitetiedosto.
  - Operaation tavoitteena vaikutti olevan tiedon varastaminen, jonka lisäksi hyökkääjä yritti lopuksi laskutuspetosta.

ANALYYSI

- Sosiaalisen median palveluita voidaan hyödyntää kohdistettujen hyökkäysten toteuttamisessa sekä suoraan että taustatietojen lähteenä.
- Työntekijöitä ja erityisesti organisaation avainhenkilöitä kannattaa ohjeistaa myös muutoin kuin sähköpostitse tapahtuvien yhteydenottojen varalta.

Vakoilu

- Poliittiseen päätöksentekoon ja vaaleihin liittyvä vakoilu ja vaikuttaminen olivat tapetilla kesäkuussa muun muassa Yhdysvalloissa ja Australiassa.
  - Googlen tietoturvatutkijat kertoivat Yhdysvalloissa presidentinvaalikampanjoiden työntekijöille lähetetyistä kohdistetuista kalasteluviesteistä. Hyökkääjät olivat lähettäneet viestit työntekijöiden henkilökohtaisiin sähköpostiosoitteisiin, mutta hyökkäykset jäivät tiettävästi yrityksiksi.
  - Joe Bidenin kampanjaan kohdistuneen tunkeutumisyrityksen taustalla oli Googlen mukaan todennäköisesti Kiinaan yhdistetty APT31-ryhmä. Donald Trumpin kampanjaan kohdistunut kiinnostus puolestaan yhdistettiin Googlen arvioissa Iraniin linkitettyyn APT35-ryhmään.
  - Australiassa puolestaan pääministeri ja puolustusministeri ottivat julkisesti kantaa maahan kohdistuneeseen kybervakoiluun. Ministerit totesivat Australian olevan yhä enenevässä määrin kybervakoilun kohteena, joka ulottuu eri toimialoille valtionhallinnosta yksityiseen sektoriin ja kehottivat organisaatioita varautumaan kybervakoiluun.

ANALYYSI

- Poliittinen päätöksenteko ja sen valmistelu on kybervakoilun perinteinen kohde. Toisaalta huomattavan monenlaiset organisaatiot voivat olla valtiollisen toiminnan kohteena joko oman toimintansa, hallussa pitämänsä tiedon tai toimitusketjun osana olemiseen liittyvän asemansa vuoksi.

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

- Hallituksen esitys laiksi sähköisen viestinnän palveluista annetun lain muuttamisesta (HE 98/2020 vp) annettu eduskunnalle

ANALYYSI

- Ehdotuksella pannaan täytäntöön EU:n ns. teledirektiivi sekä muista EU-säädöksistä ja kansallisista tarpeista johtuvia muutoksia, mm.:
- Uudet säännökset viestintäverkon kriittisissä osissa käytettävistä laitteista, verkkoturvallisuuden neuvottelukunnasta sekä poistettavaksi määrätyistä viestintäverkkolaitteista maksettavasta korvauksesta (244 a - b §, 301 a §) .
- Muutoksia hätäliikennettä sekä vaara- ja viranomaistiedotteita koskeviin säännöksiin (278 - 280 §, 321 §).
- Tarkennuksia viestintäverkon kriittisen järjestelmän Suomeen palauttamista koskevaan säännökseen (283 §).
- Traficomille tehtävä toimia EU:n kyberturvallisuusasetuksen mukaisena kansallisena kyberturvallisuussertifioinnin viranomaisena (304 §).
- Lue lisää: https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_98+2020.aspx

Oikeudelliset asiat

- Hallituksen esitys laiksi tartuntatautilain väliaikaisesta muuttamisesta (HE 101/2020 vp) ja mobiilisovellus tartuntaketjujen jäljittämiseksi

ANALYYSI

- Eduskunnassa on käsitelty tartuntatautilakiin ehdotettua väliaikaista muutosta, jossa Liikenne- ja viestintävirastolle säädetään tehtäväksi arvioida THL:n korona-sovelluksen tietojärjestelmän tietoturvallisuus ennen sen käyttöönottoa.
- Sovelluskehityksestä vastaavat sosiaali- ja terveysministeriö sekä Terveyden ja hyvinvoinnin laitos. Kyberturvallisuuskeskuksen tehtävänä on arvioida sovellus.
- Lue lisää:
  https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_101+2020.aspx
  https://www.eduskunta.fi/valtiopaivaasiakirjat/StVM+17/2020
  https://www.eduskunta.fi/valtiopaivaasiakirjat/LiVL+3/2020

Oikeudelliset asiat

- Traficomin suositus kyberturvallisuuden edistämisestä raideliikenteessä annettu 29.6.2020
- Suositus sisältää perustietoa kyberturvallisuudesta raideliikenteessä, tuo esiin keinoja kyberturvallisuusuhkiin varautumiseksi sekä esittää toimenpidesuosituksia, joita raideliikenteen toimijat voivat hyödyntää kyberturvallisuutensa kehittämisessä.

ANALYYSI

- Suosituksen tavoitteena on edesauttaa raideliikenteen kyberturvallisuuden kokonaisvaltaista kehittämistä.
- Traficom suosittelee, että raideliikenteen toimijat huomioisivat suosituksen toimenpiteet 1.6.2021 mennessä.
- Määräaika on yhteensovitettu Traficomin uuden valmiussuunnittelun järjestämisestä liikennejärjestelmästä (TRAFICOM/308489/03.04.04.00/2019) antaman määräyksen sovellettavaksi tulemisen ajankohdan (1.6.2021) kanssa.
- Lue lisää: https://www.traficom.fi/sites/default/files/media/regulation/Suositus%20kyberturvallisuuden%20edist%C3%A4misest%C3%A4%20raideliikenteess%C3%A4.pdf

Arjen kyberturvallisuus – koijausten kesäkuu

Myös kansalaisiin kohdistuu tech support scam -huijauspuheluita

- Koronasta aiheutuneen tauon jälkeen huijauspuheluita soitetaan taas runsaasti. Teknisenä tukena esiintyvä soittaja pyrkii saamaan pääsyn kohteen tietokoneelle.
- Puheluun vastaaminen ei ole vaarallista. Älä kuitenkaan anna huijarille mitään tietoja tai pääsyä koneelle. Ilmoita onnistuneista huijauksista Kyberturvallisuuskeskukselle ja tee rikosilmoitus.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vaarennettyja-puheluita-teknisen-tuen-nimissa

Ohjeet hyvän salasanan tekemiseen: pidempi parempi!

- Eri palveluissa on tärkeää käyttää yksilöllisiä salasanoja. Pitkä salasana, esimerkiksi kokonainen lause, on turvallisin.
- Tutustu uuteen ohjeeseen: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan

Kesälomakaudella esiintyy runsaasti kalastelua ja huijauksia organisaatioissa

- Esimerkiksi laskutus- ja toimitusjohtaja-huijaukset ovat taas lisääntyneet.
- Rikolliset hyödyntävät lomakaudella vähentyneitä henkilöstöresursseja ja kokemattomia työntekijöitä. Varmista, että kaikki työntekijät tuntevat oikeat toimintatavat.
- Lisäohjeita löytyy seuraavalta sivulta.

Kesämyrskyt aiheuttavat verkkohäiriöitä

- Kesäkuun lopun Päivö-myrsky aiheutti häiriöitä ja katvealueita televerkoissa sekä sähkökatkoja eri puolilla Suomea.
- Jos hätäpuhelun soittaminen ei onnistu verkon häiriötilanteessa, sen voi soittaa käynnistämällä kännykän uudelleen ja soittamalla hätäpuhelun, kun puhelin kysyy suojakoodia tai PIN-koodia.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/nain-soitat-hatapuhelun-verkon-hairiotilanteessa

Vietä #KyberturvallinenKesä

Toimitusjohtajahuijauksessa rikollinen lähettää organisaatiolle valelaskun.
Palkanmaksuhuijauksessa rikollinen pyrkii ohjaamaan organisaation työntekijän palkan itselleen.

Vahvistusprosessi

Organisaation olisi hyvä suunnitella erillinen vahvistusprosessi tilitietojen muutoksia varten.

Edelleenlähetys

Organisaation kannattaa rajoittaa sähköpostiviestien edelleenlähetyssääntöjä ja tarkastaa niitä säännöllisesti.

Varmista

Laskun maksaminen kannattaa varmistaa aina erikseen esimieheltä tai kollegalta.

Perehdytä

Kesäsijaiset tulee perehdyttää organisaation laskutuskäytäntöihin perusteellisesti.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

POLIISI
KESKUSRIKOSPOLIISI

Ajankohtaista Kyberturvallisuuskeskuksesta

Uusi normaali -turvallisuusopas poikkeusolojen jälkeiseen aikaan

- Koronakevät jätti jäljen myös nettiarkeemme. Uusi aika vaatii uudistettuja ajattelu- ja toimintatapoja. Kyberturvallisuuskeskuksen uudessa oppaassa jaetaan tietoturva- ja kyberturvallisuus-neuvoja jokaiseen kotiin.
- Oppaan teemoja ovat liikkumisen vapautuminen, ajan viettäminen internetissä, rahojen suojaaminen verkossa, sekä lasten turvallisuus.
- Tutustu: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/turvallisuusopas-poikkeusolojen-jalkeiseen-aikaan

Blogiteksti mobiilisovellusten tietoturvasta

- Traficomin blogitekstissä muistutetaan, että hakkerointi ja muut tietoturvauhkat koskevat myös mobiilisovelluksia.
- Käyttäjän on syytä kiinnittää huomiota sovellusten tietoturvaan. Muista esimerkiksi vertailla vaihtoehtoja, ladata vain virallisista sovelluskaupoista, tarkastella sovellustietoja, päivittää ja tarkistaa asetukset.
- Traficom myöntää tietoturvamerkkejä sovelluksille, jotka täyttävät Kyberturvallisuuskeskuksen asettamat tietoturvavaatimukset.
- https://www.traficom.fi/fi/ajankohtaista/blogit/tietoturva-ykkosjuttu-myos-mobiilisovelluksissa

Vinkit tietotekniikkajätteen tietoturvasta huolehtimiseen

- Tietoteknisten laitteiden kierrättäminen ja uudelleenkäyttö unohtuvat monesti organisaatioiden tiedonhallinnassa.
- Tietotekninen jäte tulee käyttää mahdollisimman pitkälle uudelleen. Huolimattomasti tehtynä uudelleenkäyttö voi kuitenkin kasvattaa tietovuodon riskiä.
- Käytöstä poistettavien laitteiden tiedot tulee tuhota. Tärkeää on myös tunnistaa kaikki laitteet, joihin on tallennettu suojattavia tietoja.
- Lue lisää Kyberturvallisuuskeskuksen julkaisusta: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/hallitse-myos-tietotekniikkajatteen-tietoturvaa

Sinustako arjen kybersankari? – Spoofy-mobiilipeli koululaisille

- Spoofy-mobiilipeli opettaa lomaileville alakoululaisille hauskalla tavalla salasanoihin, yksityisyyteen ja netin käytöstapoihin liittyviä digitaalisen turvallisuuden perustaitoja sekä huijauksilta ja nettikiusaamiselta suojautumista

- CGI:n yhdessä Traficomin ja Valtion kehitysyhtiö Vaken toteuttaman Spoofy-pelin voi ladata ilmaiseksi Google Play -kaupasta ja Applen App Storesta
- **Hyvää kyberturvallista kesää!**

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)