Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuuskeskuksen ajankohtaiskatsaus

Älyliikenteen ja automaation ajankohtaiset

29.5.2020

Virpi Tuulaniemi
erityisasiantuntija
liikenteen kyberturvallisuuden koordinaattori

TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Huhtikuu 2020

Poimintoja

Kybersää huhtikuu 2020

Tietomurrot ja -vuodot

- Office 365 –tietomurtojen määrä on noussut takaisin alkuvuoden tasolle.
- Kalastetulla haltuun saatuja O365 -tunnuksia käytetään myös muihin tietomurtoihin.

Huijaukset ja kalastelut

- Edistyneissä huijauksissa käytetään uhrin oikeita henkilötietoja, tilitietoja, sähköpostia ja tekstiviestejä.
- Kaapattua tiliä käytetään yhdessä salasananpalautustoiminnon kanssa varastamaan monien palveluiden salasanoja.

Haittaohjelmat ja haavoittuvuudet

- Kuukauden aikana paljon kriittisiä haavoittuvuuksia, uusia hyväksikäyttömenetelmiä ja hyökkäykselle alttiita palveluita.
- Älä laiminlyö kriittisiä päivityksiä, varsinkin jos palvelu on avoinna Internetiin.

Automaatio

- Kyberturvallisuuskeskuksen vuosittainen selvitys suomalaisten tietoverkkojen suojaamattomista automaatiolaitteista meneillään.
- Päivittämättömiä laitteita, kuten teollisuusautomaatio- tai lääkintälaitteita on saastunut tunnetuilla haittaohjelmilla.

Verkkojen toimivuus

- Toimivuushäiriöitä oli tavanomaista enemmän ja ne vaikuttivat laajasti.
- Telian internetyhteyksien häiriö 25.4. vaikutti moniin yhteiskunnan toimintoihin.
- Huhtikuu oli palvelunestohyökkäysten osalta rauhallinen.

Vakoilu

- Koronavirukseen liittyviin teemoihin, kuten rokote- ja muuhun tutkimukseen voi kohdistua vakoilua.
- Myös valtioiden päätöksenteko ja sen valmistelu ovat perinteisiä kohteita, jotka ovat ajankohtaisia myös pandemia-aikana.

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

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

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

Vappuvisassa tunnistettiin huijauksia

Kyberturvallisuuskeskus julkisti vappuviikolla leikkimielisen kuvavisailun, jonka takana oli kuitenkin vakava asia: huijauksiin tehdyt tietojenkalastelusivut.

Lähes 3700 vastaajaa yritti tunnistaa kuvista, onko verkkosivu aito vai huijarin tekemä tietojenkalastelusivu. Kuten vastaajat saivat huomata, pelkästä kuvasta on vaikea tunnistaa petkutusta, vaan rinnalle tarvitaan muutakin tietoa.

Lue lisää artikkelistamme: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vappuvisan-tulokset-petkuhuiputusta-vaikea-tunnistaa

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 60 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.

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

CASE

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 päivittäiseen toimintaan. Tämän seurauksena on, että kyberriskit ja niiden vaikutukset aliarvioidaan eikä niiden hallintaan osoiteta riittävästi resursseja.

Oikeudelliset asiat

- Liikenne- ja viestintävirasto Traficom antoi 4.5.2020 uuden määräyksen (M71) verkkotietojen ja verkon rakentamissuunnitelmien toimittamisesta. Määräyksen vaatimukset kohdistuvat sektorirajat ylittäen viestintä-, energia-, vesihuolto- ja liikenneverkkotoimijoihin.

ANALYYSI

- Määräyksen tarkoituksena on ennen kaikkea vähentää maanrakennustöistä verkkoinfrastruktuurille aiheutuvia vikatilanteita sekä edistää verkkojen yhteisrakentamista ja –käyttöä.
- Määräys tulee voimaan 1.6.2020. Fyysistä infrastruktuuria ja aktiivisia verkon osia koskevat velvoitteet tulevat kuitenkin voimaan vasta 1.10.2022, jolloin tietojen tulee olla toimitettu Sijaintitietopalveluun.
- Tutustu tarkemmin määräykseen ja sen perusteluihin: https://www.finlex.fi/fi/viranomaiset/normi/480001/45988

Arjen kyberturvallisuus – huhtikuu on kuukausista hakkeroiduin

Vappuvisa toi esille tunnistamisen vaikeudet

- Kalastelua tehdään käytännössä lähes kaikkien palveluiden nimissä jatkuvasti. Huijausta ei aina voi tunnistaa ulkonäöltä.
- Lue lisää vappuvisan tuloksista: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vappuvisan-tulokset-petkuhuiputusta-vaikea-tunnistaa
- Lue lisää neuvoista epäilyttävien sivujen tunnistamiseksi: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-epailyttavien-sivujen-tunnistamiseksi

Kiristyshuijauksia liikkeellä runsaasti – älä usko huijarien väitteitä

- Huijarit ovat jälleen aktivoituneet aikuisviihdeteemaisten kiristysviestien lähettelyssä.
- Viestit ovat huijausta, eikä huijareille pidä missään nimessä maksaa lunnaita.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kiristyshuijauksia-liikkeella-runsaasti-ala-usko-huijarien-vaitteita

Team Whackin uusi kausi julkaistu

- Ylen dokumenttisarjassa Team Whack - kaikki on hakkeroitavissa, kolme ammattihakkeria paljastaa, kuinka sinunkin elämäsi voidaan sekoittaa.
- Toisella kaudella kohteeksi joutuvat yksityiset älylaitteet, pelistriimi ja vakuutusyhtiö. Tämä kaikki tehdään kohteiden luvalla.
- Tavoitteena ammattihakkereilla on auttaa suojautumaan oikeilta hyökkäyksiltä.
- https://areena.yle.fi/1-4664681

Kutsumattomia vieraita linjalla

- Etäkokouksissa, tapahtumissa ja nettikonserteissa on nähty kutsumattomia vieraita, jotka levittävät haitallista sisältöä tavalla tai toisella.
- Striimaustapahtumia on häiritty ja oikeita linkkejä yritetään vaihtaa hyökkääjien omiin linkkeihin, jotka johtavat kalastelusivuille ja tilausansoihin.
- Etäkokouksen asetukset on hyvä tarkistaa, ettei mukaan pääse kutsumattomia osallistujia: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/valitse-videoneuvotteluratkaisu-kayttotarpeen-ja-tiedon-luottamuksellisuuden-mukaan

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)

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Muuta ajankohtaista Kyberturvallisuuskeskuksesta

Logistiikkatoimialan organisaatioille toimialakohtaista tietoa kyberturvallisuudesta

- **Kyberturvallisuuskeskuksen tilannekuvatuotteet** tarjoavat ajankohtaista tietoa kyberturvallisuuteen vaikuttavista tapahtumista ja ilmiöistä**.**
  - **Viikkoraporttiin** koostamme viikon merkittävimmät tapahtumat ja uutisnostot. Viikkoraportti lähetetään kaikille toimialakohtaisten sähköpostilistojen tilaajillemme.
  - **Tietoturva Nyt!** -julkaisut käsittelevät kyberturvallisuuden ajankohtaisia ilmiöitä ja tapahtumia. Julkaisut lähetetään automaattisesti kaikille toimialakohtaisten sähköpostilistojen tilaajillemme ja lisäksi ne julkaistaan kyberturvallisuuskeskuksen verkkosivuilla.
  - **Kybersää** on kuukausittain ilmestyvä säätiedote, joka antaa kattavan kuvan edellisen kuun kybertapahtumista. Kybersää on ensisijaisesti kohdennettu tietoturvasta vastaaville henkilöille. Liittymällä toimialalistalle, saat uusimman kybersään myös sähköpostiisi.
  - **Varoitukset**-osiossa julkaistaan varoituksia merkittävistä tietoturvauhkista. Varoituksen väri on ilmoitettu julkaisussa. Kun punainen varoitus julkaistaan, sekä käyttäjien että palvelujen ylläpitäjien on ryhdyttävä korjaaviin toimiin välittömästi. Keltainen varoitus puolestaan kertoo tilanteesta, jossa käyttäjien ja ylläpitäjien on noudatettava yleistä varovaisuutta tai valmistauduttava mahdollisiin korjaaviin toimiin.
  - **Haavoittuvuustiedotteiden** avulla välitämme tietoa merkittävimmistä tietoomme tulleista ohjelmistohaavoittuvuuksia.
- Tilannekuvatuotteet saa käyttöönsä liittymällä logistiikkatoimialan organisaatioille tarkoitetulle toimialakohtaiselle sähköpostilistalle.
- Toimialakohtaiselle sähköpostilistalle lähetetään myös tietoa **logistiikkatoimialan kyberturvallisuuteen** liittyvistä muista ajankohtaisista aiheista.
- Toimialakohtaiselle sähköpostilistalle liittymistä voi tiedustella lähettämällä viesti sähköpostiosoitteeseen cert@traficom.fi.
- Lisätietoa tilannekuvatuotteista osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen.

Kyberturvallisuuskeskuksen ohjeita – Turvallinen tuotekehitys

TRAFICOM

TURVALLINEN TUOTEKEHITYS: KOHTI HYVÄKSYNTÄÄ

SECURE DEVELOPMENT – TOWARDS APPROVAL

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/turvallinen-tuotekehitys-kohti-hyvaksyntaa

SISÄLLYSLUETTELO

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Nostoja älyliikenteen kyberturvallisuudesta

ENISA (Euroopan unionin verkko- ja tietoturvavirasto) julkaisuja

https://www.enisa.europa.eu/publications/smart-cars

https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

Haavoittuvuudet

- Älyliikenteenkin ja automaationkin tarvitsemissa järjestelmissä on haavoittuvuuksia, joita on pystyttävä hallitsemaan. Alla ajankohtainen esimerkki.

- CERT-VDE on julkaissut 28.5.2020 kriittisen haavoittuvuuden liittyen Swarco Traffic Systems:n CPU LS4000 -mallisiin kortteihin.
  - Haavoittuvuustiedote CVE-2020-12493 / VDE-2020-016 osoitteessa: https://cert.vde.com/en-us/advisories/vde-2020-016
  - Haavoittuvuus koskee kaikkia CPU LS4000 -järjestelmiä versiosta G4:Sta alkaen.
  - Avoimen hallinnointi/ylläpitoportin (debug-portti) kautta kuka vaan voi päästä laitteelle pääkäyttäjän (root) oikeuksilla.
  - CERT-VDE:n mukaan Swarco Traffic Systems on julkaissut haavoittuvuuteen korjaavan päivityksen.

Kokemuksia kyberturvallisuuden huomioimisesta

- Millaisia kokemuksia kyberturvallisuuden huomioimisesta on kokeiluhankkeissa saatu?
- Informaatiota asiasta otetaan mielellään vastaan sähköpostitse osoitteella virpi.tuulaniemi@traficom.fi

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kiitos!

virpi.tuulaniemi@traficom.fi

https://www.kyberturvallisuuskeskus.fi/