TLP:WHITE

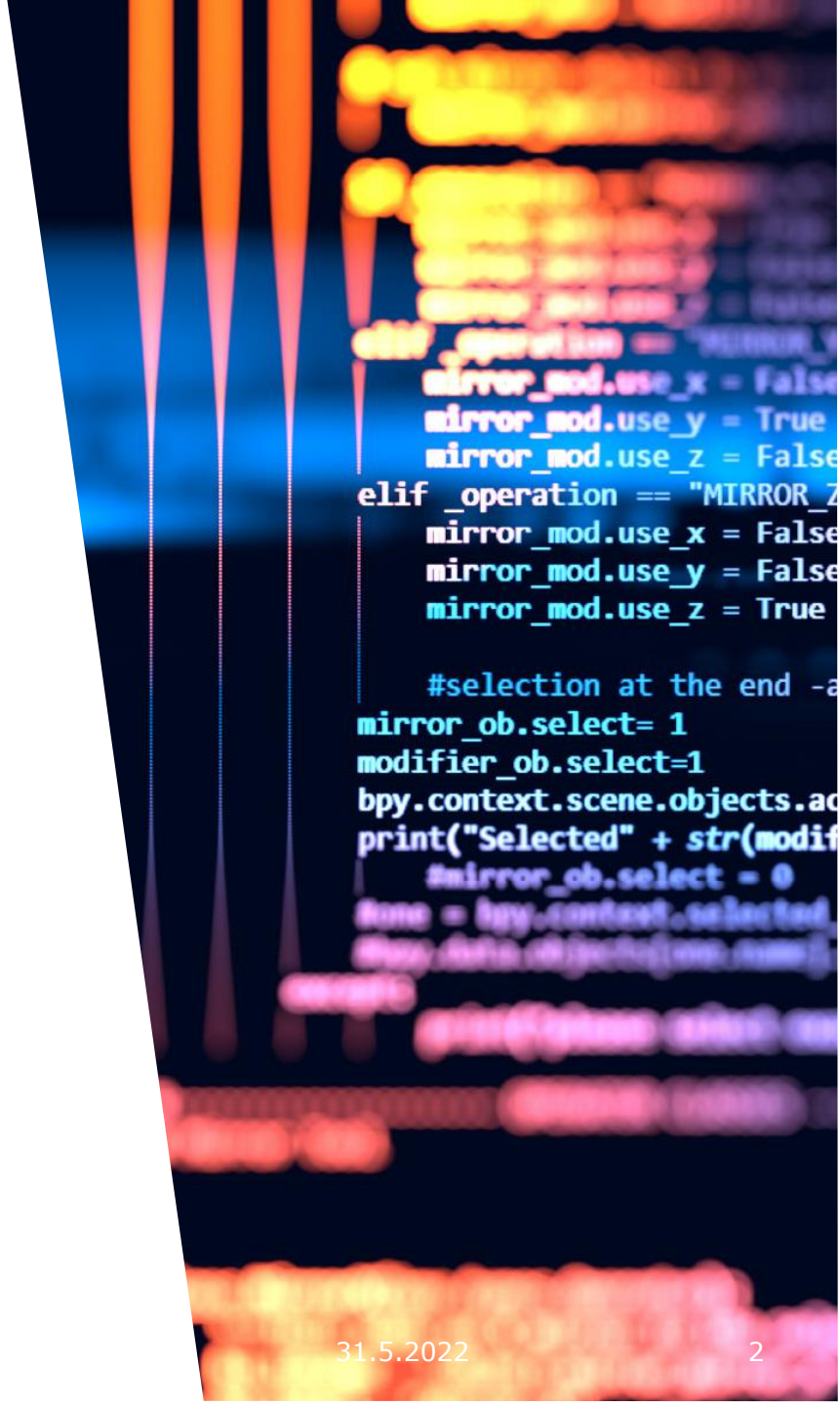
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Matkailualan kyberturvallisuus

Perttu Halonen
31.5.2022

Kyberturvallisuuskeskus

- Tuotamme tilannekuvaa asiakkaillemme päätöksentekoa tukemaan ja tiedolla johtamisen tarpeisiin.
- Olemme tukena rakentamassa maailman toimivinta ja turvallisinta digitaalista yhteiskuntaa.
- Huolehdimme, että suomalaisilla on käytössään toimintavarmat ja tietoturvalliset verkot ja palvelut.
- Turvaamme yhteiskunnan elintärkeitä toimintoja kyberturvallisuusuhkilta.
- Tarjoamme kansalaisille ajankohtaista ja luotettavaa tietoa kyberturvallisuudesta.
- Toimimme läheisessä yhteistyössä eri viranomaisten, yritysten, järjestöjen, kansainvälisten kumppanien kanssa ja oppilaitosten kanssa.



CERT

- Computer Emergency Response Team
- CERT-toiminnon tehtävänä on
  - ennaltaehkäistä tietoturvaloukkauksia
  - tiedottaa tietoturva-asioista.
- CERT-toiminnan tavoitteena on
  - yleisten viestintäverkkojen ja viestintäpalveluiden turvallisen ja häiriöttömän toiminnan varmistaminen
  - yhteiskunnan elintärkeiden toimintojen turvaaminen.
- CERT-palvelustamme saat apua tietoturva-asioissa. Yleisen tietoturvatietouden lisäksi voimme auttaa vakavien tietoturvaloukkausten teknisessä selvityksessä.
- Ota yhteyttä: cert@traficom.fi
- Ilmoita meille: https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

Palvelulupaus tietoturvaloukkauksissa

Neuvomme
vahinkojen rajoittamisessa

Autamme
loukkauksen analysoinnissa

Tuemme
palautumis-toimenpiteissä

Keräämme
lisätietoja Suomesta ja maailmalta

Varoitamme
muita mahdollisia uhreja

Koordinoimme
haavoittuvuuksien korjaamista

Luottamuksellisesti ja maksutta

Kyberturvallisuutta uhkaavia toimijoita ja motiiveita

Päivittäinen kyberrikollisuus	•Tavoite: mahdollisimman nopea ja helppo rahan ansaitseminen •Hyökkäykset täysin opportunistisia tai lievästi kohdennettuja •Keinot vaihtuvat hitaasti, kohteet nopeasti
Aatteellinen hakkerointi	•Tavoite: aatteen edistäminen tai hyökkäyksen kohteen nolaaminen •Motiivina esimerkiksi koronarajoitusten vastustaminen •Voi olla myös pahantahtoinen sisäpiiriläinen.
Satunnainen hakkeri	•Tavoitteita: Omien taitojen kartuttaminen. Ansainta haavoittuvuuksista ilmoittamisella. •Motiiveita: Uteliaisuus. Maailmanparannus. •”Oho, pääsin sisälle. Mitäs nyt?”
Vakoilu ja strateginen vaikuttaminen	•Tavoite: Valtioiden strategisten tavoitteiden edistäminen •Kohde pysyy, keinot vaihtelevat
”Luonto kostaa”	•Laaja tietoliikenteen häiriö tai sähkökatko, aurinkomyrsky •Inhimillinen virhe ilman pahantahtoista tarkoitusta

Kybersää huhtikuu 2022

Tietomurrot ja -vuodot

- Kuntien ja kaupunkien sähköpostitileille on murtauduttu ja tileiltä on lähetetty runsaasti kalasteluviestejä.
- Sosiaalisen median tileihin kohdistuu edelleen tietomurtoja ja niiden yrityksiä.

Huijaukset ja kalastelut

- Fenton-huijauksissa lähetettiin tuhansittain valheellisia työtarjouksia ja houkuteltiin pyramidihuijaukseen.
- Wallpaperga-huijausviesteissä uhri huijataan klikkaamaan linkkiä, jolla perutaan maksullinen tilaus.

Haittaohjelmat ja haavoittuvuudet

- Kyberturvallisuuskeskus on jälleen saanut muutamia havaintoja Emotet-haittaohjelmasta.
- Tekstiviestien välityksellä leviävä FluBot-mobiilihaittaohjelma on aktivoitunut jälleen Suomessa.

Automaatio ja IoT

- Nähtävissä on useita merkkejä, että kyberhyökkäykset automaatiojärjestelmiin tulevat lisääntymään.
- Älykkäiden valaistusjärjestelmien valmistaja meni konkurssiin - käyttäjät eivät pysty enää säätämään valojaan.

Verkkojen toimivuus

- Kahdeksan merkittävää vikaa.
- Verkot toimivat edelleen normaalisti ja tilanne on hyvä.
- Palvelunestohyökkäykset valtionhallintoon puhuttivat.

Vakoilu

- Kyberhyökkäysten määrä on Ukrainassa moninkertaistunut sodan aikana. Myös teollisuusautomaatio on hyökkäysten kohteena.
- Lukuisat APT-ryhmät ovat huhtikuussa jatkaneet länsimaihin kohdistuvaa vakoilua. Ryhmät hyödyntävät vakoilussa muun muassa Ukrainan sotaa.

Julkaisimme varoituksen 1/2022 FluBot-haittaohjelmaa levitetään jälleen tekstiviestitse

- Julkaisimme keltaisen varoituksen 10.5.2022.
- FluBot-haittaohjelmakampanja on aktivoitunut jälleen. Kyberturvallisuuskeskus on vastaanottanut runsaasti ilmoituksia aiheesta.
- Haittaohjelma on kohdistettu Android-laitteille. Haittaohjelman tarkoitus on varastaa tietoja laitteelta ja sitä levitetään tekstiviestien ja multimediaviestien kautta.
- Viestin teemana voi olla esimerkiksi saapunut ääniviesti, vastaamaton puhelu tai ilmoitus saapuneesta lähetyksestä. Viestissä käyttäjää pyydetään avaamaan linkki.
- Huijausviesteissä olevia linkkejä ei tule avata. Pelkkä linkin avaaminen ei vielä asenna haittaohjelmaa laitteelle.
- Lue lisätietoja ja tarkemmat ohjeet: https://www.kyberturvallisuuskeskus.fi/fi/varoitus_1/2022

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen. Digitaalisuus läpileikkaa koko organisaation toimintaa ja muutokset kansainvälisessä turvallisuustilanteessa vaikuttavat merkittävästi organisaation jatkuvuuteen ja riskienhallintaan.

2

Puutteellinen tiedonvaihto heikentää kyberturvallisuuden kokonaistilannekuvaa. Organisaation kohtaama kyberuhka saattaa kohdata toisia organisaatioita seuraavana päivänä.

3

Päivittämättömät haavoittuvuudet avaavat rikollisille reitin organisaatioon. Haavoittuvuuksien hyväksikäyttö on nopeaa. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja joiden suojaustoimet ja ylläpito ovat puutteellisia.

Symbolit

Uusi

Päivitetty

4

Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille! Tarve kyberturvallisuuden osaajille monipuolistuu uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisää entisestään tarvetta osaajille.

5

Käyttöoikeudet ovat avaimet organisaatioon. Käyttöoikeuksien kontrollointi on organisaatioissa tärkeää. Erilaisia hyökkäyskeinoja voidaan hyödyntää tunnusten haltuun saamiseksi, jolla voi olla merkittävä vaikutus organisaation toiminnalle tunnusten ollessa väärissä käsissä.

Tietomurrot ja -vuodot

- Sosiaalisen median tilit tietomurtojen kohteena.
  - Yksityisten kansalaisten, yrittäjien ja yritysten Facebook- ja Instagram-tilejä on aktiivisesti kalasteltu ja kaapattu.
  - Organisaatioiden olisi hyvä muistuttaa työntekijöitään ottamaan käyttöön monivaiheinen tunnistautuminen myös työn ulkopuolisissa asioissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi
  - Työntekijän tilillä saatetaan myös hallinnoida organisaation virallista tiliä.

Analyysi

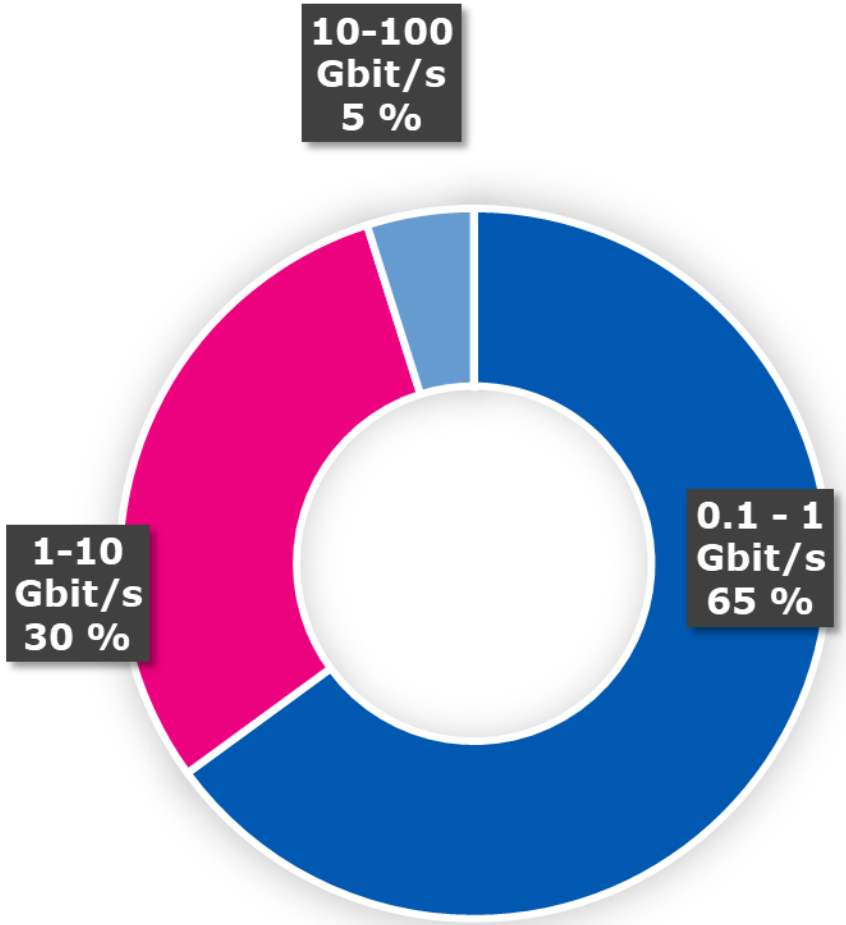
- Murrettuja sosiaalisen median tilejä voidaan käyttää petoksen tekemiseen tai johtamaan muita ihmisiä harhaan.
- Kaupallisessa käytössä olevat tilit, joilla on paljon seuraajia voivat joutua rikollisten kiinnostuksen kohteeksi myös taloudellisten motiivien vuoksi.
- Omia tunnuksia tai salasanoja ei tulisi luovuttaa muiden käyttöön. Myös monivaiheinen tunnistautuminen on tärkeä turvallisuutta parantava ominaisuus.

Tietomurrot ja -vuodot

- Tietosuojavaltuutetun toimisto on vastaanottanut kaksi ilmoitusta helsinkiläishotelleihin kohdistuneista tietoturvaloukkauksista.
  - Vuotaneita tietoja ovat tietosuojavaltuutetun toimiston tämänhetkisen tiedon mukaan ainakin asiakkaan nimi, syntymäaika, yhteystiedot sekä tietoja virallisista asiakirjoista: https://tietosuoja.fi/-/tietosuojavaltuutetun-toimisto-on-vastaanottanut-kaksi-ilmoitusta-helsinkilaishotelleihin-kohdistuneista-tietoturvaloukkauksista-tutustu-neuvoihin-tietovuodon-kohteeksi-joutuneille
  - Tutustu neuvoihin tietovuodon kohteeksi joutuneille: https://tietosuoja.fi/-/neuvoja-tietovuodon-kohteeksi-joutuneille

Palvelunestohyökkäysten tunnuslukuja

- 126 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q1/2022.
- Noin 75% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit
(Q1/2022 - tilasto päivitetään kvartaaleittain.)

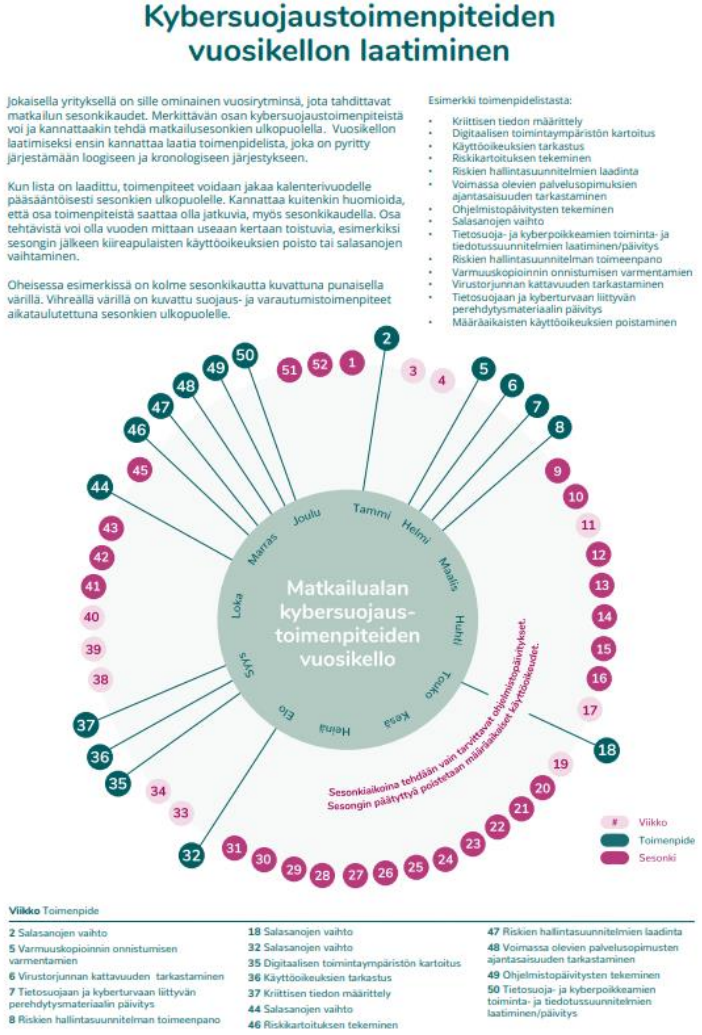
Matkailualan hyvät kyberturvallisuuden käytännöt

1. Tunnista ja listaa yrityksen toiminnan kannalta kriittinen tieto
2. Kartoita yrityksen digitaalinen toimintaympäristö ja listaa siihen kuuluvat järjestelmät
3. Varmista tietojen varmuuskopiointi
4. Asenna haittaohjelmien torjuntasovellus ja viimeisimmät ohjelmistopäivitykset
5. Selvitä yrityksen käyttämien ulkoisten palveluiden tietosuojaan ja kyberturvallisuuteen liittyvät vastuut ja velvollisuudet

Lähde: https://visitjyvaskyla.fi/professionals/wp-content/uploads/sites/2/2021/09/10-kohtaa-kyberturvallisuuden-parantamiseksi-matkailualalla.pdf

Matkailualan hyvät kyberturvallisuuden käytännöt

6. Laadi toimintaohjeet tietomurtojen tai tietosuojaloukkausten varalle
7. Ota käyttöön vahvat salasanat ja poista oletussalasanat käytöstä
8. Varaudu mobiililaitteiden anastamiseen tai häviämiseen
9. Vastuuta yrityksestä yksi henkilö huolehtimaan yrityksen tieto- ja kyberturvallisuudesta
10. Laadi yrityksen riskikartoitus ja kirjallinen riskienhallintasuunnitelma



Tapaus: Majoitusliikkeen tietomurto

Tapaus: Majoitusliikkeen tietomurto

- Suomalainen majoitusyritys ilmoitti varausten välityspalveluun kohdistuvasta tietomurrosta, joka mahdollisesti vaaransi asiakkaiden varaustietoja.
- Hotellin tunnuksilla päästiin kirjautumaan välityspalveluun, jolloin asiakkaiden tietoja päätyi vääriin käsiin. Luottokorttitietoihin pääsy vaati erillisen kertakäyttöisen koodin, joka niin ikään päätyi vääriin käsiin. Verkkorikolliset pääsivät käsiksi yli sataan luottokorttitietoon.
- Selvitystyössä kävi ilmi, että varaustietoja käsiteltiin vastaanotossa olevalta koneelta, jolla mm. varattiin takseja, konsertti- ja muita lippuja jne. Kyseiseltä koneelta käytiin myös sähköpostipalvelussa, jonne kertakäyttöinen koodi lähetettiin.

Tapaus: Majoitusliikkeen tietomurto

- Vastaanoton tietokoneeseen oli asentunut etäohjelma, jonka avulla verkkorikolliset saivat haltuunsa luottokorttimaksuihin tarvittavat tiedot.
- Ainoastaan luottokorttiyhtiön automatisoitu järjestelmä esti tässä tapauksessa suuremmat vahingot.
- Asennettiin uusi erillinen kone varaustietojen käsittelyyn. Kaikki salasanat ja osa käyttäjätunnuksista uusittiin.
- **Tapauksen opit:**
  - Pidä maksutietoja käsittelevät tietokoneet päivitettynä (ml. tietoturvatuotteet)
  - Älä käytä maksutietojen käsittelyyn käytettävää järjestelmää yleiseen internet-selailuun tai anna asiakkaiden käyttää konetta.
  - Toteuta monivaiheinen tunnistautuminen oikein.

https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

cert@traficom.fi

kyberturvallisuuskeskus@traficom.fi

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

TLP:WHITE