

Ajankohtaista kyberturvallisuudesta

*Leo Niemelä, tietoturvaajohtaja
LähiTapiola*



Kyberturvallisuus tänään

- Valtioilla on rajat, mutta internet ei tunne rajoja
- Uhka joka on toisella puolella maailmaa on uhka myös Suomessa
- Kyberuhkat ovat opportunistisia – kohteeksi voi joutua kuka tahansa
- Kyberturvallisuusuhkat koskettavat kaikkia toimialoja ja yrityksiä aina yhdistyksistä suuryrityksiin
- Laitteet, järjestelmät ja kodinkoneet menevät verkkoon
- Korona-aika on nostanut kyberturvallisuuden uhkia merkittävästi



Suurimmat uhkat

- Megatrendi 2020 on tehdä kyberrikoksilla rahaa
- Toimitusjohtaja- ja laskutushuijaukset
- Microsoft O365 -huijaukset
- Erilaisia korona-aiheisia kalastelu- ja huijausviestejä sähköpostilla, tekstiviesteillä ja Whatsup –viesteillä
- Kiristyshaittaohjelmat kasvaneet COVID-19 aikana

Lähtettäjä: Koponen Juha <ss2716003@tutanota.com>

Lähetetty: keskiviikko 18. marraskuuta 2020 12.41

Vastaanottaja: [REDACTED]

Aihe: Anssi

Hei Anssi

Oletko vapaa tällä hetkellä?

Kiitos.

Lähetetty iPadiltani

Lähtettäjä: Genesis Vazquez <christopher.d62@aol.com>

Lähetetty: tiistai 17. marraskuuta 2020 19.40

Vastaanottaja: [REDACTED]

Aihe: Contract No 7276 information

Hello.

https://docs.google.com/document/d/e/2PACX-1vRVWSTpwy6PhVnpcRXqkpMbqej7ccvzvPysnqAMut275ynHVjP-ApSawN5-TNiSaay-aPi-M_xOtT0j/pub

Most sincerely, Genesis Vazquez

COVID-19 - Huomioitavaa nyt ja korona-ajan jälkeen

- Dokumentoi IT-ympäristön muutokset
 - On tärkeää tietää mitä muutoksia korona-aikana on tehty, jotta niistä ollaan tietoisia ja niistä muistetaan tarvittaessa palautua
- Varmistu organisaation etätyöratkaisujen turvallisuudesta
 - Nopealla aikataululla pystytetyt etätyöratkaisut voivat yhä sisältää tietoturvariskejä organisaatiolle
- Huolehdi henkilöstön koulutuksesta ja tiedottamisesta
 - Töiden siirryttyä etätöiksi henkilöstön omilla toimilla voi olla entistä suurempi merkitys ja tiedottaminen korona-aikana korostuu
- Paluu koronaa edeltävään aikaa ei välttämättä toteudu
 - Korona-ajalle tehdyt ratkaisut ja omaksutut työtavat voivat jäädä elämään osaksi organisaation toimintaa
- Taloustilanteen heikentyminen voi vaikuttaa organisaation investointeihin
 - Kyberturvallisuudessa saatetaan vaatia investointien priorisointia ja voidaan keskittyä ainoastaan tärkeimpiin uudistuksiin

Pienet teot merkitsevät paljon

1. Pidä ohjelmistot ja järjestelmät päivitettyinä
2. Käytä monivaiheista tunnistautumista
3. Älä käytä samoja salasanoja useammassa eri palvelussa
4. Muista varmuuskopiot

Ota salasanat haltuun: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Salasanat_haltuun.pdf

Miten varmistaa liiketoiminnan jatkuvuus tietoturvapoikkeamassa?

- Ota yhteyttä Kyberturvallisuuskeskukseen:
<https://www.kyberturvallisuuskeskus.fi/fi/ilmoita>
- Tee rikosilmoitus Poliisille
<https://poliisi.fi/tee-rikosilmoitus>
- Varmista lokitietojen saatavuus
<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja>
- Muista viestintä asiakkaille, yhteistyötahoille ja julkisuuteen. Muistakaa avoimuus ja läpinäkyvyys.
- Harkitse pk-yrityksille suunnatun kyberturvapalvelun hankintaa. Palvelu sisältää kybervakuutuksen, koulutuksen sekä puhelinpalvelun.
<https://www.lahitapiola.fi/yritys/vakuutukset/omaisuus-ja-toiminta/kybervakuutus>

Tavoitteena positiivinen kyberturvallisuuden kulttuuri

- Tärkeintä ei ole päämäärä vaan matka
- Tietoturvasuus on sopiva sekoitus teknologiaa ja ihmisiä
- Ei-syyllistävä tietoturvakulttuuri avain menestykseen
- Ennakkoasenteena optimismi





facebook.com/lahitapiola
twitter.com/Lahi_Tapiola
instagram.com/lahitapiola_lokaltapiola/
linkedin.com/company/l-hitapiola
youtube.com/user/TapiolaGroup



Turvallisuus • Talous • Terveys