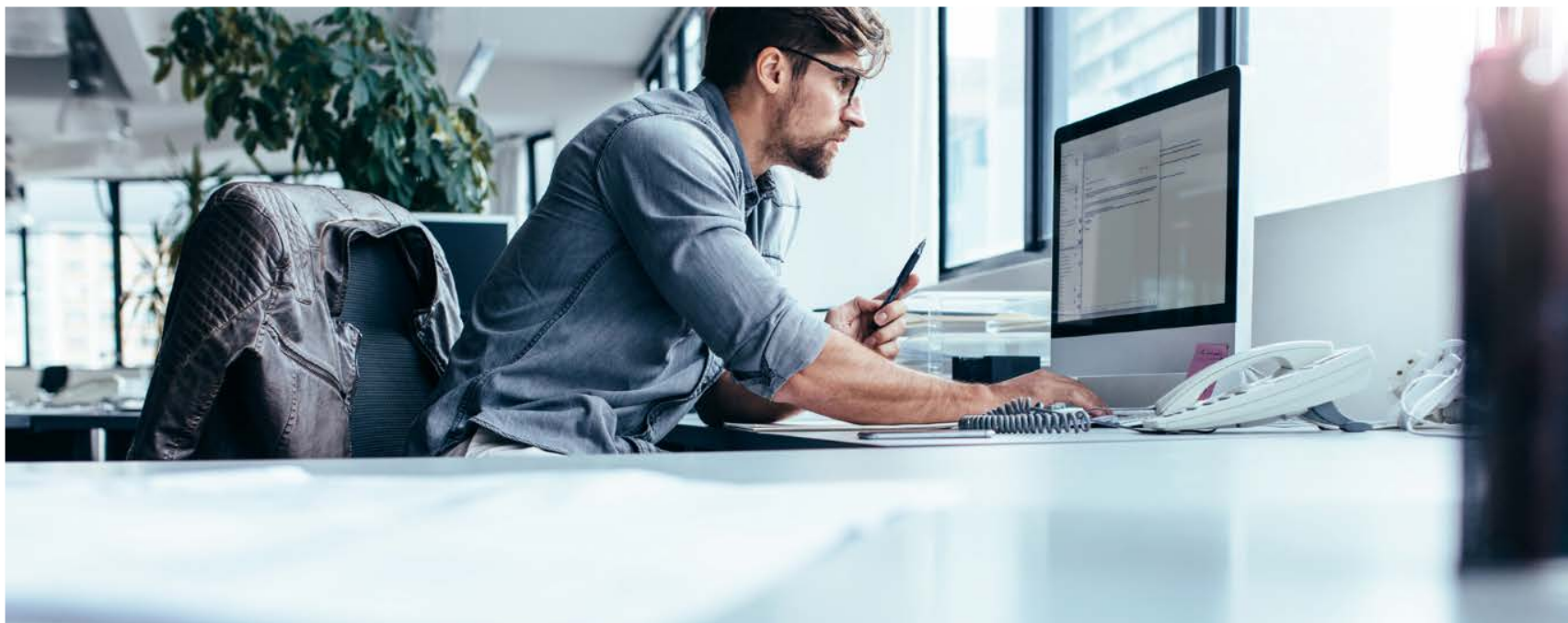




Kyberturvaopas





Kyberturva – Kyberturvalla tarkoitetaan digitaalisen tiedon ja toiminnan turvaamista.

Tietoturva – Tietoturvalla tarkoitetaan tiedon turvaamista. Digitaalisen tiedon osalta tietoturva on osa kyberturvaa.

1. Yrityksesi virustentorjuntaohjelmistot

MAKSULLISESTA PALVELUSTA SAAT APUA ONGELMATILANTEISIIN

Ilmainen tietoturva tuntuu helpolta ratkaisulta, mutta muista, että ilmaiset tietoturvat rahoittavat toimintaansa mainonnalla eivätkä välttämättä takaa kunnon suojaa.

Maksulliset tietoturvatuotteet sen sijaan sisältävät mm. suojan erilaisten tiedostojen lukitsevien haittaohjelmien varalle (toiselta nimeltään kiristyshaittaohjelma tai englanniksi Ransomware), pankkitoimintojen suojauksen sekä selauksen suojauksen. Ilmaisista versioista nämä puuttuvat lähes aina.

Maksulliset toimijat kehittävät jatkuvasti tuotteitaan ja reagoivat uusimpiin tietoturvauhkiin, ja heiltä löytyy tuki myös ongelmatilanteiden varalle. Ilmaiset tietoturvatoimijat tarjoavat harvoin asiakas- ja tukipalveluita.

TURVAA KAIKKI KONEET JA PALVELIMET

Kaikki tietokoneet – sekä Windows- että Mac-koneet – ja palvelimet on syytä turvata nykyaikaisella tietoturvasovelluksella.

Mobiililaitteet ovat henkilöstön henkilökohtaisimpia ja käytetyimpiä laitteita. Näissä laitteissa on usein enemmän tietoa yrityksestä kuin muualla: sosiaalisen median sisällöt, valokuvia, videoita, sähköposteja, tekstiviestejä jne.

Mobiililaitteilla käytetään myös verkkopankkia ja tehdään verkko-ostoksia. Kaiken tämän vuoksi niiden suojaaminen on tärkeää.

Onko yrityksesi tietokoneisiin ja mobiililaitteisiin asennettu virustentorjuntaohjelmisto?

2. Fyysinen tietoturva

MUKANA KULJETETTAVAT LAITTEET OVAT RISKI

Nykyaikana työkalut – mm. kannettavat tietokoneet ja älypuhelimet – kulkevat työntekijän mukana koko ajan. Nämä laitteet voivat helposti unohtua jonnekin tai ne voidaan varastaa, ja näin niiden sisältämät tiedot voivat päätyä väärin käsiin.

Myös kaikki salasana- ja erilaiset pääsykoodit kannattaa pitää kunnossa ja turvassa (lue lisää kohdasta 4).

LAITTEET POIS NÄKYVISTÄ

Laitteita ei koskaan kannata jättää valvomattomaan tilaan, esim. autoon. Myös työpaikalle jätettävä kannettava kannattaa laittaa yöksi pois näkyvistä, esim. lukittuun kaappiin.

Käytöstä poistetut laitteet tulee hävittää asianmukaisesti, muistit tyhjennettynä. Tähän voi käyttää esim. kovalevysilppuria.

Onko yrityksesi koneiden ja laitteiden fyysinen tietoturva kunnossa?

3. Varmuuskopiot

KOPIOIMALLA TURVAAT TOIMINNAN JATKUVUUDEN

Yritykseen tehdyn kybermurron yhteydessä voidaan lukita tai hävittää yrityksen häiriöttömän toiminnan kannalta tärkeitä tietoja.

Helpoin tapa saada tiedostot takaisin, on huolehtia siitä, että materiaalista on tehty varmuuskopiot ja kopioida ne takaisin käyttöön.

Varmuuskopiot ovat nimensä mukaisesti "varmuuden varalle tehdyt kopiot tiedostoista".

VARMISTA KYLLIN USEIN

Yrityksen kriittiset tiedot on hyvä varmuuskopioida päivittäin, vähintään viikoittain.

Huomaathan, että pilvipalveluun synkkaaminen (google drive, Microsoft onedrive jne.) ei ole sama asia kun varmuuskopiointi, sillä tuhottu tai lukittu tiedosto synkkautuu tuhottuna tai lukittuna myös pilvipalveluun.

Tehdäänkö varmuuskopiointi yrityksessäsi kyllin usein?

4. Salasanojen hallinta

MYÖS SALASANALLA SUOJAAT YRITYKSEN TIETOJA

Tutkimusten mukaan 63 % vahvistetuista tietomurroista johtui:

- heikoista salasanoista
- varastetuista salasanoista
- oletussalasanoista.

Hyvän salasanan luominen ei ole vaikeaa. Nykyaikainen digitaalinen yhteiskunta tekee siitä kuitenkin vaikeaa, koska jokaiseen palveluun pitäisi pystyä luomaan hyvä ja uniikki salasana.

HYVÄ SALASANA EI AUKENE MUILLE

Hyvä salasana on riittävän pitkä (12 merkkiä). Siinä on numeroita, ISOJA ja pieniä kirjaimia sekä erikoismerkkejä.

Salasanoja ei kannatta kierrättää, vaan kaikkiin palveluihin tulee luoda omat uniikit ja vahvat salasanat.

Jos mahdollista, ota kaikissa tärkeissä palveluissa kaksivaiheinen tunnistus käyttöön. Kaksivaiheisessa tunnistuksessa palveluun kirjaudutaan salasanan lisäksi jolloin muulla keinolla, esim. erillisellä tekstiviestinä saatavalla kertakäyttöisellä pin-koodilla.

Onko yrityksesi salasanakäytännöt kunnossa?

5. Langattoman lähiverkon suojaus

PALOMUURI SUOJAA ULKOISILTA UHKILTA

Yritystoiminnassa lähiverkon suojaus on selvästi tärkeämpää kuin kotikäytössä.

Salauksen tulisi olla vähintään WPA2-tason suojaus. Salauksen suojataso määritellään lähiverkon reitittimen asetuksista. WPA2 on tällä hetkellä vahvin käytössä oleva suojataso

Julkiset avoimet langattomat verkot (WiFi-hotspot) ovat usein suojaamattomia, mikä tarkoittaa sitä, että samaa verkkoa käyttävät ulkopuoliset henkilöt voivat avoimen verkon kautta saada pääsyn yrityksenne työntekijän käytössä oleviin laitteisiin tai verkkoliikenteeseen.

Verkon liikennettä ja ulkoverkosta tulevia uhkia voi ehkäistä erillisellä palomuurilla tai muulla luotettavien toimijoiden tarjoamilla palveluilla.

ESTÄ VERKKOLIIKENTEEEN KUUNTELU SALASANALLA

Langattoman verkon suojaaminen salasanalla estää verkkoliikenteen kuuntelun ja ulkopuolisten liittymisen verkkoon.

Jos verkkoliikenne itsessään ei ole salattua (https), voidaan langattomasta verkosta lukea sähköposteja, käyttäjätunnuksia tai muita tietoja.

Onko langaton lähiverkkonne (wlan/wifi) suojattu salasanalla?

6. Säännölliset ohjelmistopäivitykset

MYÖS SALASANALLA SUOJAAT YRITYKSEN TIETOJA

Tutkitusti voidaan sanoa, että lähes kaikissa onnistuneissa tietomurroissa hyökkäys on onnistunut, koska yrityksen perusasiat on hoidettu huonosti.

Kyberturvallisuuden näkökulmasta onkin tärkeää, että yritysten laitteiden käyttöjärjestelmät ovat ajan tasalla ja niissä käytettävien sovellusten päivitykset ovat myös kunnossa.

PÄIVITÄ OHJELMISTOT AUTOMAATTISESTI

Salli käyttöjärjestelmän ja ohjelmistojen automaattiset päivitykset. Myös palomuurien asetukset tulee tehdä huolella ja ylimääräiset portit sulkea.

Onko ohjelmistopäivitykset tehty säännöllisesti?

7. Huijausten tai kalastelun tunnistaminen

HUIJARI NÄYTTÄÄ LUOTETTAVALTA TOIMIJALTA

Verkossa huijaukset on usein tehty hyvällä suomen kielellä ja jonkun tunnetun brändin nimissä. Käyttäjä luottaa brändiin, eikä välttämättä näe huijauksen läpi.

Tyypillisessä huijauksessa varastetaan luottokorttitietoja, salasanoja, käyttäjätunnuksia tai pankkitunnuksia.

Tietojen kalastelussa päätelaite ei välttämättä saastu, koska tieto urkitaan itse käyttäjältä eikä päätelaitteesta.

Kohdistetuissa hyökkäyksissä tarkoitusperät saattavat olla vielä syvempiä.

EPÄILYTTÄVÄ LINKKI KIEHTOO KÄYTTÄJÄÄ

Vaikka käyttäjä epäilee linkin turvallisuutta, niin jopa puolet käyttäjistä klikkaa sitä kuitenkin. Tietämyksen lisäämisellä, terveellä epäluulolla ja kouluttamisella voidaan selvästi vaikuttaa huijausviestien tehoon.

Kohdistetuissa hyökkäyksissä voidaan esimerkiksi:

- vedota tuttuun tai huomiota herättävään lähettäjään
 - pelotella auktoriteetilla, esim. oman toimittajan tai asiakasyrityksen johtajan nimissä
 - uhata jollain kovalla toimella, esim. tunnusten sulkemisella
-

Onko yrityksessäsi mietitty, kuinka tunnistetaan vaikka laskuhuijaukset tai tunnusten kalastelu?

8. Kiristyshaittaohjelma

KIRISTYSHAITTAOHJELMA SAASTUTTAA TIETOKONEEN

Yleisimmät haittaohjelmistot ovat viime vuosina olleet erilaiset kiristysohjelmat (ns. Ransomware). Kiristysohjelma on haittaohjelma, joka saastuttaa tietokoneen, lukitsee sen tai sen sisältämät tiedostot, ja vaatii lunnaita lukituksen purkamiseksi.

Tiedostoja ei saa auki ilman salauksen purkuavainta, joka palauttaa tiedostot takaisin entiselleen. Purku-avainta vastaan pyydetään lunnaita. Rikolliset vaativat usein lunnaat Bitcoineina ja summa vastaa yleensä 300–500 € per laite.

TEHOKAS SUODATUS ESTÄÄ SAASTUMISEN

Tehokas DNS-suodatus pystyy estämään 90 % kiristyshaittaohjelmistoista estämällä niiden latautumisen tietokoneelle. DNS-suodatuksella estetään verkkoliikenne sellaisista epäluotettavista osoitteista, joista suurin osa kiristyshaittaohjelmista hakee asennustiedostonsa.

Edistyselliset tietoturvaohjelmistot pitävät sisällään erityisen kiristysohjelma suojauksen, joka antaa lisäsuojaa kiristysohjelma hyökkäyksiä vastaan

Tunnistetaanko yrityksessä kiristyshaittaohjelmat?

9. Sähköpostisuojaus

SUOJAUKSELLA SUODATETAAN MM. VIRUKSIA

Sähköpostin suodatuksella tarkoitetaan kykyä suodattaa tulevista sähköposteista virukset, haittaohjelmat, kalasteluviestit sekä huijausviestit. Tärkeää on, että suodatus pystyy suodattamaan myös väärennetyt sähköpostiviestit.

Erityisesti huijaus- ja kalasteluviestit ovat kasvussa ja kohdentamattomina ne kohdistuvat kaikkiin yrityksiin koosta riippumatta.

DNS-SUODATUS

DNS-suodatuksella voidaan suojata käyttäjien toimia internetissä. Suodatus estää käyttäjiä menemästä haitallisille sivustoille.

Tehokas suodatus voi estää 90 % kiristyshaittaohjelmistoista estämällä niiden komentoyhteydet.

Onko sähköpostisuodatus jo tuttu juttu?

Sanasto

Kyberturva – Kyberturvalla tarkoitetaan digitaalisen tiedon ja toiminnan turvaamista.

Tietoturva – Tietoturvalla tarkoitetaan tiedon turvaamista. Digitaalisen tiedon osalta tietoturva on osa kyberturvaa.

Virus – haittaohjelma, ohjelma joka tavalla tai toisella häiritsee tai haittaa tietojärjestelmän käyttöä

Kiristysohjelma – myös tunnettu nimellä ”Ransomware”, ”Cryptolocker”; haittaohjelma joka lukitse tiedostot. katso kohta 8

IOT – ”Internet of Things”, esineiden internet, internettiin kytketyt koneet ja laitteet joita voidaan hallinnoida netin yli.

Pilvi, Pilvipalvelut – Kielikuvallinen yhteistermi internetin yli käytettäville palveluille, esim. Microsoft OneDrive ja Office Online tai Google Apps.

DNS-palvelin – ”Domain name server”, on internetin nimipalvelujärjestelmä, eräänlainen ”osoitekirja.” DNS muuntaa kirjoitetut osoitteet (www.lahitapiola.fi) numerosarjoiksi (IP-osoitteeksi esim. 193.209.71.53)

URL – ”Uniform Resource Locator”, verkko-osoite esim. www.lahitapiola.fi

Reititin – Reititin yhdistää esim. lähiverkossa olevat laitteet palvelimiin tai internetin. Ns. ”wlan-purkki” on yhden tyyppinen reititin

Tietojen kalastelu – ”Phising”, verkkourkinta, tapa millä epärehellisin keinoin koitetaan saada käyttäjätunnuksia ja salasanoja itselleen.

Kybervakuutus - www.lahitapiola.fi/kybervakuutus

Kiitos

Lue lisää LähiTapiolan tarjoamasta Kyberturvapalvelusta
www.lahitapiola.fi/kybervakuutus



TERVEYS • TURVALLISUUS • TALOUS