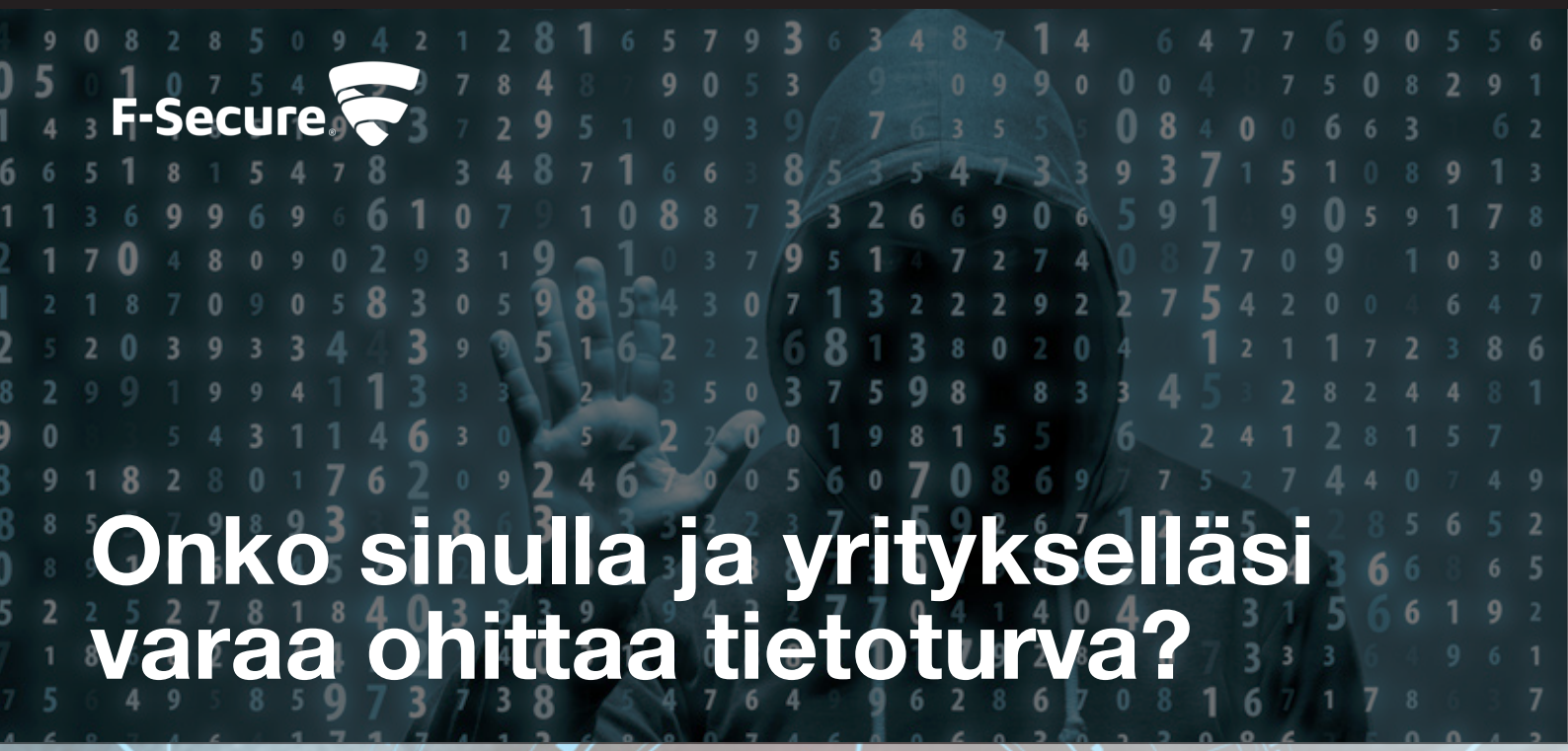


# Onko sinulla ja yrityksellläsi varaa ohittaa tietoturva?

*Yhteenveto webinaarista. Yhteistyössä F-Secure.*

**Viimeisen vuoden aikana maailmassa on tehty vakavia tietoturvahyökkäyksiä, joilla on haavoitettu esim. Yhdysvaltain hallintoa, yhdysvaltalaisen putkiyhtiön öljynjakelua, mikä aiheutti hätätilan 17 osavaltioon, sekä Microsoft Exchange -palvelimia, jolla oli vaikutuksia myös Suomessa. Tämän hyökkäyksen seurauksena erään suomalaisen sähköpostipalveluiden tarjoajan palvelimet olivat poissa käytöstä yli viikon, jolloin myös yrityksen asiakkaiden sähköpostiliikenne oli pysähdyksissä.**

Yksi merkittävämpiä tunkeutumisväyliä yritysten järjestelmiin ja verkkoon ovat haittaohjelmat. Ne leviävät eniten sähköpostien mukana (51 % tapauksista), kun käyttäjät klikkailevat huijausviestien linkkejä, mutta myös käyttäjien itse lataamien ohjelmien mukana (31 %) sekä mainosten (9 %) ja eri ohjelmien mukana (5 %).

F-Securen tutkimuksen mukaan huijausviestien määrä nousi viime vuonna peräti 52,9 prosenttia. Huijausviestien avulla meiltä urkitaan tietoa muun muassa salasanoista ja kirjautumistunnuksia.

Näiden yritysten nimissä lähetetään eniten huijausviestejä: Microsoft, DHL ja Google. (Lähde: Check Point Research issues Q1 Brand Phising Report)

## Myös suomalaisyritykset kiinnostavat rikollisia

Usein hyökkääjät vaativat lunnaita, ja uhrit niitä maksavat. Monesti hyökkääjälle riittää pienikin summa rahaa, sillä rahaa tärkeämpi motiivi on aiheuttaa vahinkoa. Suomalainen pk-yrityskin on hyökkääjille kiinnostava. Esimerkiksi vuonna 2020 suomalaisen varaosaliikkeen järjestelmiin tuli haittaohjelma ja yritys sai hyökkääjältä kiristysuhkauksen. Tämän seurauksena yrityksen liiketoiminta oli muutaman päivän pysähdyksissä.

Printcomin esimerkkitapauksessa, kiristyshaittaohjelma iski suomalaisyritykseen, ja toiminnanohjausjärjestelmään ei enää päässytkään kirjautumaan. Huomattiin, että palvelimet ja tiedot oli kryptattu. Yritys oli kyllä huolehtinut varmuuskopioista, mutta hyökkääjä oli poistanut varmistukset. Myös virustoimintaohjelmistot oli asianmukaisesti asennettu. Yrityksellä oli ollut käytössään vanha palvelu, joka oli tarkoitus uusia lähiaikoina. Tämän vanhentuneen palvelun käyttöjärjestelmän kautta hyökkääjä oli päässyt yrityksen järjestelmiin sisään.

Yritys otti hyökkääjään yhteyttä, joka lupasi tehdä yhteistyötä, mutta halusi vastineeksi rahaa. Samanaikaisesti aloitettiin asentamaan IT-infraa uudelleen ja tutkimaan, mitä haavoittuvuuksia infrassa oli. Tutkimuksissa kävi ilmi, että hyökkääjä oli ollut palvelimilla useamman viikon ajan. Asennuksen jälkeen uudessa ympäristössä oli huomioitu kaikki tarvittavat palvelut, jatkuvat päivitykset ja valvonta.

Toisessa Princomin esimerkissä tunnistettu henkilö oli yrityksen verkossa. Tietoturvahälytys tuli yhdestä laitteesta, jolla yritettiin ottaa yhteyttä eri verkkoalueilla useisiin olemattomiin palveluihin ja osoitteisiin. Kun hälytys tuli, laite eristettiin verkosta. Ongelma loppui siihen. Hälytyksen aiheutti yrityksen ulkopuolinen henkilö, joka oli työskennellyt alihankkijana kyseissä yrityksessä. Tämä henkilö oli saanut oikeudet kytkeytyä yrityksen verkkoon omalla tietokoneellaan. Laitteessa oli ollut haittaohjelma, joka lähti leviämään yrityksen verkossa.

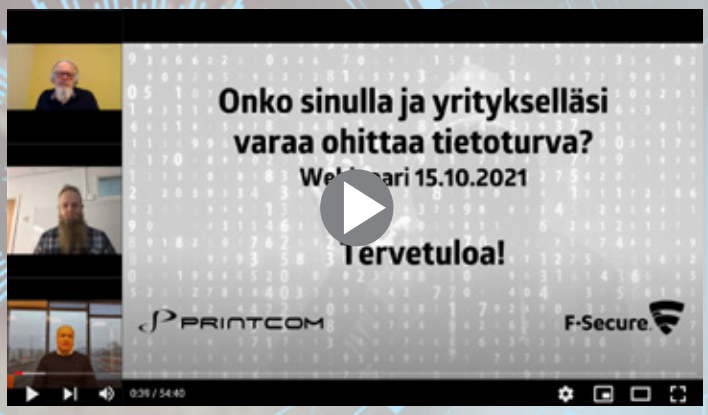
## Ennaltaehkäisevät toimet ovat avain suojaukseen

F-Securen mukaan pk-yritysten päättäjistä 60 prosentilla ei ole strategiaa, miten toimitaan, jos hyökkäys sattuu. Heikoin lenkki tietoturvassa on ihminen. Ensin pitää miettiä riskit yrityksen toiminnassa. Kun riskit on arvioitu, pitää suojata kriittisimmät. Tutkimusyhtiö Gartnerin mukaan tänä vuonna yrityksissä käytetään tietoturvaan 12,4 % enemmän rahaa kuin aiemmin. Sokkona tietoturvaa ei kuitenkaan kannata hankkia. Ratkaisuiden tulee tukea yrityksen toimintaa. Tärkeää on saada koko yrityksen IT-infra sekä laitteet suojauksen piiriin. Verkosta pitää saada myös tietoa, mitä verkossa tapahtuu ja miten käyttäjät verkossa toimivat.

## Puhelimet ovat päätelaitteita ja siis myös hyökkäyksen kohteena

Puhelimessa on sekä henkilökohtaisia että yrityksen sovelluksia. Siihen on myös mahdollista hyökätä, suhteellisen helposti. Esimerkiksi tekstiviestihyökkäyksissä lähettäjän nimi on helppo väärentää. Tällöin tutulta kuulostavan yrityksen viestissä olevia linkkejä klikkaamalla päästetään haittaohjelma puhelimeen. Puhelin on kuitenkin vielä toistaiseksi turvallisempi laite kuin tietokone.

## Katso koko webinaari täältä:




## Printcom auttaa yritystäsi suojautumaan hyökkäyksiltä

Printcomin tietoturva-asiantuntijat kartoittavat mahdolliset haavoittuvuudet sekä puutteet yrityksesi tietoturvassa. Kartoituksen perusteella valitaan teknologiat, joilla suojataan mm. tietojärjestelmiä. Cyber Security Operations Center (CSOC) -asiantuntijatiimimme valvoo yrityksesi tietoturvaa ja on tiiviisti yhteydessä yrityksesi tietoturvaryhmään tai tietoturvasta vastaavaan henkilöön.

**Suosittelemme mielummin enemmän suojausta kuin vähemmän.**
**Jälkikäteen korjaaminen on aina kalliimpaa kuin ennakointi.**

**Ota yhteyttä**

puh. 020 756 2460 | myynti@printcom.fi
printcom.fi

PRINTCOM