

Millaisilla suojakertoimilla työkannettava lähtee lomalle?

Helsinki, 16. kesäkuuta 2009 - Suomalaisten vilkkain lomakausi käynnistyy juhannuksena. Riippumatta siitä, vietetäänkö lomaa kotona vai mökillä, kotimaassa vai ulkomailla, yhä useamman lomavarustukseen kuuluu myös kannettava tietokone. Läppäri saattaa kuitenkin olla työnantajan omaisuutta, jolloin työnantajaa saattaa kiinnostaa, mihin kone on lähdössä ja miten se on suojattu. Entä kuka vastaa koneesta ja sen sisältämästä luottamuksellisesta materiaalista?

”Nyt on hyvä aika tarkistaa, mitä firman turvallisuuspolitiikassa sanotaan työvälineiden käytöstä vapaa-ajalla, sekä muistuttaa lomille lähtijöitä ohjeistuksesta”, sanoo tietoturvayhtiö Stonesoftin tietoturvapäällikkö Joonas Airamo. ”Jos minkäänlaista ohjeistusta ei ole, kannattaa tämä puute korjata viimeistään nyt.”

Stonesoftilla, kuten monessa muussakaan yrityksessä, ei työkoneen käyttöä vapaa-ajalla ole rajoitettu. Näin ollen on tärkeää kiinnittää huomiota siihen, että kone on suojattu asianmukaisesti. Vaikka vastuu läppäristä olisikin loman aikana työntekijällä, mahdollisista väärinkäytöksistä tai varkauksista kärsii viime kädessä yritys itse.

”Vaikka yrityksen oma verkko olisi kuinka hyvin suojattu, ei yhteys sieltä Teneriffan hostellin verkosta välttämättä ole”, Airamo muistuttaa. ”Jälleen kerran kannattaa siis tarkistaa, että ohjelmistojen - erityisesti tietoturvaan liittyvät - päivitykset ovat ajan tasalla ennen lomalle lähtöä. Varkautapausten osalta olisi myös tärkeää, että koneen sisältö, eli käytännössä koneen kovalevy, on oletusarvoisesti aina salattu. Tällöin varas ei saa käyttöönsä yrityksen tietoja, vaikka läppäri saisikin. Ensisijaisen tärkeää koneen salauksessa on kuitenkin käyttää riittävän vahvoja salasanoja. Heikko salasana on helposti murrettavissa, jolloin koko salaus menettää merkityksensä.”

Yritysten olisi hyvä ohjeistaa työntekijänsä alun alkaenkin niin, että kannettavan koneen kovalevyllä ei tallenneta tarpeettomasti yrityksen luottamuksellisia tietoja, vaan pääosin tällainen materiaali säilytetään sisäisillä verkkolevyillä.

Ennakoimalla selviää tietoturva-asioissa pisimmälle, mutta lisävarovaisuus ei koskaan ole pahasta. Esimerkiksi autolla kuljettaessa läppäri kannattaa aina laittaa tavaratilaan varkaiden katseilta piiloon. Moni läppäri on varastettu apukuskin paikalta avoimen ikkunan kautta, jopa suoraan liikennevaloissa.

”Vene, grilli, tai muu kesäväline tarkistetaan ennen talviteloille laittamista, joten samalla tavoin tulisi huolehtia myös tietokoneesta loman päätyttyä. Yritysten tulisi jatkuvasti tarkkailla sisäistä liikennettä varmistaakseen verkkonsa turvallisuus, mutta mahdollisuuksien mukaan koneen voi myös käyttää tarkistettavana yrityksen IT-osastolla ennen sisäverkkoon kytkemistä. Näin vältetään mahdollisten loman aikana tarttuneiden pöpöjen leviämistä.”

Vinkit lomalle lähtijöille

Työnantaja:

- Ohjeista henkilöstö yrityksen tietoturvasäilytyksestä ja työvälineiden käytöstä vapaa-ajalla
- Varmista, että kannettavat on suojattu asianmukaisesti: ohjelmistojen päivitykset ajan tasalla, konekohtainen virustentorjunta ja palomuuuri asennettuna ja koneen sisältö salattu vahvalla salauksella
- Mahdollisuuksien mukaan tarkistuta koneet IT:n kautta ennen koneen kytkemistä sisäverkkoon työntekijän palattua

Työntekijä:

- Noudata yrityksen antamia ohjeistuksia: jos työkannettavan käyttö vapaa-ajalla ei ole sallittua, jätä se toimistolle. Näin välttyt myös vastuulta mahdollisen vahingon sattuessa.
- Huolehdi itse siitä, että koneen ohjelmistot on päivitetty. Pyydä tarvittaessa apua yrityksen IT-vastaavalta.
- Älä asenna koneelle pelejä tai omia ohjelmia äläkä surffaa epämääräisillä sivuilla, etenkin jos olet kytkettynä vieraaseen tai suojaamattomaan verkkoon
- Jos et välttämättä tarvitse tietokonetta, jätä se suosiolla kotiin ja nauti lomasta lomana!

Stonesoft Oyj

Stonesoft Oyj (NASDAQ OMX: SFTIV) on innovatiivinen integroitujen verkkotietoturvaratkaisujen toimittaja, joka on keskittynyt hajautettujen organisaatioiden tiedonkulun turvaamiseen. Asiakkaidemme liiketoiminta edellyttää vaativaa verkkoturvallisuutta ja sovellusten luotettavaa saatavuutta.

StoneGate™ on tietoturvaratkaisu, jossa yhdistyvät palomuuuri, VPN, IPS (tunkeutumisen havainnointi- ja estojärjestelmä) sekä turvallisen etäkäytön mahdollistava SSL VPN. Ratkaisu yhdistää verkkotietoturvan, jatkuvan saatavuuden sekä palkitun kuormantasausteknologian yhtenäiseksi, keskitetysti hallittavaksi järjestelmäksi. StoneGate-tietoturvaratkaisu tarjoaa alhaiset käyttökustannukset, erinomaisen suorituskyvyn ja tehostaa verkko-investointien tuottavuutta. Virtuaalinen StoneGate-tietoturvaratkaisu suojaa verkkoa ja takaa liiketoiminnan jatkuvuuden sekä virtuaali- että fyysisessä ympäristössä.

StoneGate Management Center -hallinnan avulla StoneGate-palomuuria, VPN-, IPS-, sekä SSL VPN -ratkaisua voidaan hallita keskitetysti. StoneGate-palomuuuri sekä hyökkäyksen havainnointi- ja estojärjestelmä toimivat saumattomasti yhdessä muodostaen koko yritysverkon kattavan kehittyneen kerroksellisen puolustuksen. StoneGate SSL VPN tarjoaa tehokkaan suojan mobiili- ja etäkäytön tarpeisiin.

Vuonna 1990 perustettu Stonesoft Oyj on maailmanlaajuisesti toimiva yhtiö, jonka pääkonttori on Helsingissä ja Amerikan alueen pääkonttori Atlantassa, Georgiassa. Lisätietoa osoitteesta www.stonesoft.com sekä yhtiön blogissa <http://stoneblog.stonesoft.com>.



Lisätietoja:

Joona Airamo, tietoturvapäällikkö

Stonesoft Oyj

Puh. (09) 476 711

Sähköposti: joona.airamo@stonesoft.com