STONESOFT

Lehdistötiedote

Stonesoft: 10 vinkkiä sosiaalisen median turvalliseen käyttöön

Helsinki, 6. heinäkuuta 2010 – Sosiaalisen median merkitys kasvaa jatkuvasti. Tutkimusyhtiö Gartnerin* mukaan vuoteen 2014 mennessä 20 prosenttia yrityksistä käyttää Internetin sosiaalisia verkostoja tärkeimpänä viestintäkanavanaan. Samaan aikaan yritysten johto ja IT-osastot ovat kuitenkin huolissaan näiden verkostojen tietoturvallisuudesta.

Uusimpien tutkimusten mukaan neljäsosa yrityksistä kieltää sosiaalisen median käytön työaikana, joidenkin lähteiden mukaan jopa puolet. Tietoturvaan liittyvät huolet rajoittavat niitä potentiaalisia hyötyjä, joita sosiaalinen media voisi tarjota yritysten markkinoinnille, myynnille ja viestinnälle.

Stonesoft antaa kymmenen vinkkiä, miten yritykset voivat hyödyntää sosiaalista mediaa tietoturvaa vaarantamatta.

1. **Lisää työntekijöiden tietoisuutta** – Ihmisten on vaikea muuttaa käyttäytymistapojaan, jos he eivät tiedä niihin liittyvistä riskeistä. Yritysten pitäisi tiedottaa työntekijöilleen sosiaaliseen mediaan liittyvistä tietoturvariskeistä ja korostaa, että joskus harmittomaltakin vaikuttava tieto tai kommentti voi paljastaa liikaa yrityksestä tai työntekijästä henkilönä. Hyvä käytäntö on jakaa ja ylläpitää tietoa uusimmista uhista sekä siitä, kuinka sosiaalisessa mediassa tulee toimia. Vielä parempi käytäntö on nimetä asiantuntija vastamaan työntekijöiden sosiaalista mediaa koskeviin kysymyksiin.

2. **Panosta prosesseihin** - Järjestelmänvalvojat tarvitsevat ajantasaista tietoa verkossa liikkuvista uhkista. Yritysten tulisi panostaa prosesseihin, jotka on systemaattisesti linkitetty päivittäisiin toimintatapoihin. Esimerkiksi järjestelmänvalvojien tulisi ladata säännöllisesti viimeisimmät tietoturvapäivitykset. Näin heidän on myös helpompi havaita ja tunnistaa verkkohyökkäykset ajoissa tai välttää ne kokonaan.

3. **Määrittele käyttöoikeudet riittävän tarkkaan** – Riittävän tarkkaan rajatuilla ohjeistuksilla ja säännöillä järjestelmänvalvojat voivat määritellä, mille verkon alueille ja sovelluksiin kullakin yrityksen työntekijällä on pääsy ja milloin. Näin verkkoliikennettä - erityisesti kriittisiin tietoihin kohdistuvaa - on helpompi valvoa, ja riski tiedon menettämisestä on huomattavasti pienempi. Ohjeistuksen luomisen jälkeen on tärkeää ylläpitää sitä sekä tietysti seurata, että ohjeistusta noudatetaan.

4. **Estä pääsy haitallisille sivustoille** - Ohjeistuksista ja sisäisestä koulutuksesta huolimatta troijalaisen lataaminen saastuneelta sivustolta yhdellä klikkauksella on valitettavan helppoa. URL-suodattimien avulla haitallisiksi tiedetyille tai epäillyille sivustoille pääsy voidaan estää. Suodattimet on pidettävä jatkuvasti ajan tasalla.

5. **Käytä uuden sukupolven palomuureja** - Yritysten tulee huolehtia tietoturvateknologiansa ajanmukaisuudesta. Nykyaikaiset uuden sukupolven palomuurit analysoivat verkkoliikennettä kokonaisvaltaisesti, ja liikenteen syväluotaus mahdollistaa minkä tahansa kaltaisen tiedon monitoroinnin - oli kyseessä sitten Internetissä surffailu, vertaisverkkosovellus tai salattu liikenne. Uuden sukupolven palomuuri avaa salatun verkkoliikenteen tarkistusta varten ja lähettää sen taas salattuna eteenpäin. Tämä menetelmä tarjoaa työpisteille, sisäverkoille ja palvelimille tehokkaan suojan SSL-tunneleihin kätkettyjä hyökkäyksiä vastaan.

6. **Määrittele pääsy yrityssovelluksiin** - Matkustavat tai etätyötä tekevät työntekijät, kumppanit ja alihankkijat tarvitsevat usein pääsyn yrityksen järjestelmiin ulkopuolelta. Näiden käyttäjäryhmien

sisällä sosiaalisen median käytön seuraaminen voi olla hankalaa tai jopa mahdotonta. Sitä tärkeämpää onkin määritellä keskitetysti, mitä sovelluksia kukin taho tarvitsee, ja mahdollistaa yhteys näihin ainoastaan salatun VPN-portaalin kautta. Käyttäjätasolla vahva tunnistautuminen kertakirjautumisella on järjestelmänvalvojan kannalta helpoin hallinnoida, ja silloin myös varmistetaan henkilön pääsy vain niille verkkoalueille ja niihin sovelluksiin, joita hän tarvitsee.

7. **Suojaudu haavoittuvuuksilta** - Erilaiset haavoittuvuudet merkitsevät erityishaasteita missä tahansa verkossa. Tämän lisäksi sosiaalisessa mediassa tapahtuvien haavoittuvuuksia hyödyntävien hyökkäysten määrä kasvaa jatkuvasti. Tunkeutumisen havainnointi- ja estoratkaisut (Intrusion Prevention System, IPS) suojaavat tällaisissa tapauksissa tehokkaasti, koska ne pysäyttävät sosiaalisesta mediasta verkon yli leviävät hyökkäykset ja estää niiden pääsyn yritysverkkoon. Ratkaisu suojaa myös palvelimia ja sovelluksia, jotka haavoittuvaisina odottavat seuraavaa huoltoikkunaa ja sen mukanaan tuomaa tietoturvapäivitystä.

8. **Suojaa Intranet** - Intranetit sisältävät aina yrityksen sisäistä tietoa. Ne tulisikin aina erottaa muusta sisäverkosta. Palomuurisegmentoinnin avulla yrityksissä voidaan eristää esimerkiksi talous- ja laskentatietoja sisältävät alueet muusta sisäverkosta ja siten estää mahdollisten tartuntojen leviäminen näille kriittisille alueille.

9. **Sisällytä tietoturvaohjeistuksiin myös langattomat laitteet** - Monet käyttävät sosiaalisia verkkoja kannettavien, kämmentietokoneiden tai matkapuhelinten kautta, eli samojen laitteiden, joilla kirjaudutaan myös yritysverkkoon. Langattomat laitteet tulee siis myös huomioida turvallisuusohjeistuksissa. Kirjautumiseen käytettävän laitteen tietoturva-asetukset ja ohjelmistojen ajantasaisuus tulisi automaattisesti arvioida joka kerta kun sillä kirjaudutaan yritysverkkoon. Tarkistuksessa voidaan esimerkiksi määritellä, millainen palomuuri ja virustentorjuntaohjelmisto laitteessa tulisi olla käytössä, ja milloin niiden tulisi olla viimeksi päivitetty. Jos joku määritellyistä ominaisuuksista puuttuu, yhteys kyseisestä laitteesta estetään automaattisesti, tai yhteys rajataan. Tarvittaessa laite voidaan myös ohjata suoraan verkkosivustolle, josta puuttuvat päivitykset ovat ladattavissa.

10. **Käytä keskitettyä hallintaa** – Verkon tietoturvan keskitetyn hallinnan avulla järjestelmänvalvojat voivat hallita yrityksen koko verkkoa ja kaikkia siihen liitettyjä laitteita yhden järjestelmän kautta. He pystyvät muokkaamaan järjestelmien asetuksia sekä hakemaan raportteja siitä, kuka verkossa liikkuu ja minkälaista tietoa sieltä haetaan mihinkin aikaan. Mahdollisten hyökkäysten estäminen ja pysäyttäminen tehostuu ja tarvittavien tietoturvatoimenpiteiden määritteleminen on helpompaa. Keskitetyn hallinnan avulla myös tietoturvaohjeistusten jakaminen ja ylläpitäminen on vaivatonta.

“Sosiaalisen median jatkuvasti kasvava käyttö asettaa yritykset täysin uudenlaisten tietoturvariskien eteen. Henkilöstön jatkuva kouluttaminen on usein haasteellista, eikä silti ratkaisevasti poista ongelmia. Parempi vaihtoehto ovatkin sisäverkkoon luodut turvamekanismit, jotka havaitsevat ja pysäyttävät mahdolliset hyökkäykset ajoissa. Asianmukainen tietoturvastrategia yhdistää henkilöstön kouluttamisen ja uusimman teknologian, jolloin yrityksellä ei ole mitään estettä sosiaalisen median täydelle hyödyntämiselle”, Stonesoftin tietoturva-asiantuntija **Olli-Pekka Niemi** sanoo.

Lisätietoa Stonesoftin tarjoamista palomuuri/VPN-, IPS-, ja SSL VPN-ratkaisuista löytyy osoitteesta www.stonesoft.com. Kaikki Stonesoftin ratkaisut ovat keskitetysti hallittavissa.

* Gartner, Inc. "Predicts 2010: Social Software Is an Enterprise Reality", Joulukuu 2009

Lisätietoja:

Stonesoft Oyj

Klaus Majewski, markkinointijohtaja
Puh. (09) 476 711
Sähköposti: klaus.majewski@stonesoft.com

Stonesoft Oyj

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

StoneGate(TM) on tietoturvaratkaisu, jossa yhdistyvät palomuuri, 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 -palomuuri ja 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 ja http://stoneblog.stonesoft.com/