STONESOFT

Lehdistötiedote

Stonesoft: Vinkkejä pilvipalveluiden tietoturvahaasteilta suojautumiseen

Helsinki, 14. huhtikuuta 2010 - Kansainvälisesti tunnettu tutkimusyhtiö Gartner arvioi hiljattain, että vuoteen 2012 mennessä jopa 60 prosenttia virtualisoiduista palvelimista on vähemmän turvallisia kuin fyysiset edeltäjänsä (*Gartner: Addressing the Most Common Security Risks in Data Center Virtualization Projects, January 2010)*. Verkkotietoturvayhtiö Stonesoftin mukaan pilvipalveluiden suurin haaste onkin virtuaalinen tietoturva. Siihen löytyy kuitenkin monta eri ratkaisua.

Suurin osa tämän päivän yrityksistä hyödyntää jo virtuaaliteknologiaa, mutta harva ymmärtää, mitä tietoturvan saralla tulisi ottaa huomioon muutoksen myötä. Fyysisiin ympäristöihin luodut tietoturvaratkaisut eivät suojaa virtuaaliympäristöjä riittävällä tasolla, jolloin verkkoon voi kohdistua odottamattomia uhkia. Pilvipalveluita käyttäville yrityksille tämä voi muodostua yllättäväksi haasteeksi.

Stonesoft on listannut viisi tapaa, joilla yritykset voivat suojautua pilvestä tulevia tietoturvauhkia ja verkkohyökkäyksiä vastaan, sekä samalla parantaa IT-strategiaansa.

1. **Kertakirjautuminen:** Pilviympäristöissä toimiessaan käyttäjän tulee kirjautua useisiin eri sovelluksiin ja palveluihin. Tässä piilee kuitenkin vaara, että yritys joutuu luovuttamaan käyttäjä- ja tunnistamistiedon hallinnan usealle eri pilvipalvelutarjoajalle. Samalla se menettää mahdollisuuden hallinnoida tunnistautumista riittävän hyvin käyttäjätasolla. Minimoidakseen tämän riskin yritysten tulisi ottaa käyttöön ”single sign-on” –eli kertakirjautumismenetelmä, jonka avulla käyttäjä voi kirjautua useisiin eri sovelluksiin ja palveluihin (myös yritysverkon ulkopuolella, julkisessa pilvessä sijaitseviin) samoilla tunnuksilla. StoneGate SSL VPN - ratkaisu mahdollistaa lisäksi käyttäjä- ja tunnistamistiedon säilyttämisen yrityksen omissa järjestelmissä tavalla, joka on yhteensopiva useimpien pilvipalveluntarjoajien kanssa.

2. **Häiriötön yhteys:** Kun suurin osa yrityksen kriittisistä tiedoista on tallennettuna pilveen, verkon käyttökatkosten aikana myös liiketoiminnan jatkuvuus kärsii. Yhteys pilveen pitäisikin olla aina varmistettu, myös ylläpitotoimenpiteiden aikana. Yritysten tulisi valita tähän tarkoitukseen teknologiaratkaisuja, joissa yhden laitteen tai yhteyspalvelutarjoajan häiriö ei vaaranna koko järjestelmän toimivuutta. Esimerkkinä tästä on usean yhtäaikaisen Internet-yhteyden käyttö kahden tai useamman operaattorin kautta. Näin saavutetaan toimivin, helpoimmin hallittava ja kustannustehokkain kokonaisuus.

3. **Monitasoinen tarkistus:** Pilviteknologian yleistyminen ja yhä monimutkaisemmat uhat ovat luoneet tarpeen monitasoiselle tietoturvalle, joka sisältää sekä verkon ulkoreunan suojauksen ja tunkeutumiseneston että sisäverkon suojan. Ensimmäisen sukupolven palomuurien sijaan Stonesoft suosittelee käytettäväksi virtuaalisia seuraavan sukupolven palomuurilaitteita, kuten StoneGate Virtual NextGen Firewall,

joka on yhdistelmä palomuuri- ja tunkeutumisenestoteknologiaa sekä älykästä verkkoliikenteen analysointia.

4. **Keskitetty hallinta:** Käyttäjien tekemät inhimilliset virheet ovat edelleen suurin tietoturvauhka niin fyysisissä kuin virtuaalisissakin verkkoympäristöissä. Kun organisaatio ottaa käyttöön uusia keinoja virtuaaliverkkojen suojaukseen, inhimillisten riskien mahdollisuus kasvaa. Usein laitehallinta, monitorointi ja asetusten muutokset tehdään jokaisen tuotteen omasta hallintaohjelmasta, jolloin kokonaistilanteen hallinta on haastavaa ja muutosten koordinointi puutteellista. Tämän vuoksi Stonesoft suosittelee käytettäväksi yhtä hallintakonsolia kaikkien laitteiden hallintaan, olivatpa ne fyysisiä, virtuaalisia tai muiden laitevalmistajien toimittamia.

5. **Suojattu virtuaalinen työpöytä:** Yhä useampi yritys ottaa käyttöön virtuaalisia työpöytiä säästääkseen käyttö- ja ylläpitokuluissa. Virtuaaliset työpöydät ovat kuitenkin yhtä haavoittuvia kuin fyysisetkin; asianmukainen suojaus edellyttää niiden eristämistä muista verkkosegmenteistä. IPS- eli tunkeutumisen havainnointi- ja estoratkaisujen avulla voidaan suojata virtuaalisten työpöytien yhteydet yrityksen palveluihin ja Internetiin, ja siten torjua niihin kohdistuvat sisäiset ja ulkoiset uhat.

Stonesoftilla on useita ratkaisuja virtuaalisten ja pilviympäristöjen suojaamiseen, kuten StoneGate Virtual NextGen Firewall, StoneGate Virtual IPS and StoneGate Virtual SSL VPN. Lisätietoja osoitteessa www.stonesoft.com.

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

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 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.

STONESOFT

StoneGate Management Center -hallinnan avulla StoneGate-palomuuria, VPN-, IPS-, sekä SSL VPN -ratkaisua voidaan hallita keskitetysti. StoneGate-palomuuri 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 Hesingissä ja Amerikan alueen pääkonttori Atlantassa, Georgiassa. Lisätietoa osoitteesta www.stonesoft.com sekä yhtiön blogissa http://stoneblog.stonesoft.com.