STONESOFT

LEHDISTÖTIEDOTE

Vuoden 2010 merkittävimmät tietoturvariskit

Helsinki, 4. helmikuuta 2010 - Suomalainen tietoturvayhtiö Stonesoft on kartoittanut vuoden 2010 merkittävimmät tietoturvariskit. Stonesoft kehottaa kiinnittämään huomiota erityisesti luottokorttimaksamisen, sosiaalisen median käytön, pilviteknologian ja mobiililaitteiden tietoturvaan.

Viime vuoden lopulla Espanjassa tehdyssä laajassa tietomurrossa varastettiin jopa kymmenien tuhansien suomalaisten luottokorttien tiedot. Kohteena oli korttimaksuja välittävä yritys ja tuhannet suomalaiset joutuivat vaihtamaan korttinsa uuteen.

Kun yritys kadottaa asiakastietojaan, menettää se samalla arvokasta luottamuspääomaansa. Monet yritykset suojaavat asiakkaidensa luottokorttitietoja palomuurein, mutta tämä ei tarjoa riittävää suojaa rikollisilta. Yritysten tulisikin keskittää tietoturvainvestointinsa kattavampiin ratkaisuihin, kuten tunkeutumisen havainnointi- ja estojärjestelmiin (IPS, Intrusion Prevention System). Maksukortteja koskevan tietoturvastandardin (PCI-DSS, Payment Card Industry Data Security Standard) astuttua voimaan on riittävän suojan hankkiminen pakollista kaikille organisaatioille, jotka prosessoivat tai siirtävät suuria määriä maksu- tai luottokorttitietoa.

Sosiaalinen media rikollisten huomion kohteena

Yksi suurimmista tietoturvauhista vuonna 2010 on niin kutsuttu sosiaalinen manipulointi (social engineering). Hyökkääjät hakevat tietoja organisaation työntekijöistä esimerkiksi sosiaalisesta mediasta ja käyttävät näitä hyväkseen väärennetyn identiteetin luomiseen. Tämä tarkoittaa, että myös tutuilta tai ystäviltä tulleet viestit voivat sisältää haitallista ohjelmakoodia. Tulevaisuudessa hyökkääjät etsivät ja löytävät yhä enemmän keinoja tunkeutua niin yksityisiin kuin yritystenkin verkkoihin. Sisäiset sähköpostit voivat olla riski siinä missä yksityisviestit sosiaalisen median palveluissa. On tärkeää, että käyttäjät kiinnittävät tähän huomiota.

Pilvilaskennan tumma reunus

Yritysten ulkoistaessa IT-palvelujaan ulkopuoliselle kumppanille, ne myös ulkoistavat hallinnoimansa tiedon luottamuksellisuuden, koskemattomuuden ja helpon saatavuuden. Vaikka palvelun laatu on turvattu palvelutason sopimuksilla (SLA, Service Level Agreement), tietoturvaa nämä sopimukset kattavat vain harvoin. Tietoturva hankitaan tässä yhteydessä ”sikana säkissä”, josta asiakas maksaa osana kokonaispakettia. Asiakasyrityksen yksilöllisiä tietoturva tarpeita ei oteta huomioon. Palveluntarjoajaa valitessaan yritysten järjestelmävastaavien tulisi kiinnittää yhä enemmän huomiota tietoturvaan. Voiko asiakas käyttää omaa käyttäjätietokantaansa tai autentikointipalveluaan pilvipalvelun kanssa esimerkiksi

federated authentication -menetelmän, eli yhdistetyn todentamisen avulla? Vastaako järjestelmä yrityksen yksilöllisiä tarpeita? Mitä takuita palveluntarjoaja antaa? Onko raportointi riittävän kattavaa? Mitä tapahtuu mahdollisen tietomurron yhteydessä? Ja kuka on vastuussa?

Mobiililaitteet portti yritysverkkoon

Mobiililaitteet, kuten älypuhelimet ja kämmentietokoneet ovat löytäneet tiensä yritysmaailmaan jo vuosia sitten, tarjoten pääsyn liiketoimintakriittiseen tietoon myös tien päällä. Mobiililaitteissa tietoturvan taso on kuitenkaan harvoin sama kuin tietokoneissa. Tämän vuoksi ne kiinnostavat kasvavassa määrin myös tietoturvarikollisia. Pääasiallinen ero tietokoneisiin on, että vaikeammin käytettävän näppäimistön vuoksi käyttäjät suosivat yksinkertaisia ja lyhyitä salasanoja. Työntekijät käyttävät mobiililaitteitaan sekä henkilökohtaisiin että työasioihin, ja unohtavat virustorjuntaohjelmiston tai palomuurin päivittämisen. Viruksen on tämän vuoksi helppoa saastuttaa paitsi käyttäjän laite, myös yritysverkko mobiililaitteen kautta. Tämän ongelman tehokas ratkaiseminen tulevaisuudessa vaatii mobiililaitteiden keskitettyä hallintaa, samaan tapaan kuin tietokoneissa. Keskitetyn hallinnan avulla on mahdollista varmistaa, että tietoturva-asetukset ja -päivitykset ovat ajan tasalla jokaisessa mobiililaitteessa. Tällä hetkellä todellisuus on kuitenkin karumpi.

Lisätietoja PCI-tietoturvastandardista maksukorteille:
https://www.pcisecuritystandards.org/.

Tiedote kokonaisuudessaan on luettavissa Stonesoftin sivuilla:
http://www.stonesoft.com/en/press_and_media/releases/fi/2010/04022010.html.

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.

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 Helsingissä ja Amerikan alueen pääkonttori Atlantassa, Georgiassa. Lisätietoa osoitteesta www.stonesoft.com sekä yhtiön blogissa http://stoneblog.stonesoft.com.