STONESOFT

Lehdistötiedote

Stonesoft: Tietoturva kaipaa uudelleenajattelua

Johtoryhmien ja hallitusten panostettava tietoturvan tason ymmärtämiseen

Helsinki, 2.8.2011 - Tietoturvayhtiö Stonesoft kehottaa organisaatioita arvioimaan riskienhallintansa ja tietoturvansa tasoa uudelleen. Useat viime aikoina puhuttaneet uhat, kuten Wikileaks, Stuxnet, kehittyneet evaasiotekniikat ja RSA -murto ovat muuttaneet tietoturvan toimintaympäristöä pysyvästi ja toimivat herätyksenä myös strategisesta näkökulmasta. Stonesoft muistuttaa, että niin tietoturvassa kuin muussakin yrityksiä koskevassa riskienhallinnassa, viime kädessä vastuu on ylimmällä johdolla ja hallituksella.

Vuosi 2010 ja vuoden 2011 alkupuolisko ovat mullistaneet tietoturvamaailman pysyvästi. Wikileaks, Stuxnet, kehittyneet evaasiotekniikat ja SecurID -lähdekoodin varastaminen ovat ravisuttaneet tietoturva-ajattelua ja herättäneet pohtimaan aihetta strategisesta näkökulmasta. Viime aikojen lukuisat verkkohyökkäykset ovat näyttäneet, että nyt jos koskaan on aika toimia. Ennen vuotta 2010 luodut tietoturvastrategiat pitää päivittää ja tietoturvan suunnittelu ja toteutus kaipaavat perusteellista uudistusta. Mitä arvokkaampaa tietoa yrityksellä on, sitä todennäköisemmin se joutuu hyökkäyksen kohteeksi. Organisaatioiden tulee arvioida tietoturvansa taso uudelleen – myös johtoryhmä- ja hallitustasolla.

Wikileaks- paljastussivustoa on kritisoitu luottamuksellisen tiedon julkaisemisesta, kansallisen turvallisuuden vahingoittamisesta, kansainvälisen diplomatian vaarantamisesta sekä toimituksellisen hienotunteisuuden puutteesta. Yritysten on pohdittava, onko niillä tietoa, jonka vuotaminen voi vahingoittaa niiden liiketoimintaa tai jopa tuhota sen. Jos yrityksen ydintieto ei saa päästä julkisuuteen, tulee sitä myös suojella korkeimmalla mahdollisella tietoturvatasolla.

Stuxnet osoitti, että on olemassa ryhmiä ja yksilöitä, joilla on käytössään kehittyneisiin, kohdistettuihin hyökkäyksiin tarvittavat resurssit. Näin ollen aiempi uskomus, jonka mukaan verkkomurtojen toteuttaminen tiettyihin kohteisiin olisi liian vaikeaa tai vaatisi liian paljon resursseja, ei enää pidäkään paikkaansa. Jos rikoksesta saatu taloudellinen, poliittinen tai sotilaallinen hyöty on siihen käytetyn vaivannäön arvoista, tarvittavat resurssit kyllä löytyvät.

Kehittyneet evaasiotekniikat ovat uusi ja koko ajan muuttuva tapa kuljettaa vahingollista sisältöä ja hyökkäyksiä kohteisiin siten, että tietoturvajärjestelmät eivät havaitse niitä. Erilaisista evaasioista koostetut yhdistelmät toimivat tehokkaana yleisavaimena, joiden avulla rikolliset pääsevät tiukasti suojattuihin kohteisiin, tietokantoihin ja järjestelmiin. Riskienhallinnan näkökulmasta on erittäin vaarallista, jos organisaation tietoturvaratkaisut eivät kykene tarjoamaan jatkuvasti päivittyvää suojaa uusimpia evaasiotekniikoita vastaan. Asiaa hankaloittaa se, että kilpailutilanne tietoturvalaitteiden markkinoilla on vaatinut ratkaisuilta jatkuvasti lisää nopeutta ja alempia kustannuksia, jolloin on jouduttu tinkimään niiden ydintoiminnallisuudesta, eli tietoturvan tasosta. Evaasiotekniikoiden tutkimus on paljastanut vakavan haavoittuvuuden ja tilanne paranee vain, mikäli koko tietoturvayhteisö suhtautuu asiaan riittävän vakavasti.

RSA -tietoturvamurto teki mahdolliseksi sen, että verkkorikolliset voivat läpäistä tietoturvajärjestelmiä luomalla kopioita EMC:n omistaman tietoturvayhtiö RSA:n kehittämistä elektronisista SecurID-tunnistusavaimista. SecurID-avaimet on tunnettu yleisenä ja luotettavana tunnistautumismenetelmänä, koska ne luovat joka kerta järjestelmään kirjautumista varten uudet tunnukset. SecureID-avaimet luotiinkin alun perin suojaamaan hyökkääjiltä, jotka hyödyntävät ns. key-logging-viruksia varastamaan salasanoja. Maaliskuussa 2011 EMC ilmoitti, että yhtiön verkkoon oli murtauduttu ja sieltä oli varastettu SecurID-avaimiin liittyviä tietoja, joita väärinkäyttämällä yhtiön asiakkaiden verkkojen tietoturva on murrettavissa.

STONESOFT

Yhteenveto viime aikojen tietoturvamurroista

Vuosina 2010-2011 on toteutettu useita tietoturvamurtoja tai murtoyrityksiä ympäri maailmaa

- **Nasdaq, 2010**
  - Verkkorikolliset yrittivät toistamiseen tunkeutua Nasdaqin pörssiä ohjaavan yhtiön tietoverkkoon. Tapaus tuo esille kaksi viranomaisia huolestuttavaa asiaa: onko verkon kautta tapahtuva osakekauppa enää luotettavalla pohjalla, ja luottavatko sijoittajat enää järjestelmään. Pörssit tietävät olevansa usein tietomurtojen kohteena.
- **RSA, maaliskuu 2011**
  - Verkkorikolliset murtautuivat tietoturvayhtiö RSA:n järjestelmiin ja varastivat tunnistautumisratkaisuihin liittyviä kriittisiä tietoja.
- **SONY, 2011**
  - Ongelmat alkoivat 19. huhtikuuta, kun yhtiö lopulta havaitsi massiivisen murron, joka oli kohdistettu sen PlayStation -verkkoon. Tuloksena oli verkkoskandaali, joka saattoi vääriin käsiin yli 100 miljoonan käyttäjän henkilötiedot.
- **Comodo, maaliskuu 2011**
  - Yhdysvaltojen digitaalisten sertifikaattien viranomaistaho Comodo on myöntänyt, että aiempien lisäksi vielä kahteen rekisteröintiviranomaiseen on kohdistunut tietomurto. Aiemmissa ns. ”Iranian lone” -tietomurroissa ainakin viisi eri asiakastiliä oli vaarannettuna.
- **Barracuda, huhtikuu 2011**
  - Useita tunteja kestäneen automatisoidun tunnustelun jälkeen verkkorikolliset löysivät SQL-aukon Barracuda-verkkosivustolta ja onnistuivat viemään sen kautta yhtiön kumppanien, asiakkaiden ja työntekijöiden tietoja.
- **Lockheed Martin, toukokuu 2011**
  - Tuntemattomat verkkorikolliset murtautuivat maailman suurimman aseteollisuuden konsernin Lockheed Martinin verkkoon.
- **L-3 Communications, 2011**
  - Ilmailu- ja puolustusteollisuusalalla toimivan L-3 Communicationsin verkkoon yritettiin murtautua tavoitteena viedä luottamuksellisia tietoja. L-3 ei ole julkaissut tarkempia tietoja hyökkäysyritykseen liittyen.
- **Citibank, toukokuu 2011**
  - Noin 200 000 pohjoisamerikkalaisen asiakkaan korttitiedot varastettiin. Mukana oli myös muita tietoja, kuten nimiä ja sähköpostiosoitteita.
- **IMF, kesäkuu 2011**
  - Kansainvälinen valuuttarahasto IMF (International Monetary Fund), joka valvoo maailmanlaajuista rahoitusjärjestelmää, oli viimeisimmän merkittävän verkkohyökkäyksen kohteena.

Yhteinen nimittäjä kaikille yllä listatuille yrityksille ja organisaatioille on se, että niiden verkkotietoturvaratkaisut toimivat korkeimmalla mahdollisella tasolla. Näillä kaikilla organisaatioilla on ammattitaitoiset tiimit, jotka valvovat ja hallinnoivat tietoturvaa keskitetysti. Siitä huolimatta niiden järjestelmiin murtauduttiin. Vastaavanlaisia murtoja tullaan varmasti näkemään lisää. Uusien hakkerointityökalujen ja -menetelmien kehittyessä ja yleistyessä tulemme näkemään onnistuneita hyökkäyksiä myös sellaisiin kohteisiin, jotka ovat heikommin suojattuja, mutta huomattavasti laajemmassa käytössä. Tällaisia ovat muun muassa sosiaalisen median ympäristöt.

“Tietoturvauhat ovat muuttuneet pysyvästi. Vanhat tietoturvamenetelmät eivät enää pysty tarjoamaan suojaa niitä vastaan, joten yritysten on arvioitava tietoturvansa taso uudelleen. Tietoturvastrategian

merkitys osana riskienhallintaa on korostunut ja kasvaa jatkuvasti, ja ylimmän johdon on myös tiedostettava tämä. Tietoturvan laiminlyöminen ja vastuun jättäminen vain IT-hallinnon harteille on selkeä osoitus huonosta johtamisesta", Stonesoftin toimitusjohtaja **Ilkka Hiidenheimo** sanoo. "Myös yritysten hallitusten tulisi perehtyä aiheeseen ja kartoittaa yrityksen riskiprofiili."

Lisätietoja:

Ari Vänttinen, markkinointijohtaja
Stonesoft Oyj
Puh. 040 5959 577
Sähköposti: ari.vanttinen(AT)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(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, www.antievasion.com ja http://stoneblog.stonesoft.com/