

- » Home
- » First Looks
- » Group Test
- » Features
- » Reviews
- » Pipeline
- » Top Products
- » Editorial
- » Analysis & Trends
- » Tutorials
- » العربية

You are here: PC Magazine MNE Home > Features > Insider Threats

Print E-mail



Click to enlarge

Friday, 20th April 2007
Insider Threats

The damage caused by an insider threat can take many forms, including the introduction of viruses, worms, or Trojan horses; the theft of information or corporate secrets; the theft of money; the corruption or deletion of data; the altering of data to cause inconvenience or falsify criminal evidence; and the theft of the identities of specific individuals in the enterprise. New threats on the horizon are those like spear phishing that masquerade as an acquaintance, making you open threat-carrying attachments, disclose confidential information or click on otherwise suspicious URLs. This is leading to the entry of spyware, phishing, pharming, viruses, etc., and compromising enterprise security.

Internal users are the biggest security threat to enterprises today. The Reasons are:

1. User Ignorance

External threats take advantage of user ignorance to gain entry into the network. External threats are increasingly targeting the individual users for financial gain. Lacking up to date security knowledge, internal users tend to engage in harmful activity like P2P file transfers, surfing unsafe sites, leaving email ids for updates on suspicious sites and more. These acts result in higher levels of spam, increase in the entry of spyware, phishing, pharming into the network in addition to the traditional viruses, worms, Trojans and more.

2. Malicious Intent

Internal users can have far more serious negative impact than external threats since they are aware of the shortcomings of enterprise security implementation as well as the location of key IT and other resources and practices.

3. Disgruntled employees

Insider threats are often caused by disgruntled employees or a few ex-employees who believe that the business, institution, or agency has "done them wrong" and feel justified in gaining revenge.

According to the Yankee Group, 50 percent of security problems originate from internal threats. In its 2005 survey, "The Global State of Information Security," PricewaterhouseCoopers found that 33 percent of information security attacks originated from internal employees, while 28 percent came from ex-employees and partners. We have come across a corporate in which an ex-employee had taken over the Yahoo messenger id of the company employee. Using this id, he accessed other contacts to perpetrate malicious information.

Since the user is proving to be the weakest link in the security chain today, linking user identity to security is the solution to ensuring high levels of security and to fight against insider threats. Most commonly prevalent security solutions that have existed and have been an integral part of any network periphery are firewall which demarcates the intranet and the Internet boundary. However with the firewall rule, eventually the administrator would get the information based on a machine's IP address and it is not enough as it sorely lacks in completeness.

The stalwarts of the network security solutions are buzzing with the concept of user identity and mapping it to the access patterns and physical resources in a network. If a network security solution can recognise an end user, the system administrator can formulate and apply customised access policies according to the individual's professional needs. Every person or a group can exist as a microcosm on the network, where its traffic patterns can be scrutinised and the access rights awarded. A threat can be detected on time and dealt with before it matures into a full scale attack if the user's identity is deciphered. The control mechanism, however strong, would prove meaningless if they are not directed and focused on the right target, thus identity plays an important role in the current scenario to counter the insider threats.

BREAKING NEWS

- Sun, 18th March 2007
Trend Micro Promotes Layered Messaging Security
- Touchmate Unveils What it Claims is the World's Smallest Mobile Phone
- Oracle Announces General Availability of Oracle Enterprise Manager 10g Release 3
- Tally Value Pack Addresses Need for Updating Accounting Software

Tue, 13th March 2007

- Watch the Cricket World Cup Live on Your Phone
- i2 Club Now Available on Nokia Phones
- HP Makes Data Backup and Recovery Easy for Small and Medium-size Businesses
- Sun empowers students at German-Jordanian University
- 988 Billion Gigabytes of Digital Information to be Created by 2010

Mon, 12th March 2007

- HTC Makes a Smart Move on Middle East
- HP's Dial a Cartridge Service Comes to the Region
- Kyocera Launches its Advanced Document Management Solution

Thu, 8th March 2007

- More News >

» Pipeline

ExpressCard with 16GB Storage



Nokia's Multimedia Computer



AMD Opteron

PC MAGAZINE M&NE

SUBSCRIPTION OFFER



FREE! ONE YEAR NOD 32 ANTIVIRUS LICENSE

- Product Reviews
- » Desktops
 - » Notebooks
 - » Inkjet Printers
 - » Graphics Cards
 - » Scanners
 - » Digital Cameras
 - » MP3 Players
- View all reviews >>>

Ads by Google Dell TFT LCD Displays