Computer IDs problematic on networks

May 19 2006

IT managers can only identify between 55 percent and 65 percent of the computers connected to a network, according to a recent Gartner study. The unknown 35 percent to 45 percent of the network can be a security nightmare, one company says.

"If you go to an IT manager and ask him what he knows about the network, he can identify a couple of elements: routers, switches, firewalls. But he has no idea where the desktops connected to the network are," Lior Tal, the co-founder and chief executive officer of Ra'anana, Israel-based Insightix, told United Press International in a telephone interview.

He added that the growing use of wireless technology and laptops means computers are plugged into and out of the network constantly, and if they are not connected exactly when the traditional security software scans the network, IT managers can't find them.

Wireless networks, especially, pose security risks such as "easy access, 'rogue' access points and unauthorized use of service," wireless network expert Matthew Gast wrote for O'Reilly Media.

Personal firewalls like those found on Windows XP and Windows 2003 are another obstacle to overseeing a network, Tal continued, because they too make computers invisible to the network.

Tal's company aims to eliminate that uncertainty with its Enterprise Collector 2.0 software, unveiled last month. The program allows IT managers to identify every element in their networks and to see changes to the network in real time.

"The software takes 7 minutes to install on a single device in the network," Tal said. "After 30 minutes the software (performs an) initial discovery, and from then on it is monitoring the network for changes."

Most security programs use "active discovery" to monitor the network -- every so often, the program goes out looking for elements on the network, but between these searches there is no monitoring.

Insightix combines active discovery and passive discovery, which alerts IT managers to changes in the network at all times, to give a real-time picture of what's going on with the network, Tal said.

"Enterprises cannot manage their IT infrastructures without comprehensive and timely knowledge of their IT networks," Michael Dortch, a principal business analyst at the Robert Frances Group, said via an Insightix statement.

"Enterprise Collector 2.0 delivers the necessary network information to help enterprises validate what they already know and discover what they do not know about critical IT resources. The real-time knowledge provided by Enterprise Collector 2.0 can aid enterprise IT initiatives ranging from capacity planning to regulatory compliance, helping to mitigate risks and increase business value for almost every type of IT investment."

The program also allows the IT manager to install security-patch upgrades on all the computers in the network.

The innovation is sorely needed among IT managers, Tal said. He cited two Israeli examples where inadequate network information led to security breaches: One wireless user surfed from outside Israel's Postal Bank network to inside and stole money; in another case, a consultant managed to steal a database of people who owed the National Bank money -- "he was able to access sensitive information from what seemed to be an innocent connection," Tal said.

Being able to see all the computers and changes on a network seems like a simple enough concept, so why has no one thought of it until now?

Tal cited two reasons: First, the algorithm needed for the monitoring had not yet been developed, and second, "the out-of-the-box thinking from Ofir (Ofir Arkin, the company's second co-founder and chief technology officer)."

Arkin is a world-renowned security researcher in the fields of operating systems and passive and active discovery, Tal said. "He was the first to talk about this concept (of a "smart combination of active and passive discovery) four or five years ago," Tal added.

Insightix has customers in the Unites States, France, Italy, England, Germany, Israel, China, Argentina, Brazil and Japan, Tal said.

In two months the company is planning to unveil a system that will disconnect unauthorized devices from the network automatically, according to Tal.