Networking: Content filtering grows

April 24 2006

A gullible young employee sends out a confidential document -- over the Internet -- that should have been sent only by overnight courier. A spy, hired by a rival firm, snags the file, with a packet-sniffing device, as it transitions from the corporate network to the Internet. Trade secrets are divulged, and the company is ruined. Experts tell United Press International's Networking column that corporations, both large and small, are seeking to stop "information leaks," like that, with outbound content filtering software.

"When critical data escapes, either intentionally, or accidentally, organizations face financial, legal and reputational costs," a spokesman for Fidelis Security Systems, based in Bethesda, Md., told Networking. "As a consequence, the outbound content filtering market is experiencing exponential growth."

As organizations choose to deploy network content control solutions to stem the unauthorized flow of confidential information, they have a number of architectural choices, said Trent Henry, senior analyst, at The Burton Group, an IT research firm, based in Midvale, Utah. "For some enterprises, it's preferable to avoid any potential network disruption by deploying a content filtering tool out-of-band. They don't necessarily want to give up remediation capabilities, though: so a flexible solution is a key consideration," said Henry.

One such solution being used on corporate networks is the latest version of Bethesda-based Fidelis Security Systems content filtering software. Officially known as extrusion-prevention software, the software is

designed to fit into existing IT infrastructure, and prevent the unauthorized transfer of sensitive or critical information over a network. This includes e-mail, Web mail, FTP, instant messaging and even peer-to-peer communications.

The software scans all outbound documents. Pre-built policies use information profiles to prevent any sensitive information from "leaking," or being sent outside the company. The software can be programmed to include state regulations protecting personally identifiable information, prevalent in California, for example, or the Pentagon's data classification standards, or health regulations, and computer source code.

"The incidents of data leakage continue to grow and the market, brand, legal, operational and financial consequences can be significant," said Timothy Sullivan, chief executive officer of Fidelis.

Cupertino, Calif.-based Symantec last week announced that it had integrated some new features into its famed anti-spam software. The software now protects against inbound, as well as outbound, e-mail threats. One organization already using the software is the Brisbane Girls' Grammar School in Brisbane, Australia, which has 175 teachers and administrators and 1,150 students.

"Today's enterprises rely heavily on e-mail for both internal and external business communications," said Brian Burke, research manager for the market research firm IDC's security division, based in Framingham, Mass., adding that he believes organizations are looking for "comprehensive" solutions to the content management problem. In addition to setting policies, network administrators can use the software to regularly scan the networks, by keyword or expression, for more than 200 recognized file attachment types, including ZIP files, executables, spreadsheet and presentation file formats.

External threats are still valid - viruses, malware and the like, though there is an increasing recognition that insiders can cause all manner of problems for corporate IT security too, experts tell Networking.

Smaller companies, in particular, are looking for tools that can combine both scanning of outbound and inbound messages, so as to reduce their IT costs. A firm called eSoft, Inc. has developed an "intelligence" sharing program that allows small companies, throughout its customer base, to share information on the latest threats. This kind of collaboration can give the smaller firms access to information about IT threats that they may not previously have had. It may also level the playing field with potential network intruders, whether they be Eastern European cyber-criminals, or kooky kids in a college dorm. "IT managers at smaller companies have not had the ability to collaborate in an effort to strengthen their security posture, while at the same time hackers and malware generators have collaborated to amplify the effects of their exploits," said Jeff Wilson, a principal analyst at Infonetics Research, a market research firm.