

Mobile devices danger signal



Have you just connected that mobile device to my network? Did you follow corporate policy? No! How can you guarantee it will not transfer malicious code onto our network? John Costello investigates.

It was inevitable. The more we saw people everywhere using mobile phones, the more we knew they would, sooner or later, want to connect them to our elaborately designed and managed data networks. And it's not just mobile phones they want to connect to the network. It appears just about any device that can be connected is being connected.

First, a word of warning. No end-user organisation wanted to be identified for this article but plenty of vendors in the security business were willing to raise their hands. The most startling news came from the security audit of "a large Australian organisation". The audit revealed more than 1800 breaches of security on its computer network over a 10-day period. Being attached to the network were Apple iPods and removable media devices via USB connectors.

The company conducting the audit was Lync Software. Its managing director is Kym Welsby. "I've no doubt we would get similar results from almost any other large organisation in Australia," he said.

"Removable media devices such as iPods, Blackberries and digital cameras get under the radar of network security systems," he said.

"This creates major risks ranging from corporate espionage and business disruption to malicious viruses. Unless businesses can identify and control iPods and other removable media devices, they are leaving a gaping hole in their security systems."

He said companies are locking the back door to their networks with firewalls but leaving the front door wide open, with people coming and going with uncontrolled removable devices.

Lync Software is an Australian company that has its management and security solutions installed at more than 2000 organisations worldwide including Boeing, Pepsi and Hilton Hotels. The Adelaide-based company says it has been successful in the US through a marketing partnership with auditing software specialist Layton Technology.

Security risks arise from iPods and other music players, USB memory sticks, personal organisers and PDAs, mobile phones and digital cameras that can connect undetected to corporate networks, downloading gigabytes of data in a matter of seconds and even introducing viruses. But there is some good news from the Lync Software security audit. While it revealed uncontrolled attachments to the network it did not detect any intrusion by malicious software.

Kym Welsby said the organisation it audited has now created a mobile device usage policy to secure its network against accidental or deliberate damage from removable media devices.

ringing a for networks



Lync Software has teamed with Layton Technology to develop DeviceShield, a solution that directly addresses the problems of identifying and controlling removable digital devices. The very fact a software vendor like Lync Software has seized the initiative on highlighting the dangers associated with attaching mobile devices to networks is one of the problems facing the industry. According to Professor Bill Caelli, it is being driven by vendors — not users.

“The whole security and safety issue is being market driven,” Professor Caelli said. He is recognised internationally as an expert on computer security. He is the head of the school of data communications and a member (and the founder) of the Information Security Research Centre at the Queensland University of Technology. He has served on the information security and privacy technical committee of the International Federation for Information Processing (based in Vienna, Austria) since 1984 and was chairman of that committee from 1988 till 1995.

“User organisations have got to take responsibility for security — not vendors,” Professor Caelli said. “We’re seeing the public increasingly being turned off initiatives like internet-based banking because of fears about security.

“The mobile device issue is another critical one. These devices simply get around system privileges.”

But if the organisations running networks are slow to wake up to the perils of mobile devices, there is no shortage of vendors beating the drum.

Colin Lim is the sales manager for Australia and New Zealand at Fortinet. He said in June 2004, the Cabir worm became the first significant security threat to infect mobile phones. “Cabir spread itself through Bluetooth connections,” Colin Lim said. “Although it deleted no data or transmitted personal information to strangers, it did block

subsequent Bluetooth connections and drained the mobile phone’s battery.”

He said Cabir demonstrated that viruses, worms and other security threats could reach beyond personal computers to other electronic devices.

“There are antivirus and anti-spyware programs for computers but how do you protect your mobile phone from viruses and worms?” Colin Lim said.

You will not be surprised to learn Fortinet has developed a suite of products that addresses mobile security threats.

“We’re facing the same kind of security issues we had when people started connecting PCs to networks,” Colin Lim said.

“We’re seeing more organisations calling us because they understand the threat,” he said. “Others seem to be content to rely on existing anti-virus software.”

For mobile devices, Fortinet will launch UTM (unified threat management) client security products later this year. This will extend the security capabilities of its current FortiClient product to include wireless mobile devices running Microsoft Windows Mobile and Symbian

“Removable media devices such as iPods, Blackberries and digital cameras get under the radar of network security systems.”

operating systems. It says this new mobile client software, deployable by mobile operators, handset providers or enterprises, will be the first on the market to deliver full anti-virus scanning, firewall, anti-spam, web content filtering, anti-spyware, network address translation (NAT) traversal and a VPN client.

If the threat to your network comes from your fellow employees, then that is where you should start to tackle the problem.

IBM recently conducted a survey of more than 3000 CIOs — 150 of them from Australia. It showed most were concerned about the threat to their business from cyber crime originating from within the organisation.

Interestingly, Australian CIOs believe more strongly than their global peers that employees now pose a threat to corporate security, according to the IBM survey. Seventy five per cent of local CIOs who spoke to IBM perceive that threats originate internally compared to a global benchmark, based on a total of 17 countries, of 66%.

IBM found 80% of Australian CIOs (84% globally) believe that lone hackers are increasingly being replaced by organised and technically proficient criminal groups.

"The rapidly changing nature of cyber crime means that we advise companies to be prepared to combat a whole new generation of security threats that extend well beyond

"Interestingly, Australian CIOs believe more strongly than their global peers that employees now pose a threat to corporate security, according to the IBM survey."

computer networks," said Claudia Warwar, a managing consultant in IBM Australia's security and privacy practice. "When we talk about security today, it means considering an entire organisation and much of its ecosystem of partnerships and relationships — from the network to the workforce, and from the workplace to the supply chain. Meeting this challenge requires an industry-wide approach — no one company can do it alone."

Despite highlighting the potential threat from employees IBM said, it seems Australian CIOs are concentrating on protecting their organisation from external threats. While 32% of respondents are intent on upgrading firewalls, for example, only 15% plan to invest in awareness and education training for employees. Another 10% will restrict the use of mobile devices such as wireless handheld computers not specifically sanctioned by the IT staff. "We strongly endorse educating employees who are in the first line of defence

The problems with USBs

The security audit by Lync Software identified three main problems caused by unsecured and unmonitored mobile devices. These were theft of data (unintentional and intentional), malicious code and increasing support costs. The problem is growing. Last year, it was estimated there were 85 million shipments of USB storage devices each with an average capacity of 462 megabytes.

Gartner estimates this will climb to almost 170 million annual shipments by 2010 with each USB device having an average capacity of 4.8 gigabytes.

The audit involved the installation of Lync USB to monitor removable media devices connecting to the organisation's main networks. Over a period of 10 days 768 users were monitored.

Key findings included:

- 296 users connected a USB device (39% of users audited);
- 154 different types of devices were connected;
- 1805 files were transferred between the network and the devices.

Image files were in the majority (1093 of the 1805 files transferred). This was followed by files in an MS Office format (455 out of 1805) and music files (109 of the 1805). Of the total number of devices attached (154), USB storage devices including flash drives and removable hard drives accounted for 99 devices. Cameras and scanners accounted for 10 while smart phones came close behind with seven.

Prior to the audit the organisation was unaware of who used USB devices and what information was being transferred from the network to these devices. Nor did they know what potentially malicious files were brought onto the network from removable media while inside the firewall.

"While no damage was done to the organisation we audited, you can see the potential risk is enormous," said Lync Software's Kym Welsby.

"Every organisation running a network must have a policy to protect that network before the threats arrive," he said.

to be cybercrime aware," Claudia Warwar said. As software becomes more secure, computer users will continue to be the weak link for an organisation. Criminals will focus more efforts on convincing end users to execute the attack instead of wasting time in lengthy software vulnerability discovery," said Ms Warwar.

IBM said it commissioned the research to better understand attitudes towards cybercrime, the costs incurred and how companies are responding to it.

Traditional anti-virus specialists are also coming to the party. Armagan Cetindas is the manager for systems engineering at Symantec. "We recognise the risk associated with attaching devices such as memory sticks," he said. "We haven't seen a huge amount [illegal] of activity in this area but we believe there will be an increasing threat from 'smart' phones.

"If they can send and receive emails they have the potential to breach your security," Armagan Cetindas said.

Symantec has expended virus protection for handheld devices with its MobileTrax product — part of a package of products designed to secure wireless devices running on Palm OS, Microsoft Windows Mobile and Pocket PC platforms.

"We estimate only about 1% of mobile devices such as PDAs have any form of protection against viruses," Armagan Cetindas said. "If they are being connected to your network, you could be in trouble.

"Wireless technology has changed the way we conduct business, offering mobile workers constant access to business-critical applications and data," he said.

"While this flexibility expands productivity, it introduces complexity and security risk as wireless devices become a new target for hackers looking to infiltrate a corporate network."