ON THE GO

By Deb Canning

Part 2: Understanding the risk assessment posed by the mobile construction workforce

In this second installment of a three-part series, Deb Canning, technical services manager for Computer Guidance Corporation, describes the security risks and outlines risk assessment and prevention—including implementation of effective policies and procedures.

Although there are many advantages to a mobile work environment, there are also serious risks. Risk assessment and prevention—including implementation of effective policies and procedures, employee education, and follow-up—are keys to ensuring the safety of mobile devices and the corporate information networks with which they communicate. Today, construction companies need to address mobile security in the same manner that they address the security of their local area network (LAN). In particular, they should target the following sources of security risk:

Network configuration. First and foremost, ensure that the corporate network is secure enough to handle mobile employees. In particular, administrators need to invest time and resources into maximizing LAN security, including its connections with mobile devices in field and jobsite offices and in employees' homes and cars. In fact, most security flaws are found in remote sites, devices, and the actions of the employees who operate them. Effective, well-enforced corporate and network policies are absolutely necessary to keep mobile users and the corporate network safe. Companies need to educate their employees about the security features of their mobile equipment because all the network-based defenses won't help if mobile users are connecting to the network while using compromised devices.

For construction companies and their network administrators—whether they are in-house or a third-party consultant—it is critically important to enforce security and configuration policies. For example, as jobs are closed out and project managers move from one jobsite to the next, network administrators must be able to limit or bar access to old project databases and enable their creation of and/or access to new data.

Virtual private network (VPN). Consider the potential security vulnerabilities of a VPN—the "tunnel" that is constructed using public lines, typically, the Internet, to connect from the mobile user to the corporate network. A VPN connection is designed to protect information between software applications and the VPN server itself; however, it does not provide complete end-to-end security. Encryption and other security mechanisms are used so that only authorized users can access the corporate network and the data cannot be intercepted. Antivirus software, updated system patches, layers of encryption, and user vigilance are required to establish a secure link between the mobile user and the corporate network. Additionally, firewalls and other security measures are also recommended.

Internet access control. It is advisable for companies to restrict inappropriate Web surfing and enforce Internet usage policies pertaining to workers connected to the LAN through a VPN connection. Install software on the network that will allow the administrator the flexibility to completely block Internet access as needed, allow access only to specific Web sites,

ABOUT the AUTHOR

Deb Canning is technical services manager for Computer Guidance Corporation, a Scottsdale, Arizona-based developer of financial and project management software solutions for the construction industry. She manages a technical support team and oversees installation of hardware and software, as well as internal IT efforts. She can be reached at 480.444.7000 or dcanning@computerguidance.com.

deny Web access to unauthorized Web sites, and, if necessary, restrict Internet access at certain times of day. Access to FTP sites, non-corporate Internet e-mail accounts, instant messaging, and newsgroups can also be restricted.

Router security. A router is a device that forwards informaion packets between networks. It may be hard-wired or wireless. And just as cell phones are less secure from eavesdropping than are land lines, wireless routers are not as secure as hard-wired routers. To ensure that a wireless router is secure, be sure that the system administrator devotes time to setting up the security features of the company's wireless network.

Some router settings are often overlooked, but can offer greater security:

- ***Turn off UPnP (universal plug and play):*** Although UPnP is a nice feature that lets devices on the network self-configure, it is also a security hazard. A virus on a computer inside the network could use UPnP to open a "hole" in the router's firewall to let outside computers in. That is why it is important to turn off UPnP when it is not in use.
- ***Change the administrator's password:*** Routers come with a default user ID and password to protect the router's configuration. System administrators must be sure to change the password so unauthorized wireless users cannot get into the router and change its configuration settings.
- ***Filter media access control (MAC) addresses:*** A MAC address is a unique identifier that is assigned during the manufacturing of a network device. A device's MAC address can usually be found on the device. MAC address filtering is a good way to limit which devices are allowed to connect wirelessly to the network and keep unauthorized wireless surfers out of the company's network.
- ***Update the firmware:*** Firmware is the software that operates inside the router. The router vendor will periodically issue firmware updates to solve system glitches. Make sure that system administrators stay current with updates, checking the vendor's Web site quarterly for new updates.

Operating system (OS) security. Remote PCs and mobile computing devices are at risk of a virus infection or susceptible to being compromised by an attacker. Maintaining a secure, reliable operating system requires users to regularly check the system's files and services, diligently download OS patches, "hot fixes," and service packs from the manufacturer's Web site, and properly install these. Mobile workers should be responsible for maintaining their OS at this basic level of security and reliability. For example, Microsoft Windows "Automatic Update" should be configured to allow automatic downloads of patches as they are released. System administrators should perform regular audits and any maintenance requiring a higher level of technical expertise.