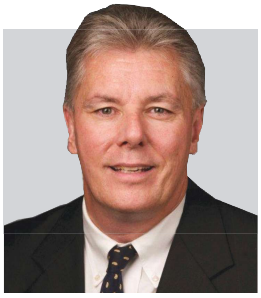
IT Intelligence

6 WAYS TO GUARD AGAINST CYBERATTACKS

by Bob Stockwell



Bob Stockwell is Global Technology Leader for STANLEY Security. From 1997-2012, he was Niscayah's Director of Systems Operations.

bob.stockwell@sbdinc.com

According to recent Advanced Threat Reports, the average business experiences an advanced malware or cyberattack every three minutes. These attacks originate from multiple sources and any or all of them can significantly compromise a business' enterprise system to allow an attacker to illicitly take over enterprise access control, video, fire and intrusion systems. With so many current security platforms relying on the IT infrastructure, crucial systems can be put at risk without preventative measures in place.

Cyberattacks on a business' enterprise platform can compromise physical security and safety, reveal proprietary and personal info and cost up to millions of dollars to recover. Following are vulnerabilities and practices to avoid:

BYOD (Bring Your Own Device) — The practice of allowing personal iOS, Android, Windows and Blackberry devices to be used in a business is saving companies money and improving employee mobility, productivity and job satisfaction. However, these devices are largely unregulated in the business environment and are often susceptible to hacking. Unbeknownst to an employee, he or she could bring a hacked device to work, potentially compromising the entire company infrastructure. TopPatch, a security patch management firm, found more than 1,700 Android apps carrying malware, including Livelocker, a lock screen tool with 100,000+ downloads, and the Photoshop Tutorial app with nearly 700,000 downloads. Both of these free apps steal user information when installed.

Cyberattacks on a business' enterprise platform can compromise physical security and safety, reveal proprietary and personal info and cost up to millions of dollars to recover.

Social Engineering — Often, a trusted Web site that's been hacked will inform the user that a virus has been detected and to download XX software to remove it. Running this software will infect the user's computer, along with others on the network.

Unpatched Software — Many security systems run on Microsoft platforms, and patches released from Microsoft must be tested against a business' enterprise platforms. The time delay between testing and approval can increase a company's risk of system compromise.

Spearphishing — This attack is sent through an E-mail that appears valid, asking for confidential or personal information and may go as far as including a warning against fraudulent E-mails. What gives these away as malware-carrying is a rogue link to the Web site.

APT (Advanced Persistent Threat) — Similar to phishing but will include an attachment, usually in the form of a .zip file. The E-mail subject typically contains keywords or phrases associated with business, such as false UPS notifications. This E-mail is sent to multiple users in the hopes that at least one recipient will fall for the scam.

Per these and other methods, hackers are very creative and persistent. Recently, a hacker mailed a hacked smartphone with a high-capacity battery to a business. This phone sat in the mailroom with the Wi-Fi turned on and attached to the unsecured internal wireless network to allow the hacker unrestricted access to the internal systems.

Stuxnet, the virus responsible for disrupting the Iranian nuclear program, proved that even disconnected isolated systems can be hacked given enough time. Imagine an employee attends a trade show and is given a jump drive with product information. There isn't a way to know what is truly on the drive until it is inserted into a computer — at which point, it may already be too late to prevent the system from being compromised.

Here are six steps to reduce cyberthreat exposure:

1. Educate employees by providing updates on what to watch for and information on new trends. A knowledgeable employee base offers a great defense system and an inexpensive source of protection.
2. Prioritize establishing, enforcing and educating staff on a solid security policy.
3. Keep patch management up to date. Unpatched software, such as Adobe and Java, can allow an attacker a backdoor into the system. This is commonly overlooked.
4. Always keep antivirus systems current.
5. Create multiple layers of defense; don't depend on just the corporate firewall.
6. Segment and segregate systems to help protect critical platforms. Installing additional firewalls between the segments inside the business infrastructure will create a multilayered defense. ■