Combat the Insider Threat

ION

As seen in:

NETWORKWORLD®

May 12, 2008 Issue

Top 5 Ways Insiders Exploit Your Network...and What You Can Do About It

by: Bill Whitney with Tara Flynn Condon

Recently, Cox Telecom employee William Bryant pleaded guilty to information technology sabotage, having caused the loss of computer, telecommunications, and emergency 911 services for thousands of Cox's business and residential customers throughout Dallas, Las Vegas, New Orleans, and Baton Rouge[1]. The now-former employee faces a potential 10-year jail sentence and $250,000 fine, but the future is less certain for Cox. According to the company, services were fully restored and the damage repaired. However, the incident's affect on Cox's reputation has yet to be determined.

The Cox story, along with recently publicized incidents at NASA[2], Accenture[3], Gap[4], and Medco[5], serve as a harsh reminder that insiders represent a common and often misunderstood threat. The acts of data theft and sabotage insiders perpetuate can result in hard costs, compliance-related problems, legal fees, productivity loss, and possibly more costly than any other result, a tarnished reputation. Furthermore, the Cox and Gap stories in particular, illustrate how the negative or careless actions of a vendor (more specifically, a vendor's employee), can have a similarly negative impact.

Insider threats are up 17% according to the latest Computer Security Institute survey[6]. (Recent surveys by consultants Deloitte[7] and another by CSO magazine[8] echo this trend.) As IT and communication systems grow in complexity, so too do the numbers of employees, contractors, and managed service providers required to maintain them. The spike in threats is not surprising given the often unfettered and unmonitored access these insiders have to critical corporate networks.

Recent incidents have awakened companies to the need to monitor trusted insiders as aggressively as they do the outsiders who try to breach network security. However, policing both actual and trusted insiders can prove challenging given the privileged access they require to do their jobs. This article explores the five most common methods insiders use to access network resources, along with simple measures enterprise IT departments can take to protect against their threats.

#1: Modems

A lack of central management combined with easy-to-guess static passwords make modems an ideal entry point for insiders with detailed knowledge of the network. Many companies have tried to address this challenge by simply unplugging the modems until needed. However, paradoxically, unplugging modems makes it impossible to use them for their intended purpose, namely remotely restoring critical systems in times of emergency or outage. Given that modems are a necessity, enterprises must extend the same security and identity confirmation measures to modems that they do to other remote network entry points. Extending corporate two-factor authentication measures to modems or replacing legacy modems with newer, more secure models with embedded multi-factor authentication can provide appropriate and cost-effective protection.

#2: Open File Transfer

Most organizations use open file transfer to patch network infrastructure devices. Internal technicians and vendors use this poorly secured, unrestricted

www.ion-networks.com

access to quickly troubleshoot, apply appropriate fixes, and correct problems. However, they can also misuse this freedom to change files, remove critical components, or disrupt systems, resulting in non-operational systems, web site defacements, data theft and other extremely negative situations. Certainly a disgruntled or former employee has both the knowledge and motivation to commit these acts. However, more often, the insider threat can be less dramatic but equally troublesome. Even well intentioned employees can be careless or make inadvertent mistakes. As such, protecting your information assets requires you to have control over who can upload and download files, and a clear and easily retrievable record of all changes made to the system and the person who made them. Traditionally, limiting and monitoring open file transfer required that individual permissions be set on each machine, causing headaches for IT departments. However, new technologies, such as Vendor Access and Control (VAC) systems, can limit access and monitor activities organization-wide or for specific systems.

#3: Open Telnet and SSH Ports

Companies that use third parties to remotely access and troubleshoot systems should properly secure or close telnet and SSH ports. Without these protections in place, all a remote technician needs is a single internal IP address to get anywhere on your network without your knowledge. It is dangerous to assume that remote technicians have limited knowledge of your IP addressing schemes, as it is possible the same technician has worked on site at your facility. Also, infrastructure equipment often shares one easily guessed password, making it simple for an insider to access unauthorized equipment. As a standard practice, it is recommended that companies restrict third party access via telnet or SSH to systems beyond the typical scope of their services, unless the session is recorded or actively shadowed by a member of your team. Alternatively, many organizations use intermediary systems to create a proxy for these sessions, adding the needed level of control and tracking.

#4: Server Console Ports

Technicians frequently connect to serial console ports, very often on routers and Linux/Unix servers. To provide scalable access, companies will often connect to serial console ports using terminal servers. However, terminal servers, by default, offer minimal security. By gaining access to a single terminal server, an insider can access and potentially disable thousands of systems within the organization. As such, it is recommended that companies regularly review terminal server security capabilities and place security devices outside the console ports of systems hosting sensitive data (for example, financial records, customer data, human resources information).

#5: Unmonitored Extranet Traffic

Extranets provide a convenience for companies, allowing them to open their networks to vendors, customers, and partners to support real-time collaboration. Extranets (for example, IPSec, SSL, remote desktop) work reasonably well when the number of systems that must be shared with outsiders is small, and the authorization level on those systems can be tightly controlled. However, typical extranets, where access to many systems is required or where high level authorization must be granted, can be problematic. Often, too much access is granted inadvertently, and activities cannot be closely monitored and controlled. As opposed to typical extranets, VAC systems offer the extra layer of control needed to prevent sabotage and data theft.

While many third party providers are trustworthy, it is risky to make that assumption. Regardless of whether employees and/or third party providers access your network, human motivations remain the same. With any insider, there is the prospect of misuse, possibility of mistakes, and opportunity for theft. However, increased awareness combined with a few protective measures can reduce the risk an insider will take advantage of your business.

Sources: (1) Gaudin, Sharon. "Cox Telecom Worker Pleads Guilty to Sabotage." Information Week. September 28, 2007 (2) Associated Press. "NASA Reports Employee Sabotage of Computer for Space Station." USA Today. July 26, 2007 (3) Greene, Tim. "Accenture Sued by US State over Theft of Bank Account." ComputerworldUK. October 1, 2007 (4) Gaudin, Sharon, "Theft of Gap Laptop Puts 800,000 Applicants at Risk." Information Week. October 1, 2007 (5) Gaudin, Sharon. "Medco Sys Admin Pleads Guilty to Sabotage." Information Week. September 19, 2007 (6) "12th Annual Computer Crime and Survey." Computer Security Institute (CSI). September 2007 (7) Hines, Matt. "Insider Threats Remain IT's Biggest Nightmare." PC World. September 22, 2007 (8) CSO Magazine. "Press Release: Over Confidence is Pervasive Amongst Security Professionals." September 11, 2007.

About the Author: Bill Whitney is Chief Technology Officer and co-founder of ION Networks, Inc., a leading manufacturer of remote administrative management and secure access technology. A recognized authority on security, Whitney has worked with some of the world's premier organizations to improve remote management and security, including Fortune 500® financial institutions, telecommunications firms, and government and military agencies. Bill can be reached at bw@ion-networks.com. For more information about the company, visit www.ion-networks.com.