The Cyberspace Insider Threat

Kathryn Stephens, NSCI
October 20, 2010

National Security Cyberspace Institute, Inc. (NSCI)

Through the combination of research and education, NSCI supports public and private clients aiming to increase cyberspace awareness, interest, knowledge, and/or capabilities. NSCI is committed to helping increase security in cyberspace whenever and wherever possible. NSCI publishes a bi-weekly newsletter (*CyberPro*), has published numerous whitepapers on various cyberspace topics, maintains an online cyber reference library, and has established an email distribution list for sharing cyber-related resumes to interested parties. NSCI is a small, veteran-owned business headquartered in Virginia.

Issues

A federal grand jury recently indicted a former Johns Hopkins Hospital employee on fraud and aggravated identity theft charges for stealing hospital patient identity information to open fake credit accounts and make purchases. The scheme resulted in more than $600,000 in credit from more than 50 institutional and individual victims. Johns Hopkins filed a breach report with the state of Maryland which said that more than 10,000 patient records had been accessed by the employee.[1]

Insider threats have become as complex and dangerous to enterprises as attacks that come from external malicious hackers. Insider threats can come from well-meaning employees, as well as those who are disgruntled or malicious. Because employees often have access to sensitive business information, insider breaches can often be more dangerous than outside attacks.. Insider threats are especially common given the poor economy, where many workers are attacking their companies to take information to a new employer, or to steal money if they lose their job. Well-meaning employees can also put business data at risk by accidentally giving malicious hackers unauthorized access to company systems and networks or by losing devices such as USB drives or laptops containing company information.

Several insider data breaches have made recent headlines. Terry Childs, a former IT administrator for the city of San Francisco, was convicted in April of violating California hacking laws for refusing to hand over administrative control to the city's FiberWAN network in 2008. The city spent $900,000 trying to regain control of its network.[2] Last month, nine former Sprint employees were charged with abusing their access to Sprint systems to redirect phone charges to other customers by cloning their cell phones. The scheme resulted in more than $15 million in fraudulent charges. CMU's Software Engineering Institute says that insider breaches are becoming more common, and that they can be more dangerous than outside attacks because the average inside breach lasts 15 months, and often goes undetected.[3]

The 2010 Verizon Data Breach Investigations Report from Verizon Business and the U.S. Secret Service reports that 48 percent of data breaches are caused by insiders, and that another 11 percent of breaches are caused by business partners. The report also found that 48 percent of all data breaches occur because of privilege misuse.[4]

In March 2009, Information Week Analytics released a report called "Understanding the Danger Within" that discussed the different types of insider threats and how enterprises are addressing these threats. According to the

[1] Wilson, T. (2010, October 1). *Five Indicted At Johns Hopkins Hospital For Identity Theft Scam.* Retrieved October 5, 2010, from Dark Reading: http://www.darkreading.com/insiderthreat/security/government/showArticle.jhtml?articleID=227600057

[2] Wilson, T. (2010, August 9). *Former IT Admin Gets Four Years For Locking City Of San Francisco Out Of Its Network.* Retrieved September 5, 2010, from Dark Reading: http://www.darkreading.com/insiderthreat/security/management/showArticle.jhtml?articleID=226600285

[3] Lemos, R. (2010, September 8). *Fraud At Sprint Offers Lessons For Enterprises, Experts Say.* Retrieved October 5, 2010, from Dark Reading: http://www.darkreading.com/insiderthreat/security/management/showArticle.jhtml?articleID=227300424

[4] Verizon Business RISK Team. (2010). *2010 Data Breach Investigations Report.* Retrieved September 15, 2010, from Verizon Business: http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

Information Week report, 20 percent of end users admit to changing the security settings on their company-issued devices, and 35 percent of end users admit to violating corporate security policies in order to expedite their work or increase productivity. Another study from Ponemon Institute and Symantec Corporation found that more than half of employees who left their companies in 2008 took sensitive corporate data with them, although almost 80 percent of these employees said that they knew it was against company policy to take the data.

Based on data from the above mentioned studies, it is clear that employees often violate security policies and circumvent practices that were designed to protect corporate systems. Whether these violations are meant to be malicious or if they are simply mistakes, they can lead to data leaks and expose sensitive corporate information.[5]

There are three main types of insider threats that companies should be prepared to address. First, there are well-meaning employees who break security policies or unintentionally expose sensitive information. These employees are trying to increase their productivity or do their job more efficiently. Second, there are malicious employees who break security policies for personal reasons, or to steal or sabotage corporate data. Finally, trusted partners can also pose a security threat because they are given access to corporate systems.

Most corporations perceive well-meaning employees to be their biggest threat from the inside. Employees who log into public wireless networks could unknowingly leak data, and employees who remove laptops and storage devices from their office risk losing their devices, as well as the sensitive information that they store. Typical employees may even share business information on social networks, not realizing that they are providing hackers with useful information.

Threats from malicious insiders can be very dangerous, since these malicious employees often know the company’s sensitive secrets and vulnerabilities. Deliberate insider threats are carried out by employees who intentionally break security policies and usually occur as theft for financial gain, system sabotage or theft to gain a competitive advantage. There are many reasons why an employee would choose to “go bad” and steal information from a company or hurt a company system. Disgruntled employees may have been passed over for a promotion or may have been fired. These malicious employees could also be planning to take information to a new employer.[6] Malicious inside threats have increased, especially given the declining economy. Jacob West, security research director at Fortify Software, says “The biggest driver we’ve seen for malicious insiders in the past 18 months has been the economic downturn.” West explains that a bad economy can “cause unethical insiders to plant backdoors, logic bombs or other nefarious code that they believe will allow them to steal funds, information or do other damage to the company from the outside in the event that they are laid off.”[7]

Trusted partners can pose a significant threat to an organization because they can introduce infection to a network, or gain access to sensitive information. Enterprises must develop strong security policies and defenses against even their closest and most trusted partners since everything from proprietary intellectual property to customer information is at risk. Like internal employees, trusted partner threats can be completely accidental or malicious and intentional. Trusted partners pose a threat to enterprises primarily by the release of confidential information and the injection of malicious code into the network or infrastructure.

[5] Wilson, T. (2009, March). *Understanding the Insider Threat.* Retrieved September 15, 2010, from Information Week Analytics: http://i.cmpnet.com/darkreading/insiderthreat/DarkReadingInformationWeekAnalyticsTechCenterInsideThreat.pdf

[6] Olzak, T. (2010, August 2). *The barbarians are already inside the gates: Mitigating insider threats.* Retrieved September 15, 2010, from Tech Republic: http://blogs.techrepublic.com.com/security/?p=4148

[7] Prince, B. (2010, July 16). *Fighting Insider Threats Spotlighted at DEFCON Conference.* Retrieved September 15, 2010, from eWeek.com: www.eweek.com/c/a/Security/Fighting-Insider-Threats-Spotlighted-at-DEFCON-Conference-477657/

Ideas

Many companies already have policies in place to address threats from well-meaning employees, malicious employees and trusted partners. Companies often choose to focus on technology, people and processes when defending against insider threats.

Technology

Although there is no one technology or practice that can completely combat insider threats, enterprises and vendors are beginning to defend themselves by using data leak prevention (DLP) technology. The presence of DLP technology will not keep a malicious employee from stealing information, and may not prevent highly sophisticated attacks, but DLP can prevent information leaks from accidental disclosures or amateur thefts. DLP is software that seeks out sensitive data and then enforces policies for handling it. If a user tries to post sensitive information or copy it to a USB storage drive, DLP technology can find and record that activity. DLP can even keep a user from copying certain information to an external storage device, or disallow an e-mail user from sending it.[8] While DLP is good for preventing unintentional data leaks, it is usually weak at stopping malicious attacks since most malicious insiders have authorized access to internal data.

Another technology that can be used to combat insider threats is network access control (NAC), which controls access to workstations and servers, while ensuring that every machine attached to the network is using up-to-date software versions that are patched and protected by anti-malware applications. It is important to remember to ensure that all trusted partner machines are also protected by NAC or follow the same standards of network safety as the organization's own systems.[9]

All sensitive information should be encrypted, especially privileged customer information. Enterprises can also use virtual private networks (VPNs), which are established between workstations or between the network edges of two separate networks, to protect data when it is transferring between corporate and partner systems. Tunnels that are created between network edges also automatically encrypt the information that is being transferred. Workstation VPNs should be required for all remote workers connecting to the corporate network.[10]

People

There are several other things that enterprises can do to improve internal security in addition to deploying the proper technologies. User training and education is a very powerful tool to increase security practices. Employees should be taught to create strong passwords and undergo awareness training. Employees should be trained how to tell the difference between a real Web address and an obfuscated address. Some companies have even launched fake phishing scams to judge employee awareness. Organizations might also secure and restrict the use of portable devices.[11] Employees should be trained on what kinds of information can never be shared and should be trained on the risks of sharing unauthorized data. Employees could even be trained on how to recognize suspicious behavior

[8] Wilson, T. (2009, March). *Understanding the Insider Threat.* Retrieved September 15, 2010, from Information Week Analytics: http://i.cmpnet.com/darkreading/insiderthreat/DarkReadingInformationWeekAnalyticsTechCenterInsideThreat.pdf

[9] Franklin Jr., C. (2009, October). *Protecting Your Partnerships - And Your Data.* Retrieved September 15, 2010, from Information Week Analytics: http://i.cmpnet.com/darkreading/insiderthreat/Dark_Reading_IWKAnalytics_Insider_Threat_TC4.pdf

[10] Franklin Jr., C. (2009, October). *Protecting Your Partnerships - And Your Data.* Retrieved September 15, 2010, from Information Week Analytics: http://i.cmpnet.com/darkreading/insiderthreat/Dark_Reading_IWKAnalytics_Insider_Threat_TC4.pdf

[11] Bednarczyk, M. (2009, March). *Well-Meaning Employees - And How To Stop Them.* Retrieved September 15, 2010, from Information Week Analytics: http://i.cmpnet.com/darkreading/insiderthreat/DRTechCenterWellMeaningEmployees.pdf

in their coworkers that could mean a breach is occurring. Companies should also set up a method for employees to report suspicious behavior.[12]

Processes

Many corporations are also taking preventative measures to stop malicious insiders from breaking security policies or stealing information. The organizations that are most effective at stopping malicious insider breaches are those who carefully review reports that are generated by the company's systems. Organizations are also looking at environmental issues such as disgruntled employees and behavior changes to recognize when an insider attack may be taking place. Organizations should recognize the importance of detection, including network and operating system logging. Organizations should also have a strong audit process in place for reviewing system logs for any unusual activity.[13]

When developing security policies for trusted partners, companies must decide what information is appropriate for their partners to access. Partners should always be given the "least-privilege" possible, with access to only those systems and data that they truly need. Social security numbers and credit card numbers should always be blocked from being transferred to any network or system.

Answers

Detecting and preventing insider threats consists of three main areas: user training and awareness, the deployment of appropriate technologies, and monitoring behavior and system logs for abnormal activity. It is important that enterprises develop a preventative mindset that focuses on defending against insider threats, rather than reacting to data breaches after they happen.

User Training and Awareness

Data breaches can often be prevented through employee education and awareness training. Businesses should educate employees on the potential risks from insider vulnerabilities, as well as the consequences for violating corporate policies. Employees should be trained on the importance of choosing complex passwords and account management policies. Employees should also be trained to prevent stolen credentials, which is the most common way of gaining unauthorized access into an organization. Train employees to recognize behavioral changes in their coworkers that could be a warning sign for an insider attack.

Technology

Enterprises should make sure that they have the appropriate technologies in place to detect and prevent insider threats. These include VPNs, NAC, end-point security suites, encryption, and DLP. When going into business with a new partner or vendor, enterprises should ensure that their new partner has the same level of security requirements as the organization does.

Business Policies and Processes

Enterprises should build insider security policies and practices into their business plans. Businesses should identify which assets are most at risk, and then take steps to defend that information from unauthorized access. Businesses should institute enterprise-wide risk assessments and define a risk-management strategy for protecting

[12] Olzak, T. (2010, August 2). *The barbarians are already inside the gates: Mitigating insider threats.* Retrieved September 15, 2010, from Tech Republic: http://blogs.techrepublic.com.com/security/?p=4148

[13] Davis, M. (2009, May). *How To Detect And Stop Malicious Insiders In Your Organization.* Retrieved September 15, 2010, from Information Week Analytics: http://www.darkreading.com/insiderthreat/util/download.jhtml?id=176500028&cat=whitepaper

assets from insiders. New employees should always be given access to the minimum amount of information and systems for them to do their job, and businesses should also perform background checks on employees who will be in sensitive positions. Finally, no security setting or policies would be effective without continuous monitoring and auditing. Businesses should watch for even minor policy violations, which often are warning signs for more serious violations. Review logs to ensure that no information is being accessed inappropriately or transferred out of the corporate network. Enterprises should also monitor and filter incoming network traffic. When monitoring network traffic, businesses can look for unusual access patterns like a suspicious time or day or date, abnormal IP addresses, or if information is being accessed and organized according to specific type. Computer access should always be deactivated immediately following an employee's termination. Business policy should also address how to recover in case of a data breach. Finally, it is also important for businesses to share incident information. With the proper policies and procedures in place, insider threats can be successfully detected and prevented, protecting corporate information and saving enterprises time and resources.