



Information Security Practices that are Easy and Inexpensive to Implement

By Marv Chen and Kevin Tsuei, AuditOne LLC

According to a 2008 U.S. Department of Justice Report, 75 percent of businesses victimized by cyber crime said that insiders were responsible for the crime. Here we recommend some easy and inexpensive information security practices to implement that will help deter such threats.

Disabling USB Flash Drives

USB flash drives allow employees easily to take a massive amount of data out of the office or bring unauthorized (possibly malicious) software into the bank's computing environment. Many banks do not have the necessary resources to constantly monitor use of USB flash drives or software installation on workstations.

A solution may be to disable the USB ports of workstations where their use is unnecessary. This can be accomplished through Windows Domain Group Policies, Local Policies/Windows Registry changes, or physical disconnection of the USB ports. A partial implementation to allow only read-only access for USB drives can also be considered, i.e. Fedline Advantage workstations.

Disable Login during Non-Business Hours

Again, smaller banks may not have the resources to constantly monitor employees' actions. Many malicious acts occur during non-business hours because perpetrators feel safer that no one can walk in on them.

A solution may be to restrict login hours of most personnel to a limited window of an hour before and after official business hours. In addition, Domain Group Policies can also force an automatic logoff when the login time expires.

Patching Windows Operating Systems

Some network administrators don't consider this a priority since most computing devices are behind a firewall. While this is true, employees are still prone to targeted social engineering attacks such as spear-phishing e-mails. These types of attacks may lead an employee to execute a malicious attachment by mistake. This situation usually is exacerbated by the fact that most users have Local Administrator rights on the workstations because various specialized banking applications require this level of access.

Microsoft releases patches on a periodic basis to fix vulnerabilities or security holes that are often exploited by malicious software. Some patches actually purge systems infected with specific malicious programs.

Manually patching operating system on a periodic basis is both time and resource consuming. Therefore, more feasible solutions may be to turn on automatic updates on individual workstations or to employ Windows Server Update Services (WSUS). Additional hardware costs can be avoided as a WSUS server uses little resources and can be run as virtualized server (Microsoft Virtual Server) on existing hardware. Finally, running a Microsoft Baseline Security Analyzer (MBSA) periodically can determine if computing devices have the most up-to-date security patches.

Employee Social Engineering Training

Social engineering can be an effective method used by potential attackers to gain access to the inside where most of the damage can be done. Spear-phishing, as mentioned above, is becoming an increasingly popular method. Other methods may be through pre-text calling or gaining physical access to the bank, i.e. an attacker disguising himself as a utility worker.

Banks should implement robust methods to verify the identity of the person or the source. Identifying customers by using only social security number and birth dates should not be relied upon, as such information (social security, date of birth, etc.) can be easily obtained from Internet-based private investigator-type services. We recommend the use of information known only to the customer and the bank such as pass phrases or recent transactions.

Employees should be educated and reminded periodically on how to detect phishing emails (there are numerous free training resources that can be found on the web for this) and to verify the identity of utility workers and contractors.

Finally, all personnel should be aware of incident response processes in place. Social engineering is very difficult to defend against, especially for customer-service oriented community banks. An employee should never have to be afraid of admitting to a mistake and taking immediate and appropriate action to inform an incident response team.

Marv Chen (marv.chen@audit-one.com) is AuditOne's director of product development. He holds a CISSP and CISA, and has 15 years high level technical experience in the banking and financial services industries. Kevin Tsuei (kevin.tsuei@audit-one.com) is an associate of AuditOne, and has experience in database and code development, web development and network security engineering for the financial services, legal and educational industries.

http://www.wib.org/publications_resources/technology_security_digest/dec09/chen.html