Protecting Your Digital Assets within the Network's Resources

Bill Knapp The Greater Lansing Business Monthly 27 March 2012

It's hard to miss the news when 45 million customers' credit and debit card numbers are stolen from TJX Companies … or 26.5 million veterans' records are stolen from the U.S. Department of Veterans Affairs … or 1.5 million customer credit card records are stolen from DSW. In addition to damaging the organization's reputation, these incidents come with very serious financial costs. It has been reported that the DSW data breach has cost DSW more than $10 million to date.

The methods for accessing and acquiring the data in these three incidents were all different, but the end result was unfortunately the same. The lesson that can be learned from these three incidents could also be the same: Good information security comes from defense in depth. Layers of security must be built much like the moats, the castle walls and the boiling oil that protected the king in days of old.

The two previous articles discussed the need for physical security and the need for network security. With physical security, facilities are secured in layers that protect the electronic assets (locks, access control, fire suppressant, and more) as well as protect the physical instances of the data (paper, removable media, and others). Then layers of network security help guard against the entry of attackers and malware (viruses, worms, and such) that then travel across the network, both from the Internet and from within the internal network. However, if the facilities are breached or the network is compromised, then the data as well as the resources where the data reside must be protected. These data can be found within files (primarily in databases and other software application files) and within systems (servers, desktops, laptops, PDAs, cell phones). It is here where we now focus our attention on the various points and layers of the Logical Security that will protect the organization's digital assets.

Viruses

Antivirus and anti-malware programs continue to be one of the best frontlines to avoiding security breaches. As we have all become aware over the years, a virus can create havoc on your laptop or cause a denial of service (DoS) that brings your file servers down. However, the greater risk comes in the form of a Trojan or backdoor program that can capture data and network passwords for hackers to use later to gain access to systems that host otherwise confidential information. To guard against these threats anti-virus and antimalware software must be ubiquitous across all systems (workstations, servers); and since there are constantly new viruses traversing the network, there must be a vigilant effort to maintain current virus signatures used by the anti-malware applications.

Web applications

Over recent years hackers have increasingly shifted their efforts away from hacking networks and servers to attacking the organizations' Web-based applications. This approach of tunneling through in these flawed applications ultimately provides entry to the backend files and databases where sensitive data are stored. In order to guard against these new risks, secure Web application development practices needs to be implemented. Organizations such as the Open Web Application Security Project (*www.owasp.org*) provide useful guidelines for secure application development. If there is an application currently in production that is suspect of being insecure, a Web application assessment may need to be performed to identify the vulnerabilities and malicious code found within the application. This assessment should identify common application vulnerabilities, such as buffer overflow, cross-site scripting and SQL injection, as well as systems issues such as network architecture, application authentication and connectivity.

File servers

"Insider" or internal security breaches account for up to 50 percent of today's security incidents. As a measure to protect from these breaches, while still providing reasonable data access for employees, it is necessary to "harden" the servers and critical systems that host the protected data. Proper server hardening can provide increased levels of file-level security as well as minimizing security compromise risks. NSA (*www.nsa.gov*) and SANS (*www.sans.org*) offer helpful guidelines for server hardening.

System logging

With industry regulations such as HIPAA and Sarbanes-Oxley, many organizations are now required to collect log data from servers and workstations to provide an audit trail. This is a best practice that should really be followed by all organizations, independent of the need to comply with regulation, to identify performance problems as well as various security events. System logs are found in a variety of devices ranging from servers to network firewalls and routers. The log reviews should be performed by a skilled IT professional on a regularly scheduled basis to identify historic events. For an increased level of security, automated monitoring systems can be implemented to perform real-time analysis that can alert the IT staff to more quickly respond and mitigate the risk.

Disk and file encryption

As far back as 50 B.C. with Julius Caesar's invention of Caesar's cipher, we have utilized encryption to maintain the secrecy of sensitive information. For organizations that store sensitive information on workstations and laptops, full disk encryption should certainly be deployed. The encryption process transforms information to render it unreadable without the use of a special key. To begin, a thorough assessment should be completed to identify which systems contain this sensitive data. Laptops and remote systems at home offices that are considered less secure are immediate candidates, but internal workstations and tape backups should also be considered for a more comprehensive security posture. The incident with the VA would have been completely avoided if full disk encryption had been deployed.

There certainly is a strong business requirement for protecting confidential information and in some cases there is a legal requirement. Either way, when it comes to protecting an individual's privacy, it's just the right thing to do.

Bill Knapp is the security sales executive for Analysts International and has been in the information technology business for over 20 years. Knapp can be reached at bknapp@analysts.com and 517-336-1059.