Information Security Management

Mariana Hentea
Southwestern Oklahoma State University, USA

INFORMATION SECURITY MANAGEMENT OVERVIEW

Information security management is the framework for ensuring the effectiveness of information security controls over information resources to ensure no repudiation, authenticity, confidentiality, integrity and availability of the information. Organizations need a systematic approach for information security management that addresses security consistently at every level. However, the security infrastructure of most organizations came about through necessity rather than planning, a reactive-based approach as opposed to a proactive approach (Gordon, Loeb & Lucyshyn, 2003). Intrusion detection systems, firewalls, anti-virus software, virtual private networks, encryption and biometrics are security technologies in use today. Many devices and systems generate hundreds of events and report various problems or symptoms. Also, these devices may all come at different times and from different vendors, with different reporting and management capabilities and—perhaps worst of all—different update schedules. The security technologies are not integrated, and each technology provides the information in its own format and meaning. In addition, these systems across versions, product lines and vendors may provide little or no consistent characterization of events that represent the same symptom. Also, the systems are not efficient and scalable because they rely on human expertise to analyze periodically the data collected with all these systems. Network administrators regularly have to query different databases for new vulnerabilities and apply patches to their systems to avoid attacks. Quite often, different security staff is responsible and dedicated for the monitoring and analysis of data provided by a single system. Security staff does not periodically analyze the data and does not timely communicate analysis reports to other staff. The tools employed have very little impact on security prevention, because these systems lack the capability to generalize, learn and adapt in time.

Therefore, the limitations of each security technology combined with attacks growth impact the efficiency of information security management and increase the activities to be performed by network administrators. Specific issues include data collection, data reduction, data normalization, event correlation, behavior classification, reporting and response.

Cyber security plans call for more specific requirements for computer and network security as well as emphasis on the availability of commercial automated auditing and reporting mechanisms and promotion of products for security assessments and threat management (Hwang, Tzeng & Tsai, 2003; Chan, 2003; Leighton, 2004). Recent initiatives to secure cyberspace are based on the introduction of cyber-security priorities that call for the establishment of information sharing and analysis centers. Sharing information via Web services brings benefits as well as risks (Dornan, 2003). Security must be considered at all points and for each user. End-to-end security is a horizontal process built on top of multiple network layers that may have security or no security. Security is a process based on interdisciplinary techniques (Mena, 2004; Maiwald, 2004).

The following sections discuss security threats impact, emerging security management technologies, information security management solutions and security event management model requirements.

SECURITY THREATS IMPACT

Information security means protecting information and systems from security threats such as unauthorized access, use, disclosure, disruption, modification or destruction of information. The frequency of information security breaches is growing and common among most organizations. Internet connection is increasingly cited as a frequent point of attack and

likely sources of attacks are independent hackers and disgruntled employees. Despite the existence of firewalls and intrusion detection systems, network administrators must decide how to protect systems from malicious attacks and inadvertent cascading failures. Effective management of information security requires understanding the processes of discovery and exploitation used for attacking. An attack is the act of exploiting a vulnerability that is a weakness or a problem in software (a bug in the source code or flaw in design). Software exploits follow a few patterns; one example is buffer overflow. An attack pattern is defined as a "blueprint for creating a kind of attack" (Hoglund & McGraw, 2004, p. 26). Buffer overflow attacks follow several standard patterns, but they may differ in timing, resources used, techniques and so forth.

Broad categories of attack patterns include network scanning, operating system stack identification, port scans, traceroute and zone transfers, target components, choosing attack patterns, leveraging faults in the environment, using indirection and planting backdoors. Typically, an attack is a set of steps. The first phase is discovery or network reconnaissance. The attacker collects information about the target using public databases and documents as well as more invasive scanners and grabbers. Then, the attacker tries to discover vulnerabilities in the services identified, either through more research or by using a tool designed to determine if the service is susceptible. From a damage point of view, scans typically are harmless. Intrusion detection systems classify scans as low-level attacks because they don't harm servers or services. However, scans are precursors to attacks. If a port is discovered open, there is no guarantee that the attacker will not return, but it is more likely that he will and the attack phase begins. Several services and applications are targets for attack.

"Web within Web" (Castro-Leon, 2004, p. 42) or Web services such as UDDI (finding a Web site), WSDL (site description), SOAP (transport protocol) and XML (data format) are security concerns. Much Web services security technology is still being developed and has not stabilized enough to inspire confidence. For example, protocols (SOAP) are lacking security, or specifications for Web services security (WS-SEC) are still evolving, and providing security in hardware is not an option because the specifications are not ready to be set in silicon (Dornan, 2003). On the other hand, standards themselves do not guarantee interoperability or security. It depends on how vendors implement the standards (Navas, 2002). Sometimes, Web security requires use of public key infrastructure (PKI). However, PKI is complex and has been a difficult infrastructure to manage, and the cost of managing has been detrimental to many organizations (Geer, 2003). Also, PKI infrastructure is not readily available in many parts of the world.

Spam is another threat that is increasing each year. The best anti-spam solutions rely on a set of detection methods such as heuristics, white and black lists, and signature matching. Choosing the right solution for an organization implies understanding how common spam filters operate, and what their tradeoffs are. Filtering the spam requires human intervention even when tools are available. Bayesian filtering promises a future where most of the spam could be detected and blocked automatically, but these tools are too complex for a mass audience, and wide-scale adoption is probably a few years out (Conry-Murray, 2003).

A very common threat is unauthorized access. This can be prevented via access controls enhanced with biometric systems, a type of access control mechanism used to verify an individual's identity. Biometric systems fall into two categories: authentication and identification, with authentication systems by far more common. Authentication systems are reliable and efficient if the subject base is small and the biometric readers are accurate and durable. A database with biometric data presents a natural target for theft and malicious and fraudulent use (Johnson, 2004). Voice authorization products are becoming popular because they allow remote authentication (Vaughan-Nichols, 2004), but the technology is the least accurate and network administrators have to use it cautiously until researchers improve it.

Moving data over back-end networks, remote locations, shared recovery centers and outsourced information technology facilities also expose information to threats (Hughes & Cole, 2003). The next section describes major trends in information security management.