Information Security (InfoSec)

Waleed Aleid

Information security (or InfoSec) is a collection of business practices that defends information assets from unauthorized access, use, disclosure, modification, perusal, inspection recording or even destruction. It simply protects the information regardless of how the information is gathered and formatted or whether it is being processes, in transit or being restored. Moreover, it is not a simple technology but a strategy that composed of processes, tools and policies which are all necessary in preventing, detecting, documenting and countering threats digital and non-digital information. The InfoSec management has a wide array of security processes and policies, which include everything from mantraps to encryption key management and malware detection. It is important in maintaining the confidentiality, integrity and availability of different IT systems and businesses. Lastly, most of the companies have specific and dedicated security group to implement and maintain the organization or company's InfoSec program. This is usually headed by the chief information security officer (CISO).

History

The drive to make InfoSec came from the concept of computer security. During World War II, there is a rising need for computer security which includes security of physical locations, hardware, and software from threats. The need for computer security for the processors is also developed to aid computations for communication code breaking. There are multiple levels of security were implemented to protect the said processors and save the integrity of data through time. For instance, access to location information of a particular military location was controlled by means of badges, keys, and even recognition of the facial features of a specific authorized personnel. As time passed by, the increasing need for a more powerful computer security safeguards lead to the creation of more complex and more technologically advanced computer programs.

In the early years, the security of information was a straightforward process, which is composed mainly of physical security and simple document classification schemes. However, the most known threat to security is physical theft of equipment, espionage against products of the systems and sabotage. For example, in the early 1960s, when a systems administrator was working on a message-of-the-day file, another administrator was editing the password file. Thereafter, a software glitch caused the mixing of these two files which caused the printing of the entire password file on every output file.

In the 1960s

During the cold war, more processors are brought online. It is necessary for these mainframes to communicate with hack-free process that mailing magnetic tapes between

• *Author name is Waleed Aleid currently pursuing master degree in computer information systems in Florida institute of technology, Melbourne, FL, USA. E-mail: Waleed.s.aleid@hotmail.com*

computers. Thus, by examining the possibility of a redundant, networks communications system, the founder of the Internet, Larry Roberts invented the ARPANET. It is the predecessor to the Internet.

Information Security as a Science and Art

InfoSec is considered an art since the administrators and technicians who implement security are like a painter that applies oil to the canvas. He is the main maneuver on every data stored in the computer or system. Moreover, many of the used manuals are for single support systems and the big challenge is to make a security program for highly interconnected system.

InfoSec owes its design and mechanisms to the technology made by computer scientists and engineers. The y believe that specific conditions in the systems malfunction is a result of too much interaction of the hardware and software. The faults that have remained are perhaps, result of technology malfunctioning.

References

Peter Salus. "Net Insecurity: Then and Now (1969–1998)." Sane '98 Online. 19 November 1998. Accessed 29 March 2016 from www.nluug.nl/events/sane98/aftermath/salus.html

Roberts, Larry. "Program Plan for the ARPANET." Accessed 29 March 2016 from www.ziplink.net/~lroberts/SIGCOMM99_files/frame.htm.

Schell, Roger R., Downey, Peter J., and Popek, Gerald J. Preliminary Notes on the Design of Secure Military Computer System. January 1973. File, MCI-73-1, ESD/ AFSC, Hanscom AFB, Bedford, MA 01731.

Grampp, F. T., and Morris, R. H. "UNIX Operating System Security." AT&T Bell Laboratories Technical Journal 63, no. 8 (1984): 1649–1672.

Grance, T., Hash, J., and Stevens, M. Security Considerations in the Information System Development Life Cycle. NIST Special Publication 800-64, rev. 1. Accessed 29 March 2016 from http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64. pdf.

McCumber, John. "Information Systems Security: A Comprehensive Model." Proceedings of the 14th National Computer Security Conference, National Institute of Standards and Technology, Baltimore, MD, October 1991.