Free challenges of securing information: attacks, attackers and the need for defe...

Law, Security

Introduction to Security: Defending Against Attacks

Introduction to Security: Defending Against Attacks

Introduction:

Information security refers to all tasks that deal with guarding digital information with the aim of ensuring proper implementation of security measures. However, even when all security measures have been taken, it is hard to completely guarantee immunity from attacks or consider a system to be completely secure (Ciampa, 2010).

Information security can be considered as protection since its main goal is to create defenses that ward off security attacks and prevent collapse of the system in case an attack is successful. These defenses are intended to protect information that is of value to individuals and organizations. This value is derived from the characteristics of information (CIA) namely: confidentiality, integrity and availability. Confidentiality ensures that only authorized entities can access and view the information, Integrity deals with ensuring information correctness and that no unauthorized entities (people, malicious software etc.) alter data while Availability ensures that data is only available to authorized parties (Ciampa, 2010).

The AAA (Authentication, Authorization and Accounting) protocol refers to another set of protection offered by information security in addition to CIA. Authentication ensures that an individual/entity is who they claim to be and not an impostor. A person accessing an Automated Teller Machine (ATM) using their bank card has to authenticate themselves by providing a password only the owner of the card would know. Authorization comes after

person has provided authentication, and in this case an authenticated user is allowed to access the bank account associated with the card. Accounting on the other hand provides event tracking which may include records of when and where the account was accessed, cash withdrawn, and other transactions made. Accounting is used as means of determining which user is responsible for what action. For example, a bank client may complain that bank employees stole money from his account yet he withdrew it from an ATM. In this case records will show that the client withdrew money at a certain time and location. In fact, video footage of the client at that location may be provided by the bank if the ATM booth has a security camera.

Information security however involves more than protecting information only. This is because information is stored bitwise on computer hardware, manipulated using software, and transmitted through data communication channels. In this case it is important to protect the devices that transmit, store and manipulate information from attacks. Protection of these devices involves three layers: people, products, and procedures. For example, procedures provide people with an understanding of how to use security products in protecting information and defend systems from attacks (Ciampa, 2010).

It is therefore more prudent to comprehensively define information security as tasks that protect the confidentiality, integrity, and availability of information on devices that transmit, manipulate and store information through people, products, and procedures.

Importance of Information Security:

Information security has the main goals of preventing data theft, identity theft, maintaining productivity, avoiding the legal implications of not securing information, and foiling cyber terrorism. Information security is mainly associated with data theft prevention since data theft leads to loss of confidentiality and financial losses at both individual and corporate levels in case of an attack. Identity theft on the other hand involves people using other people's personal information and impersonating them usually to gain access to some crucial information the victim can access or generally for financial gain. In the legal front, various federal, state and international laws have been enacted to protect electronic data and information privacy (Bosworth & Kabay, 2002). Some of these laws include the Children's Online Privacy Protection Act (COPPA) of 1998, the US Patriot Act (2001), and the Health Insurance Portability and Accountability Act of 1996 (HIPPA) among others (Information Technology Acts: cyberessays. com).

Cyber terrorism is defined as attacks meted out by terrorist groups using the Internet and computer technologies. These attacks are usually targeted towards utility systems, financial services, telecommunications, and other high risk target that use information systems including health and defense facilities. Regardless of the level of attack, either at personal, organizational or the worst case scenarios of terrorist attacks, dealing with the consequences of successful attacks diverts resources such as money and time away from normal activities (SFGate. com).

In recent years, attacks against information security have grown exponentially regardless of the efforts and resources spent annually in securing information and putting up defenses. Information Security is a multibillion dollar industry with governments, individuals and the corporate sector as major stakeholders yet no computer system can be considered completely secure or immune from attacks (Winterfeld & Andress, 2013). Several reasons exist as to why it is difficult to defend against attacks today. Information Technology advancements have seen to it that virtually all devices have Internet connectivity making it easier for attackers to exploit multiple targets and vulnerabilities. Other reasons include increased speeds of attacks, faster vulnerability detection by attackers, greater attack sophistication, simplicity and availability of attack tools, rapid application development with disregard for security, patch delays, poor patch distribution, distributed attacks (multiple attacks from different sources), and human nature which is manipulated by social engineers.

Attackers fall into different categories, with the term hacker generally referring to someone who attacks computer systems. Spies on the other hand are person hired to break into computer systems and retrieve information. Spies usually work under governments for national security reasons and corporations that participate in industrial espionage. Script kiddies on the other hand are usually amateurs who download automated attack tools from the Internet and use them to attack computer systems. Organizations usually face a great security threat posed by employees who may be disgruntled, erroneous or susceptible to social engineering attacks. Attacks by employees can be deliberate or done unwittingly. Cyber criminals

have emerged as a new brand of attackers who utilize loose-knit networks of persons with similar interests usually consisting of financial fraudsters and identity thieves. Cyber terrorists on the other hand draw motivation from their beliefs and principles and have lethal attacks targeted towards computer and network infrastructure with the aim of causing havoc and panic among governments and their citizens (Lukasik et al, 2003).

Defending Against Attacks:

Attacks of several types can be launched against networks and computer systems. However, most attacks use the same five basic steps. These steps include: probing for information, penetrating existing defenses, modification of security settings and configurations, circulating to other systems, and paralyzing devices and network services. Multiple defenses are required to withstand these steps of an attack and thus they should be based on the five fundamental principles of information security: layering, limiting, diversity, obscurity, and simplicity. These principles provide a sound framework for building secure systems. In order to understand how these principles works, a security system at a bank will be used as an example to show how the principles are applied (Ciampa, 2010).

Layering:

A bank contains money saved up by customers in their accounts electronically and also contains cash and other valuables stored in secure safe deposit boxes. The banks physical security consists of secure vaults, tellers are protected by inch thick bullet and smash proof glass. The money and other valuables are located in secure safes and vaults with massive

walls, motion sensors, vibration sensors and even lasers. The doors to these vaults are monitored round the clock by Closed Circuit Television (CCTV) cameras which record every event. The bank itself has armed guards and alarm systems. It can thus be said that the bank security is layered and if one layer is penetrated such as armed robbers getting past the armed guards, there are still several layers to be breached. Layering helps create a multiple defense barrier that can be coordinated to prevent a wide variety of attacks. Information security on the other hand should be layered to slow down and even stop the attacker since it is unlikely for the attacker to have all the skills and tools required to circumvent the various defense layers. The layered approach is the most comprehensive approach (Ciampa, 2010).

Limiting:

The bank may allow customers and personnel to transact on the various accounts and enter vaults to view their safe deposit boxes thus increasing the security risks significantly. In this case, only authorized personnel should handle money, door passwords and other clearances. The same case applies to information systems where limiting information access reduces the threat levels significantly. This means that only authorized personnel may access data and there is a limit to what they can do with this data. For example, a human resource worker in a bank can access payroll details, employee details and other data related to HR but only for viewing. However, only the HR manager can change employee salaries or terminate their employment. Some ways of limiting data access include assigning file permissions to read, write or modify files, while others are procedural in nature such as

preventing employees from leaving with sensitive files from the premises. In this case, access should be limited to a minimum (Ciampa, 2010).

Diversity:

Diversity is close to layering in the sense that the multiple layers of security must be diverse such that attackers cannot use the same technique to penetrate different layers. A bank robber for example can evade security cameras by staying away from their angle of view but they cannot use the same evasive technique for motion detecting systems. Another case for diversity would be to utilize security products and devices from different vendors and manufacturers. Attackers can use one technique to bypass a system or device belonging to a vendor 1 but cannot use the same technique for a device from vendor 2. If however all devices in the organization are from vendor 1, then it is possible that the attacker can use the same technique to bypass all of them (Ciampa, 2010).

Obscurity:

Obscurity involves eliminating routine from security. For example, computer passwords, vault passwords and network keys should be changed randomly, say after a week, 2 weeks, a month etc. to ensure that changes cannot be ascertained in advance. The times when money is transported from the bank to another should also be random such that potential robbers cannot spot a pattern or routine. An example of obscurity in information security is hiding the details of software, hardware, security devices and vendor details for various security products. Attackers with information on a system may devise ways to circumvent it and identify vulnerabilities but if no prior

knowledge exists, then it becomes difficult for an attacker to attack a system they know nothing about. Obscurity is thus an important protection means.

Simplicity:

Attacks come from different sources and in various ways. However, the nature of Information Security lies in complexity and yet the more a system becomes complex, the more difficult it becomes to understand. An employee with no knowledge of the interactions between motion sensors and lasers trip lights may not know what to do in case an intruder attacks. Additionally, complex systems create opportunities for error since some things are overlooked.

Information security works the same way. Very complex information security systems are hard to understand, troubleshoot, maintain, monitor, and even feel secure about. Secure systems should be simple for those who are using it to understand use. Complex security systems and schemes are often compromised while trying to make them easier for trusted users to work with. This bid can make it easier for attackers too. A successful information security system should thus be complex on the outside but quite simple on the inside, and while this might be difficult to implement, successful applications of this technique usually reaps major benefits (Ciampa, 2010).

Conclusion:

The paper has highlighted the main issues to consider about information security and emphasis has been placed on the importance of defending against attacks, challenges experienced, and how to defend computer systems against cyber-attacks. While the scope of the paper does not allow

delving into the specific details and technologies used to defend against security attacks, it does provide an elaborate outline of the basic security principles utilized while defending against attacks. It is evident that no computer system is entirely secure but with the security principles at hand and future technological advancements in information security, it expected that defenses against attacks will become more powerful in preventing attackers from gaining access to people’s privacy.

References:

'Fatal System Error' has insight on cybercrime. (n. d.). SFGate. Retrieved January 29, 2014, from http://www. sfgate. com/business/article/Fatal-System-Error-has-insight-on-cybercrime-3201651. php

Bosworth, S., & Kabay, M. E. (2002). Computer security handbook (4th ed.). New York: John Wiley & Sons.

Ciampa, M. (2012). Security awareness: applying practical security in your world (3rd ed.). Boston, Mass.: Course Technology.

Information Technology Acts (ITA). (n. d.). Essay. Retrieved January 29, 2014, from http://www. cyberessays. com/Term-Paper-on-Information-Technology-Acts/63306/

Lukasik, S. J., Goodman, S. E., & Longhurst, D. W. (2003). Protecting critical infrastructures against cyber-attack. Oxford: Oxford University Press.

Voeller, J. G. (2010). Wiley handbook of science and technology for homeland security. Hoboken, N. J.: Wiley.

Winterfeld, S., & Andress, J. (2013). The Basics of Cyber Warfare

Understanding the Fundamentals of Cyber Warfare in Theory and Practice..

Burlington: Elsevier Science.