International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 11 | Nov 2019 www.irjet.net p-ISSN: 2395-0072

A Review of Information Systems Security: Types, Security Issues, and Main Systems Affected

Jean Claude MUNYANEZA[1], Felix NSENGIYUMVA[2], Papias NIYIGENA[3]

Department of Information Technology, University of lay Adventists of Kigali, Master's Program

---

Abstract - This paper discusses the different issues pertaining to security of information systems. First, the different types of information security are discussed such as network security and endpoint security. Additionally, the other important aspect of information systems security that is discussed is the different threats to information security. These are also the security issues, and they include, viruses and other malicious programs, phishing, as well as denial of service. Alongside the discussion of the different security issues, some solutions for the issues are also mentioned with techniques on how such issues can be avoided when possible. Lastly, the paper also covers the different systems that are at highest risk of security issues. These systems include the ones used in financial systems, the aviation industry, as well as consumer systems. The paper uses a research methodology to outline the manner in which data on information systems security is obtained.

Key Words: Systems, industry, information security, business,

1. INTRODUCTION

Information technology security, sometimes known as computer security, refers to protecting computer systems and information from any damage, stealing, and illicit use. This security can be done to the computer hardware, software, or any other component of the computer system (Peltier, 2016). The protection of computer hardware against security breaches is done through the same methods that are utilized to guard other precious and sensitive apparatus such as doors and locks, serial numbers, and alarms. On the other hand, information and system access are protected through the use of tactics. This protection prevents any physical access or cybercrime, which is done in different ways.

2. Literature Review

2.1 Types of Information Security

Network Security is a type of security used in preventing unauthorized and malicious users from accessing a network. This security ensures that there is no compromise on reliability, usability, and integrity of the network. It is important to maintain network security as it helps in preventing hackers from accessing data from a network (Peltier, 2016). Additionally, it is also important as it prevents hackers from having any negative effects on the ability of users in their access and use of a network. It is increasingly difficult to ensure network security in businesses as they raise the number of endpoints and carry out a migration of services to the public cloud. The other type of information security is internet security. This security involves protecting information that is transmitted and received through the use of browsers and network security that involves the use of applications that are based on the web. Additionally, this type of protection is designed to monitor the internet traffic that is incoming to ensure that malware and other unwanted traffic does not get to the system (Ahson & Ilyas, 2008). Such protection for internet security is done using different methods such as antimalware, firewalls, and antispyware.

The other common type of information technology security is endpoint security. This security ensures that there is the provision of protection at all the different levels of devices. Examples of devices that can be secured using this security are tablets, laptops, cell phones, and desktop computers. Endpoint security helps in preventing these devices from having any access to malicious networks, which can result in a threat to the organization (Peltier, 2016). Endpoint security instances include advance malware protection and software for device management. The other type of internet security is cloud security. This security covers information technology aspects such as data, applications, and identities that move to the cloud. This movement means that users connect directly to the internet, but they do not have the protection of tradition security procedures. Cloud security aids in securing the use of applications such as software-as-a-service (SaaS) and the public cloud (Stallings et al., 2012). Finally, there is application security, where the coding of applications is done in a manner that they are quite secure and ensure that their vulnerability to attacks is limited. The addition of this layer to security entails the evaluation of a code of an application and the identification of vulnerabilities that exist within the software programs.

2.2 Security Issues in Information Security

Viruses and Malicious Programs

First, there is the aspect of viruses and malicious programs. Through this increased use of the internet, it likewise poses more risks to the computer network of a business as there are more malicious programs that can affect it. A computer virus refers to a computer code that is inserted into another computer program, but it remains dormant until the moment that a user triggers it without suspecting. Such triggers can be quite simple such as opening an attachment of a file and

downloading an internet file. Viruses are sometimes quite dangerous as they can end up deleting important data files (Peltier, 2016). As a result, most people and organizations use anti-virus software throughout their networks, but it still becomes difficult to cope with the ever-increasing number and sophistication of virus programs. There are different motives that software creators have when they develop viruses, for example, seeking profit through a ransom. Additionally, others are also interested in sending particular messages such as a political message. There is also the reason for demonstrating that there is a vulnerability that exists in software. Lastly, some hackers are simply interested in exploring cyber-security issues (Stallings et al., 2012). Such malicious programs and virus often have catastrophic effects as they can end up destroying the entire network that a person or a company operates and electronic records held.

Phishing

This is also one of the most prevalent cyber-attacks and it refers to when a scammer uses deceitful texts, emails, or impersonator websites with the intention of getting other users to share their important personal information, for example, account numbers, log in identification details, social security numbers, and passwords (Stallings et al., 2012). After sharing this information, scammers normally use it to steal money from people, their identity, or even both money and identity. The use of phishing emails by scammers to gain access to a computer network from where they then install programs, for example, ransomware. These programs are used to lock a person from accessing important files in their computer system. Additionally, phishing scammers lure their target personalities such that they make them feel that they have a fake logic of protection through the spoofing of trusted and well-known logos of well-known and valid companies or even pretending to be relatives. These cybercriminals also make things seem as if they need to use the information of a target swiftly or else something bad is likely to happen to them, for example, they give out information that a bank account can be frozen and a tax refund will not be possible, among other reasons (Peltier, 2016). The different lies that they use are meant to enable them to solicit information from their targets.

For people to ensure that they are protected personally and for their companies against such malice, the United States Federal Trade Commission recommends several precautions. First, people should be secure regarding the attachments that they open and clicking links in their emails (Peltier, 2016). If wrong files or links are clicked, they may contain malware that can end up weakening the security of the computer system. The other important precaution is that people should get used to the use of two-factor authentication. For the different accounts that bear this security measure, it requires a password and other pieces of information that are needed before gaining access to an account. For example, the second part of the information may comprise a code that is sent to a phone or a random number that is often generated, which helps to protect the account even when a password may have been compromised. The other important measure that is given is that people should ensure that they maintain a backup of records in an exterior hard drive or in other times cloud storage (Von Solms & Van Niekerk, 2013). Such a backup should be done regularly to ensure that there is maximum protection against malware programs, viruses, or even ransomware attack. Additionally, the U.S. federal trade commission maintains that security should be maintained up to date. In this regard, computer systems should be protected using software that is trusted and ensure that it is updated automatically.

Denial of Service

The other method that cybercriminals use to compromise computer security is a denial of service (DoS) attacks. This kind of attack occurs when the lawful people that use a computer system are not able to access to their information systems, devices, and other network resources as a result of the actions of a malicious actor of a cyber-threat. Such actors affect services such as websites, emails, online accounts, and other services that rely on the computer system or network that is affected (Ahson & Ilyas, 2008). This kind of cyber threat is often accomplished through the flooding of the host network with traffic to ensure that the target is not able to respond or experiences a crash that prohibits legitimate users to access the information technology systems. For example, in the year 2012, six banks in the United States were the target of a different denial of service attacks. These victims were big banks in the United States, such as the JP Morgan Chase, PNC Bank, and the Bank of America.

3. Research Methodology

The research methodology employed two approaches: experiments as well as surveys.

Experiments

The purpose of the tests carried out using experiments was to find out the vulnerabilities that put information systems at risk through a verification of corporate application systems and how they are exposed to security vulnerabilities. The different methods that are used include social engineering, SQL injection, as well as brute force attack. On social engineering, attempts to penetrate are done on employees to test whether they do follow all security policies and standards. A phishing attack is used to evaluate the accuracy of policies and measurements that people follow. Secondly, SQL injection is an error based injection attack string that is done to evaluate whether the corporate web application is vulnerable to different kinds of attacks. Two different criteria are used in detection of vulnerabilities. The first one is for the web application to allow query execution from different url. Secondly, the web application should show errors for queries. Thirdly, there is brute force attack that helps to reveal human factors that make data and information systems vulnerable to attacks.

Surveys

First, surveys entail the use of a smoke-screen approach as it is more effective in capturing the security awareness of respondents if they lack awareness of their assessment. The survey utilizes seven scenarios where two of them are general ones and are employed as a diversion from the main subject. Secondly, interviews are also used in surveys, where ten professionals of information technology are interviewed. They are used to give their views regarding the issue of security on information systems.

4. Results and Discussion

There is rapid growth in the number of computer systems in different industries globally. In this regard, the different types of institutions and individuals that rely on computer systems include businesses, government institutions, industries, and individual people. In this regard, one of these groups whose systems are at risk is financial systems as the information technology systems that they use are often prominent targets for hackers and cybercriminals. Examples of financial institutions systems that are under this threat are the ones used by the United States Securities and Exchange Commission, investment banks, SWIFT, and commercial banks (Mo et al., 2011). The cybercriminals are often interested in manipulating their financial markets and make illicit gains from them. Other similar institutions whose systems are at risk for the same reasons are brokerage accounts and websites that hold information regarding bank accounts and credit card numbers.

Additionally, the aviation industry is another target market for cybercriminals. This industry heavily relies on complex systems that could be attacked and compromised by cyber threats, for example, a single power outage in an airport causes multiple repercussions globally as most systems use radio transmissions that can be disrupted badly. In such a case, the control of aircraft as they traverse oceans is dangerous as the surveillance of radar systems only goes up to 175 and 225 miles offshore (Ahson & Ilyas, 2008). The other main targets are devices that are used by consumers. These devices include desktop computers and laptops. These devices are used in gathering passwords regarding the financial information of users and use them to come up with botnets for attacking other targets. Different devices such as tablets, smartphones, mobile devices, and mobile devices have sensors such as compasses, cameras, and GPS receivers that can be exploited for security thus used for collecting sensitive information from users. The increase in the number of automated home devices, for example, the Nest thermostat, increases the chances of consumer devices being targets of cybercriminals.

Conclusion

The protection against cybercrime or physical access to information security systems are important to ensure that information is not compromised. Variable types of information security exist, and they include network security, internet security, endpoint security, and cloud security. In these information security types, multiple security issues exist. However, the main security issues are three. These include malicious programs and viruses, phishing, and denial of service. For example, six banks were the target of different instances of denial of service attacks in the United States in 2012. Lastly, there are main systems that are at the highest risk of cyber threats, and they include financial institutions and consumer devices.