University of the Potomac

Vulnerabilities Associated with Cyber Security

by

Alexandra Ngonga
Felix Laura Antezana
Sai Chadalawada

For

CBSC640 - Cyber Warfare

Paul Jaikaran, Ed.D. Advisor

August 2019

TABLE OF CONTENTS

Declaration of Originality

Names: Alexandra Ngonga, Felix Laura Antezana and Sai Chadalawada

Course Name: CBSC640 - Cyber Warfare
We confirm that this assignment is our own work and that we have:

Read and understood the guidance on plagiarism in the University of the Potomac Statement on Plagiarism

Clearly referenced, in both the text and the bibliography or references, all sources used in the work

Fully referenced (including page numbers) and used inverted commas for all text quoted from books, journals, web etc.

Provided the sources for all tables, figures, data etc. that are not my own work

Not made use of the work of any other student(s) past or present without acknowledgement. This includes any of our own work that has been previously, or concurrently, submitted for assessment, either at this or any other educational institution.

Not sought or used the services of any professional agencies to produce this work

In addition, we understand that any false claim in respect of this work will result in disciplinary action in accordance with University regulations

DECLARATION:

We are aware of and understand the University's policy on plagiarism and we certify that this assignment is our own work, except where indicated by referencing, and that we have followed the good academic practices noted above.

Signed

CHAPTER 1

INTRODUCTION

The Problem

The problems today are the many vulnerabilities that are associated with cyber security

Research Question

The purpose of this research is to determine the vulnerabilities that compromise network systems

Organization of the Study

Research will be done in 4 chapters. Chapter 2 will be comprised of all the data and research to support the premise of the topic

CHAPTER 2

LITERATURE REVIEW

According to Microsoft.com, “A security vulnerability is a weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product.” (Definition of a Security Vulnerability, n.d.). Vulnerabilities include humans, the Internet, Intranets, software, various networks as well as transmission media. These vulnerabilities can be exploited by attackers against top targeted industries that manufacture energy, oil, gas, pharmaceutical, chemical, electronics, mining and agricultural (Cisco ASR Infographic, 2014).

Knowing identify concepts such as threat, vulnerability and risk and how an incident can affect a company, will allow us to know if the company is in danger (Circus, R., 2018).

A vulnerability (in terms of information technology) is a weakness or failure in an information system that puts the security of information at risk by allowing an attacker to compromise the integrity, availability or confidentiality of the information. We will therefore need to find them and correct them as soon as possible. These "holes" can have different origins, for example: design failures, configuration errors or procedural shortcomings (Panton, B. C., Colombi, J. M., Grimaila, M. R., & Mills, R. F. 2014).

On the other hand, a threat is any action that takes advantage of a vulnerability to attack an information system. That is, it could have a potential negative effect on some element of our systems. The threats can come from attacks (fraud, theft, viruses), physical events (fires, floods) or negligence and institutional decisions (bad password management, not using encryption).

From the point of view of an organization, the threats can be both internal and external. Therefore, vulnerabilities are the conditions and characteristics of the systems of an organization

that make it susceptible to threats. The problem is that, in the real world, if there is a vulnerability, there will always be someone who will try to take advantage of its existence (Vegvizer, T., 2018).

Once we are clear about the difference between threat and vulnerability, we must know that the risk is the probability of a security incident occurring, materializing a threat and causing losses or damages. It is measured assuming that there is a certain vulnerability to a certain threat, such as a cybercriminal, a denial of service attack, a virus ... The risk then depends on the probability that the threat materializes taking advantage of a vulnerability and causing harm or impact the product of these factors represents the risk (Moschovitis, C., 2018).

There are several scanning methods to perform vulnerability analysis.

White box

The white box scanning method has a total vision of the network to analyze, as well as, access to all equipment as a super user, this is where you have the part of all the administration of services, the part of cash analysis white acts as a legitimate user within the network, who can use the services in different ways to which another person may be using them. In a more detailed way, this method will use certain users with certain privileges within the network and accessing the services, within the products, within the software to be audited and thus be able to verify if any additional action can be carried out based on the privileges that have been provided (Meyer, C., 2019).

Black box

There is also the black box scanning method, this is where network access information is normally provided, here the analysts are going to provide only network or system access information, for example, a single IP address, some name of any company, etc., from here it

starts as such to look for information, everything possible related to the exploration and thus be able to obtain as much information as possible from that IP address, of the rest of the equipment probably found within of some associated IP address range, no instructions are carried out here, only the vulnerability is detected and documented (Buckley, R., 2007).

One of the most important and major security vulnerabilities is unpatched software products. Patches in the technology world are bits of software code that are used to cover a hole in any type of software or fix a bug in it by updating it. An unpatched software is one that was created but has bugs or loopholes in the software which often go undiscovered. These vulnerabilities sometimes have mild consequences if exploited or discovered but with security vulnerabilities, the consequences can be much more catastrophic once discovered and exploited by hackers (Cisco 2014 ASR, 2014).

Unpatched software products are the most important security vulnerability because the current technological advancements. Infrastructure is increasingly becoming more dependent on computers and servers that need software to perform functions such as controlling business networks and even energy grids that support cities and countries. In addition to that, the other vulnerabilities mentioned above are interrelated to unpatched software. Systems are constantly being monitored for malicious behaviors or patterns and the software are constantly being updated with patches to prevent attackers from getting unauthorized access. However, with time, more attacks are inevitable so there is a need to keep aiming to be one step ahead of the attackers if possible. An example of software that has exploited bugs is Java. According to Cisco's 2014 annual security report, 97% of enterprise desktops and 89% of all desktops in the U.S. run Java. The report also shows Java as accounting for 91% of indicators of compromise in 2014 (Cisco 2014 ASR, 2014).

There are many types of software that are either open source meaning that source code is available to public or closed-source meaning that source code is not readily available to public. The advantages of open source software include lower cost, high quality and adherence to open standards (Stol & Babar, 2010). Open source also has its downsides being that commercial users may potentially lose a lot of funds that go into tweaking the software into the company's specifics (Kort & Zaccour, 2011).

Closed source software products that are produced frequently for commercial use also have bugs. With proper patches in place, software products like this can run for great lengths of time before being susceptible to new attacks. As long as they are updated frequently and regularly. A great example of a company that updates its operating systems and related software is Microsoft. More to consider are server side and client-side software. Client-side software are those operated at the user end and server-side are those whose operations are carried out on the server. Although they have their advantages, they often have security vulnerabilities, especially when they are not unpatched or not properly patched.

There are three main types of client-side exploits. The first is traditional client-side exploits in which botnets are used to target browsers, plugins and email clients (Gula, 2012). Secondly, client-side software can connect to a network via an opened socket and makes it much easier to exploit if it lacks a firewall without the need for human interaction (Gula, 2012). The third ties in line with server side-software where the server itself is used to attack the client directly; one example being the CVE-2005-0467 that exposed a vulnerability in PuTTY SSH and SSP clients that can be exploited by a rogue SSH Server (Gula, 2012). This also raises one key aspect that is the common factor amongst software, which is the code. Computer software codes are the underlying fundamental building blocks for creating software that can carry out required

functions. Codes are often written manually or with the help of other coding software. Complete simple codes are in general much easier to audit and test for bugs and vulnerabilities, but since these codes tend to be complex, there are often mistakes in the code that range from benign, to being vulnerabilities or even causing the software to crash and malfunction regardless of whether the code is for open source or closed-source software. This makes patches themselves potential double-edged swords.

In corporate environments, more than one operating system often exists in the computers and even servers. This means a patch can fix the problem at hand but may have hidden incompatibilities or leave other loopholes in the system especially when dealing with multiple OS platforms. Patches must be properly tested before deployment into the network and open source software owners need to test their software before releasing official versions as developers may propose a fix to a problem with an embedded vulnerability that may give them unauthorized access to information.

The Internet is the single largest network that connects networks around the world. Although it has protocols such as HTTPS that implements Secure Socket Layer amongst other protocols for safety purposes, there are many aspects that make it very unsafe. As one of the largest information pools, millions of people (including hackers and crackers) are connected to it at any one time. Since there are many ways of boycotting and evading security mechanisms of which they are at times completely absent, people can upload whatever information they want to the internet through websites and other File Transfer Protocols. (FTPs).

When an unprotected user accesses or tries to access the information from an unsafe site, their computers get infected. Sometimes the web servers are attacked directly such as with Denial of Service attacks that drastically reduce or terminate server-based services by flooding

them with packets often from zombie computers. Downloading software from unregistered third-party websites could be a nest for freeware with incorporated malware. Simply visiting pages in a website are enough to download any type of malware into your computer and these can often go undetected until significant damage is done. Web browsers often have their own vulnerabilities that have been discovered by analysts and hackers alike. According to Kerner, Internet Explorer had a vulnerability (CVE-2014-1776) in the way it accesses objects that are not properly allocated or deleted and may corrupt memory to allow attackers to execute arbitrary code within the browser and affects IE versions 6 – 11 (Kerner, 2014). It is unknown how long crackers have been using this vulnerability but the range of versions with this bug is wide. If IE had properly patched its code, the severity of some attacks will be avoided.

There are various types of networks that include MAN, WAN, WLAN, and LAN etc. They all have varying and at times overlapping purposes but they also have vulnerabilities, especially WLAN networks. They have many vulnerabilities that include the SSID, MAC address access control list, authentication mechanism vulnerabilities, 802.1X/EAP, WEP, WPA/WPA2, 4-way handshake vulnerabilities, reuse of key stream, and many more (Dhull & Singh, 2010). Wireless networks outside the company network also pose a threat with BYOD however, with proper mitigation techniques such as closing open ports, multi-level authentication, network access control amongst others, these WLAN vulnerabilities can be minimized and monitored. Wired networks add vulnerabilities of their transmission media being targeted for eavesdropping but the use of fiber optic cables, although they are very expensive, in most critical areas of the wired network can be implemented and do not pose a very difficult task for IT managers.

Types of vulnerabilities

There are some types of vulnerabilities that are mechanisms used by attackers to infect a network or steal information, among which the following types can be mentioned:

Configuration errors

Another of the main vulnerabilities are the configuration errors, for example, the default password, weak password, users with too many privileges and even the use of obsolete encryption protocols, normally one of the most typical things in the organizations is that they use some web encryption system, which with a cell phone application can be cracked in less than 10 or 15 seconds or even with a laptop. Another vulnerability error can be some SSH protocol that has not been patched or updated, for example, with some kind of vulnerability, some encryption protocol would be used, either obsolete or insecure, but normally the configuration errors part come from the part of the password default, when entering a network with the IP for example, 198.XXX and if you have the possibility of entering Google and search within it, what would be the default username and password, you can change it the configuration causing damage to the company.

Web errors

Other types of vulnerabilities are the WEB, here simply and simply have input validation errors, insecure scripts, web application configuration errors, among some other situations, that at the end of the account each and every one of those errors are the means for some XSS (Cross Site Scripting) attack or SQL injection (Heiderich, M., Niemietz, M., Schuster, F., Holz, T., & Schwenk, J., 2014).

Protocol errors

Finally, we have the part of the vulnerabilities of protocols, there are various amounts of protocols that were normally defined without the need or without taking into account precisely the part of security and often do not anticipate the growth that these would have and since the internet was not prepared to be so big, it was not thought about the security part. Some of the protocols can be a simple HTTP, which is not secure, since it only performs the authentication part, but without the encryption of the data that it finally exchanges, this may be necessary in some environments, for example, in the pages visited simply and simply by the users, but when banking transactions are carried out, normally the part of this protocol would be very insecure, it will probably require some other action such as some SSL or TSL certificate, etc. Usually the biggest problem is when defining the security framework that failures have, for example, web system use (Yasinsac, A. 2002).

Buffer overflows have been the most prominent security vulnerabilities in recent years. Rouse defines a buffer overflow as a situation in which a program tries to store more data in the temporary data storage area (buffer) than intended by overflowing the data into adjacent buffers that can corrupt and even overwrite genuine data. (Rouse, 2007). The Internet is also susceptible to buffer overflows. Since buffers are stored into the temporary data storage, malicious codes can find its way in using the excess overflowing buffers to overwrite other buffers that can cause errors in the program's execution and even modify or replace root shells. A few types of buffer overflows attacks include long jump, stack, heap, format string overflows and even a combination of two or more types. There are solutions for the different types of buffer overflows such as using direct and indirect security design models. Besides just defining the threat scenarios and test for security vulnerabilities, the experts implementing the direct design are also

tasked with working with developers to strategically incorporate necessary security protocols (Hedayatpour & Kama, 2014).

In the indirect model, experts are tasked with incorporating security checkpoints using their own predefined methods and techniques rather than working hand in hand with the developers (Hedayatpour & Kama, 2014). Another solution is the use of non-executable buffers where the legitimate user's data segments of the program's address space cannot execute commands hence rendering attacks ineffective. Other solutions include array bound checking, code pointer integrity checking and many more (Cowan, Wagle, Pu, Beattie & Walpole, 2014). Proper patches and audits to these software and protocols can aid in protecting users from the Internet and other media. One very effective way is writing the software code and protocols to incorporate control systems against buffer overflows.

Many companies have adopted the habit of bring your own device. More and more companies are looking to adapt and become flexible for the comfort of their employees to enable them to put in the maximum amount of input. In essence, bring your own device encompasses policies and protocols employers pose on employees to allow them to use their personal devices such as smartphones, laptops, iPads, tablets, and more to do work or other work related activities and procedures (Waterfill & Dilworth, 2014). The use of these policies extends into the use of various social media outlets to improve advertisement marketing and related business aspects.

In addition to increasing the flexibility of work hours, there are a lot of benefits to this such as improving efficiency levels, reducing costs for employers, and better handling since employees themselves purchase the devices (Waterfill & Dilworth, 2014). However, bring your won device poses one of their biggest vulnerabilities, which is security. Normally any computers and network equipment that are provided by the company have standards, rules and policies that

employees need to adhere to while using these devices. IT managers have to always ensure that these devices are kept up to date and monitored for security and data breaches. This alone is a hefty task for some companies as they could have thousands of computers and other devices that are in constant need of updates and patches. When you add in personal devices, IT managers have an added task of monitoring them once they are connected to the network and at times they can easily be overlooked.

Computers mostly use Apple OS X or Microsoft Windows (XP – 8) and they all provide varying degrees of software compatibilities. The employees use these devices outside the workplace unrestrictedly so data from within the company that is accessible on the devices can be exploited in the wrong hands. Viruses and malware can also be introduced into the company network though these devices. IT managers can secure the internal network but they cannot secure the outer networks, so they need to ensure these devices are secured and kept up to date with patches. Therefore, even though employees and outside networks pose vulnerabilities and threats to company data, keeping them up to date on a case-by-case employee basis can be extremely tasking.

An example of this is Accenture which is a consulting company where most office computers are iMacs and MacBook Pros. The employees are equipped with laptops and devices that they take home and can be used for personal use. Employees can easily access the online QuickBooks accounting information at home or anywhere with an Internet connection more or less from any computer. This makes data unsafe because if there are employees who do not ensure that their computer is up to date and scan for viruses as well as other malicious software on a frequent basis the entire company network can be at risk. Imagine a huge company with thousands of unpatched personal devices that can be catastrophic.

People pose as a major vulnerability to information systems and are unarguably amongst the top difficulties IT managers are faced with. Creators of software in the commercial sector often have end user license agreements before people can download and or use their software. Most people do not read these software agreements but just accept to use them. However, some businesses mandate the reading of acceptable practices and policies in the work environment. At times there is the employee who is provided data or information on a thumb drive who decides to share it with some other co-workers. The employee plugs it directly into the work computer. If any malware resides on that thumb drive a threat action may occur and cause damage. Hackers can take advantage of unsuspecting employees as a means of gaining access into the network by soliciting them for cyber espionage, hacking through their unsecured bring your own device which is taken home. Regardless of managers stressing the importance of opening email attachments from unknown senders and even suspicious looking emails from known senders, there are always a few employees that fall into the trap and could get tangled in a phishing scam or grant access to unauthorized users.

IT managers can mandate policies regarding computer use but even with severe consequences for misuse, there are still some employees that may try to find their way around it. Restricting Internet access to social media cites and others like YouTube only does so much to keep the network secure. Increasing the level of awareness through seminars and other means can be of help but the normal employees are not going to be familiar with network systems as much as the information security officers. What IT managers can do is keep the firewalls and web filters up do date and patched. Monitoring and keeping detailed event logs can aid in this situation but again without properly patched software and managed systems it can be

problematic without the safety net. Even with negligence, effective restrictions, policies, and firewalls prevent people from being the most important vulnerability.

Policies are also a part of information systems. There are properly constructed company policies, and some may be overbearing or almost absent. The hard part is getting employees to follow all the policies that are required of them. Branching into policies related to computer use and security, employees frequently violate these rules as they do not realize the risks and may not be penalized for breaking the policies. In small company settings, managing and monitoring security can be very bulky and tedious. If IT personnel have a hard time reviewing all the logs and activities of the employees, systems can be set in place to notify the IT personnel of any violations. Firewalls (Packet Filtering, Circuit-level, Application-level, and Proxy) can also aid in implementing these policies such as restricting Internet access to pornographic websites, file sharing websites, monitoring and filtering packets of data transfer long with many other features. Depending on the applications, there may be compatibility issues or multiple logging systems involved in monitoring and logging activities throughout the network. These features need to be working properly and can often fail as in the case with buffer overflows seen earlier. IT managers need to ensure that all monitoring systems are patched as deemed necessary to reduce vulnerabilities to the network.

Hardware also have their vulnerabilities in information systems. They range from simple settings errors, malfunctions, to unexpectedly loosing complete function. Even transmission media such as coaxial cables are at risk of eavesdropping. These are not a major vulnerability that IT managers need to be overly concerned about because hardware just needs to be upgraded to adapt to new software and vice versa. At times the issue can be trying to detect the source of a hardware malfunction and they can always be completely replaced. One easy fix to hardware

problems is setting up one or multiple Redundant Array of Inexpensive Disks (RAID) types or simply creating cold or hot backup centers that ensure smooth and seamless continuation of function in the event hardware fails. Unbeknownst to many, USB storage devices can harbor any type of malware if plugged into any computer that has been breached. USB ports can be disabled to prevent use. If they are required for company operations, the computers can have good scanning software that always automatically scans for any type of malware before allowing access on computer.

CHAPTER 3

METHODOLOGY

With the advancement of modern society, basic essential services (utilities) are commonly provided such that everyone can easily obtain access to them. Today, utility services, such as water, electricity, gas, and telephony are deemed necessary for fulfilling daily life routines. These utility services are accessed so frequently that they need to be available whenever the consumer requires them at any time. Consumers are then able to pay service providers based on their usage of these utility services. In1969, Leonard Klein rock, one of the chief scientists of the original Advanced Research Projects Agency Network (ARPANET) project which seeded the Internet, said: ‘‘As of now, computer networks are still in their infancy, but as they grow up and become sophisticated, we will probably see the spread of ‘computer utilities’ which, like present electric and telephone utilities, will service individual homes and offices across the country’’. This vision of the computing utility based on the service provisioning model anticipates the massive transformation of the entire computing industry in the 21st century whereby computing services will be readily available on demand, like other utility services available in today’s society. Similarly, computing service users (consumers) need to pay providers only when they access computing services. In addition, consumers no longer need to invest heavily or encounter difficulties in building and maintaining complex IT infrastructure. Hence, software practitioners are facing numerous new challenges toward creating software for millions of consumers to use as a service, rather than to run on their individual computers (Rajkumar Buyyaa, b,CheeShinYeoa).

Nevertheless, as with any new technology, cloud computing has been related with a number of security risks. While the cloud computing continues to evolve and address these

security & compliance requirements, organizations are left to wonder if cloud computing is a benefit for IT value optimization or misery for enterprise risk management.

The "Internet of things" (IoT) is becoming an emerging topic of conversation where many people don't know the phrase IoT. So what basically is IoT, it is the concept of basically connecting any device to the Internet (and/or to each other). This includes everything from cell phones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. The new rule for the future is going to be, "Anything that can be connected, will be connected.

Security is a big issue that is oftentimes brought up. With billions of devices being connected together, what can people do to make sure that their information stays secure? Will someone be able to hack into your toaster and thereby get access to your entire network? The IoT also opens up companies all over the world to more security threats. Then we have the issue of privacy and data sharing. This is a hot-button topic even today, so one can only imagine how the conversation and concerns will escalate when we are talking about many billions of devices being connected. Another issue that many companies specifically are going to be faced with is around the massive amounts of data that all of these devices are going to produce. Companies need to figure out a way to store, track, analyze and make sense of the vast amounts of data that will be generated.

A large number of applications, such as large scale sensors, information monitoring, web exploring, data from social networks like Twitter and Facebook, surveillance data analysis, and financial data analysis, deal with a large stream of data input, and consequently require an alternate ideal model of real-time data processing (Arasu, B. Babcock, S. Babu, M. Datar, K. Ito, I. Nishizawa, J. Rosenstein, J. Widom).

Several of these applications are approaching the bottleneck of current data streaming infrastructures and require real time processing of very high-volume and high-velocity data streams (also known as big data streams). The complexity of big data is defined through V4's: 1) volume – referring to terabytes, petabytes, or even Exabyte's (10006 bytes) of stored data, 2) variety – referring to unstructured, semi-structured and structured data from different sources like social media (Twitter, Facebook etc.), sensors, surveillance, image or video, medical records etc., 3) velocity – referring to the high speed at which the data is handled in/out for stream processing, and 4) veracity – referring to the quality of data. These features introduce huge open doors and enormous difficulties for big data stream computing. A big data stream is continuous in nature and it is important to perform real-time analysis as the lifetime of the data is often very short (data is accessed only once) (B.Albert, M. Dayarathna, S. Toyotaro).

Cloud Threats:

As more and more organizations are shifting focus on saving data on clouds and using cloud computing more, cloud computing security is at risk. As per McAfee Labs 2017 Threats Predictions November 2016: Cloud service providers are building trust and gaining customers. Increasing amounts of sensitive data and business critical processes are shifting to public and hybrid clouds. Attackers will adapt to this shift, continuing to look for the easiest ways to monetize their efforts or achieve their objectives.

IoT Threats:

The Internet of things (stylized Internet of Things or IoT) is the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. As per my literature

review the year 2017 will bring a large scale IoT security breach, with ecommerce, manufacturing plants, and government organizations at the biggest risk, according to experts. In the past year, IoT security has quickly emerged as a hot issue with multiple threats against the enterprise such as the Mirai botnet (Mirai (Japanese for "the future") is malware that turns computer systems running Linux into remotely controlled "bots (Software Robot", that can be used as part of a botnet in large-scale network attacks) It primarily targets online consumer devices such as remote cameras and home routers, that affected Twitter, Amazon, and Netflix. What's most alarming, however, is that it's likely only the beginning as more companies deploy IoT sensors and devices across their networks. The Threats n affects will be seen more in 2017 as IoT increases and more and more organizations get evolved.

Ransom Ware:

Ransomware is a growing threat that encrypts a user's files and holds the decryption key until a ransom is paid by the victim. This type of malware is responsible for tens of millions of dollars in extortion annually. Worse still, developing new variants is trivial, facilitating the evasion of many antivirus and intrusion detection systems. In this work, we present CryptoDrop, an early-warning detection system that alerts a user during suspicious file activity. Using a set of behavior indicators, CryptoDrop can halt a process that appears to be tampering with a large amount of the user's data. Furthermore, by combining a set of indicators common to Ransomware, the system can be parameterized for rapid detection with low false positives. Our experimental analysis of CryptoDrop stops Ransomware from executing with a median loss of only 10 files (out of nearly 5,100 available files). Our results show that careful analysis of Ransomware behavior can produce an effective detection system that significantly mitigates the amount of victim data loss.

Drone jacking:

Drones (Unmanned Ariel vehicle) which have become more and more talk of the town these days. Some consider this as a toy for fun some may use it for intruding privacy. What started as a fun toy for kids and a slightly expensive hobby for fanatics has really taken off. Drones are well on the way to becoming a major tool for transporters, law agencies, photographers, the news media, or be it covering the telecast of cricket match and more. We cannot deny the fact that drones are becoming more valuable to businesses and government agencies. As we know Amazon made its first ever delivery of product via drone in December 2016 in US and also dominos delivered its pizza in New Zealand via drone, such is the acceptability and increasing craze for using drones to reduce delivery times and attract more customers. In the coming year we could see hackers deploy drone over offices or houses for intruding privacy or intercept official communication which could be a major threat to cyber security. As per David Latimer, a researcher on the project, said large companies have not properly prepared for this threat. “A drone could just go land on the roof, sit there and record people’s keystrokes, and access the internal network over the wireless”.

Threat to Big Data:

Establishments have become very dependent on big data, using it in almost every major decision that they have to make. While data analysis is certainly helpful in many areas, some businesses are starting to forget that human intuition is also important. By taking humans almost out of the process, many fear that decisions may begin to suffer. Big data isn’t always correct, and using it as the only basis for decisions could result in poor decisions, security vulnerabilities, and other issues. Business owners need to question the validity of their data, their code, and all other information to make certain that the information they’re using is correct and current. Many

efforts on big data are focused on the 3V challenges today. However, the flourishing of big data relies not only on the promised solutions for 3V challenges, but also on the security and privacy challenges in big data analytics. It is likely that if the security and privacy challenges are not well addressed, the concept of big data cannot be widely accepted. For example, when big data is exploited in the healthcare context, it could save the health care industry up to US$450 billion. Nevertheless, as patients' data are very sensitive, privacy issues become a major concern when exploiting big data in healthcare. Similarly, when big data is exploited in smart grid, a utility company can collect customers' data every 15 minutes in a residential area to structure conservation programs that analyze existing usage to forecast future use. Although this kind of big data analytics can lead to a strong competitive position for the utility company, the near-real-time data generated every 15 minutes may be abused to disclose the privacy of customers. More important, once the reported data is fabricated, big data analytics become useless (R. Lu et al).

CHAPTER 4

FINDINGS AND CONCLUSIONS

Currently information technology and especially information is one of the main assets of organizations and companies, there are different types of threats that threaten the proper functioning of these entities, such as viruses, malware, cybercriminals, spyware and a number of threats existing, daily different equipment is used, especially mobile phones that are connected to the internet, the biggest source of security threats [1].

Prevention:

Now arises a question can these threats be prevented if yes then how or at least if we can reduce the impact of the risk which would be good. Below we are listing the prevention techniques which can be resorted to minimize the threat effect.

Information Security Awareness:

Nowadays Very little attention is paid in organization regarding to security awareness among the users, making them the weakest link in any organization. As a result, currently, cyber criminals are putting significant efforts to research and develop advanced hacking methods that can be used to steal money and information from the general public. Additionally, the high internet penetration growth rate in the world and the limited security awareness among users is making it a pretty target for cyber criminals. Hence more and more training programs should be deployed in organization, as many users have limited or no knowledge about security awareness.

Generally user education is considered one of the most important and widely-used approaches in fighting phishing attacks. Several organizations have launched awareness campaigns to educate the user on the meaning of phishing attacks and how to detect such attacks and avoid falling victims to them (D. Timko).

Making attacks less Profitable:

According to Robert Dethlefs May 01, 2015 Cyber-attack became more profitable than drug trade. Cyber criminals run highly organized and collaborative enterprises that operate with troubling and destructive efficiency. Juniper Networks conducted a study that found that global cybercrime takes in larger profits than the illegal drug trade. “The cyber black market has evolved from a varied landscape of discrete, ad hoc individuals into a network of highly organized groups, often connected with traditional crime groups (e.g., drug cartels, mafias, terrorist cells) and nation-states,” the report said. And even when the goals of the attackers are not monetary gain, the costs can be enormous. Though not a penny of its cash was stolen, the attack on Sony last December cost the entertainment company billions of dollars through the release of data. Types of data stolen can include financial data, personal health information (PHI) and associated insurance information.

Law Enforcement on Information Security:

While the web has brought businesses near without restriction for countries to get involved and do business together, many terrorists, extremist groups, hate groups, and racial-supremacy groups are also using Web sites and other online tools. We refer to the part of the Web used for such illegitimate and malicious purposes as the Dark Web. As everyday more and more information is sent, stored, and analyzed online, more and more governments are creating laws in an attempt to control it. However, the law passed by one country may be different or even directly opposing to that passed by another, leaving worldwide businesses stuck in the middle. These laws may restrict the free exchange of information, even if that was not the original act, and all businesses are going to have to deal with the fallout. The result is that some technology companies have come in direct conflict with governments by telling them that they

will not hand over certain information or decrypt specific data. This is an ongoing discussion in the information security industry, and so far, there has been no clear indication of how regulations, which is often trying to put rules on past situations, can keep up with the always changing world of data security. Hence the security and law agencies should come together for fight against crime and ensure smooth business across borders by applying strict measures, laws and enforcing regulations so as to reduce the impact of threats.

Known System Vulnerabilities:

As per report publish by Peter Davidson in beta news. It's much easier to buy software or make use of opensource programs than it is to spend the time and money to develop one in-house. However, these commercially available programs often come complete with known vulnerabilities that hackers are more than willing to take advantage of. That's why you have to do your research into software before you buy it.

Computer technology is more and more ubiquitous; the penetration of technology in society is a welcome step towards modernization but society needs to be better equipped to handle with challenges associated with technology. New hacking techniques are used to penetrate in the network and the security vulnerabilities which are not often discovered create difficultly. As the technologies are evolving based on human needs the more we are getting prone to hackers and threats which are going more persistent and sophisticated by the day. Now it's time for Academia, industry and government to work together in bold new ways to solve the grand challenges of Information security. To combat today's sophisticated Threats and meet we need a multilayer approach to threat prevention. In this paper we highlighted the latest threats to Information security emerged with technologies like cloud computing, IOT, Drones, Big Data

etc. We also discussed the literature on prevention techniques which can be resorted to minimize the threat effect.

LIST OF REFERENCES

2016 IEEE 36th International Conference on Distributed Computing Systems Crypto Lock (and Drop It): Stopping Ransomware Attacks on User Data Nolen Scaife University of Florida scaife@ufl.edu Henry Carter Villanova University henry.carter@villanova.edu,Patrick Traynor University of Florida traynor@cise.ufl.edu Kevin R.B. Butler University of Florida butler@ufl.edu.

Albert, B (2013) Mining big data in real time, Informatica 37 (1) (2013).

Arasu, B. Babcock, S. Babu, M. Datar, K. Ito, I. Nishizawa, J. Rosenstein, J. Widom, STREAM: the stanford stream data manager (demonstration description), in: Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data, 2003.

Buckley, R. (2007). How to ensure effective testing. SC Magazine: For IT Security Professionals (UK Edition), 34–38. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=26400659&site=ehost-live

Circus, R. (2018). Managing vulnerabilities in hybrid networks. Enterprise Innovation, 1. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=129413005&site=ehost-live

Dayarathna, D &. Toyotaro, S. (2013) Automatic optimization of stream programs via source program operator graph transformations, Distrib. Parallel Databases 31 (4) (2013) 543–599.

Drone jacking: https://www.ft.com/content/a06a1f5c-505f-11e6-8172-e39ecd3b86fc.

Future Generation Computer Systems 25(2009)599–616 Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility Rajkumar Buyyaa, b,CheeShinYeoa, Srikumar Venugopala,James Broberga,Ivona Brandicc.

Forbes: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-canunderstand/#28ae2da11d09.

Heiderich, M., Niemietz, M., Schuster, F., Holz, T., & Schwenk, J. (2014). Scriptless attacks: Stealing more pie without touching the sill. Journal of Computer Security, 22(4), 567–599. https://doi.org/10.3233/JCS-130494

Journal of Computer and System Sciences (www.elsevier.com/locate/jcss): A dynamic prime number based efficient security mechanism for big sensing data streams, Deepak Puthal a, Surya Nepal b, Rajiv Ranjan b,c, Jinjun Chen a- Volume 83, Issue 1, February 2017.

Known system Vulnerabilities: https://betanews.com/2016/07/22/7-information-security-trends-currently-dominating-the-market/.

Lu, R. et al., "EPPA: An Efficient and Privacy-Preserving Aggregation Sheme for Secure Smart Grid Communications," IEEE Trans. Parallel Distrib. Sys. , vol. 23, no. 9, 2012.

Making Attacks less profitable: http://fortune.com/2015/05/01/how-cyber-attacks-became-more-profitable-than-the-drug-trade/.

McAfee Labs 2017 Threats Predictions November 2016: https://www.mcafee.com/au/resources/reports/rp-threats-predictions2017.pdf

Meyer, C. (2019). Thinking Inside the Box: The results of a penetration test will depend on how much information your researcher has in advance. Security: Solutions for Enterprise Security Leaders, 56(2), 23. Retrieved from

http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=134341083&site=ehost-live

Moschovitis, C. (2018). Mitigate Cyber Risks with the Right Security Controls: What are the right controls for your organization? Here's how to be sure. Nonprofit World, 36(1), 16–17. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=128547440&site=ehost-live

Panton, B. C., Colombi, J. M., Grimaila, M. R., & Mills, R. F. (2014). Strengthening DoD Cyber Security with the Vulnerability Market. Defense Acquisition Research Journal: A Publication of the Defense Acquisition University, 21(1), 465–484. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=94909458&site=ehost-live

Timko, D. (2008) "The Social Engineering Threat", Information Systems Security Association Journal (ISSA), January 2008.

Vegvizer, T. (2018). Cybersecurity Threats in the Insurance Industry: Insurers and Their Data Are Particularly Vulnerable to Hackers. Claims, 66(1), 30–32. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=127184603&site=ehost-live

Yasinsac, A. (2002). An environment for security protocol intrusion detection. Journal of Computer Security, 10(1/2), 177. https://doi.org/10.3233/JCS-2002-101-208