Cyber security: Study on Attack, Threat, Vulnerability

TUSHAR P. PARIKH
Research Scholar,
H.N.G. Uni. Patan, Gujarat, India.

DR. ASHOK R. PATEL
Professor and Head
H.N.G. Uni. Patan, Gujarat, India.

Abstract:
The broad objective of this study is an attack, threat and vulnerabilities of cyber infrastructure, which include hardware and software systems, networks, enterprise networks, intranets, and its use of the cyber intrusions. To achieve this objective, the paper attempts to explain the importance g in network intrusions and cyber-theft. It also discusses in vivid detail, the reasons for the quickdilation of cybercrime. The paper also includes a complete description and definition of cyber security, the role it plays in network intrusion and cyber recognize theft, a discussion of the reasons for the rise in cybercrime and their impact. In closing the authors recommend some preventive measures and possible solutions to the attack, threats and vulnerabilities of cyber security. The paper concludes that while technology has a role to play in reducing the impact of cyber attacks, the vulnerability resides with human behaviour and psychological predispositions. While literature supports the dangers of psychological susceptibilities in cyber attacks investment in organizational education campaigns offer optimism that cyber attacks can be reduced.

Keywords: *Cyber-Warfare, Vulnerability, Cyber-attack, Threat*

1. Introduction

World is going on the digitalization or cash less transaction so multifold. Even the government and defense organization have experienced significant cyber losses and disruptions.The crime environment in cyber space is totally different from the real space that is why there are many hurdles to enforce the cybercrime law as real space law in any society. For Example, age in real space is a self-authenticating factoras compare to cyberspace in which age is not similarly self-authenticating. A child under age of 18 can easily hide his age in Cyber space and can access the restricted resources where as in real space it would be difficult for him to do so. Cyber security involves protecting the information by preventing, detecting and responding to cyber-attacks. [1]

The penetration of computer in society is a welcome step towards modernization but needs to be better equipped to keen competition with challenges associated with technology. New hacking techniques are used to penetrate in the network and the security vulnerabilities which are not often discovered arise difficulty for the security professionals in order to find hackers [6].

The defense mechanism mainly concerns with the understanding of their own network, nature of the attacker, inspire of the attacker, method of attack, security weakness of the network to mitigate future attacks.[13]

2. Background

Currently media, Government sectors and organization are hot discussion about the cyber security. Experts claim the topic is over-hyped and artificially inflated by fear vend, with terms such as 'cyber-warfare 'designed to excite an emotional rather than a rational response. In a recent study by Intelligence, number of the threat like 23, cyber-war has been grossly overstated. Cyber security is the key concepts of discussion topic that can inspire to independent thinking researcher and experts. Indeed, this type of discussion is proposed by many of those calling for caution such as security experts,

These are the points out that many cybercrimes are the direct result of poor security rather than lack of government polices implementation. The president of the Electronic Privacy Information Center gives suggestion against mandatory Internet identification requirements. He pointed out those countries, attribution requirements have resulted in censorship and international human rights violations.
Nevertheless of which view one may take, it is plain that cyber-security is accepted as a very important and current topic and healthy discussion on.
In this paper give the general or realistic definition of cyber-security for cyber world accepted, it does suggest different key elements for activities inclusion in Information [15]

Technology programs, these are based on a types of research documents and reports published. With the recurrence of cyber-attacks on a constant increase, governments and security organizations worldwide are taking enterprising and preemptive action to reduce the risk of successful attacks against critical infrastructures. It means the relation between the physical and cyber domains. Cyber security involves protecting that infrastructure by preventing, detecting, and responding to cyber incidents. [11]

The association between military strikes on civilians and government base organized Internet suppression was prevalent with actions in the physical world being prepare the way for cyber-events. IT Professionals may be aware of recent events besiege Supervisor Control and Data Acquisition (SCADA) systems virus.
SCADA malware using both insufficient patched vulnerabilities and new Vulnerabilities. The serious physical, financial impact these issues could have on a worldwide basis.

Providentially, all cyber-events are not connected to human loss of life yet the economic impact to a society can still be hugely damaging. It was reported that information and electronic data theft excel all other fraud for the first time rising from the previous year. This is in spite of a reduction in half of other fraud categories.

The CNCI is the first in a series of stages to establish a broader, updated national U.S. cyber-security strategy with the following summarized goals:
(1) Establish a front line of defense against today's immediate (cyber) threats.
(2) Defend against the full spectrum of threats
(3) Strengthen the future of cyber-security environment.

These goals also underline the CNCI's initiatives. Cyber security is a challenge that not only national boundaries it's beyond and requires global cooperation with no single group, country or agency claiming ownership, according to a 2009 report by the US Department of Homeland Security. The report proposes a Roadmap for Cyber-security Research. Building on the 2005 second revision of the INFOSEC Research Council (IRC) Hard Problem List, and in recognition of the aforementioned presidential directives, the roadmap identifies research and development opportunities that are scoped to address eleven "hard problems".

This defines cyber security as the "preservation of confidentiality, integrity and availability of information in the cyberspace", with an accompanying definition of cyberspace as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form". It is current topic of, that cyber-security is an area of much discussion, interest and attention[15].

3. Methodology

This is the 21st edition of the Symantec Internet Security Threat Report and much has changed since the first one. We take a fresh look at the structure and contents of the report. As well as focusing on the threats and findings from our research, it is also tracks industry trends.We try to highlight the important developments and look to future trends. This goes beyond just looking at computer systems, smartphones, and other products, and extends into broad concepts like national security, the economy, data protection, and privacy [14].

3.1 Threats

Cyber security threats encompass a wide range of potentially illegal activities on internet. Cyber security threats against utility assets have been recognized for decades. The terrorist attacks so give the attention has been paid to the security of critical infrastructures. Insecure computer systems may lead to fatal disruptions, disclosure of sensitive information, and frauds. Cyber threats result from exploitation of cyber system vulnerabilities by users with unauthorized access [7].There is crimes that target computer networks or services directly like malware, viruses or denial of service attack and crimes facilitated by networks or devices, the primary target of which is independent of the network or device like fraud, identity theft, phishing scams, cyber stalking .

a. Cyber Theft

This is the most common cyber-attack that committed in cyberspace. This kind of offence is normally referred as hacking in the generic sense. It basically involves using the internet through steal information or assets. It also called the illegal access, by using the malicious script to break or crack the computer system or network security without user knowledge or consent, for tampering the critical data and. It is the gravest cybercrimes among the others. Most of the banks, Microsoft, Yahoo and Amazon are victim of such cyber-attack. Cyber thieves use tactics like plagiarism, hacking, piracy, espionage, DNS cache poisoning, and identity theft. Most of the security web sites has described the various cyber threats.

b. Cyber Vandalism

Damaging or exploiting the data rather than stealing or misusing them is called cyber vandalism. It means effect on network services are disrupted or stopped. This deprives the authorized users for accessing the information contained on the network. This cybercrime is like a time bomb, can be set to bring itself into action at a specified time and damage the target system. This creation and dissemination of harmful software which do irreparable damage to computer systems, deliberately entering malicious code like viruses, into a network to monitor, follow, disrupt, stop, or perform any other action without the permission of the owner of the network are severe kind of cybercrimes.

c. Web Jacking

Web jacking is the forceful control of a web server through gaining access and control over the web site of another. Hackers might be manipulating the information on the site.

d. Stealing cards information

Stealing of credit or debit card information by stealing into the ecommerce server and misuse these information.

g. Cyber Terrorism

Deliberately, usually politically motivated violence committed against civilians through the use of, or with the help of internet.

h. Child Pornography

The use of computer networks to create, distribute, or access materials that sexually exploit underage children pornography in shared drives of community networks.

i Cyber Contraband

Transferring of illegal items or information through internet that is banned in some locations, like prohibited material.

j. Spam

It includes the Violation of SPAM Act, through unauthorized transmission of spam by sending illegal product marketing or immoral content proliferation via emails.

k. Cyber Trespass

l. Legal accessing of network resources without altering disturbs, misuse, or damage the data or system. It may include accessing of private information without disturbing them or snooping the network traffic for gets some important information.

m. Logic bombs

These are event dependent programs. These programs are activated after the trigger of specific even. Chernobyl virus isa specific example which acts as logic bomb and can sleep of the particular date.

n. Drive by Download

A survey is undertaken by search engine companies. Numbers of websites were acting as hosts for malware. The term “Drive by Download (DbD)” is maneuvering in software industry since its inception with different variations. It is a phenomenon in which any software program is installed automatically on a user computer while surfing on the internet. The intent of installing malicious software is to gain benefit over victim machine, e.g. it could be a stealing of confidential information like stored passwords, personal data, using victim terminal as botnet to further spread malicious contents.

o. Cyber Assault by Threat

The use of a computer network such as email, videos, or phones for threatening a person with fear for their lives or the lives of their families or persons whose safety they are responsible for (such as employees or communities). An example of this is blackmailing a person to a point when he is forced to transfer funds to an untraceable bank account through an online payment facility.

p. Script Kiddies

Novices, who are called script kiddies, script bunny, script kitty, script running juvenile is a derogatory term used to describe those who use scripts or programs developed by others to attack computer systems, networks and get the root access and deface websites.

q. Denial of service

A denial of service attack (DoS) or distributed denial of service attack (DDoS) is an attempt to make a computer resource unavailable to its intended users. The computer of the victim is flooded with more requests than it can handle which cause it to crash. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. This is also known as email bombing if via used is email. E-bay, Yahoo, Amazon suffered from this attack [1].

3.2 Attacks

Cyber-attack is a big issue in the cyber world that needs to be focus because of the effect on the critical infrastructure and data. The growth of technology is accompanied by cyber security threats or “cyber-attacks” which threaten users security when using such technologies. Cyber threats and attacks are difficult to identify and prevention. So users are not accepting the new technology due to the frequently cyber-attacks less security of data. A cyber-attack is when someone gain or attempts to gain unauthorized access to a computer maliciously [11].

a. Untargeted attacks

Un-targeted attacks in attackers indiscriminately target as users and services possible. They find the vulnerabilities of the service or network. Attacker can take the advantage of technologies like: Phishing:

Phishing means fake people sending the emails to numbers of users and asking the personal information like baking, credit card. They encouraging the visits of fake website and give the good offers. The customers click on the links on the email to enter their information, and so they remain

unaware that the fraud has occurred. [8].
Water holing:
Publish the fake, as well as dummy website or compromising a legitimate one in order to exploit visiting user's information.
Ransom ware:
It includes spread disk encrypting extortion malware.
Scanning:
Attacking wide swathes of the Internet at random.

b. Targeted attacks:

Targeted attacks in attackers, attack on the targeted users in the cyber world.
Spear-phishing
Sending links of malicious software and advertisement via emails to targeted individuals that could contain for downloads malicious software. Deploying a botnet. It is deliver a DDOS (Distributed Denial of Service) attack Subverting the supply chain.

To attack on network or software being delivered to the organization In general attackers will, in the first instance use tools and techniques to probe your systems for an exploiting vulnerability of the service [3].

3.3 Vulnerability

Vulnerabilities are weaknesses in a system or its design that allow an intruder to execute commands, access unauthorized data, and/or conduct denial-of service attacks. Vulnerabilities can be found in variety of areas in the systems. They can be weaknesses in system hardware or software, weaknesses in policies and procedures used in the systems and weaknesses of the system users themselves. Vulnerability were identified due to hardware compatibility and interoperability and also the effort it take to be fixed. Software vulnerabilities can be found in operating systems, application software, and control software like communication protocols and devices drives. There are a number of factors that lead to software design flaws, including human factors and software complexity. Technical vulnerabilities usually happen due to human weaknesses. [10]

There is no system is automatically immune from cyber threats, the consequences of ignoring the risks from complacency, negligence, and incompetence are clear. In 2015, an unprecedented number of vulnerabilities were identified as zero-day exploits that have been weaponized, and web attack exploit kits are adapting and evolving them more quickly than ever. As more devices are connected, vulnerabilities will be exploited [14].

4. Results and Analysis

Secure the System
There are basic three methods to secure the system from outsider threat and attack.
Prevention: If you were to secure your network, prevention would be using the firewall, security software and end user use the antivirus software. You are doing everything possible to keep the threat out.
Detection: You want to be sure you detect when such failures happen. Everyday update the security software as well as hardware.
Reaction: Detecting the failure has little value if you do not have the ability to respond. If anything it's happen so your security software warn.

4.1Preventing from Attack and Threats

- Recovering from Viruses, Worms, and Trojan Horses
- Avoiding Social Engineering and Networking Attacks
- Avoiding the Pitfalls of Online Trading

- Using Caution with USB Drives
- Securing Wireless Networks

4.2 Preventing from Email and communication

- Using Caution with Email Attachments
- Reducing Spam
- Using Caution With Digital Signatures
- Using Instant Messaging and Chat Rooms Safely
- Staying safe on social Network Sites

4.3 Safe Browsing

- Evaluating Your Web Browser's Security Settings
- Shopping Safely Online
- Web Site Certificates
- Bluetooth Technology [5].

5. Conclusion

Cyber security incidents involving attacks, research supports the most effective defense is a computer literate user. To consider is those most vulnerable which are identified in this research as new employees within an organization, as specifically, with the attacker seeking personal identifiable information from those engaged. Further supported in this research are the psychological variables that contribute to user and network vulnerability. This paper concludes that while technology has a role to play in reducing the impact of cyber attacks, threat and vulnerability resides with human behaviour, human impulses and psychological predispositions that can be influenced through education. cyber attacks can be reduced, but an absolute solution to overcome such cyber security threats has yet to be put-forward. In the future work of the cyber attack, threat and vulnerability reduce in the network implement the cyber security model.

References

1. Razzaq, Abdul, et al. "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. “Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on. IEEE, 2013.
2. Byres, Eric, and Justin Lowe. "The myths and facts behind cyber security risks for industrial control systems." Proceedings of the VDE Kongress. Vol. 116. 2004.
3. “Common Cyber Attacks: Reducing The Impact Gov.uk” https://www.gov.uk/...data/.../Common_Cyber_Attacks-Reducing_The_Impact.pd
4. “CYBERSECURITY: CHALLENGES FROM A SYSTEMS, COMPLEXITY,KNOWLEDGE MANAGEMENT AND BUSINESS INTELLIGENCE PERSPECTIVE” Issues in Information Systems Volume 16, Issue III, pp. 191-198, 2015
5. “Cyber security: risks, vulnerabilities and countermeasures to prevent social Engineering attacks” International Journal of Advanced Computer Research, Vol 6(23) ISSN (Print): 2249-7277 ISSN (Online): 2277-7970 http://dx.doi.org/10.19101/IJACR.2016.623006
6. Ahmad, Ateeq. "Type of Security Threats and It’s Prevention." Int. J. Computer Technology & Applications, ISSN (2012): 2229-6093.
7. Ten, Chee-Wooi, Chen-Ching Liu, and Govindarasu Manimaran. "Vulnerability assessment of cyber security for SCADA systems." IEEE Transactions on Power Systems 23.4 (2008): 1836-1846.
8. “Cyber Crime-Its Types, Analysis and Prevention Techniques”, Volume 6, Issue 5, May 2016 ISSN: 2277 128X www.ijarcsse.com
9. “A Review of types of Security Attacks and Malicious Software in Network Security” Volume 4,

Issue 5, May 2014 ISSN: 2277 128X www.ijarcsse.com

10. Abomhara, Mohamed, and G. M. Kien. "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks." Journal of Cyber Security 4 (2015): 65-88.
11. "Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users" International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:9, No:3, 2015
12. "Detection and Prevention of Passive Attacks in Network Security" ISSN: 2319-5967 ISO 9001:2008 Certified International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 6, November 2013
13. Al-Mohannadi, Hamad, et al. "Cyber-Attack Modeling Analysis Techniques: An Overview." Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on. IEEE, 2016.
14. "Internet Security Threat Report Internet Report "VOLUME 21, APRIL 2016https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
15. Rowe, Dale C., Barry M. Lunt, and Joseph J. Ekstrom. "The role of cyber-security in information technology education." Proceedings of the 2011 conference on Information technology education.ACM, 2011.