IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

Significance of Cyber Security in Cyber World

Shivani Gurunath Mohit
Student, Department of MCA
Late Bhausaheb Hiray S. S. Trust's Institute of Computer Application, Mumbai, India

Abstract: *Cyber security has its unique role in securing information in every sector. Protecting information from is hackers have become more challenging. Almost everyone recognizes the important of cyber world as a fact of daily life. Various policies and regulation acts were being implemented by organizations and governments to prevent cyber crimes. The cybersecurity the main thing that originates in mind is 'cybercrime' which are aggregate colossally daily. This paper focuses on cyber security challenges, the world is facing and required techniques and technologies to prevent them.* No technology we use is ever infallible

Keywords: Cyber security, cyber governance, cyber institutions, information sharing, CERTs, ISACs, information technology, cyber world, information security, cyber threats, cybercrimes prevention, cyber security challenges, cyber ethics, cyber-crimes, PAM.

I. INTRODUCTION

Maintaining security over sensitive information has become the most considerable challenge. Today an individual can receive and send any information may be video, or an email or only through the click of a button but did s/he ever ponder how safe this information transmitted to another individual strongly with no spillage of data? The proper response lies in cybersecurity. The cybersecurity department not only deals with the security measures of common devices like computers, smart phone and other internet of things but also technologies like virtual machines, network topology, cloud services, servers and more. As digital forensics is also a part of this, there is a huge requirement for IT companies to analyse and investigate cyber-attacks. Though there are teams like OWASP, EC-Council, SIEM, CISSP, information security analysts are working for the companies to provide good performances, attackers coming up with different patterns to affect the CIA triad.

1.1 Importance

Today Internet is playing very crucial role in every day's life, this makes hacker to exploit in more possible ways. Therefore, maintaining the speed of internet is as important as maintaining its security. Most of the commercial transactions, business deals, private information, human interests and emotions are processing via internet. Cybersecurity is one of the fast-growing tech fields, not only in IT sectors but also in health, banking, educational, military, government and public sectors as well. Even governments of every nation introducing new cybersecurity laws and policies to prevent confidentiality, integrity and availability of the data and services. In every sector cybersecurity has its own importance to secure companies' data. Training employees with proper knowledge and following security policies are necessary to prevent accidental insider attacks. Recruiting cyber analysts for the company's security can help not only in identifying threat but also in incident response process. For investigating the incident and implementing countermeasures to prevent attacks, system security professionals are important.

II. LITERATURE REVIEW

Digitization and internet in today's world changed the human lifestyle by increasing business opportunities and social connections. On the other side, cyber criminals taking this platform as an advantage and exploiting systems to grab sensitive information. This risk of exploitation can be defended cybersecurity experts in IT sectors. The term cybersecurity came into existence in 1970s with a research project called ARPANET. After observing traceable footprints along the network path using a program developed by the researcher named Bob, he started calling it CREEPER. Later Ray Tomlinson who is the creator of email service, redesigned the same program with self-replication capability. That invented first computer worm and to defend that he developed a program called REAPER. Today there are many techniques developed in cyber security to defend national and international cybercrimes. As this digital ecosystem is just

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

a triangle of process, people and technology, the chance of being a victim is high. According to the data gathered from large scale business sectors funds has been raising with 63% in 2018 and 67% in 2019 and small-scale companies with 50% in 2018 and 66% in 2019 competitively to maintain security. Protecting from cyber threats, identifying threats in less time, recovering data loss, preventing system from further risk are the main functions of cybersecurity which are also considered as major concerns in companies and private lives.

III. HYPOTHESIS TESTING

There are many potential benefits with cybersecurity which supports in company's growth, trust and reputation in the society. Implementing firewalls or access control lists can block malwares like viruses, trojans, worms and other spam or junk files and prevent systems for vulnerabilities exploitation. This results in protected systems against hacking techniques like ransomware, DDOS and more. Security techniques are helpful in preventing data loss and exposure of sensitive information. System or server crashes can be minimized and availability can be maintained. Though there are considerable positive points with this, few disadvantages are also to be considered. Securing systems with centralized architectures like unified threat management systems are easy to compromise with a single point of failure. According to a proverb "don't put all your eggs in one basket" may fail with a single point of breakdown. Establishing security architectures and security engineers are budget dependent in case of large networks. Training staff with proper cybersecurity knowledge can cause intentional insider attacks. Sometimes even firewalls can fail to identify patterns of malicious files with incorrect configuration. In case of small-scale start-up companies and individual lives cybercrimes are more frequent for financial benefits. As the company grows, resources and data increases which results in increase of network complexity. This makes a challenging task in separating network and implementing security. Following security policies without exemptions and implementing security matrices with scalability is also a problem to consider.

3.1 Cyber Security

As the technology is growing rapidly, there is no limits for cyber threats and no scope of slowing down. Even after following security rules and policies, companies are suffering from threat actors performing cybercrimes like insider threats, storage devices thief, social engineering. cyber threats are not only limited to companies and individual lives but also extended to power plants and other utility services resulting in cyber war between nations. Cyber criminals are now focusing on financial benefits worldwide. WannaCry and Not Petya ransomware attacks are the suitable examples of global cyber threats. Skimming technique in individual bank accounts and bitcoin mining are the recent approaches resulting in massive financial scam. These impact in financial loss as well as trust in the banks sectors and government. In the context of IT industries, Companies are more focused on financial and global growth and less concerned with the security. Providing advanced technology system for the company's security is as important as implementing it with proper configurations for a protected environment. Smart ways of securing a company is by identifying and stopping threats in the initial stage and defining own security policies for safeguarding data. This can be done by cyber specialists. In every sector, malware are the most common threats seen in computers and networks which includes computer virus, worms, trojans, adware, spam, ransomware and more. These are intended to harm computers either intentionally or accidentally. As malware programs can be developed with different patterns to cross firewalls, adopting technologies like machine learning techniques to secure websites and spam filters like intrusion detection and intrusion prevention systems are useful for identifying and blocking suspected files. As long as the security design and operations are related to the organization's business model, confidentiality and integrity can't be disturbed.

For maintaining standards and managing structure in an organization, PPT framework is the fundamental component. This framework is the structure of people, process and technology which is also helpful in incident response. Considering an example, DDOS attack in the company's server is identified resulting in-service unavailability. The action can be divided as the person who performed the crime, the technique he used and the equipment he used. With the three components, the framework is also called 3 pillars of cybersecurity.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

3.2 Cyber Security Implementation

Cyber Security assumes a critical role in the area of data technology. Buying smart high-tech gadgets to secure the system or an organization is successful only when the technology is implemented properly with required configurations. Some main trends that are changing cybersecurity give as follows:

Web servers:

As internet is dealing most of the everyday things, companies started developing web-based application to make it more convenient. Attacks are also increasing on the web in the same way to expose or to steal sensitive data. Cyber criminals are using web as an open platform to spread malicious files via weak secured web servers. So, securing web securing and application turned into a major concern. Using virtual private network build-in browsers can prevent cyber-attacks.

Mobile Networks:

Though people using laptops and desktops, mobile technology is dominating the internet world. Unless in companies or organizations, people are more habitual in using smart phones and tables in which security is a concern. In individual life, most of the everyday private things are recorder in personal mobile phones. Therefore, ignoring security updates lead to higher compensation. With the change in mobile network generations from 4G to 5G, security and network speed is having been improving to prevent network intrusion attacks.

Changing to IP6 Version:

Internet protocol version 4, popularly known as IPV4 has been the backbone of internet by connect large number of devices. Now internet protocol versions 6 is changing the trend by replacing IPV4 to IPV6 which supports more number of connective devices with better security capabilities. Implementing IPV6 technology can reduce number of attacks not only in private lives but also in large scale IT industries.

Cloud based Services:

Targeted database attacks are increasing not only in IT and health sectors but also in public and military sectors as well. With the problem, cloud storage turned out to be the suitable solution to prevent SQL inject attacks. Therefore, most of the small- and large-scale industries around the world are adopting cloud services. With increase in information, cloud storage capacity changes which creates security flaws. Services also include software as a service, platform as a service, infrastructure as a service. This also help users to secure and save resources.

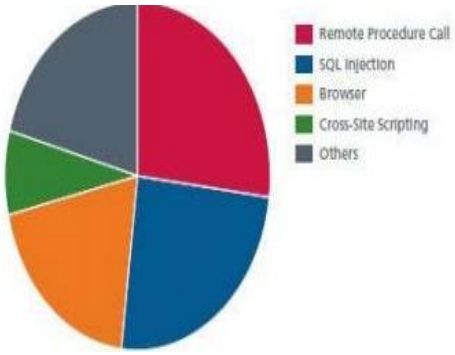
Data encryption:

Encryption is the method of converting human readable format to code format. The technique is used to prevent attacks like eavesdropping and man in the middle. In the process to encryption few technical encryption algorithms are used to convert data with a key which describes the encryption type. Though is this not a new technique, encrypting data with number of bites determine its strength. Salting is the technique used in encryption which makes hard to crack. This maintains data confidentiality though it is exposed.

ADP's and Targeted Attacks:

Advanced Persistent Threat (APT) is a whole of the dimension of cybercrime ware. For quite a long-time network security capacity. For example, IPS or web filtering have had a key influence in distinguishing such focused-on assaults (Bendovschi, 2015). As attackers become bolder and utilize increasingly dubious methods, network security must incorporate with other security benefits to identify assaults. Thus, one must recover our security procedures to counteract more dangers coming later on. Subsequently the above is a portion of the patterns changing the essence of cybersecurity on the planet. The top network threats are showing in figure 1.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252



IV. SUITABLE TECHNOLOGY

The suitable technologies used to maintain security system stronger are as follows.

4.1 Firewall

For a system or an organization firewalls act as the first layer of security. A firewall is used to block junk files or unauthorized packets entering from the network. This can be a hardware or in-built software. Though the function of a firewall is inspecting and filtering packets, setting up with suitable configurations matter. Firewall with incorrect configurations can be bi-passed by changing the file pattern.

4.2 Anti-Virus Applications

Malware in a system can delete or overwrite files, slow down the system, crashes the system and sometimes helps the attacker to compromise the system or servers. These include viruses, trojans, worms, ransomware, spyware and more. These malwares can be detected using malware scanners popularly called anti-virus software. The function of anti-virus software is to identify, block or delete the suspected files by scanning the entire system. But there are few disadvantages which include more RAM consumption, sharing personal information and not supporting comprehensive protection [13].

4.3 Honeypots

In the recent years honeypots are developed to as a security alarm which helps the admin or security analyst in finding the intruder. These are used to deflect the hacker to different path and prevent the information. Though using this technology attack can be prevented in the initial stage, false alarms can occur with improper configurations.

4.4 User Credentials

For computer or web application accessing entering user credentials in first step for authentication and authorization purpose. The usual way of accessing is by entering username and password which specifies uniqueness of every user. As these can be stolen by the hacker to pretend like the user. This is known as social engineering attack. This problem can be overcome with the latest solution, one time password (OTP). This is a unique password sent to the mobile or email. This is also known as 3-way authentication.

4.5 Access Control Lists:

Maintaining ACL (Access control list) for accessing files depending upon their sensitivity is trending with the growing cyber threats. ACL is creating a specific list of people with privileges to access files or directories or to block specific group of people. This is mostly used in organization to secure highly confidential files from insiders. List usually depends on role and criteria on the employee.

V. CONCLUSION

Furthermore, “No technology we use can ever be infallible”, but we can make an attempt to get pretty close to making it impenetrable. One way to do that is by practicing seeking of weaknesses and vulnerabilities in our systems. That is where the significance of the ethical hacker comes into picture.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

Cybersecurity has endless benefits followed by few disadvantages. Even large scaled security organizations were the victims on these cyber-attacks. Organizations dealing with sensitive information and having low cybersecurity knowledge like medical and banking sectors have huge risk cyber threats. Hiring a role to perform cybersecurity operations for the organization is helpful to defend cybercrimes. Including that companies has a respectability to train their employees with proper cybersecurity knowledge. This help employees to identify the attack at the initial stage which may not be helpful in defending the attack but can help in minimizing the loss. Though this indirectly trains employees to perform insider attack without any traces, this can be reduced by implementing constant surveillance and security policies

REFERENCES AND SOURCE MATERIALS

[1]. https://www.cnbc.com
[2]. https://www.zdnet.com
[3]. https://www.researchgate.net
[4]. https://www.rapid7.com
[5]. https://resources.infosecinstitute.com
[6]. https://www.theglobeandmail.com
[7]. https://www.oxfordlearnersdictionaries.com
[8]. https://www.researchgate.net/publication/335322600_Cyber_Security
[9]. https://www.researchgate.net/publication/280101879_The_Cyberspace_Redefining_A_New_World
[10]. https://www.researchgate.net/publication/352477690_Research_Paper_on_Cyber_Security
[11]. https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies
[12]. https://owasp.org/www-project-top-ten/