Cyber Security: A Literature Review

Akrati Singh[1], Anoushka Pathak[2], Aditi Pansari[3]
[1, 2, 3]Mody University Of Science And Technology,Lakshmangarh,Rajasthan

Abstract- *Amongst the increase in number of technologies, there has been an exponential rise in the cyber security threats. The counters help to ensure the integrity and availability of information systems by preventing asset losses from cyber security attacks. In this paper, we are accumulating literary data regarding cyber security as well as the different automation software which have been introduced or are being devised for securing our data. For developing such software, many techniques are used like OTP, event log analysis, malicious attack detection and virtualization.*

Keywords- Cyber Security, technologies, automation

I. INTRODUCTION

In information technology industry, data security and protection is emerging as a major challenge. For as long as the technology has existed, cyber threats have been loitering around.

With handheld devices becoming more and more ubiquitous each day and networking having its roots so deeply embedded in our lives, the world around us is becoming more and more cyber and technologically advanced with each passing day and it is hard to avoid the threats it entails.

Cyber attackers range from sophisticated hackers to naive teenagers using cyber vulnerabilities to their advantage. Some of the threats involved are: spoofing, phishing, pharming, malware, ransomware, viruses, worms, trojan horses, etc.

One such threat reported as of May 2017, when the world witnessed one of the worst cyber outcries, Wanna Cry Ransomware, a malicious malware that affected thousands of companies in over 150 countries. Britain's Nation Health Service was worst hit by the attack and it also brought many of Spain's top companies to a halt. This malicious malware first targeted computers functioning on obsolete versions of Microsoft Operating System and then infected other systems on the network. The attack lasted 4 days bringing about an extensive damage of hundred billion dollars.

II. WHY DID THE NEED FOR CYBER SECURITY ARISE?

Bob Thomas observed that the computer software can actually travel across network. It was all part of a research project. He designed a computer program and made it move across network. Its name was Creeper. Ray Tomlinson, the man who invented Email, found it really intriguing and decided to catch it. He designed a program Reaper to catch it. This was a virus designed to catch another virus.

This was the start of new era in cyber security. Earlier, the cyber security was only limited to providing security against threats from inside people. But this was about 70s and 80s.There was a switch from an academic beginning to criminality when virus programs were used by nations to exercise their cyber power.

In 1988, Robert Morris, in a pursuit of measuring size of internet, designed a program to travel across internet which intruded into Unix Terminals and spread by self- replicating. But the last instruction of self-replication proved to be massive threat. The virus multiplied so rapidly that the speed of internet was slowed down by many folds. And Robert Morris became the first person to be reported under Computer Emergency Response Team. This organization works to resolve internet issues on the whole. This event appears to have acted as a harbinger of today's virus affected world [1].

III. CONVENTIONAL METHODS

Numerous businesses and institutions now function solely on technology and share sensitive data and effectuate transactions over networking. This advancement makes cyber security indispensable and calls for a robust and standardized solution to remedy technological vulnerabilities that can compromise one's identity and privacy and at times cost livelihood [2].

Enlisted are some of the most effective measures to protect a computer and keep the data intact:

- Strong Passwords: Implementing complex and various alpha-numeric combinations for a password can prevent an attack or an unwanted encroachment of your devices to an extent.

• Data back-up: Performing regular back-up for your data is a key feature of data security. In case our security systems get compromised causing loss of data, we still have access to our data.

• Implementing control access and updating systems and installing Intrusion Detectors: Restricting data and service access to limited authorized personal and controlling physical approach to the premise can help keep threats at bay. Also keeping critical data offline and its limited sharing is crucial. Timely updating our security systems can help us stay one step ahead of the attackers. Intrusion Detectors helps monitor network traffic and alerts and issues warning on detecting any suspicious activity.

• Installing Firewalls, Antivirus programs: Firewall filters the incoming and outgoing data on a network and blocks malicious content from infecting your systems. This also prevents navigating to unsecure websites and potentially threatening content from being downloaded to your computers. Antivirus programs, on the other hand, monitors your system for any unusual behavior, traces and destructs any dangerous software or virus.

• Data Encryption: Encryption adds an extra wall of security to sensitive information stored on a system or a network. It employs a systematic algorithm to encrypt data to a code formally called ciphertext which can only be read if one has the permitted key or password to access that data , restricting data interpretation and manipulation.

• Cybercrime Insurance: Small or large scale business projects shall issue a cybercrime insurance that can cover for their losses in case of a cyber attack.

• OTP (One Time Password): Various business institutions can enforce OTP's to ensure secure financial transactions with customers. OTP's are generated by employing various algorithms and they have a limited validity of one transaction/session. OTP's are more secure than static passwords as they are not vulnerable to encroachment or accidental revelation.

• CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart): Hackers can employ various web applications or design specific algorithms to make spurious entries or hoax registrations and create a passage to upload malicious content on your systems or network. CAPTHA is a real-time test that calls for an immediate response to a random distorted piece of information that can only be interpreted by humans, thus differentiating bots and humans [4].

IV. FUTURE SCOPE

In this age of the internet, it is a moral obligation to ensure proper data security. According, to current situation any device connected to the internet can be hacked. The hackers are smarter than ever before. How can we be prepared? What measures can be taken?

4.1 Context Aware Behavioral Analytics [CABA]

Context-Aware Behavioral Analytics treats unusual behavior as nefarious activities. It is related to examining the context in which data is used by the users.

The important technologies that form an integral part of CABA include:

• Monitoring behavioral profiles: The companies can monitor habits of users, accountants, clients, contractors by creating their behavioral profiles. These profiles are monitored from month to month and device to device. Any significant change in behavior in real time from past behavior may pose a security issue to the company.

• Mobile Location Tracking: Tracking the geological location is an importantdeterminant of a person's behavior.

• Bio printing: Bio print markers indicate how the employee uses a simple input device such as a mouse.

•Phone Printing: It includes the analysis of acoustic information to identify the fake caller's identity [3].

4.2 Virtual Dispersive Networking [VDN]

The hackers have found a way of injecting messages into a communication channel.

Therefore, the conventional traditional encryption technologies don't stand a chance.

MIM (Man in Middle) attacks are becoming popular. Here the, hacker controls the messages between the transmitter and receiver by relaying it. The transmitter and receiver remain completely unaware about the fact that their conversation is being controlled by a third person.

The solution devised is based on the dispersive technology. The signal being transmitted can be split into several simultaneous parts. Not only this, the parts of message can be separately encrypted and routed on different protocols following independent paths [5].

4.3 Cloud Computing Security

Cloud computing and cloud storage are the latest trends in this world of constantly evolving web applications and cyber security. The idea is to make data more mobile and accessible and also creating an effective scheme to securely store data online than on local storage devices.

Cloud computing is internet-based computing that helps us retrieving various IT based services and several other web resources and data by the means of internet. Cloud Storage enables seamless data storage on the web on remote databases which can be accessed anywhere, anytime on any devices with appropriate permission. Cloud Computing saves the effort of large data movement and facilitates recovery on device destruction, loss or if the device becomes obsolete.
The term 'cloud' basically stresses on fact the information is available on the 'cloud'

i.e. on the web and that one can easily gain access to data and myriad other softwares via internet without being physically restricted to a specific location to gain access to it [6].

Cloud Computing and Storage benefits a lot of businesses and institutions on monetary grounds as it save them from the need for a storage infrastructure and devices that could cost them in millions otherwise.

But internet being so prone to data breaches and hacking, there's raising concern regarding the safety of data stored on clouds and calls for the need of robust security arrangements i.e. Cloud Computing Security. Data not only needs security from breaches and hacking but also the notorious employees of the Cloud service providers. Therefore it is usually advised to choose your cloud service providers wisely. The demanding question of as to why one should choose Cloud Computing and Cloud Storage over our conventional means of data management is because cloud service providers have superior security provisions like firewalls, encryption and VP's and skilled data experts to deal with any technical casualty [2] .

REFERENCES

[1] A. M. Tonge, "Cyber Security:challenges for society-A literature review,"IOSR Journal of Computer Engineering (IOSR-JCE), vol. 12, no. 2, pp. 68-69, 2013.

[2] U. D. Deore, "A Literature Review on Cyber Security Automation For Controlling Disturbed Data," International Journal of Innovative Research in Computer and Communicatioon Technology, vol. 4, no. 2, pp. 1-3, 2016.

[3] "SentinelOne," 10 March 2017. [Online]. Available: https://www.sentinelone.com/blog/history-of-cyber-security/. [Accessed January 2018].

[4] Cisco, "Annual Security Report: Highlighting Global Security Threats and
Treands," Cisco, 2009.

[5] B. Kotiyal and R. H. Goudar, "A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India," International Journal of Information and Education Technology, vol. 2, no. 2, 2012.

[6] R. Sharma, "Study of Latest Emerging Trends on Cyber Security and its challenges to society," International Journal of Engineering and Scientific Research, vol. 3, no. 6, 2012.