International Journal of Innovative Research in Technology & Science
ISSN: 2321-1156 www.ijirts.org Volume VIII Issue IV, July 2020

Protection of System from Data Breaches

Ankur Gupta[1], Bhupendra Malviya[2], shital Gupta[3]; SORT Peoples University Bhopal
[1]ankurucgupta@gmail.com, [2]bhupendra09sm@gmail.com, [3]email4sgupta@gmail.com

Abstract*—the tremendous increase in computer users, internet & cyberspace is giving rise to more number to cybercrimes. Technocrats or popularly known as cybercriminals make use of technology, social engineering & other techniques to extract the confidential information. So there is a new need to have a comprehensive understanding of cyber-attacks and its classification & how one can get secured. In this paper, we provided a noble metric concept to test data breaches algorithm. Cybersecurity ensures the protection of information systems including software, hardware and information (data). The purpose of this paper is to give a review on Cybersecurity, its goals, impacts, issues and noble concept. The article also includes a brief description of various types of data breaches that have occurred in the past.*

Keywords: — cybercrime, cyber-attacks, cyber espionage, cyber terrorism.

I. INTRODUCTION

With the wide-spread growth in technology, Cybersecurity has gained implicit importance in recent years due to which several cybersecurity threats or cyberattacks are increasing day by day. The digitalization of the data is giving rise to more number of cybercrimes which involves the use of a computer, internet, World Wide Web, cyberspace. Cybercriminals are becoming more sophisticated & are targeting consumer's as well as public & private organizations. Lack of Cybersecurity is the main reason behind the rapid increase in cybercrimes. Cybersecurity is not just about protecting the information, but it is beyond that [1]. There is now an industrial scale of computer espionage. The only thing that is new about Cybersecurity is that there is more information moving around faster in cyberspace that there ever was when it could only be paper-based, but it is still & always about preventing the people from accessing information they have no right to and using it for malicious purposes. It is more than a further step in a continuum of managing the complexity of data. Cyber attack commonly known [2] as a computer network attack (CNA) is the deliberate exploitation of computer systems, companies and networks dependent on technology. Attackers use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft. Cybercrime can be categorized as-computer used as a target- using a computer to attack other computers. Computer used as a weapon-using a computer to commit real-world crimes. The extraction of sensitive information is done when a cybercriminal Data breaches occur successfully infiltrates a data source. To steal local files, a computer or network can be accessed by the cybercriminal physically or by bypassing prevent network security remotely. There are many steps usually involved in data breach operations:

1. *Research*: The network attackers or cybercriminal looks for the multiple gaps or loopholes in the company's security, including the employee, devices, systems and network.
2. *Attack*: The employee, devices, systems and network is vulnerable by criminal tries to make initial contact by using either a web or social attack.
3. *Network/Social attack*: A system assault happens when a cybercriminal utilizes framework, framework, and application requirements to invade an association's system. Social crimes include deceiving or goading representatives into offering access to the organization's network. A worker can be tricked into giving his/her login accreditations or might be tricked into opening a malignant connection.
4. *Exfiltration*: Once the attacker has access into one computer, then the confidential & sensitive data of the organization can steal. The attack is considered successful when the hacker extracts the data.

II. RELATED WORK

The author proposed a paper in which they discussed the different type of cyber attacks& techniques. Cyber attack techniques have improved drastically in the last few years. Criminals or technocrats have adopted advanced technologies to perform illegal activities to extract confidential information & harm people. Some precautions that must be taken who use the internet daily are also discussed which should be made a part of our lifestyle that will assist us in challenging these major cybersecurity threats. Therefore this paper analyses the different type of cyber-attacks to find the best

approach to protect sensitive and confidential data against these attacks. Cyber Attacks Awareness and Prevention Method for Home Users by HaydarTeymourlouei. The full-fledged purpose of this paper is too aware and informs home users about different types of cyber-attacks and teaches different steps to prevent themselves from such attacks. Importance of identification of cyber-attacks and essential steps to take after that are discussed here. Aspects such as what is a cyber attack effect of a cyber attack on home user, different types of cyber-attacks and methodology to prevent these attacks are discussed here. M. Uma and G. Padmavathi proposed a survey paper on Various Cyber Attacks and Their Classification in which they discussed the rapid growth in cyberspace & how it has led to an increased rate in cyber attacks. They addressed the characterization of attacks, purpose & motivation of various attacks & also classified attacks based on intent, scope, network, the severity of Involvement etc. & their further classification. Survey also included how to get prevented from these attacks as well as how to spread awareness among the masses so that appropriate defences & approaches can be initiated against such attacks. A survey of Cyber Attack Detection Strategies by Jamal Raiyn discussed various strategies that help in the detection of cyberattacks. This paper also included the classification of the attacks & offered solutions that included different approaches like Embedded Programming Approach, Agent-based approach, Software Engineering Approach, Artificial Intelligence Approach, Cyber Attack Detection in Cloud etc. To overcome the lack of traditional cyberattacks detection schemes, they proposed a new system for real-time and short-term response to actual attacks.

Ammar Yassir and Smitha Nayak proposed a paper on Cybercrime**:** A threat to Network Security in which they discussed the issues in details, types & effects of cybercrimes on the network. So this paper focussed on network security threats & how to prevent them.

III. CYBERSECURITY ISSUES

Nowadays, technology executives and business men's' are most concerned about their data security. The different hacking organization has hacked the 80 % United States businesses according to a report by CBS Money Watch. Hackers know about the regular vulnerabilities of any associations; they keep security experts continually considering. Here are some Cyber Security concerns associations may confront:

A. Unprecedented Attacks

The measure of significant data put away in numerous information sources has developed exponentially in ongoing years [4]. The open door for various associations to have their information bargained when the number of gadgets that store private information increments. The Internet of Things (IoT), which began in these gadgets, loaned itself well to making a remarkable assault that surface security experts have never looked previously. Associations must make security arrangements because of this assault, and not merely consider their business frameworks and gadgets

B. Cyber Espionage

Today, both strong and little associations have begun to store probably a portion of their information in the cloud. As of late, Right Scale found that associations have expanded private cloud appropriation to 77%; Hybrid distributed computing has additionally expanded. On the off chance that the cheat is inner or outside, saults on closed, open or crossbreed cloud advances, exchange privileged insights and other profitable licensed innovations are in danger. Here is obviously notwithstanding important client information. Associations must know about prescribed procedures and controls on cloud advances that encompass touchy data [5] Configuring the cloud and observing it is essential. For instance, a similar Right Scale study found that security is never again the primary worry with the cloud; it has been replaced by the absence of experience and assets in the zone.

C. Data Theft

According to the SEC, "small and medium-sized enterprises (" SMEs ")] are not only targets of cybercrime, but are their primary objective especially the targeted cyber-attacks last year were aimed at small and medium-sized enterprises" Many criminals refer to these companies as "gateways" for more substantial companies since small businesses do not have large and robust security protocols to prevent theft. The SEC refers to, for example, the Target violation. Now occurred as a result of a first cyber-attack in a small company that served the organization's heating and air conditioning, customer data was stolen in a breach that affected both a minute and a large organization. The SEC likewise focuses on that information security dangers are comparative for private companies and extensive associations, yet they should address them with fewer assets and less experience. 83% of the time, entrepreneurs handle dangers alone. A review featured by the SEC

demonstrates that just 29% of private ventures and associations realize what they have to do to enhance their safety efforts; another investigation found that organizations that gain not precisely $ 100 million have diminished digital security costs even notwithstanding progressively natural occurrences. Vulnerabilities increase for both large and independent companies in another period of digital security dangers. Understanding a programmer's philosophy can help relieve the unavoidable risk of information burglary. By exploiting digital security, it is conceivable to keep away from the gigantic harm that outcome from substantial-scale information ruptures.

IV. MAJOR SECURITY GOALS

There are five major security goals for network security. They are:

- ❖ Confidentiality
- ❖ Availability
- ❖ Authentication
- ❖ Integrity
- ❖ Non-repudiation

A. Confidentiality

The data or information of any association must be overseen in a way that isn't available to unapproved clients. The mystery memory of the substance of correspondence must be there, which assumes major job insecurity.

B. Availability

The detailed data or information of an association or government workplaces must be put away in a mystery and secure way, however, should be evident to approved clients and must not be available to unapproved clients. Some real clients should, likewise be limited.

C. Authentication

The identity of approved clients must be confirmed when it is essential to get to the data or information before getting to the data. There are three manners by which system can verify the character of the real client. They are passwords, documents and biometric information. Utilizing these techniques it is anything but complicated to isolate approved and unapproved clients.

D. Integrity

The data or information ought not to be adjusted or changed amid transmission. The data needs to achieve the goal definitely as it has been sent from the source.

E. Non-repudiation

The data or information is sent or got; it must be guaranteed that both know about the postponement in sending and accepting information or data. Notwithstanding the principle security goals, other optional targets are essential to look after security. They are access and accessibility.

V. BUILDING METRICS TO TEST ALGORITHM ACCURACY

An identity platform like ForgeRock is the backbone of an enterprise, with a view of all apps, identities, devices, and resources attempting to connect. This position good to gather rich log identity data to use to prevent data breaches. To measure accuracy, we have to build our measuring stick, which comes in the form of a series of metrics against which we can evaluate the algorithms:

1. Core Metrics: We use multi-stage Data and ML pipelines and embed different metrics into each stage to measure the effectiveness of our models and pipelines. We introduce various weighted scores to estimate the model accuracy, computation latency, and efficiency of our pipelines.

2. Business Metrics: We put some context around our metrics because we know we are working with identity use cases. Here our job is to build a real correlation between core metrics and business metrics, without which we will not be able to gauge the success/failure of the models. We track Anomalies Detected, Positive Action Rate, Negative Action Rate and False Anomalies Detection Rate, and many other relevant metrics. These metrics measure the real-world health of our ML models and help in making executive decisions Decoded as the Laptops and other compact gadgets that are decoded are helpless against assault. The presented graph shows the high and medium risk event.

Fig: 1 risk events results analysis compare between HR & MR

VI. CONCLUSIONS

Cyber-attacks are happening at an alarming rate in the world. According to studies, a hacker attack occurs every 39 seconds. & the most surprising thing is the unawareness among the masses. A common man is unaware of the fact that he or his system is at the risk of getting attacked. Keeping this in our minds in this paper, we discussed the number of attacks, their prevention & types. We have also focused on the security issues faced by the organizations & the security goals that should be maintained to prevent the attacks. People need to be known that the more they depend on technology, the more vulnerable they are to an attack. Cybercriminals are using new measures to extract the confidential information & the techniques are advancing day by day. However, 80% of cyber-attacks can be avoided thanks to cyber-based hygiene. There is, therefore, an emerging need to find a better approach to protect sensitive and confidential data and take appropriate measures against the cyber-attack.

REFERENCES

[1]. Atul M. Tonge, Suraj S. Kasture, Surbhi R. Chaudhari, IOSR Journal of Computer Engineering (IOSR-JCE) CSE, Cybersecurity: challenges for society, ISSN: 2278-0661, p- ISSN: 22788727, Volume 12, Issue 2 (May. - Jun. 2013).

[2]. Forensic technology services cybercrime survey report 2014 kpmg.com/in

[3]. Atul Kumar, Sr. Analyst, Chiranshu Ahuja, Sr. Analyst, Cyber Security Research Developments Global and Indian Context, A NASSCOM® Initiative

[4]. Cyber Security: Protecting Our Federal Government from Cyber Attacks, the 2009 data breach investigations report, 2009.

[5]. GFI Software, GFI Targeted Cyber Attacks. http://www.gfi.com

[6]. C. Barry, L. Lee, and M. Rewers, International Cyber Security Conference Final Report, Center for Technology and National Security Policy, National Defense University, June 2009.

[7]. J. Vijayan, Targeted Cyber Attacks Testing IT Managers, April 19, 2010.

[8]. N. Ye, et al., "A system-fault-risk framework for cyber attack classification", Information Knowledge Systems Management, pp. 135-151, 2005

[9]. Pennsylvania State University, (2013, March 14). Types of Attacks. Retrieved from Pennsylvania State University Personal WebServers: http://www.personal.psu.edu/users/j/m/jms6423/Engproj/Types%20of% 20Attacks.xhtml

[10]. Schwarz, C. D. (2014, December 26). Five ways to prevent a personal cyber attack. Retrieved from http://hereandnow.wbur.org/2014/12/26/cyber security-sony.

[11]. Margel, Shiri, Itsik Mantin, and Amichai Shulman. "Unobtrusive protection for large-scale data breaches utilizing user-specific data object access budgets." U.S. Patent 9,674,201, issued June 6, 2017.

[12]. Talesh, Shauhin A. "Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses." *Law & Social Inquiry*, 43, no. 2: 417-440, 2018.

[13]. Adlakha, Richa, Shobhit Sharma, Aman Rawat, and Kamlesh Sharma. "Cyber Security Goal's, Issue's, Categorization & Data Breaches." In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), pp. 397-402. IEEE, 2019.

[14]. Margel, Shiri, Itsik Mantin, and Amichai Shulman. "Techniques for preventing large-scale data breaches utilizing differentiated protection layers." U.S. Patent 10,382,400, issued August 13, 2019.

[15]. Tao, Hai, Md Zakirul Alam Bhuiyan, Md Arafatur Rahman, Guojun Wang, Tian Wang, Md Manjur Ahmed, and Jing Li. "Economic perspective analysis of protecting big data security and privacy." *Future Generation Computer Systems* 98: 660-671, 2019.