Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

STUDY OF CYBERSECURITY IN DATA BREACHING

Dr.Veena.S[1], Divyalakshmi. M[2], Poornima. M[3]

[1]*Professor, Department of Computer Science and Engineering*
[2]*Student, Department of Computer Science and Engineering*
[3]*Student, Department of Computer Science and Engineering*
S. A Engineering College.

Abstract— *The role of Cybersecurity is to provide the necessary protection to the user's data. It prevents the data from theft and corruption. Data breaching is the unauthorised access of sensitive data and disclosing it worldwide. It is one of the most important and serious issue in this decade. We desire to provide a clear understanding of data breaching, security issues and management of Cyber threat.*

Keywords—*data breach, cybersecurity, threat management, vulnerability, tools, frangibility.*

I. INTRODUCTION

Data breaching is an act of disseminating the highly sensitive data which are intended to be kept secret. Disclosing the data to the unsecured domain either with a motive or unintentionally. It occurs when the third-party or an unauthorized individual tries to steal or access the data which may comprises of top secrets, company shares, transaction details or legal information. There are different types of data breaching which includes phishing, denial of service attack, malware and exfiltration. From time to time we hear about several companies and industries announcing that their systems have been breached. This might happen by illegal action of the intruders. Or also by an individual within the organization. They might even belong to an organized group of criminals whose main target is money.

This is known as cyber attack and those who perform such illegitimate practices are known as cyber criminals. Overcoming this situation is not an easy task. But, several steps of prevention towards data security can be followed. Maintenance of data can be improved by adopting to new technologies. There are several threats and consequences in data breaching. Cyber Threat Management can be taken into consideration.

II. THREATS IN DATA BREACHING

Threat is an exposure of vulnerability which remain as a loop hole for the interlopers. The threats of data breaching is increasing day by day.

Though there have been strides of improvement in preventing the data leak that can be undertaken by the concern, still there are many possibilities of theft and consequences to occur.

Threats may rise from different origins such as natural disaster, technical collapse, accidental or intentional. The political activist or the company's opponent can also be the origin for the threat. Some of the threats are misuse, violation of permissions and overloading of the network.

Some of the information which the hackers try to collect include the trade secrets of a corporate, medical information of the patients, confidential statements, access keys, network and firewall information, etc.,. Above this, trust issues are considerably increasing because the violators might not be an external agent, he can even belong to the same concern he's working for.

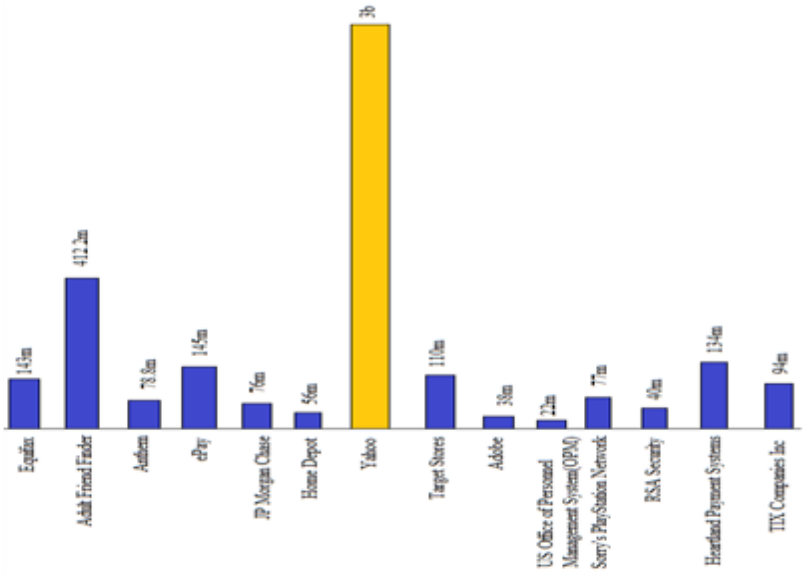

Fig 1: Threats in different countries

III. CONSEQUENCES OF DATA BREACHING

There are many serious consequences of data breaching. Some of the security breaching may result in misuse of highly confidential data. The unauthorised access may lead to denial of service attack. Disruptions in the functioning of system hardware and corrupting the system software is also a significant consequence. Most of the time data breaching leads to loss of revenue for the company or an industry.

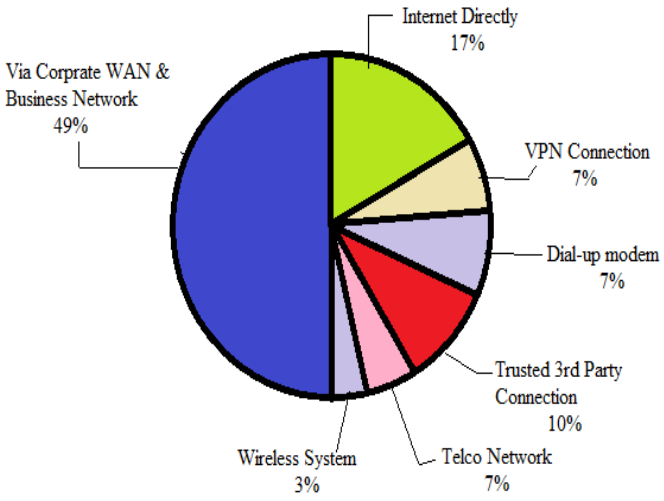

Fig 2: Various cyber attacks.

By the end of 2014, Sony pictures faced an infamous security incident which had expenditure estimation of around $35million as reported by the Senior General Manager. Also by the end of 2016, one of the major internet service company Yahoo announced two serious breach attacks. Even the quality of data decides the consequences of security breaching.

The hackers can corrupt or make use of the original data in different types. The attack may be from different devices or network.

IV. CYBER SECURITY

Cyber security provides prevention of data spill. As we all know, it is always better to prevent than to cure. Since the number of data breach is rapidly increasing as the years pass by, preventing data breaches has become the need of the hour. To eliminate the threats of data breaching, we have many cyber security techniques. These Cyber security techniques play a vital role in the prevention of data breaches.

Some of the most common ways of preventing data breaches are as follows:-

a) Reduce transfer of data:
It would be better to ban the migration of data from one device to another in an organization since loss of removable media will put the data under risk.

b) Shred files:
Shredding files, folders and disks involves deleting the selected data files permanently without leaving a copy of the file. Hence shredding of the confidential data prevents data breaches.

c) Banning of unencrypted devices:
The unencrypted devices are more prone to data leakage. So, it is important to ensure that all the unencrypted portable devices used in an organization are banned.

d) *An erratic password*:
It is vital to set a password that is hard to crack and unpredictable in order to prevent illegal access of data. Also, it is preferable to change the passwords at regular intervals.

e) Automate security:
Automated systems may be employed for checking the password settings, server and firewall configuration which helps in reducing the risk of data breaching.

f) Restrict download:
Imposing restrictions on downloading of the confidential data reduces the chances of transferring data to an external device.

g) *Protect information:*
The sensitive information should be protected wherever it is used. The personal information should not be revealed unwittingly.

h) *Breach response:*
Setting up a breach response plan will help in sending alerts to the management in case of data breaches by notifying them about the attacks and thereby reduce the risk of data breaches.
These are all the common ways of preventing data breaching.

V. CYBER THREAT MANAGEMENT

The cyber threat management (CTM) involves the following:

- Automated intelligence
- Threat analytics
- Cyber threat hunting
- Advanced analytics and security intelligence
- Rapid decisions

These techniques can be implemented to predict the threat before they occur. CTM paves way for preventing the system's software. Situational awareness must be enabled either manual or automated.

CYBER SECURITY TOOLS

a.) Contrast Security:
It provides security for the applications. To prevent false forging, the agents of contrast security are embedded into the application program which becomes a part of the program. It has undergone over 2000 tests without generating any data breaching on OWASP security standards. All the normal apps are converted into an application which are destined on security.

b.) Crossbow:
Crossbow security provides vulnerability testing and platform for assessment. It is the most defensive program against frangibility. Historical attacks can be deployed for any vulnerability by exposing it to a secured network.

c.) Red Seal:
Red seal is used to manage the firewall complications. A firewall is a system which ceases the merge of assured network and unsecured network. All the network elements hand-over their statistics to the Red Seal. Mapping of all the possible incoming and outgoing trackway. It is an extension of normal mapping, made possible by Red Seal.

Table1. COMPARISON OF VARIOUS OPEN SOURCE TOOLS

Sl No	TOOLS	OBJECTIVE	ADVANTAGE
1	Wire Shark	Monitors data traffic over the grid system.	It protects confidentiality of the data
2	OSQuery	Manages the changes in the host by enabling visibility.	More secure in terms of vulnerability.
3	Cryptostopper	Situates trap files.	Traps and responds to cyber threats
4	Metasploitable	Exploits the intended report.	Vulnerability assessment and practice.
5	SQL invader	Combating vulnerabilities for web applications.	Enabled with database visibility.
6	OSSIM	Cost effective solution for host security	Intrusion detection system. Preservation of information.

VI. CONCLUSION

It would be appropriate to say that cyber security is at a medium risk and is predicted to grow along the years. This can be controlled by increasing the number of ethical hackers in future. Additionally, large tech companies like Google, Amazon and Facebook offers bounty programs to users who identify website vulnerabilities and report it to them. To conclude, cyber security environment would become more safer if the concepts of Artificial Intelligence comes into existence in the near future.

VII. REFERENCES

1. , *Forbes, September 7, 2017.*
2. *"5 IT Security Lessons from the Comelec Data Breach". IT Solutions & Services Philippines - Aim.ph. Retrieved 2016-05-06*
3. *Goel, Vindu (December 14, 2016). "Yahoo Says 1 BMathews, Lee, "Equifax Data Breach Impacts 143 Million Americans"illion User Accounts Were Hacked". The New York Times. Retrieved December 14, 2016.*
4. *Daniel, Schatz,;Rabih, Bashroush,; Julie, Wall, (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. **12** (2). ISSN 1558-7215. Archived from the original on 28 December 2017.*
5. *Szoldra, Paul. "A cybersecurity firm is telling two very different stories of the Yahoo hack to news organizations". Retrieved October 15, 2016.*
6. *Daniel, Schatz,;Rabih, Bashroush,; Julie, Wall, (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. **12** (2). ISSN 1558-7215. Archived from the original on 28 December 2017.*

