A CRISP VIEW ON CYBER SECURITY ATTACKS AND ITS PREVENTION

Mr. Rajesh Yadav

Department of Computer Science, Assistant Professor, V.K.Krishna Menon College, Mumbai, Maharashtra

---

Abstract - *Present situation is evidently proving that businesses are in loss due to covid.Every organization small or large have suffered a lot. On a verge , people have lost their jobs and this has force them to do something good or bad for their livelihood. Cyber attack is one of these bad thing that has been part of their earning and businesses are pointed as prime center to attacks. Hence there is a gradual need to protect business from these attacks. Here , I have tried to provide a view on cyber attacks its association with machine learning, examples of cyber attacks and solution that can be utilized to protect these attacks.*

***Key Words*: Business, Attacks, Cyber, Phishing ,Malware**

1.INTRODUCTION

In today's digital era, most people use computer and internet. Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime specially in business or Organization **B**usiness is an activity of making our or someone's living or earning money by production of goods or buy or sell of products i.e goods and services. In simplest words, it is "An activity or organization that is formed for earning and profit. A business can thus be thought with each alphabet having different meanings:

B-**Basic** U-**Usages** S-**Support** I-**Investments** N-**Networking** E-**Earnings** S-**Supply**. S-**Sales**.

Cyber attack is done by cyber-criminals on one or more computers network by use of computers.Cyber-criminals utilizes attack methods to fulfill their devil intentions. Reputed Organization always have the fear of being attack. Thus there is a need to control this attacks.

2. TYPES OF CYBER-ATTACKS

Cyber-criminal can do cyberattacks using any of the following form which occur on a website or web applications.

A)Phishing : An act of sending false interchanges that seem to come from a legitimate source. It is generally done through email. The goal is to head up delicate information , to introduce malware on the intended machine.

B)Man-in-middle attack: A typical kind of network safety attack that permits an attacker to snoop on the correspondence between two targets.

C)SQL infusion threat:A web security weakness that permits an attacker to meddle with the questions that an application makes to its data set.

D) Cross Scripting Site: A kind of safety weakness commonly found in web applications. XSS attacks empower attackers to infuse customer side contents into website pages seen by different clients. A cross-site prearranging weakness might be utilized by aggressors to sidestep access controls like the equivalent beginning strategy.

E) DDOS:The point at which an aggressor, or assailants, endeavor to make it incomprehensible for an information to be conveyed.

F)Password attack: A secret word attack is just when a programmer tries to take your secret key.Since passwords can unfortunately contain a limited number of letters and numbers, passwords are turning out to be less protected. Programmers realize that numerous passwords are inadequately planned, so secret key assaults will stay a technique for assault as long as passwords are being utilized.

G)AI controlled attack: It distinguishes and mimics legitimate client conduct to conceal dangers from traditional security controls.

H)Ransomware: A malware that utilizes encryption to hold a casualty's data at recovery. A client or organization's basic information is scrambled so they can't get to documents, data sets, or applications. A payment is then requested to give access.

3. EXAMPLES OF CYBER ATTACKS

Here are some of the most notable cyber attacks in recent history.

a. Capitol One breach
b. The Weather Channel ransomware
c. U.S. Customs and Border Protection/Perceptics
d. Citrix breach
e. Texas ransomware attacks
f. WannaCry
g. NotPetya
h. Ethereum
i. Equifax
j. Yahoo
k. GitHub

4. SOLUTIONS TO PREVENT CYBER ATTACKS

1.Encrypt the data: An encryption is a way to make an understandable into non understandable form using algorithmic procedure and thus making it non vulnerable to attacks. Since business information may contain private data, secret and confidential points which they cannot afford to loss.At this pace ,encryption will act as "salt to dish". Admin of the company just need to ensure that whenever confidential information is sent it is encrypted to the other party.

2. **Use Strong Passwords**: The weaker a password the more it is vulnerable to attacks.Password is an entry point to get access to various systems.Every system is secured using password with strong options like mixture of capital letter, small letter, number,special character. So users in personal or private are never recommended to keep short passwords or which can be easily identified . Also practicing the habit of keeping strong passwords will provide a user a relief in efforts of living in stress of getting attacks.

3.Use Anti-virus : An effective tool to protect entry of viruses into system. It is strongly recommended that every system must have an anti-virus installation to scan and protect entry of unnecessary worms , virus or any other bugs that is sent to computer through outside source.

4.Use Firewall : Firewall configuration can be included in a computer in the form of hardware or software. It acts as an intermediary of internal network and outside traffic. It monitors trials to acquire access to the operating system and thereby blocks( ) unnecessary and non recognized incoming traffic source.

5.Update Operating systems: An old operating system is vulnerable to more attacks.Hence it is necessary to keep check on updates and thereby use an updated operating system with advanced security features.

6.Intrusion Detection installation : An IDS installation as a software application is necessary to see a network or systems for dangerous activity / policy violations.

7.Backup data: An act of copying important information from their primary location to a secondary , to secure data in a situation of accidental or malicious action.

8.Access Restricted information : It is necessary to restrict information access from unauthorized use. This practice is usually termed as "confidentiality".

9.Appoint Security Expert : Security Experts are generalised as white hackers . Some hackers make users aware of security flaws and patch them by exposing security challenges for the need of helping others. They can help an organization or business by providing extra Security to risk issues which companies are unaware of.

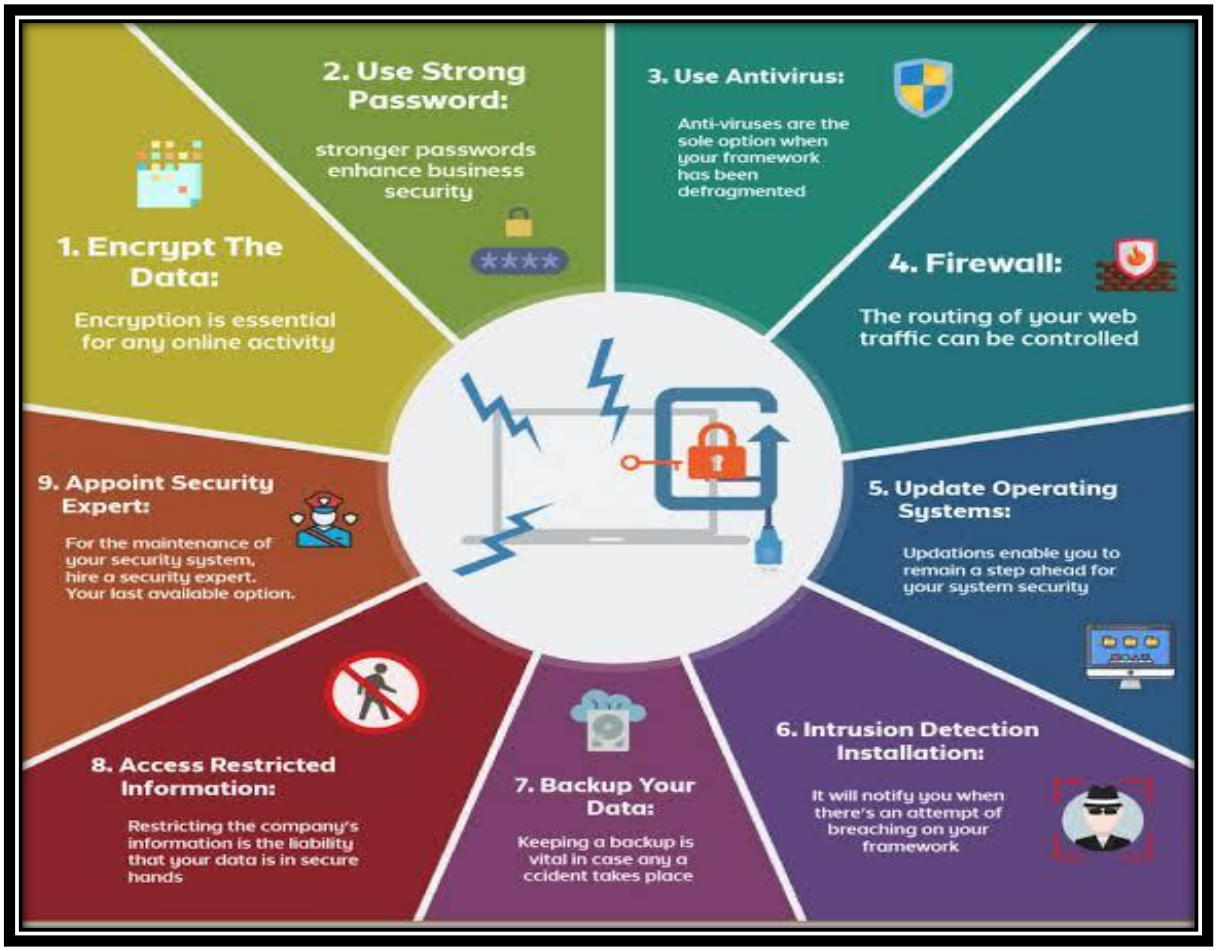

Fig .1. SOLUTIONS TO CYBER ATTACKS

5. CYBER SECURITY ATTACKS AND MACHINE LEARNING

Previously, cyber security systems depends on manual defined rules and human introspection to identify and diversify security incidents. It appeared effective but scope was limited, due to need of high level of expertise for managing security tools, and overloaded security staff.Modern security tools use device techniques automating security decision , without need of rules to be defined in advance. This can save a lot of time for security experts and result in a faster and more accurate response to threats.

A few examples of the use of machine learning in cyber attacks security are:

1.Next-generation antivirus (NGAV) tools utilizes automated malware classification, introspecting malware even if it does not match any known binary pattern.

2.Data loss prevention (DLP) systems use machine learning to read documents or other materials and thus automatically divides by classifying their sensitivity.

3.Email protection systems are designed using a large dataset of phishing vs. legitimate/spam emails, and can identify emails that “look like” they might be phishing attempts.

CONCLUSION

Cyber-Security is the most tensing issue in today's world. From all above points as main discussion it can be concluded that cyberattacks can pose a great threat to business services or data.However utilizing various solutions, this threat can

be reduced to an extent that will help a business to run in a smooth manner and much more efficiently without an pressure on security requirements.

REFERENCES

[1] Jeba Praba. J (2016). Cyber Security and Threats. In proceedings of 9th National Level Science Symposium. February 14, 2016, Rajkot, India. (Vol.3, pp.201-205). ISBN: 9788192952123. Christ Publications

[2] Stallings, William. Network security essentials: applications and standards. Pearson Education India, 2007

[3] Stallings, William, and Lawrie Brown. "Computer security." Principles and Practice (2008). 4]. Landwehr, Carl E. "Computer security." International Journal of Information Security 1.1 (2001): 3-13.

[4] Kahate, Atul. Cryptography and network security. Tata McGraw-Hill Education, 2013

[5] Shiravi, Hadi, Ali Shiravi, and Ali A. Ghorbani. "A survey of visualization systems for network security." Visualization and Computer Graphics, IEEE Transactions on 18.8 (2012): 1313-1329

[6] http://www.solarwinds.com/landingpage/types-of-cyber-attacks.aspx.

[7] https://www.imperva.com/learn/application-security/cyber-security/

[8] https://portswigger.net/web-security/sql-injection.

[9] https://en.m.wikipedia.org/wiki/Intrusion_detection_system

BIOGRAPHY

Mr. Rajesh Yadav is working as Assistant Professor in V.K.Krishna Menon College with an overall teaching experience of 6 + years. He has completed his M.Sc. (Computer Science) along with NET and B.Ed. He has also completed his diploma in machine learning using R Studio. He has participated in more than 250 seminars, webinars , workshop (at national and international level) all inclusive.He has successfully completed more than 60 Faculty development programmes and more than 12 certificate courses in online mode.He has presented 11 research papers in a national and international conferences. He has published 23 research papers in reputed peer reviewed international journal and conference proceedings. His research areas of interest are Machine Learning, Data science, Cloud Computing, Automata, Internet of things.