International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Overview of The Most Recent Cyber Security Attacks and Their Mitigation Strategies

Irfan Bagawan

Bharat Ratna Indira Gandhi College of Engineering, Solapur

ABSTRACT

The emergence of advanced media, the Internet, the web, and online virtual entertainment has brought attention to the relevant investigation local region in particular and created several new exploration issues on network protection. A significant amount of money is being lost by people, organisations, and states all around the world as a result of cyberattacks. As a result, network security is now perhaps one of the biggest and most complicated problems in the world. In the area of Internet security, cyber assault is a delicate topic. Countless resources are being put forth by governments and commercial enterprises worldwide to secure their data. While competitors attempt to penetrate security and deliver malicious software like viruses, Trojans, and botnets, they are utilising a variety of tools and strategies to maintain the business..New forms of malware that target networks are developing daily, making the situation worsening. To better secure our systems, it is crucial to comprehend these attacks both before and after they take place. Understanding attack models gives additional information into how vulnerable a network is, which may be utilized to defend against attacks in the future. Without knowing the network's weakness, it is challenging to anticipate a prospective assault in the field of cyber security. In order to safeguard the network, it is crucial to analyze the network and identify the top potential vulnerabilities.

1. INTRODUCTION

Cyber Security is a process that's designed to protect networks and devices from external threats. It is important because it protects all categories of data from theft and damage. This paper addresses Cyber Security, need of Cyber security and its Measures**.** Security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber attacks. It aims to reduce the risk of cyber attacks and protect against the unauthorized exploitation of systems, networks, and technologies.Cyber security is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems.

1.1. Goals

The definitive objective of cyber security is to defend the data from actuality stolen or co-operated.

To attain this Objective there are three important aspects of cyber security.

1. **Defensive**: The Privacy of Information.
2. **Conserving**: The Integrity of Information.
3. **Controlling** the ability of information only to the approved users .

These objectives practice the confidentiality, integrity, availability **(CIA)** triad, the base of entirely safety agendas.

This CIA triad model is a safety model that is intended to guide strategies for data security inside the places of a society or corporation.CIA model similarly mentioned to in place of the **AIC** (Availability,Integrity and Confidentiality) triad to side-step the mistake with the Central Intelligence Agency.

2. METHOD SELECTION

Simulation and formal theoretical are the two main methodologies used in theoretical cyber security research. Many other research fields have a lot in common with the theoretical components of cyber security research. In addition to cyber security, mathematics, theory of computation, and linguistics are all used in the research domains of cryptography and cryptanalysis, as was previously indicated. The interdisciplinary aspect of the field might occasionally set theoretical cyber security research apart from other areas of study. The fundamental ideas of theoretical research are the definition of

abstract concepts, whether they be mathematical or computational models that describe the cyber realm. Methods may vary depending on the type(s) of attack(s).

Fig. types of cyber attacks.

Depending on the resources available and individual interests, one should determine whether to use a formal theoretical approach or a simulation method for Mitigation approach.

2.1 ASSESSMENT METHODS

When analysing the performance of the enterprise's cyber-security system, there are several other approaches that are employed in addition to vulnerability assessment and are just as significant. Typically, vulnerability assessment is thought of as the only method available.

Nine techniques for evaluating cyber security will be identified in this paper:

1. Vulnerability assessment method.
2. Network assessment method.
3. Virus detection assessment method.
4. Authentication assessment method.
5. Penetration testing assessment method.
6. Human assessment method.
7. Hardware threats assessment method.
8. Policy and countermeasure assessment method.
9. Natural threats assessment method.

3. DISCUSSION

NEED OF CYBER SECURITY EXPERT

U.S. Defense Secretary Robert Gates addresses the audience with Gen. Kevin Chilton, commander, U.S. Strategic Command, during the activation ceremony of the U.S. Cyber Command at Fort Meade, MD, May 21, 2010. **Credit: Cherle Cullen / U.S. Department of Defense**

4. RESULTS

Cyber threats are a big deal. Cyber attacks can cause electrical blackouts, failure of military equipment, and breaches of national security secrets. They can result in the theft of valuable, sensitive data like medical records. They can disrupt phone and computer networks or paralyze systems, making data unavailable. Cyber security and cyber incident recovery isn't an IT problem. Instead, it's a business imperative. Adopting a comprehensive security strategy today can help you avoid having to shut up shop if hackers strike tomorrow.

4.1 The impact of a cyber security breach

Significant revenue loss as a result of a security breach is common. Studies show that 29% of businesses that face a data breach end up losing revenue. Of those that lost revenue, 38% experienced a loss of 20% or more. A non-functional website, for example, may cause potential customers to explore other options.

Fig: Impact of Vulnerable system

5. ADVANTAGES

It consists of numerous plus points. As the

Term itself says, it offers security to the network or system, and we all know that securing anything has a lot of advantages. Several benefits are declared below.

(i). Protecting society - Protecting an organization's network from external threats is the main goal of cyber security.

(ii). Cybersecurity will protect us against serious cyberattacks.

(iii). Cybersecurity will protect us from virus and hacking attacks. Our PC's cyber security application needs to be updated every week.

(iv). On our computer, internet security processes all incoming and exiting data. It lessens crashes and computer chilling, gives us discretion.

6. FINDINGS AND CONCLUSION

Finding 1. Cyber security is a never-ending battle. A permanently decisive solution to the problem will not be found in the foreseeable future.

For the most part, cyber security problems result from the inherent nature of information technology (IT), the complexity of information technology systems, and human fallibility in making judgments about what actions and information are safe or unsafe from a cyber security perspective.

Finding2. Network security improvements for individuals, businesses, governments, and the entire nation are extremely valuable for reducing the harm and loss that may result from breaches in digital protection.

Finding 3. Openly accessible data and strategy activities to date have been deficient to inspire a sufficient need to get going and responsibility for security issues distressing the United States as a country.

CONCLUSION:

Understanding cyber security requires knowledge and expertise from many different fields, including but not limited to computer science and information technology, psychology, economics, organisational behaviour, political science, engineering, sociology, decision sciences, international relations, and law. Cyber security is a complex topic. In reality, despite the fact that technological measures constitute an essential component, cyber security is not primarily a technical issue, despite the fact that it is simple for policy analysts and others to get bogged down in the technical intricacies. In addition to thwarting risks as they materialise, cyber security may also serve to facilitate the advantageous opportunities presented by the information revolution.

References:

1. 1.The 45th President's cybers ecurity agenda. (January 5, 2017). the 45th president's cybersecurity plan was retrieved from https://www.csis.org/news
2. A Job Market Analysis for Cybe rsecurity. (n.d.)from http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf
3. Applications are now open for the new cyber security "Boot Camp" at City Colleges of Chicago. (2017, March 18). Applications are now open for the City Colleges of Chicago's new cyber security boot camp, as retrieved from http://www.ccc.edu/news/Pages/Applications-Now-Available-for-CCC.aspx.
4. Investments by Apprenticeship USA. (2017, June 22). The following was taken from https://www.dol.gov/featured/apprenticeship/grants
5. M. Assante and D. Tobey (2011, February improving the workforce in cybersecurity. The document was retrieved from http://ieeexplore.ieee.org/document/5708280 Assessment Act. Obtainable from https://www.congress.gov/bill/114th-congress/senate-bill/2007/text
6. ATE Facilities (n.d.). obtained from www.atecenters.org
7. National Science Foundation and ATE Centers (n.d.). Impact Report for ATE Centers. retrieved from ATEIMPACT 2016-17.pdf www.atecenters.org/wp-content/uploads
8. 8.THE CYBER SECURITY STRATEGY OF AUSTRALIA fostering prosperity, growth, and innovation [PDF]. (n.d.). Extracted from PMC-Cyber-Strategy.pdf at https://cybersecuritystrategy.pmc.gov.au/assets/img