IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 7, July 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307092|

Research Paper on Cyber Security

Miss. Gayatri Netaji Bhosale

Department of BCA, K.V.R.S.S.S'S Shivraj College of Arts, Commerce & D.S.Kadam Science College, Gadhinglaj, India

ABSTRACT: Cyber Security is working on electronic devices like Mobile, Electronic Systems, Computers, Servers and Networks etc. Security is the protecting shield of malicious attacks which will corrupt or damage of your data. It will protect against unauthorized access or attacker on your system. Cyber Security is related to cybercrimes which occurs when group of activities perform by people by causing network disruption, stealing private and confidential data.

KEYWORDS: Cyber Security, Threats, Risk & Detection, Merging Technologies

I. INTRODUCTION

This article aims to domain of cyber security.exploring,its principles, challenges and innovative of solutions in new daily updated technologies. Cyber-attacks come in various forms, ransomware and phishing attacks. This attacks are not only disrupting critical services and infrastructure but also in digital systems of our interconnected society. Moreover, such technologies are relating like Artificial Intelligence (AI), internet of things (IOT), Block Chain has introduced new dimensions to cyber security.

II. UNDERSTANDING CYBER THREATS

Cyber threats are malicious activities and techniques are exploiting in digital systems and networks. Understanding of various types of cyber threats is developing in cybersecurity strategies. Some of them are as follows:

1. **Malware**: Malicious Software, developed by Cyber Criminals (Hacker's). Stealing information and corrupt or damage confidential data.

2.**Phishing**: It is an technique working on Web site to aquire like Bank accounting releted confidential numbers through website or fraud emails, and messages.

3.**Denial Of Service(DoS) and Distributed Daniel OF Service(DDoS):** DoS and DDoS are working on disrupt functioning of a websites, servers and networks. These attacks are work while load traffic on server inaccessible to users. Cause loss of financial and down the loading time.

4.**Insider Threat's:** its working on involving malicious actions such as used within that organization known person who misuse of their access to their organization network and data.

Fig. Ref image On site - https://www.linkedin.com/pulse/importance-cybersecurity-business-teamleasedigital

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307092|

III. RISK DETECTION AND CHALLENGES

Cyber Security Faces lots of challenges and risks while connecting with Today's digital Network world. To understanding these Cyber Risks and challenges while developing strategies to protect against cyber crime threats.
Some of them:

- **Cyber Threats: -**

cyber threats like malware, ransomware, phishing attacks, and advance persistent Threats (APT's) these threats can target organizations and critical infrastructure.

- **Data Losses: -**

Data losses of sensitive information, such as personal data, financial records to unauthorized access to do it fraud and damage their sensitive data information.

- **Complex It Environments:**

The Increasing IT environments, including hybrid deployments of cloud, Internet Of Things(IOT) devices, and mobile endpoints and complicates cybersecurity efforts.

IV. MERGING TECHNOLOGIES WITH CYBER SECURITY

- **Artificial Intelligence (AI) and Machine Learning (ML)**

AI and ML technologies are revolutionary cybersecurity by enabling threat detection, behavior analysis.
ML algorithm can adopt and real-time cyber threats and response capability.

- **Block chain Technology**

Block chain technology offers and system enhance data and transparency. In cybersecurity block chain can be securely identify management and secure data exchange.

- **Internet Of Things (IoT)**

The **IoT** devices introduce new cyber security challenges due to their interconnected process and limited features of security.
Technologies such as a device authentication, booting systems, encrypt communication protocols are essential for security purpose. IoT Security must use for accessing devices and less risk management processes.

- **Cloud Security**

Cloud computing provides more scalability, flexibility, and cost efficiency. Its introduce uniquely secured challenges like data privacy and sharing responsibility. Cloud native security monitoring to protect cloud-based assets and data. **DevSecOps** practices to integrate security in deployment lifecycle.

- **Biometric Authentication**

Biometric recognition like authentication such as fingerprint recognition, face detection, iris scanning are some of based on it. Its working in **MFA** Multi Factor Authentication combine biometric with authentication factors.

- **Security Automation**

Security automation working on automated create and task performs its schedule wise working of its tasks and threat hunting activities. Automatic threats detects and response automatically handle of that detected threats and reduce its response time to find and resolve that response.

V. CASE STUDIES AND PRACTICAL APPLICATIONS

1. THE WANNA CRY RANSOMWARE ATTACK (2017):

The WannaCry ransomware attack targeted hundreds of thousands of computers worldwide, encrypting data and demanding ransom payments in Bitcoin.
Organizations affected by WannaCry, including healthcare institutions and government agencies, faced significant disruptions and financial losses.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307092|

The attack underscored the importance of patch management, regular software updates, and robust backup and recovery strategies in mitigating the impact of ransomware attacks.

2. Equifax Data Breach (2017):
The Equifax data breach exposed the personal information of over 147 million consumers, including names, Social Security numbers, birth dates, and credit card numbers.
The breach was attributed to a vulnerability in the Apache Struts web application framework, which was exploited by cyber attackers to gain unauthorized access to sensitive data.
The incident highlighted the importance of vulnerability management, intrusion detection, and incident response capabilities in detecting and responding to data breaches.

3. Stuxnet Cyber Weapon (2010):
Stuxnet was a sophisticated cyber weapon designed to target Iran's nuclear program by sabotaging centrifuges used for uranium enrichment.
The Stuxnet malware exploited multiple zero-day vulnerabilities and utilized advanced techniques to evade detection and propagate within targeted systems.
The incident raised concerns about the use of cyber weapons for offensive purposes and highlighted the need for enhanced cybersecurity measures to defend against state-sponsored cyber-attacks.

4. NotPetya Cyber Attack (2017):
The NotPetya cyber-attack targeted organizations globally, encrypting data and disrupting critical infrastructure, including transportation, healthcare, and finance sectors.
The attack exploited a vulnerability in the Windows operating system and spread rapidly through infected networks, causing widespread chaos and financial losses.
The incident emphasized the importance of network segmentation, data backups, and incident response planning in mitigating the impact of large-scale cyber-attacks.

5. Sony Pictures Cyber Attack (2014):
The Sony Pictures cyber-attack involved the theft and release of sensitive corporate data, including internal emails, employee records, and unreleased films.
The attack was attributed to a group of hackers linked to North Korea, who targeted Sony Pictures in retaliation for the production of a controversial film.
The incident highlighted the need for robust perimeter defenses, employee training, and incident response capabilities to defend against targeted cyber-attacks and insider threats.

6. Target Data Breach (2013):
The Target data breach compromised the credit and debit card information of over 40 million customers, resulting in financial fraud and reputational damage to the retail giant.
The breach was facilitated by malware installed on point-of-sale (POS) systems, which allowed cyber criminals to steal payment card data during transactions.
The incident underscored the importance of secure payment processing, network segmentation, and continuous monitoring to detect and respond to cyber threats in real time.

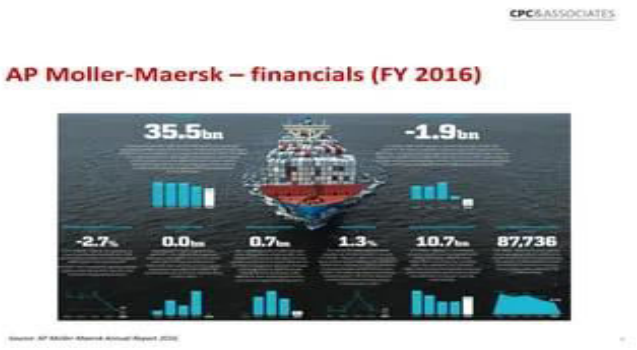
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

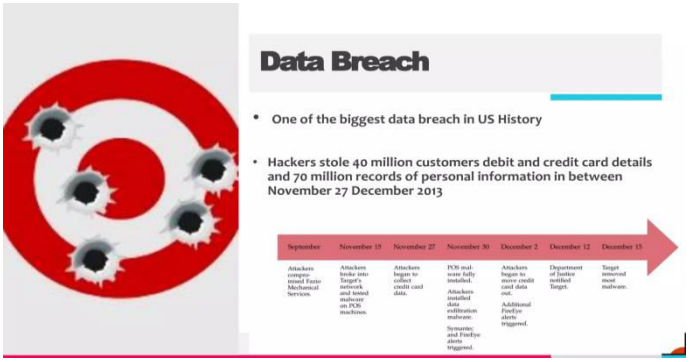
|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

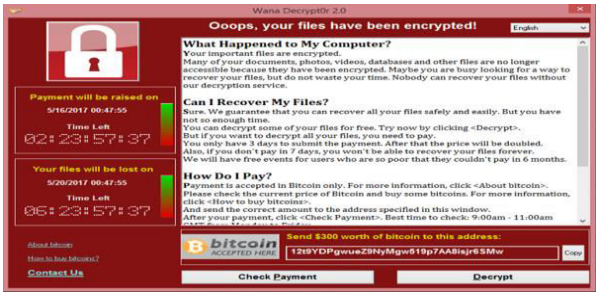
|DOI: 10.15680/IJIRSET.2024.1307092|



Ref Image From :-NotPetya Cyber Attack Ref. Image from google: -
https://en.wikipedia.org/wiki/WannaCry_ransomware_attack



Ref Img From: - Equifax Data Breach Ref.ImageFromGoogle.
https://sevenpillarsinstitute.org/case-study-equifax-data-breach/



Wanna Cry Ransomware Attack Live Image from google
Ref Image from: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

VI. FUTURE DIRECTIONS

1.AI and Machine Learning in Security: AI and machine learning are increasingly being integrated into cybersecurity systems to identify and respond to threats more effectively. These technologies can analyze large volumes of data to detect patterns and anomalies indicative of cyberattacks.

2.Zero Trust Architecture: The Zero Trust model assumes that threats may exist both inside and outside the network. It requires strict identity verification for anyone trying to access resources on the network, regardless of whether they are inside or outside the organization's perimeter.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307092|

3.Cloud Security: As more organizations move their data and services to the cloud, securing cloud environments becomes critical. Cloud security encompasses measures to protect data, applications, and infrastructure hosted in cloud environments from unauthorized access, data breaches, and other threats.

4.IoT Security: With the proliferation of Internet of Things (IoT) devices, securing these connected devices and the data they generate is becoming increasingly important. IoT security involves implementing measures to protect IoT devices, networks, and data from cyber threats.

5.DevSecOps: DevSecOps integrates security practices into the DevOps process, ensuring that security is built into software development and deployment pipelines from the outset. This approach helps identify and mitigate security vulnerabilities early in the development lifecycle.
6.Quantum Cryptography: As quantum computing technologies advance, traditional cryptographic algorithms may become vulnerable to attacks. Quantum cryptography offers a potential solution by leveraging the principles of quantum mechanics to secure communications and data against quantum attacks.

7.Biometric Security: Biometric authentication methods, such as fingerprint scanning, facial recognition, and iris scanning, are increasingly being used to enhance security and improve user authentication processes.

8.Supply Chain Security: With the increasing complexity of supply chains, securing the software and hardware components sourced from third-party vendors is essential to prevent supply chain attacks and ensure the integrity of products and services.

9.Cybersecurity Regulations and Compliance: Governments and regulatory bodies are implementing stricter cybersecurity regulations to protect consumer data and ensure the resilience of critical infrastructure. Compliance with these regulations is becoming a top priority for organizations across various industries.

10.Cybersecurity Awareness and Training: Human error remains one of the leading causes of cybersecurity breaches. Investing in cybersecurity awareness training programs can help educate employees and end-users about cybersecurity best practices and mitigate the risk of social engineering attacks.

VII. CONCLUSION

In conclusion, cybersecurity is an essential component of our digital world, encompassing a wide range of technologies, practices, and strategies aimed at protecting digital assets, data, and privacy from cyber threats. As technology evolves and becomes more intertwined with our daily lives and critical infrastructure, the importance of cybersecurity continues to grow. Effective cybersecurity requires a multi-faceted approach that includes implementing robust technical controls, employing security best practices, fostering a culture of cybersecurity awareness, and complying with relevant regulations and standards.

REFERENCES

1. https://go.crowdstrike.com/2023-global-threat-report.html?utm_campaign=cao&utm_content=crwd-cao-apj-ind-en-psp-x-wht-gtr-tct-x_x_x_x-x&utm_medium=sem&utm_source=goog&utm_term=cyber%20threats&cq_cmp=10902423503&cq_plac=&gad_source=1&gclid=CjwKCAiAq4KuBhA6EiwArMAw1BOfRBGUM_PDevFL0JrCSl_GdXMrEj44vvYunzhWuZZKV7udz2tz-RoC-D8QAvD_BwEW.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, 1993, pp. 123–135.
2. https://www.linkedin.com/pulse/importance-cybersecurity-business-teamleasedigital
3. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
4. https://sevenpillarsinstitute.org/case-study-equifax-data-breach/
5. https://en.wikipedia.org/wiki/Stuxnet
6. https://www.slideshare.net/AbhilashCV3/target-data-breach-case-study

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details