MAAUN INTERNATIONAL MULTIDISCIPLINARY JOURNAL OF RESEARCH AND INNOVATIONS (MIMJRI)
A Publication of the Institute of Africa Higher Education Research and Innovations (IAHERI)
in Collaboration with
Maryam Abacha American University of Niger (MAAUN) Maradi, Niger Republic
Volume 2 Number 1, June, 2024
ISSN: 3027 – 0294 DOI: https://doi.org/10.59479/jiaheri.v2i1.85

Emerging Threats and Fortifying Defenses in Digital Age (A Review of cyber-security threats)

Hassan Jibrin[1]
Email: hassanjibrin97@gmail.com

Aminu Idris[2]
Email: aminuidris@icdfa.org.ng

[1]Maryam Abacha American University of Nigeria

[2]International Cyber Security and Digital Forensic Academy

Abstract
This paper reviews dynamic advantage of staying updated with the current computer related threats and countermeasures by providing overview on the current threats by reviewing the cybersecurity threats, vulnerabilities, countermeasures, and future trends. It begins with an overview of prominent cybersecurity threats, including malware, phishing, and Distributed Denial of Service (DDoS) attacks, highlighting their impact on systems and data. Furthermore, it examines emerging trends in cybersecurity, including new types of cyber-attacks and advancements in cybersecurity technologies, and discusses their potential implications for cybersecurity professionals. By understanding the current cybersecurity landscape and anticipating future trends, organizations and individuals can better prepare for and mitigate the risks posed by cyber threats. It also drafts a clear recommendations base on the findings. The review found that there is a daily attack of cyber-security using different tactics to infiltrate into others privacy.

Keywords: cyber-storm, threat, digital age, cyber-security, cyber-threats, data mining, cybercrime, cyber terrorism

Introduction
A cyber-attack is a conscious attack by a person or organization to obtain the confidential data or information of individuals or organizations. In this process, the attacker (hacker) establishes an attack on the network, disabling applications, malfunctioning systems to alter routine services, and obtaining confidential information. With the everyday evolution of internet of a thing (IoT), cyber security has become a one of the major challenges in day-to-day internet related stuff as it faces a great threat in the form of cyber attacked by hackers in which it is affecting the integrity, confidentiality and the availability of digital related assets. Having a clear view of cyber security threats is of paramount in designing a defense mechanism to safeguard our sensitive information, assets and important infrastructure be it at the financial institution, academic institutions,

MAAUN INTERNATIONAL MULTIDISCIPLINARY JOURNAL OF RESEARCH AND INNOVATIONS (MIMJRI)
A Publication of the Institute of Africa Higher Education Research and Innovations (IAHERI)
in Collaboration with
Maryam Abacha American University of Niger (MAAUN) Maradi, Niger Republic
Volume 2 Number 1, June, 2024
ISSN: 3027 – 0294 DOI: https://doi.org/10.59479/jiaheri.v2i1.85

governmental and non-governmental establishment. Cyber security is a means to safeguard data, information and system from unauthorized access by hackers. This paper provides an overview of paramount threats related to cyber security and an effective approach. Threats has the potential to Cause harm to a system or network that means, that even the existence of an unidentified vulnerability means a threats.

A single security breach might cost an organization hundreds of hours in work (lost) hours busy repairing the damage that occurred, loss of vital data assets, and millions of naira in lost revenue due to theft, ransomware, and fines and penalties caused by the cyber-crime.

Even if new preventative measures are employed, cybercriminals are finding a new way to counter them. These threats are real threats and are not going away.

Rationale

Cyber-security threats encompass a broad range of malicious activities posed by threat actors with numerous motivations and capabilities. Malware, one of the most prevalent threats, includes viruses, worms, Trojans, and ransom-ware, among others (Smith, 2015). Understanding the above statement means that those actors might not have specified reason of attacking a network or system as their motives remains unidentified. These malicious software programs are created to penetrate systems, exfiltrate data, or alter work by disrupt operations, posing significant threats to individuals, organizations, and government.

In addition to malware, phishing attacks pose another big cyber-security threat. Phishing involves the use of deceptive tactics, such as fraudulent emails or websites, to trick individuals into divulging sensitive information, such as login credentials or financial details (Gupta et al., 2018).

Cyber-Security

According to (Starodubtsev et al., 2020) emphasis that Cyberspace is a global domain combining computer communication systems with technology. (Berman et al., 2019) define "*cyber-security"* as the process of protecting hosts in networks, applications, computing devices, and data from adversaries' attacks. This involves the collection of policies, processes, techniques, and technologies to prevent vulnerabilities/attacks.

SECURITY IS A DAILY ISSUE, AND IT'S IMPORTANT TO STAY TUNE WITH THE LATEST SECURITY MEASURES, FOLLOW GENUINE RECOMMENDATIONS, AND MONITOR SECURITY ADVISORIES TO KEEP YOUR DATA, INFORMATION AND SYSTEM SECURE.

YOU CAN EFFECTIVELY SAFEGUARD YOUR DATA, INFORMATION AND SYSTEM FROM POTENTIAL THREATS BY STAYING PROACTIVE AND UPDATED

There is a need for novel and efficient methods in cyber security as there is an emergence of new smart network technologies (Duić et al., 2017). The systems should be safeguarded from any sort of digital attack, damage, or unauthorized access. Efficient Cyber security measures are

MAAUN INTERNATIONAL MULTIDISCIPLINARY JOURNAL OF RESEARCH AND INNOVATIONS (MIMJRI)
A Publication of the Institute of Africa Higher Education Research and Innovations (IAHERI)
in Collaboration with
Maryam Abacha American University of Niger (MAAUN) Maradi, Niger Republic
Volume 2 Number 1, June, 2024
ISSN: 3027 – 0294 DOI: https://doi.org/10.59479/jiaheri.v2i1.85

needed in numerous domains especially business applications, online transactions, cloud computing, mobile computing, software solutions, etc. Cyber Security measures is very much needed as it encloses safeguarding sensitive data from unauthorized access by hackers. There is a need to employ threat intelligence and Machine Learning approaches to identify, analyze and defend against cyber security risks in real time. In recent years, emerging technologies that can be used in the detection of cyber-attacks are Dynamic Networks, Predictive Semantics, Quantum Computing, Behavioral Identity, Cloud Computing, etc., (Geluvaraj et al., 2019).

Research Challenges and Issues in Cyber Security

Cyber threats can be of any form based on the motives of the attacker, such as Cybercrime, Cyberwarfare, Cyberterrorism, and Cyber Espionage (Rohith and Batth, 2019). Cybercrime leads to various criminal activities causing significant financial losses to businesses and individuals. Because of Cyber Espionage, a great amount of data, sensitive information, and intellectual property are stolen from government and private sector websites base on the attacker's motives. Statistics revealed that 11% of cyber-attacks are because of espionage.

Cybersecurity is a dynamic area where challenges will always proliferate and professionals or individuals must be ready to face these challenges the major sectors affected by Cyber-attacks in the year 2021 (Gmcdouga, 2022) are E-business, online transactions are more vulnerable to cyber threats. It results in the loss of confidential information, reputation damage and even being liable for legal issues.

(Duić et al., 2017) stated that the Aerospace and defense sectors face cyber threats with intentions of stealing intellectual property and defense secrets. In Cyber warfare, Cyber attackers monitor, infiltrate and subvert other nations' defense to disrupt their critical infrastructure. Cyberattacks on defense have cascading effects and breach the national security system. Cyber-attacks are launched covertly to weaken or strike at an adversary to achieve political objectives. The enemy is unseen and the victim is unsure how and where to react. The attacker does not leave any proof of their involvement in these attacks. The attackers are called non-state attackers (Goel and Nussbaum, 2021).

Satellite communication systems, navigation systems, and Earth observation systems often pose threats from cyber- attacks (Caprolu et al., 2020). Cyber attackers can use software mechanisms, amplifiers, transmitters, and steerable antennas to interfere with or generate satellite signals. The vulnerabilities in the satellite communication systems are mission-critical as they can disturb launch systems, telemetry, tracking, and command and communications. Continuous monitoring and protection measures have to be taken to protect these space-based systems. Cybersecurity is a dynamic area where challenges will always proliferate and professionals or individuals must be ready to face these challenges. Figure 1 gives the major sectors affected by Cyber-attacks in the year 2021 (Gmcdouga, 2022)

MAAUN INTERNATIONAL MULTIDISCIPLINARY JOURNAL OF RESEARCH AND INNOVATIONS (MIMJRI)
A Publication of the Institute of Africa Higher Education Research and Innovations (IAHERI)
in Collaboration with
Maryam Abacha American University of Niger (MAAUN) Maradi, Niger Republic
Volume 2 Number 1, June, 2024
ISSN: 3027 – 0294 DOI: https://doi.org/10.59479/jiaheri.v2i1.85

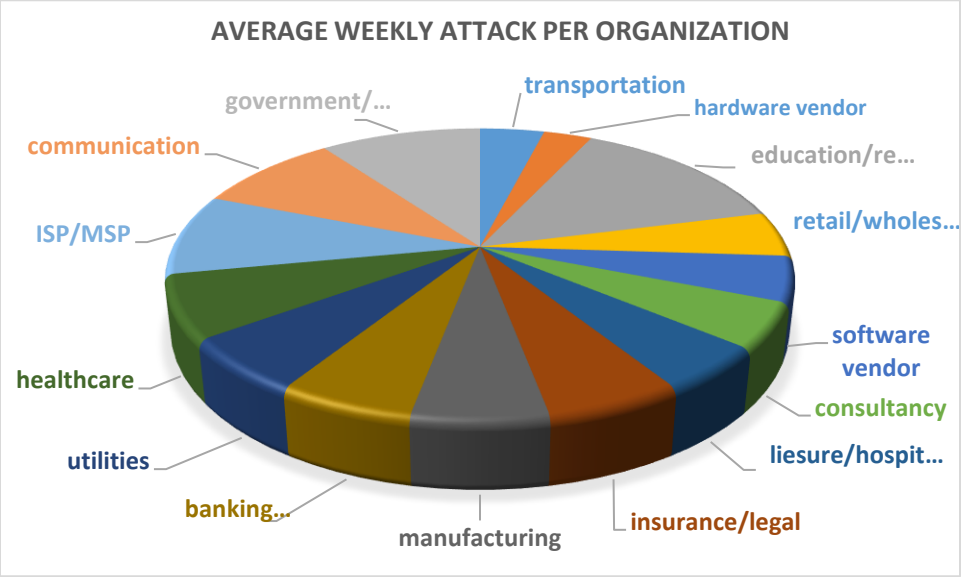
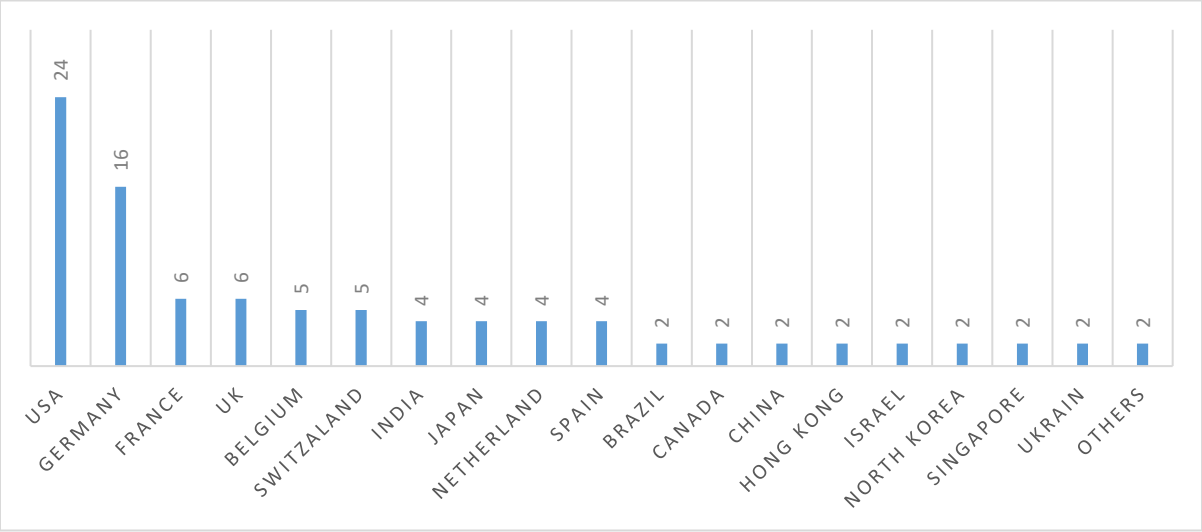


Fig 1. Showing the average weekly attack per organization by industry in 2021

A myriad of cyber threats plays the health sector. Data privacy in healthcare is more concern in many countries. Cyber threats to the health sector may arise from Malware that compromises the virtue of the system or from DDOS attacks by losing patients' privacy or disrupting the facilities available to patients. Cyber threats in the health sector have ramifications beyond financial loss and breach of privacy (Thamer and Alubady, 2021).



MAAUN INTERNATIONAL MULTIDISCIPLINARY JOURNAL OF RESEARCH AND INNOVATIONS (MIMJRI)
A Publication of the Institute of Africa Higher Education Research and Innovations (IAHERI)
in Collaboration with
Maryam Abacha American University of Niger (MAAUN) Maradi, Niger Republic
Volume 2 Number 1, June, 2024
ISSN: 3027 – 0294 DOI: https://doi.org/10.59479/jiaheri.v2i1.85

Fig 2. Countries affected by major cyber-attack in January 2022

Importance of Understanding and Addressing Cybersecurity Threats

In today's complex world, where digital technologies support critical infrastructures and economic and financial activities, the ramifications of cybersecurity breaches are far-reaching and severe. A comprehensive understanding of cybersecurity threats is essential for devising proactive defense strategies and mitigating potential risks (Choo et al., 2012). By staying abreast of emerging threats and evolving attack vectors, organizations can better protect their assets and minimize the impact of cyber incidents on their operations and reputation. Furthermore, addressing cybersecurity threats requires a multifaceted approach that encompasses technological solutions, organizational policies, and user awareness and training (Aljawarneh, 2018).

Types of Cybersecurity Threats

As Cloud Computing relies on the Internet, the usage of the cloud is increasing tremendously and has become a competitive need; securing could architecture is a significant concern (Krishnaveni et al., 2021). Some major threats to the could architecture are DoS Attacks, Insider Risks, Account hijacking, Data breaches, Misconfiguration, and Reduced Infrastructure Visibility

Cybersecurity threats are vast and constantly changing, posing significant threats to individuals, organizations, and governments. This part examines three major types of cybersecurity threats: malware, spoofing, phishing, Botnet Evasion Attacks and Distributed Denial of Service (DDoS) attacks.

DDOS Attacks

Known as Distributed Denial of Service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming it with a flood of internet traffic. DDoS attacks can be launched from multiple sources simultaneously, making them difficult to mitigate (Mirkovic et al., 2004). DDoS attacks can have devastating effects on targeted systems, causing service disruptions, financial losses, and reputational damage. By flooding the target with an excessive amount of traffic, DDoS attacks can render websites and online services inaccessible to legitimate users, highlighting the need for robust DDoS mitigation strategies (Garber et al., 2013).

Phishing

Phishing is a type of cyber-attack that involves tricking individuals into revealing sensitive information, such as usernames, passwords, or financial details, by posing as a trustworthy entity. Phishing attacks typically use email, instant messaging, or fake websites to deceive users (Dhamija et al., 2006). Phishing attacks can have serious consequences, including financial loss, identity theft, and unauthorized access to sensitive information. Cyber criminals often use social engineering techniques to manipulate victims into divulging confidential information, highlighting

MAAUN INTERNATIONAL MULTIDISCIPLINARY JOURNAL OF RESEARCH AND INNOVATIONS (MIMJRI)
A Publication of the Institute of Africa Higher Education Research and Innovations (IAHERI)
in Collaboration with
Maryam Abacha American University of Niger (MAAUN) Maradi, Niger Republic
Volume 2 Number 1, June, 2024
ISSN: 3027 – 0294 DOI: https://doi.org/10.59479/jiaheri.v2i1.85

the importance of user awareness and education in combating phishing attacks (Alsharnouby et al., 2015).

Malware

Malware, short for malicious software, refers to a broad category of software programs designed to infiltrate, damage, or gain unauthorized access to computer systems or networks. Examples of malware include viruses, worms, Trojans, ransomware, and spyware (Kumar et al., 2014). The impact of malware on systems and data can be severe. Malware can disrupt normal operations, steal sensitive information, or render systems unusable. For example, ransomware encrypts files on a victim's computer and demands a ransom for decryption, while spyware silently collects user information without their knowledge (Andronio et al., 2018).

Malware got different names based on its behavior and its purpose. The most common types of malwares include Malvertising, Cryptojacking, Spyware, Adware, Ransomware, Trojan horse, Worms, Rootkits, Man-In- TheMiddle (MitM), Backdoors, Viruses, Bot, Scareware, Man-InThe-Mobile (MitMo), etc., (Al-Janabi and Altamimi, 2020). According to the author (TM, 2020), the recent malware attacks were Shlayer, ZeuS, Agent Tesla, NanoCore, CoinMiner, Delf, Gh0st, Jupyter, Arechclient2, Mirai. Generally, the analysis and detection techniques for malware attacks are classified into (Al-Janabi and Altamimi, 2020; Top 10 Malware, 2020; Albasir et al., 2018; Lin et al., 2020; Baptista et al., 2019):

1) Dynamic 2) Static and 3) Hybrid

Spoofing

In spoofing, the attacker steals the user authentication credentials to gain unauthorized access to the services. The user credential can be obtained by eavesdropping on the network or can be stolen from the device using a phishing attack. The attacker links their MAC address to the IP address of an unprotected network. It becomes easy for the attacker to perform theft or delete the data in this vulnerable network. Spoofing can be commonly categorized into ARP (Address Resolution Protocol) Spoofing, IP Spoofing, and DNS Spoofing (Hamid et al., 2019; Chaabouni et al., 2019).

Botnet Evasion Attacks

The botnet attack is a multi-stage, predominant cyber- attack that begins with scanning network devices. It infects the devices with malicious software, like viruses (Hussain et al., 2021). To increase the magnitude of their attacks, attackers can gain control of a botnet without the device owner's understanding. Further, a botnet overwhelms systems in networks in a DDoS attack. Even though the actual target for botnets is computers, in recent years' adversaries are targeting Internet of Things (IoT) devices more often (Yamaguchi, 2020). In 2016, the Mirai botnet targeted half a million IoT devices with open telnet ports and used default usernames and passwords to log in to those devices and turn them into zombies (Kambourakis et al., 2017). The intention of launching a botnet attack is to initiate malicious activities such as spam generation, key logging, copyright

MAAUN INTERNATIONAL MULTIDISCIPLINARY JOURNAL OF RESEARCH AND INNOVATIONS (MIMJRI)
A Publication of the Institute of Africa Higher Education Research and Innovations (IAHERI)
in Collaboration with
Maryam Abacha American University of Niger (MAAUN) Maradi, Niger Republic
Volume 2 Number 1, June, 2024
ISSN: 3027 – 0294 DOI: https://doi.org/10.59479/jiaheri.v2i1.85

violation, etc. Habitually bots use various invasive approaches to gain the maximum benefit (Karim et al., 2014). The originator of botnets is commonly known as Bot Masters, typically a person or an association of people who have the intention of launching malicious activities. Botnet communications are classified into (Dhayal and Kumar, 2018):

1) Centralized botnet (i.e., the client-server model) 2) Decentralized Botnet (i.e., peer to peer communication model), and 3) Hybrid model

Cybersecurity Countermeasure

Antivirus Software

Antivirus software is designed to detect, prevent, and remove malicious software from computers and networks. It works by scanning files and comparing them against a database of known malware signatures. If a match is found, the antivirus software takes action to quarantine or delete the infected files (Kaur et al., 2017).

Though its effectiveness, but antivirus software has limitations. Its effectiveness relies on regular updates to its signature database to able to detect new threats. To maximize the effectiveness of antivirus software, there should be regular update.

Encryption

Encryption is the process of converting plaintext data into ciphertext, making it unreadable to unauthorized users. It plays a critical role in cybersecurity by ensuring the confidentiality and integrity of sensitive information, such as passwords, financial data, and communications (Stallings, 2017)

Firewalls

Firewalls are network security systems that monitor and control incoming and outgoing network traffic based on predetermined security rules. They act as a barrier between trusted internal networks and untrusted external networks, such as the internet, and can be implemented as hardware, software, or a combination of both (Chowdhury et al., 2017).

Conclusion

Keeping your organization’s data safe from intruder’s eyes is important. You must have a clear understanding of where data is situated, who can access that specific data, the regulations and rules that is applied to the data's security, and how the data can be recovered in the event of an attack.

It is very vital to know that threats are not always external to the organization. Threats can also exist within the organization itself, including employees, vendors, and partners—even high ranked executive management. It's not ok to know who has access to your systems. You also need to know what they are doing with that access.

The reality is that prevention offers a better ROI than reacting to an attack. Moreover, companies should adopt the attitude of what they will do WHEN an attack occurs, not IF.

MAAUN INTERNATIONAL MULTIDISCIPLINARY JOURNAL OF RESEARCH AND INNOVATIONS (MIMJRI)
A Publication of the Institute of Africa Higher Education Research and Innovations (IAHERI)
in Collaboration with
Maryam Abacha American University of Niger (MAAUN) Maradi, Niger Republic
Volume 2 Number 1, June, 2024
ISSN: 3027 – 0294 DOI: https://doi.org/10.59479/jiaheri.v2i1.85

Assuming that an attack is inevitable helps to ensure safeguards are prioritized and implemented quickly.

All companies should have security plans to protect themselves from ransomware attacks. Maintaining security updates to your devices and networks, enforcing cyber-hygiene practices across the organization, and regularly performing and testing backups are actions that can minimize the impact of an attack when it does occur.

Keeping devices up to date is critical to securing you from attacks. For example, the recent Log4j attacks exploited vulnerabilities that had already been identified and fixed, but the fix had not been installed.

Recommendations

Use Strong Authentication

To enhance security and prevent unauthorized access, it is recommended to implement robust authentication mechanisms like multi-factor authentication (MFA). This method adds an extra layer of protection by requiring users to provide additional verification factors, such as a code sent to their mobile device or email address.

Stay Current on Software Updates and Patches

Software updates often include security patches for known vulnerabilities. Make sure that these updates are installed quickly. Also, be sure to maintain other components of your cloud application, including the operating system, web server, and database

Employ Data Encryption

Use secure communication protocols (e.g., SSL/TLS) to protect data transferred between users and the cloud application. In addition, use encryption to safeguard sensitive data stored in databases or file storage systems

Implement Regular Logging and Monitoring

Enable logging mechanisms to record and monitor activities within your cloud application. Set up intrusion detection systems to identify and mitigate potential threats. Regularly review logs to identify any suspicious activities.

Implement Strong Access Controls

Most applications allow administrators to grant or deny read/write access to specific user types or roles. Be sure to limit user permissions and restrict access to sensitive data and functionality. Follow the principle of least privilege, granting users only the privileges necessary for their specific roles.

Maintain Compliance with Industry Regulations

Certain industries and governments have rules and regulations governing the security of cloud-based applications and data. Maintaining compliance with these regulations is essential to avoid significant fines and loss of customer confidence

MAAUN INTERNATIONAL MULTIDISCIPLINARY JOURNAL OF RESEARCH AND INNOVATIONS (MIMJRI)
A Publication of the Institute of Africa Higher Education Research and Innovations (IAHERI)
in Collaboration with
Maryam Abacha American University of Niger (MAAUN) Maradi, Niger Republic
Volume 2 Number 1, June, 2024
ISSN: 3027 – 0294 DOI: https://doi.org/10.59479/jiaheri.v2i1.85

Educate Your Staff

Provide security awareness training to your employees to help them understand common security risks and best practices. Ensure they know how to respond to various attacks and the proper escalation procedure once a security incident has been identified.

Implement Data Backup and Disaster Recovery Plans

Regularly back up your data and develop a comprehensive disaster recovery plan to mitigate the impact of potential data breaches, system failures, ransomware attacks, or other incidents. Test your backup and recovery processes regularly to ensure their effectiveness.

Conduct Regular Security Assessments

Perform periodic security assessments, including penetration testing and vulnerability scanning, to identify and address potential weaknesses in your cloud application to help you stay ahead of new threats and ensure ongoing security.

Regularly Review and Update Security Policies

Maintain up-to-date security policies and procedures that align with industry best practices. Periodically review and update these policies to address evolving security threats and changes in your cloud environment

Below are several recommended practices to help minimize the risk posed by internal threats

Define User Roles

Modern business applications allow administrators to define user roles. These roles assign privileges that identify the software applications a user can access and the actions that user can perform. Giving too much access to sensitive company information can lead to errors, fraud, and intellectual property theft.

Least Privilege Access (LPA)

LPA assigns user roles with the minimum privileges they require to perform their job functions and no more to limit the impact one person can have on a system. LPA applies to everyone, including employees, suppliers, vendors, customers, partners, and even APIs and cloud services.

Zero Trust Model

Zero Trust is a network security model built on the assumption that every attempt to access a network or application represents a potential threat. All access requests are authenticated and continuously validated, whether they originate from inside or outside the organization.

Segregation (or Separation) of Duties (SOD)

Any time a single person can complete both sides of a transaction (for example, the ability to create a vendor and then authorize payments to that vendor), there is a potential for fraud. SoD requires that these types of transactions are divided between two or more people.

Temporary Elevated (Or Emergency) Access Provisioning

There are times that require a person to temporarily upgrade their roles or privileges to a higher level of access than their job would typically need. Temporarily granting elevated privileges to an

MAAUN INTERNATIONAL MULTIDISCIPLINARY JOURNAL OF RESEARCH AND INNOVATIONS (MIMJRI)
A Publication of the Institute of Africa Higher Education Research and Innovations (IAHERI)
in Collaboration with
Maryam Abacha American University of Niger (MAAUN) Maradi, Niger Republic
Volume 2 Number 1, June, 2024
ISSN: 3027 – 0294 DOI: https://doi.org/10.59479/jiaheri.v2i1.85

employee should also have an expiration date to ensure those privileges are automatically removed after a specified period.

Periodic Access Reviews

Management should periodically review the access privileges of users on all company networks and applications to ensure Least Privileged Access is maintained.

Single Sign-On (SSO)

SSO allows users to log into the system once and access multiple sites and applications without having to re-authenticate every time. Users only have to remember one set of credentials and administrators have greater control over user access to company applications. The downside is that setting up SSO can be complex and may pose a security risk if not properly monitored.

Monitor for Unusual Activity

Administrators should monitor for questionable or unusual activity. Conditional access policies can help prevent suspicious or fraudulent activity by imposing restrictions on how users can access the system based on time of day, geographic location, IP address, and more.

Continuous Training on Fraud and Cybersecurity Threats

The best way to keep your company safe is to train your users, including employees, contractors, and vendors, on how to secure company networks, applications, and data. Investing in user education provides the best ROI when it comes to avoiding unnecessary risk.

What to do in the event of a ransomware attack?

1) Isolate and disconnect
2) Assess the impact
3) Report the attack
4) Bring in experts
5) Preserve evidence communicate with stakeholders
6) Restore from backups
7) Consider your options
8) Conduct a review

Ethics

I undersigned that this article has not been published elsewhere. The authors declare no conflict of interest

Reference

Smith, A. (2015). The science of cybersecurity: A review of literature. Information & Computer Security, 23(4), 410–445

Gupta, B., Walia, G. K., & Saxena, K. K. (2018). An extensive survey on phishing attacks and their detection techniques. Computers & Security, 76, 1–25.

Starodubtsev, Y. I., Balenko, E. G., Vershennik, E. V., & Fedorov, V. H. (2020, October). Cyberspace: terminology, properties, problems of operation. In 2020 International Multi-Conference on Industrial

MAAUN INTERNATIONAL MULTIDISCIPLINARY JOURNAL OF RESEARCH AND INNOVATIONS (MIMJRI)
A Publication of the Institute of Africa Higher Education Research and Innovations (IAHERI)
in Collaboration with
Maryam Abacha American University of Niger (MAAUN) Maradi, Niger Republic
Volume 2 Number 1, June, 2024
ISSN: 3027 – 0294 DOI: https://doi.org/10.59479/jiaheri.v2i1.85

Engineering and Modern Technologies (FarEastCon) (pp. 1-3). IEEE. https://doi.org/10.1109/FarEastCon50210.2020.927 1282

Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. Information, 10(4), 122. https://doi.org/10.3390/info10040122

Duić, I., Cvrtila, V., & Ivanjko, T. (2017, May). International cyber security challenges. In 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1309-1313). IEEE. https://doi.org/10.23919/MIPRO.2017.7973625

Geluvaraj, B., Satwik, P. M., & Ashok Kumar, T. A. (2019). The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In International Conference on Computer Networks and Communication Technologies (pp. 739- 747). Springer, Singapore

Rohith, C., & Batth, R. S. (2019, December). Cyber warfare: nations cyber conflicts, cyber cold war between nations and its repercussion. In 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (pp. 640-645). IEEE

Gmcdouga, (2022). "Check Point Research: Cyber Attacks Increased 50Year." https://blog.checkpoint.com/2022/01/10/check- point-research-cyber-attacks-increased-50-year-over-year/

Goel, S., & Nussbaum, B. (2021). Attribution Across Cyber Attack Types: Network Intrusions and Information Operations. IEEE Open Journal of the Communications Society, 2, 1082-1093.

Caprolu, M., Di Pietro, R., Raponi, S., Sciancalepore, S., & Tedeschi, P. (2020). Vessels cybersecurity: Issues, challenges, and the road ahead. IEEE Communications Magazine, 58(6), 90-96. https://doi.org/10.1109/MCOM.001.1900632

Thamer, N., & Alubady, R. (2021, April). A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research. In 2021 1st Babylon International Conference on Information Technology and Science (BICITS) (pp. 210-216). IEEE.

Manjula M, V. a. (2023). Cyber Security Threats and Countermeasures using Machine and Deep Learning Approaches: A Survey . *Journal of Computer Science* , 2023, 19 (1): 20.56.

Choo, K.-K. R., Smith, R. G., & McCusker, R. (2012). An empirical study of the effectiveness of cyber security governance in public sector organisations. In Proceedings of the 2012 45th Hawaii International Conference on System Sciences (pp. 4743–4752). IEEE.

Aljawarneh, S. A. (2018). Cyber security awareness and education for cyber security students: A questionnaire analysis. Journal of King Saud University - Computer and Information Sciences, 30(4), 512– 519.

Mirkovic, J., Prier, G., Reiher, P., & Hussain, A. (2004). Attacking DDoS at the source. IEEE Network, 18(1), 23–29.

Garber, L., Huth, C., & Krawczyk, P. (2013). How to stay alive when the grid dies: Surviving a cyber attack. Communications of the ACM, 56(5), 35–37

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 581–590). ACM

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Designing and evaluating phishing training tools. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (pp. 4039– 4048). ACM.

Kumar, S., Azees, M. A., & Bhaskaran, R. (2014). A survey on malware detection methods. Procedia Technology, 14, 435–442

MAAUN INTERNATIONAL MULTIDISCIPLINARY JOURNAL OF RESEARCH AND INNOVATIONS (MIMJRI)
A Publication of the Institute of Africa Higher Education Research and Innovations (IAHERI)
in Collaboration with
Maryam Abacha American University of Niger (MAAUN) Maradi, Niger Republic
Volume 2 Number 1, June, 2024
ISSN: 3027 – 0294 DOI: https://doi.org/10.59479/jiaheri.v2i1.85

Andronio, N., Migliardi, M., & Daidone, A. (2018). A survey on ransomware: Evolution, prevention, and mitigation. Computers & Security, 78, 131–148

Kaur, R., Kaur, M., & Singh, R. (2017). A survey of antivirus detection techniques. International Journal of Computer Applications, 164(4), 40–44.

Stallings, W. (2017). Cryptography and network security: Principles and practices (7th ed.). Pearson

Chowdhury, M. M. H., Mahmud, M. R., & Islam, S. H. (2017). A survey of network firewalls and their applications. In 2017 5th International Conference on Networking Systems and Security (NSysS) (pp. 1– 6). IEEE

Hamid, B., Jhanjhi, N. Z., Humayun, M., Khan, A., & Alsayat, A. (2019, December). Cyber security issues and challenges for smart cities: A survey. In 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS) (pp. 1-7). IEEE.

Al-Janabi, M., & Altamimi, A. M. (2020, November). A comparative analysis of machine learning techniques for classification and detection of malware. In 2020 21st International Arab Conference on Information Technology (ACIT) (pp. 1-9). IEEE.

Albasir, A., James, R. S. R., Naik, K., & Nayak, A. (2018, April). Using deep learning to classify power consumption signals of wireless devices: An application to cybersecurity. In 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 2032-2036). IEEE. https://doi.org/10.1109/ICASSP.2018.8461304

Baptista, I., Shiaeles, S., & Kolokotronis, N. (2019, May). A novel malware detection system based on machine learning and binary visualization. In 2019 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 1-6). IEEE. https://doi.org/10.1109/ICCW.2019.8757060

Hussain, F., Abbas, S. G., Pires, I. M., Tanveer, S., Fayyaz, U. U., Garcia, N. M., ... & Shahzad, F. (2021). A Two-Fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks. IEEE Access, 9, 163412-163430.

Yamaguchi, S. (2020, January). Botnet Defense System: Concept and Basic Strategy. In 2020 IEEE International Conference on Consumer Electronics (ICCE) (pp. 1-5). IEEE.

Kambourakis, G., Kolias, C., & Stavrou, A. (2017, October). The mirai botnet and the iot zombie armies. In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM) (pp. 267- 272). IEEE.

Karim, A., Salleh, R. B., Shiraz, M., Shah, S. A. A., Awan, I., & Anuar, N. B. (2014). Botnet detection techniques: Review, future trends and issues. Journal of Zhejiang University Science C, 15(11), 943-983. https://doi.org/10.1631/jzus.C1300242

Dhayal, H., & Kumar, J. (2018, April). Botnet and p2p botnet detection strategies: A review. In 2018 International Conference on Communication and Signal Processing (ICCSP) (pp. 1077-1082). IEEE. https://doi.org/10.1109/ICCSP.2018.8524529

Krishnaveni, S., Sivamohan, S., Sridhar, S. S., & Prabakaran, S. (2021). Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing. Cluster Computing, 24(3), 1761-1779.