Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2020, 7(9):94-99

Research Article ISSN: 2394 - 658X

Studying The Effectiveness of Current Cybersecurity Measures

Mohammed Mustafa Khan

ABSTRACT

The defense-in-depth approach is a fundamental approach that organizations have widely adopted due to the nature of sophisticated cyber threats used by cybercriminals to compromise data or damage IT systems. The current cyber threat landscape is an overgrowing field that requires multiple techniques and tactics to counteract them. The rise of cyberattacks has forced organizations to comply with one universal non-negotiable thing, which is cyber security, to ensure confidentiality, integrity, and availability of data and IT systems. Organizations employ various cyber security measures to ensure data and IT systems are protected at all costs and minimize the risks associated with data breach incidents. Despite the huge investments and various steps taken by organizations to implement cyber security measures, they still find themselves being the victims of cyberattacks. To address the issue of being preyed on by cyberattacks, it is crucial to study the effectiveness of current cyber security measures in preventing, detecting, and responding to cyber threats. Investigating the effectiveness of current cyber security measures serves as a validation check to ensure that the implemented cyber security measures operate as intended. To ensure the effectiveness of current cyber security measures, it is a tremendous aspect to constantly scrutinize their effectiveness in protecting the organizational IT infrastructure against cyber threats. This paper aims to study the efficacy of various contemporary cybersecurity measures deployed at various segments of IT infrastructure, including network security, critical infrastructure security, endpoint security, cloud security, mobile security, application security, perimeter security, and data security.

Keywords: Cybersecurity measures, Firewalls, encryption, SIEM, endpoint device, cloud Computing, IoT.

INTRODUCTION

The rapid growth in digital technology and cyber infrastructures has amplified the significance of cybersecurity. Organizations that rely on IT infrastructure to support their business operations have understood the benefits of cybersecurity, and a lot of focus is put on adopting all possible measures to counteract cyber threats. Cyber security refers to the protection of digital information and its associated infrastructure. Cybersecurity focuses on how best organizations can protect, detect, and respond to cyber threats appropriately to eliminate or reduce disruption of business operations due to cyber threats. Buying the latest technology solutions or devices like antivirus and antimalware, firewalls, and others is not enough to guarantee defense against modern threats. The effectiveness of cybersecurity measures can be investigated by ascertaining the economic impact of cyber threats. A study conducted by Herjavec (2019) on the economic impact of cyber threats shows that the cost of cybercrime is estimated to grow exponentially by $3 trillion USD in 2015 to $10.5 trillion USD yearly by 2025 [12].

The importance of cybersecurity measures is growing globally due to the rapid adoption of digital technology. When conducting business nowadays, it is nearly impossible to avoid the internet. The moment the business operations have an online presence, they get exposed to cyber threats. The year 2020, associated with the covid pandemic, forced people to work at home using the internet platform. This era was flooded with cyber threats such as ransomware and phishing that had a devastating impact on organizations. For this reason, it is important to study the effectiveness of cyber security measures in protecting digital infrastructure against cyber threats. This research paper targets to scrutinize the efficacy of current cybersecurity measures by studying the various components of cybersecurity, including network security, critical infrastructure security, data security, endpoint security, application security, cloud security, internet of Things security, mobile security, and perimeter security.

NETWORK SECURITY

Network security refers to the practice of protecting the network infrastructure from unauthorized access or use and related devices. Corporate networks have become the prime target for cybercriminals since they convey sensitive

information. There are various types of network security measures that can be deployed to protect against cyber threats [2].

Firewalls

A firewall is a barrier that separates the corporate network from the internet. It is responsible for filtering the incoming and outgoing network traffic. Firewall rules and policies must be properly configured to ensure they work as expected [2]. The effectiveness of a firewall in blocking or allowing network traffic depends on the configured rules and policies. A network firewall protects the corporate network from unauthorized access, therefore minimizing the risks of cyberattacks. There is escalating demand for the next generation firewalls, which are the modern firewall solutions that provide high capabilities for dealing with advanced cyber threats. Next-generation firewalls provide extra context to security policies and, thus, are effective in dealing with the emerging threat landscape.

Network Segmentation

Network segmentation is the practice of logically dividing networks into separate groups in order to enhance security and simplify management. The primary objective of network segmentation is to boost the security of networks. Once an intruder manages to get unauthorized access to one section of the network, it makes it hard for the intruder to get access to the rest of the company's network [2]. Additionally, network segmentation prevents the lateral spread of malicious traffic to the entire section of the network. Network segmentation is effective in remediating the lateral spread of malware.

Virtual Private Networks

The entire value chain, such as partners, employees, suppliers, and executives, access data using multiple devices from distributed and remote locations. They successfully connect to the company network without worrying about the dangers. Virtual private networks have enabled secure remote access to the company's network and resources [2]. Executives can access the company's sensitive data from remote locations safely as long as they leverage the use of virtual private networks.

ENDPOINT SECURITY

Endpoints refer to devices connected to an organizational network. They include computers, servers, and mobile devices like laptops. Endpoint devices store sensitive data that must be safeguarded from cyber threats. Endpoint devices may act as the gateway for attackers to gain access to the corporate network. Social engineering, like phishing, involves sending malicious email attachments. When downloaded, they execute spontaneously and are related to endpoint devices. The downloaded malware may stay in the basement for a long as they spy on the network events while sending it back to the intruder. Endpoint security is needed to prevent, detect, and disrupt these kinds of cyber threats. The different types of endpoint security measures include:

Antivirus and Antimalware Software

They are software solutions that are designated to scan the device and identify, prevent, and remove viruses and malware like worms, spyware, and trojans. Antivirus/antimalware software is installed in endpoint devices like computers and laptops. They are effective in preventing malware-related incidents, such as malicious email attachments that are downloaded and executed spontaneously to wreak havoc [2]. They engulf the malware and remove/block it from compromising or damaging the data.

Data Loss Prevention and Encryption

Data loss prevention (DLP) is a security solution that detects and prevents sensitive data from loss, misuse, or unauthorized access. Data has become an integral component of an organization [2]. It is a fundamental aspect to protect against any data leakage that can ruin the reputation of an organization and also attract regulatory fines. Organizations must implement DLP solutions on specific endpoint devices like servers and computers to prevent data breach incidents. DLP is effective in ensuring the overall data security of endpoint devices in an organization. Encryption is the practice of scrambling data to an unreadable format for unauthorized access. Encryption helps to prevent data at rest and in transit from being read by cybercriminals in case they get access [2]. They need to have a decryption key to read the encrypted data.

Authentication and Authorization

All endpoint devices must be password-protected to prevent unauthorized access. The password must conform to the password best practices. Any endpoint device that wants to connect to the corporate network must be verified through authentication. After authentication, the resources that the device accesses must be regulated through authorization. Multifactor authentication must be enabled for endpoint devices [2]. Additionally, cryptography enables the creation of digitally assigned certificates for endpoint devices to automatically authenticate to the network [13].

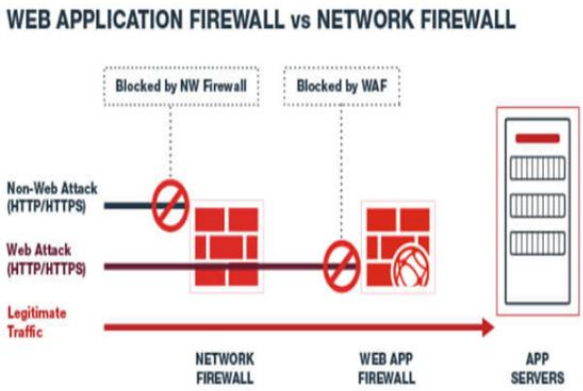
APPLICATION SECURITY

Application security is a conglomeration of best practices, functions, or capabilities added to organizational software to shield and remediate threats from cyber attackers. There are different kinds of application security

solutions and methodologies an organization can use. Securing applications enhances data security for cloud-native applications. Effective cyber security measures for applications can include proper configuration of security settings for individual applications and the deployment of a web application firewall.

Web Application

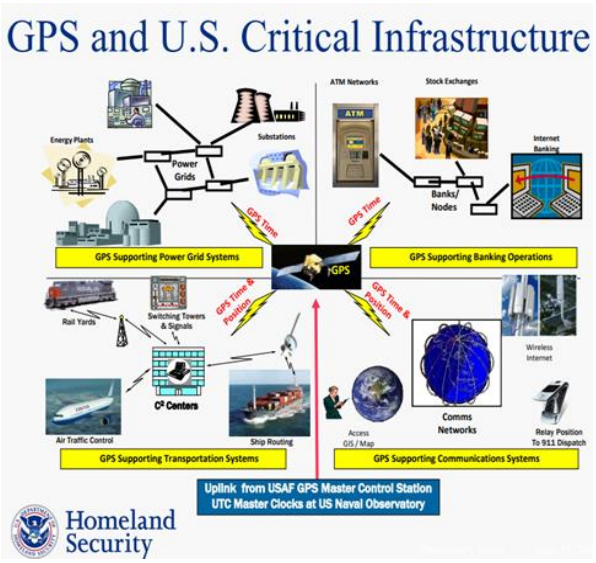
Web application firewalls (WAF) are effective at protecting web applications by screening and monitoring HTTP and HTTPS traffic. WAF resides between the web applications and external users to oversee all the HTTP/HTTPS communication. It ensures there is maximum security at the application layer of the OSI model [3]. It detects and disrupts malicious requests by blocking them before they reach web applications. WAF effectively protects business-critical applications and web servers from cyber threats like SQL injections, Cookie manipulation, and URL attacks. One of the limitations of WAF is that it cannot protect against attacks at the network layer; thus, it is crucial to supplement it with network application firewalls.



***Source**: https://www.fortinet.com/content/dam/fortinet/images/cyberglossary/waf-vs-network-firewall.png*

CRITICAL INFRASTRUCTURE SECURITY

Critical infrastructure are the assets, systems, and facilities that are trivial for the operation of an economy. They are considered vital since their disruption would result in devastating consequences on security, national economies, health, and public safety. Critical infrastructure entails tangible and intangible components that are interconnected, and disruption of one component can cascade to other components. There are almost 16 critical infrastructure sectors, including the energy sector, financial services sector, transportation sector, and healthcare sector, among others. Most countries and governing bodies provide guidance on the management of these critical infrastructures. In the United States, the Department of Homeland Security (DHS) collaborates with the Cybersecurity and Infrastructure Security Agency to define regulations and standards for the safety of critical infrastructure. For instance, the Ukraine power grid attack of 2015 and 2016 resulted in unplanned power outages affecting more than 200,000 consumers [1]. The blackout lasted for several hours, which had detrimental effects on security, business disruptions, and national economies.



***Source:** https://www.gps.gov/multimedia/presentations/2014/11/ICG/dhs.pdf*

Cybersecurity Frameworks

The National Institute of Standards and Technology (NIST) helps organizations in the development and implementation of effective protection of organizational critical infrastructure [10]. The NIST Cybersecurity Framework was initially established to safeguard America's critical infrastructure. Today, NIST CSF has been adopted by various businesses and organizations to protect their critical infrastructure. The framework has become an integral component of cybersecurity risk management. The core components of NIST CSF are the cornerstone in ensuring effective cybersecurity measures have been implemented to secure critical infrastructure. The core elements include identifying, protecting, detecting, responding, and recovering.

CLOUD SECURITY

As the adoption of cloud computing continues to grow, so do cyberattacks. Organizations need cloud security as they shift to their digital transformation environment and employ cloud-based tools. Cloud security refers to the activities of protecting computer networks and workloads like user data in cloud computing platforms. Cloud cybersecurity measures involve policies, procedures, and technologies that protect cloud-based systems, infrastructure, and data from cyberattacks [11]. A business that stores sensitive data in the cloud must implement effective cybersecurity measures that protect against data breach incidents like data loss or leakage. Some of the security measures organizations can implement include identity and access management, cloud-native backup solutions, and Security information and event management.

Identity and Access Management (IAM)

IAM tools and services enable enterprises to provision policy-driven enforcement protocols for all users trying to gain access to services on-prem or cloud-based environments. IAM focuses on the reaction of digital identities for all users to facilitate monitoring and restrictions when interacting with workloads. IAM is an effective cybersecurity measure since it prevents unauthorized access to workloads hosted in the cloud [4].

Security Information and Event Management (SIEM)

SIEM operates by automating threat monitoring, detection, and response in cloud-based platforms. SIEM collects data from heterogeneous sources and stores them in a central log file database that simplifies management [2]. SIEM is infused with artificial intelligence-powered technologies to correlate log data on various platforms. This provides security teams with the capacity to appropriately apply their network security protocols, therefore allowing them to counteract any possible threats. Additionally, SIEM technology enforces regulatory compliance, ensuring the company conforms to underlying regulatory standards like Health Insurance Portability and Accountability Act among others.

Cloud Backup Solutions

Cloud backup solutions provide external backup of files and virtual machines that can be restored in the event of disasters. These solutions provide backup and recovery capabilities designed to protect networks and workloads that are deployed and operate in the cloud environment. Cloud backup solutions expedite the disaster recovery process since files and virtual machines can be recovered and restored to normal operations. This ensures there is business continuity in the event of a digital disaster like ransomware attacks. Additionally, the solutions store data in an immutable format, thus protecting it from ransomware and malicious deletions. Some of the cloud backup solutions include Veeam backup, among others. These solutions can be integrated with cloud services like Amazon Web Serives.

MOBILE DEVICE SECURITY

Organizations are increasingly adopting the use of mobile devices to support business functions. Some of these devices include laptops and tablets. These devices offer the advantages of portability and flexibility, allowing employees to work from a distributed location, which can enhance productivity and operational efficiency. Additionally, some organizations have now comfortably supported employees in utilizing their personal mobile devices to carry out their duties. This practice is referred to as Bring Your Own Device [5]. It enables employees to remotely access organizational resources. However, this increased mobility also brings about security challenges that organizations need to implement effective cybersecurity measures.

Remote Wipe

The portability of mobile devices also raises a security concern. Mobile devices may be stolen or lost, or if you do not want the person having the mobile device to get access to some information, it is important to wipe the data remotely. A remote wipe is a deliberate deletion or destruction of data on a mobile device. Remote wipe enables protection of enterprise data from unauthorized access. Additionally, the employee may quit using the assigned mobile device, and if you do not want him to continue accessing the data, it is crucial to remotely wipe the data. It is crucial to activate remote wipe settings on any device or utilize third-party solutions like Enterprise Mobile Device Management (MDM) Solutions [5]. MDM solutions have a range of capabilities for managing the mobile device. The core functionalities of MDM solutions are deleting or destroying organizational data only, leaving personal data, and wiping all data files in the device and the operating system of the device.

INTERNET OF THINGS (IoT) SECURITY

Smart homes, smart cities, autonomous vehicles, and advanced industrial systems have been made possible by the Internet of Things Technology. The quantity of IoT devices is rapidly increasing to support various industries, including manufacturing, healthcare, and agriculture, among others. However, the security of the IoT ecosystem remains an area of concern [8]. Most of the IoT devices utilize cloud platforms to store, manage, and process data. The interaction of IoT devices with cloud platforms weakens the security of cloud environments since IoT devices are vulnerable to attacks. It is important to manage the IoT ecosystem security. Security measures that can be deployed for effective protection of the IoT ecosystem include intrusion detection systems and patching IoT devices.

Intrusion Detection Systems

Monitoring the IoT ecosystem is a fundamental aspect that is effective in the early discovery of cyber threats before they cause harm. The use of intrusion detection systems can help monitor any suspicious activity in the network [7]. Additionally, SIEM solutions can boost the security of the IoT ecosystem since they correlate data from multiple sources and respond to a cyber threat in real time, or security teams can regularly review the log data to find out any deviation that is likely to compromise the system or data.

Pseudocode Example for Intrusion Detection

```
def detect intrusion(packet):
suspicious patterns = ["maliciousPattern1", "maliciousPattern2"]
for pattern in suspicious patterns:
if pattern in packet:
alertSecurityTeam(packet)
return True
return False
```

Updating and Patching of IoT Devices

The cyber threats associated with IoT devices can be minimized by investigating cybersecurity firmware and software updates. During the acquisition process of IoT devices, it is crucial to procure IoT devices that support software and firmware updates since some IoT devices can not be updated or patched. Choosing IoT devices that can accept updates and patching is one of the prescient approaches to mitigating future risks [6]. Updates can be installed to address the inherent IoT vulnerabilities. Additionally, specific patches can be used to fix any bugs that might be identified in the future.

CONCLUSION

In conclusion, the increasing sophistication of cyber threats demands continuous assessment of cybersecurity measures to ensure their effectiveness in protecting digital infrastructure. Despite significant investments in advanced tools and techniques like firewalls, endpoint security, and cloud protection, organizations remain vulnerable. To mitigate risks, it is crucial to implement a holistic approach encompassing both technological solutions and strategic frameworks, such as NIST, to ensure superb defense mechanisms. As the threat landscape evolves, constant adaptation and vigilant monitoring are essential to maintain the confidentiality, integrity, and availability of data and systems.

REFERENCE

[1]. J. Telo, "A Comparative Analysis of Network Security Technologies for Small and Large Enterprises," International Journal of Business Intelligence and Big Data Analytics, vol. 2, no. 1, pp. 1–10, Jan. 2019, Available: https://research.tensorgate.org/index.php/IJBIBDA/article/view/14

[2]. S. Prandl, M. Lazarescu, and D.-S. Pham, "A Study of Web Application Firewall Solutions," Information Systems Security, pp. 501–510, Dec. 2015, doi: https://doi.org/10.1007/978-3-319-26961-0_29.

[3]. D. H. Sharma, C. A. Dhote, and M. M. Potey, "Identity and Access Management as Security-as-a-Service from Clouds," Procedia Computer Science, vol. 79, no. 1, pp. 170–174, Jan. 2016, doi: https://doi.org/10.1016/j.procs.2016.03.117.

[4]. F. Aguboshim and J. Udobi, "Security Issues with Mobile IT: A Narrative Review of Bring Your Own Device (BYOD)," 2019. Available: https://core.ac.uk/download/pdf/234677445.pdf

[5]. P. Morgner, C. Mai, N. Koschate-Fischer, F. Freiling, and Z. Benenson, "Security Update Labels: Establishing Economic Incentives for Security Patching of IoT Consumer Products," 2020 IEEE Symposium on Security and Privacy (SP), May 2020, doi: https://doi.org/10.1109/sp40000.2020.00021.

[6]. A. Remesh, D. Muralidharan, N. Raj, J. Gopika, and P. K. Binu, "Intrusion Detection System for IoT Devices Publisher: IEEE Cite This PDF," IEEE Xplore, Jun. 2020. https://ieeexplore.ieee.org/abstract/document/9155999

[7]. R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," IEEE Xplore, Dec. 01, 2015. https://ieeexplore.ieee.org/document/7412116

[8]. H. Faria, "A Backup-as-a-Service (BaaS) software solution," Rlbea.unb.br, Jul. 2018, doi: http://repositorio.unb.br/handle/10482/34076.

[9]. NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," Framework for Improving Critical Infrastructure Cybersecurity, Apr. 2018, doi: https://doi.org/10.6028/nist.cswp.04162018.

[10]. A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," Journal of Network and Computer Applications, vol. 79, pp. 88–115, Feb. 2017, doi: https://doi.org/10.1016/j.jnca.2016.11.027.

[11]. Herjavec Group, "2019 Official Annual Cybercrime Report," Cybersecurity Ventures, Feb. 2019. Available: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

[12]. K. Foltz and W. Simpson, "Secure Endpoint Device Agent Architecture," Proceedings of the 21st International Conference on Enterprise Information Systems, pp. 547–554, 2019, doi: https://doi.org/10.5220/0007658705470554.