Endpoint Security Report
BY
Victor Onukwu

Table of Content

Introduction

This report centres on the identification and discussion of effective network endpoint protection strategies that can be used to mitigate against threats faced by corporate networks.

The mitigation strategies discussed in this report are based on the endpoint threats identified in the Endpoint Security Research activity conducted earlier: Malware threats, Phishing threats, DoS attacks, Identity-Based attacks, and Code Injection attacks.

Endpoint Threat Mitigation Strategies

Each of the following strategies plays a crucial role in mitigating threats and protecting the network. However, it's important to note that no single strategy can provide complete protection. A layered approach that combines multiple strategies will provide the most effective defense.

1. Security Policies

   Security policies are a set of rules and procedures that govern how an organization and its employees should handle, protect, and access sensitive information. These policies can help mitigate threats by setting clear guidelines for acceptable behaviour and actions within the network. For example, a security policy might specify that employees should not open email attachments from unknown sources, which can help prevent phishing and malware attacks.

2. Multi-Factor Authentication (MFA)

   MFA is a security measure that requires users to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. This makes it more difficult for attackers to gain access to the network or sensitive information, even if they manage to obtain a user's credentials. MFA can be particularly effective in preventing identity-based attacks.

3. Principle of Least Privilege(PoLP)

   The principle of least privilege involves providing users and systems with the minimum levels of access necessary to perform their functions. This

can help to limit the potential damage caused by an attack. For example, if a user's account is compromised, the attacker will only have access to the information and systems that the user has access to. This principle can be particularly effective in mitigating the risks of code injection attacks and identity-based attacks.

4. Encryption

   Encryption involves converting data into a code to prevent unauthorized access. It can be used to protect data in transit (such as data being transferred over the internet) and data at rest (such as data stored on a hard drive). Encryption can help to prevent a variety of threats, including man-in-the-middle attacks and data breaches.

5. Employee Education

   Educating employees about cybersecurity risks and best practices is a crucial part of any security strategy. Employees need to understand the potential threats they face and how their actions can either prevent or contribute to these threats. Regular training can help employees to recognize and avoid phishing attempts, use strong and unique passwords, and understand the importance of regularly updating and patching software.

Conclusion

The key to effective cybersecurity lies in recognizing that it requires constant vigilance, ongoing commitment, and the ability to adapt to new threats. Hence, the need for continuous vigilance and adaptation in cybersecurity is paramount because cyber threats are constantly evolving. Cybersecurity is not a one-time task but an ongoing commitment. As cybercriminals evolve their tactics, techniques, and methods of exploitation, continuous monitoring and adaptation of cybersecurity measures help organizations mitigate risk and prevent security incidents. This involves regularly updating systems and security protocols, continuously monitoring networks for suspicious activity, and regularly training staff on the latest cybersecurity threats and prevention techniques.

References

MITRE. (n.d.). Endpoint security. MITRE ATT&CK®. Retrieved November 22, 2023, from https://attack.mitre.org/mitigations/M1032/

CrowdStrike. (2023). Most Common Types of Cyber Attacks. Retrieved from https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

Palo Alto Networks. (2020, October 13). 5 Common Cybersecurity Threats. Retrieved November 22, 2023, from https://www.paloaltonetworks.com/blog/network-security/5-common-cybersecurity-threats/

KnowledgeHut. (2020, June 15). Threat analysis: A complete guide. KnowledgeHut Blog. https://www.knowledgehut.com/blog/security/threat-analysis