THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Viswanath Srinivasan Chirravuri
D.Eng. | DC7 | G34657239 | October 5th, 2024

CSCI 6015: Homework-6

Defending Against Cybersecurity Attack Vectors: Malware, Web Security, Supply Chain Security

As the Chief Information Security Officer (CISO) of an organization, protecting the company's data, assets, and reputation from cybersecurity threats is a top priority. In today's digital age, cyber-attacks come in many forms, and three common vectors are malware, web compromise, and software supply chain attacks. Below are simple strategies to defend against these threats.

Defending Against Malware

Understanding the Threat

In its simple definition, malware is a harmful software that can infect computers and networks, causing damage, stealing information, or gaining unauthorized control. Common types of malware include viruses, ransomware, worms, and spyware. Malware can enter through email attachments, infected websites, or USB devices.

Defense Strategy

The best way to protect the organization from malware is to implement EDR (Endpoint Detection and Response) tools. These tools monitor the behavior of devices connected to the network, detect suspicious activity, and stop the malware before it spreads. Regular security updates and patches should be applied to all devices to fix known vulnerabilities.

In addition to that, conducting employee training is crucial. Teach staff not to click on suspicious links or open attachments from unknown senders. This reduces the chance of malware entering through phishing emails. Also, ensure staff understand the risks of using external devices like USB drives without scanning them first. Backup Systems should also be in place so that important data can be restored in case of a ransomware attack.

Defending Against Web Compromise

Understanding the Threat

In its simple definition, web compromise happens when attackers exploit weaknesses (referred to as vulnerabilities) in websites or web applications to steal data, inject malicious code, or gain unauthorized access. Some common methods include SQL injection, Cross-Site Scripting (XSS), and API attacks. Hackers can also target e-commerce platforms to steal sensitive customer data like credit card information.

Defense Strategy

To defend against these types of attacks, organizations should adopt secure coding practices. Software developers must follow DevSecOps methodologies, which integrate security from the beginning of the software development process. By performing code reviews and penetration testing (ethical hacking), vulnerabilities can be identified and fixed before attackers find them.
In addition to that, the organization should install a WAF (Web Application Firewall). A WAF monitors traffic coming to and from the website and blocks malicious attempts to exploit vulnerabilities. Regular patching of all website components, including the operating system and content management systems, ensures known bugs and security flaws are fixed.

To further strengthen the defense against web compromise, organizations can implement RASP (Real-Time Application Self-Protection). RASP is a security technology that runs within the application itself, monitoring and protecting it in real time. It automatically detects and blocks malicious activity such as SQL injections, XSS, and other exploits by analyzing the application's behavior and stopping suspicious actions before they cause harm. Unlike traditional security measures that monitor traffic externally, RASP provides more accurate and immediate protection by being integrated directly into the application's runtime environment. This reduces false positives and enhances the organization's ability to respond quickly to attacks.

And last but not least, setting up MFA (multi-factor authentication) for accessing the website or web applications can add an extra layer of security, reducing the chance of attackers gaining access with stolen credentials.

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Viswanath Srinivasan Chirravuri
D.Eng. | DC7 | G34657239 | October 5th, 2024

Defending Against Software Supply Chain Attacks

Understanding the Threat

In its simple definition, in a software supply chain attack, hackers exploit vulnerabilities in third-party software or services used by an organization. This could happen through compromised software updates or flaws in the systems of suppliers and vendors. Since companies rely on many external tools and services, this attack vector is growing.

Defense Strategy

To protect the organization, a Zero-Trust Architecture should be adopted. This means no system, user, or device is trusted by default, even if they are inside the network. Every connection must be verified before access is granted. The use of strong access controls can limit what a compromised third-party software or system can access within the organization.

In addition to that, vendor management is also essential. Organizations must conduct regular security audits of their vendors and ensure they follow good security practices. Software Bill of Materials (SBOM) can help track all components of third-party software to ensure that they are secure and up-to-date. Finally, employing automated tools that scan and monitor for vulnerabilities in software updates ensures that any malicious code is detected before being installed in the organization's systems.

Conclusion

Cybersecurity threats such as malware, web compromise, and software supply chain attacks can have serious consequences for any organization. However, by using advanced tools like EDR, secure coding, WAFs, RASP, Zero-Trust Architecture, and employee training, organizations can minimize the risks. A strong focus on patch management, vendor audits, and penetration testing will help build a secure environment that can withstand these common attack vectors.

References

ISACA Cybersecurity. (n.d.). 15 common cybersecurity attack vectors and how to defend against them. ISACA Cybersecurity. Retrieved October 5, 2024, from https://isacybersecurity.com/15-common-cybersecurity-attack-vectors-and-how-to-defend-against-them/

Imperva. (n.d.). Web application firewall (WAF) and runtime application self-protection (RASP). Imperva. Retrieved October 5, 2024, from https://www.imperva.com

Forrester Research. (n.d.). Zero trust. Forrester. Retrieved October 5, 2024, from https://www.forrester.com/zero-trust/

Sonatype. (n.d.). State of the software supply chain: Introduction. Sonatype. Retrieved October 5, 2024, from https://www.sonatype.com/state-of-the-software-supply-chain/introduction

Trellix. (n.d.). Helix: Security information and event management (SIEM). Trellix. Retrieved October 5, 2024, from https://www.trellix.com/products/helix/

***** END OF DOCUMENT *****