Southern New Hampshire University

CYB 250 Module Four Stepping Stone Two Template

Complete this template by replacing the bracketed text with the relevant information.

Threat Model

Incident	Bank Attacks	Bluetooth Bug
Attackers	Primarily from Nigeria, Cameroon, and Spain, the group coordinated their efforts across Europe using social engineering to plant malware and perform Man-in-the-Middle attacks.	Any attackers within physical proximity (within 30 meters) who exploit the Bluetooth vulnerability without needing advanced equipment.
Tools	The tools involved were malware, phishing emails, forged websites, and social engineering techniques.	Exploitation of the Bluetooth specification flaw, specifically the lack of mandatory public key validation during pairing.
Vulnerability	The vulnerability exploited was the lack of proper email security measures in companies, which allowed the attackers to intercept and manipulate email communications for fraudulent transactions.	The main vulnerability was in the Bluetooth specification itself, which allowed manufacturers to opt-out of implementing public key authentication for certain Bluetooth features, facilitating man-in-the-middle attacks.
Action	The attackers monitored corporate email accounts, intercepted payment requests, and set up fraudulent transactions by duplicating the payment sites.	Attackers could intercept, forge, and inject Bluetooth pairing messages between devices, intercepting data or causing denial of service.
Target	Medium and large European companies were targeted, specifically those with less stringent email security protocols.	Devices that incorporated Bluetooth connectivity, including phones, laptops, tablets, and more, specifically those from vendors that did not require public key validation in their Bluetooth implementations.
Unauthorized Result	Unauthorized access was gained to corporate email accounts, leading to financial fraud and data breaches.	The unauthorized results included interception of sensitive information, unauthorized access, and potential data manipulation or loss.
Objective	The objective of the attackers was to illegally transfer large sums of money from companies by redirecting payment transactions to bank accounts they controlled.	The objective of exploiting this vulnerability was to gain unauthorized access to devices and data, intercept sensitive information, and possibly disrupt device functionality.

In the European bank attacks, organizations were expected to have implemented standard encryption protocols to protect email communications involving sensitive transactions. Protocols such as Secure/Multipurpose Internet Mail Extensions (S/MIME) or Transport Layer Security (TLS) would have been used to encrypt emails, ensuring that sensitive information like payment requests remained secure during transmission (*49 Busted in Europe for Man-in-the-Middle Bank Attacks*, 2015). These protocols encrypt data to prevent unauthorized access and authenticate the source of the messages to avoid spoofing attempts. This dual function is crucial in maintaining the integrity and confidentiality of communications. However, these measures were compromised, highlighting the need for robust endpoint security measures to complement cryptographic protections, ensuring the data remains secure even after decryption at the endpoint (*49 Busted in Europe for Man-in-the-Middle Bank Attacks*, 2015).

The effectiveness of the man-in-the-middle attack against European banks was primarily due to its ability to exploit endpoint vulnerabilities after the decryption of communications. By installing malware through phishing techniques, attackers could discreetly intercept and manipulate the decrypted communications (*49 Busted in Europe for Man-in-the-Middle Bank Attacks*, 2015). This breach underscores a critical vulnerability: while encryption can safeguard data from sender to recipient, it does not protect data once decrypted on the recipient's device. Therefore, securing endpoints is equally crucial as securing the data in transit, underscoring the need for comprehensive security strategies encompassing encryption and endpoint protection (*49 Busted in Europe for Man-in-the-Middle Bank Attacks*, 2015).

Practical strategies to mitigate such vulnerabilities include implementing multi-factor authentication (MFA), which significantly enhances security by requiring more than one verification method to gain access, making unauthorized access considerably more challenging

even if credentials are compromised (Julia, 2024). Regularly updating software and systems with the latest security patches is critical in protecting against known vulnerabilities and should be a mandatory practice across all devices to prevent exploitation (*Endpoint Security Guide and Best Practices - Red Canary*, 2024). Additionally, deploying endpoint detection and response (EDR) systems can provide continuous monitoring and response to suspicious activities, thus identifying and mitigating threats in real time (Brenduns, 2024). Moreover, educating employees about the dangers of phishing and other social engineering attacks can prevent many breaches at their initial stage. Organizations should also enforce strict access controls and adopt a zero-trust security model, ensuring that all users and devices are authenticated and authorized before granting access to sensitive data and systems (Brenduns, 2024).

Southern New Hampshire University

References

49 busted in Europe for Man-in-the-Middle bank attacks. (2015, June 11). Sophos News. https://news.sophos.com/en-us/2015/06/11/49-busted-in-europe-for-man-in-the-middle-bank-attacks/

Julia. (2024, May 20). *Endpoint Security: Best Practices & 10 Top Solutions for 2024 | V2 Cloud*. V2 Cloud. https://v2cloud.com/blog/endpoint-security-best-practices-and-solutions

Endpoint security guide and best practices - Red Canary. (2024, April 22). Red Canary. https://redcanary.com/cybersecurity-101/endpoint-security/endpoint-security-guide-and-best-practices/

Brenduns. (2024, March 26). *Manage endpoint security in Microsoft Intune*. Microsoft Learn. https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security