7-1 Project Two: Speaker Notes

Joshua Merren

Southern New Hampshire University

CYB-400-13637-M01 Security Assessment & Auditing

Professor Jillian Seabrook

10 December 2024

Slide 1: Title Slide

Speaker Notes:
Good morning, everyone. My name is Josh, and I'm a cybersecurity analyst at Grey Matter LLC. Today, I will present the findings of our recent security assessment conducted on BrainMeld's systems. This presentation highlights critical vulnerabilities we discovered, their potential impacts, and actionable steps to address them. These recommendations aim to protect Grey Matter's operations, finances, and reputation as we integrate BrainMeld into our organization.

Slide 2: Introduction

Speaker Notes:
The acquisition of BrainMeld brings exciting opportunities and introduces new risks. Our cybersecurity team conducted a detailed assessment to ensure we integrate BrainMeld's systems securely. This presentation focuses on the vulnerabilities we identified, the actions needed to mitigate them, and long-term strategies to strengthen our security posture. Addressing these risks is crucial to protecting our business and ensuring a smooth transition during this acquisition.

Slide 3: Key Findings

Speaker Notes:
Our assessment identified three main areas of concern: unpatched systems, weak password practices, and outdated encryption methods. These vulnerabilities create entry points for attackers. For example, hackers can exploit unpatched systems to access sensitive data, while weak passwords make it easier for unauthorized users to break into accounts. Outdated encryption leaves communications and data exposed to interception. Addressing these issues will significantly reduce our exposure to cyber threats.

Slide 4: Unpatched SMB Server Vulnerabilities

Speaker Notes:
One of the critical findings was unpatched SMB server vulnerabilities. These are especially dangerous because attackers can exploit them for unauthorized access to our systems. For instance, the WannaCry ransomware attack 2017 spread rapidly by exploiting unpatched SMB servers, causing millions in damages globally (Morphisec, 2023). By applying the necessary patches and disabling outdated protocols like SMBv1, we can prevent similar attacks and protect our systems from unauthorized access.

Slide 5: Weak Password Practices

Speaker Notes:
Weak passwords are a significant security risk. During our assessment, we found that some systems still use default credentials or passwords that are easy to guess. Hackers often exploit these weaknesses using automated tools to gain access. For example, brute-force attacks are a standard method that uses weak passwords (Business Tech Weekly, 2022). We can drastically reduce this risk by implementing strong password policies, enforcing password complexity, and locking accounts after repeated failed login attempts.

Slide 6: Outdated Encryption Methods

Speaker Notes:
Outdated encryption protocols like HTTP expose sensitive information to interception. For example, HTTP connections do not encrypt data, allowing hackers to see information like login credentials or customer data in transit. Modern encryption protocols like HTTPS and updated SSL/TLS certificates provide robust protection by encrypting all communications (Business Tech Weekly, 2022). Transitioning to HTTPS and replacing outdated certificates will secure our communications and protect sensitive data.

Slide 7: Potential Impacts

Speaker Notes:
If these vulnerabilities are not addressed, the consequences could be severe. A data breach could expose sensitive information, leading to financial losses, legal penalties, and damage to our reputation. Operational disruptions could impact our ability to serve customers, resulting in lost revenue. These risks are preventable, but only if we act now to strengthen our defenses. Addressing these vulnerabilities today will save us from far more significant challenges in the future.

Slide 8: Recommended Immediate Actions

Speaker Notes:
To address the most critical vulnerabilities, we recommend taking immediate actions such as applying software patches to our systems, disabling outdated protocols like SMBv1, and enforcing strong password policies. These actions are straightforward and cost-effective, boosting our security immediately. By prioritizing these steps, we can significantly reduce the likelihood of cyberattacks and protect our systems from the most pressing threats.

Slide 9: Long-Term Strategies

Speaker Notes:
While immediate actions are essential, long-term strategies are equally important to maintain a strong security posture. These include regular system audits to identify and fix new vulnerabilities, continuous employee training to build awareness about cybersecurity, and updating our policies to reflect best practices. For example, companies that invest in ongoing training see fewer phishing incidents and human errors (Business Tech Weekly, 2022). These efforts will ensure we remain resilient against evolving threats.

Slide 10: Visual Aid

Speaker Notes:
This table summarizes the key vulnerabilities identified during the assessment, their potential impacts, and the recommended actions to address them. For example, unpatched SMB servers pose a high risk of unauthorized access, which can be mitigated by applying security patches immediately. Color coding helps prioritize these issues, with red indicating critical areas that require immediate attention. This structured approach ensures we address the most significant risks first.

Slide 11: Benefits of Implementation

Speaker Notes:
By implementing these recommendations, Grey Matter will enhance its security posture, protect customer trust, and avoid costly disruptions and fines. Proactive measures like these safeguard our operations and give us a competitive advantage by demonstrating our commitment to security. Addressing these vulnerabilities is an investment in the future of our company, ensuring that we remain a trusted leader in our industry.

Slide 12: Conclusion

Speaker Notes:
In conclusion, our security assessment revealed critical vulnerabilities that require immediate and long-term attention. The proposed actions will address these risks, protecting Grey Matter's operations, reputation, and future growth. As we progress, ongoing efforts will be essential to adapt to new challenges. Together, we can secure Grey Matter’s success by addressing these risks today. Thank you for your time, and I look forward to your feedback on the recommendations.

References

Antonenko, D., & Antonenko, D. (2023, August 25). *InfOSec Best practices: Implementing Effective password Policies*. Businesstechweekly.com. Retrieved December 10, 2024, from https://www.businesstechweekly.com/cybersecurity/password-security/password-policies/

Gorelik, M. (2024, November 26). NTLM Privilege Escalation: The Unpatched Microsoft Vulnerabilities No One is Talking About. *Morphisec*. Retrieved December 10, 2024, from https://blog.morphisec.com/5-ntlm-vulnerabilities-unpatched-privilege-escalation-threats-in-microsoft