Cybersecurity Software Vulnerability Review & Remediation

Background

This case study outlines a two-week engagement with a client to evaluate their cybersecurity posture, specifically focusing on threat vulnerability, cyber insurance preparedness, and security review. The team analysed over 400 computers across 15 locations, identifying software packages and operating systems that were unsupported, unpatched, and potentially vulnerable to cyberattacks. The review identified 13 core operating system vulnerabilities, 65 productivity applications, and 24 other tools that posed security risks. The final deliverables included a list of vulnerabilities, a remediation proposal, and an action plan for the client.

1. Our client, a leading company in the pharmaceutical industry, sought to strengthen their cybersecurity posture by assessing their current infrastructure and identifying areas of improvement. They engaged our services to conduct a comprehensive review that included a threat vulnerability assessment, cyber insurance preparedness, and a security review.
2. Our team employed a systematic approach to conducting the review:

a. Data Collection: We gathered information on the client's IT infrastructure, including hardware and software inventory, network architecture, and access controls.

b. Vulnerability Assessment: We analysed over 400 computers across 15 locations to identify unsupported, unpatched, and potentially vulnerable software packages and operating systems.

c. Risk Analysis: We evaluated the likelihood and potential impact of identified vulnerabilities, prioritizing them based on risk level.

d. Remediation Proposal: We provided a proposal to address the identified vulnerabilities, considering the client's business requirements, resources, and existing security measures.

e. Action Plan: We developed a detailed action plan for our client outlining the steps necessary to remediate the identified vulnerabilities and improve their cybersecurity posture.

f. Findings: Our review identified a total of 102 vulnerabilities across various systems and applications:

- 13 core operating system vulnerabilities
- 65 productivity applications
- 24 other tools

These vulnerabilities posed a significant risk to our client as they could be exploited by hackers and malware, potentially leading to data breaches, system downtime, or reputational damage.

Remediation Proposal

Our remediation proposal included the following key recommendations:

a. Patch Management: Implement a robust patch management process to ensure that all software and operating systems are up-to-date and secure.

b. Software Support: Replace or upgrade unsupported software packages to versions that receive regular security updates.

c. Network Segmentation: Segregate critical systems and data from the rest of the network to limit the potential impact of a successful cyberattack.

d. Security Awareness Training: Provide regular training to employees on cybersecurity best practices and how to recognize and report potential threats.

e. Incident Response Plan: Develop and maintain a comprehensive incident response plan to effectively manage and recover from security incidents.

f. Action Plan: Our action plan provided our client with a roadmap to improve their cybersecurity posture. The plan included:

- Short-term actions: Immediate steps to address high-risk vulnerabilities, such as applying critical patches and updating unsupported software.
- Medium-term actions: Enhancements to network architecture and access controls to reduce the attack surface.
- Long-term actions: Strategic initiatives, such as implementing continuous monitoring and adopting a risk-based approach to cybersecurity.

Conclusion

The engagement with our client highlighted the importance of a proactive approach to cybersecurity. By identifying and addressing vulnerabilities, our client can better protect their valuable assets and reduce the likelihood of a successful cyberattack. Our comprehensive review, remediation proposal, and action plan provided them with the necessary guidance to strengthen their cybersecurity posture and safeguard their business operations.

NewEdj LLC
Info@NewEdj.com
+1 561-660-1129
+44 7894 738599