Acme Manufacturing Cloud Migration: Security Assessment Report

Document Version: 1.0
Date: December 6, 2024

This report details the security assessments conducted before and after the cloud migration project for Acme Manufacturing. The migration project ran from November 1, 2024 to December 6, 2024. It outlines identified vulnerabilities and the remediation steps taken.

I. Pre-Migration Security Assessment:

A comprehensive security assessment of Acme Manufacturing's on-premises infrastructure was conducted from October 21, 2024, and completed on October 28, 2024. The assessment included:

- **Vulnerability Scanning:** Network and system vulnerability scans were performed using Nessus. This identified 47 vulnerabilities, categorized as follows:
    - **Critical (Immediate Remediation):** 5 vulnerabilities. Examples include: outdated Apache Tomcat (version 8.5.72), unpatched Microsoft Windows Server 2016 instances, and weak default passwords on network devices.
    - **High (Prompt Remediation):** 12 vulnerabilities. Examples include: missing security patches on several servers, outdated OpenSSL libraries, and weak encryption algorithms used for internal data transfer.
    - **Medium (Remediation within 2 weeks):** 20 vulnerabilities. Examples include: insecure configurations on several firewall rules, default credentials on some network devices, and outdated firmware on network switches.
    - **Low (Remediation as resources permit):** 10 vulnerabilities. Examples include: outdated documentation, minor misconfigurations in firewall rules, and lack of proper logging on some systems.
- **Penetration Testing:** Penetration testing, conducted by TBC, identified 3 critical vulnerabilities related to insecure web application configurations and insufficient input validation. Detailed findings are documented in Appendix A.
- **Security Architecture Review:** A review of Acme Manufacturing's existing security architecture identified a lack of comprehensive logging and monitoring capabilities as a major area for improvement. The use of default credentials on several systems was also noted as a significant risk.

II. Remediation of Pre-Migration Vulnerabilities:

Based on the pre-migration assessment, the following remediation steps were taken between October 29, 2024 and November 5, 2024:

- **Critical Vulnerabilities:** Outdated software was updated, default credentials were changed to strong, unique passwords, and impacted systems were rebooted. Verification involved re-running vulnerability scans and confirming that the critical vulnerabilities were resolved.
- **High Vulnerabilities:** Missing security patches were applied, OpenSSL libraries were updated, and stronger encryption algorithms were implemented. Verification involved re-running vulnerability scans and penetration testing.
- **Medium Vulnerabilities:** Insecure configurations were corrected, default credentials were changed, and firmware was updated. Verification involved manual checks and configuration reviews.
- **Low Vulnerabilities:** Documentation was updated, and minor misconfigurations were addressed.

III. Post-Migration Security Assessment:

A post-migration security assessment was conducted from November 25, 2024, and completed on December 2, 2024, to validate the effectiveness of the security measures implemented during the cloud migration. The assessment included:

- **Vulnerability Scanning:** Nessus scans identified only 2 low-severity vulnerabilities related to minor misconfigurations in the AWS security group rules. These were quickly addressed.
- **Configuration Review:** The AWS configurations (security groups, IAM roles, encryption, CloudTrail, GuardDuty) were reviewed and found to be correctly configured and aligned with security best practices.
- **Penetration Testing:** Post-migration penetration testing, conducted by [Penetration Testing Company Name], identified no critical or high-severity vulnerabilities. Detailed findings are documented in Appendix B.

IV. Remediation of Post-Migration Vulnerabilities:

The two low-severity vulnerabilities identified in the post-migration scan were immediately remediated by adjusting the security group rules. Verification involved re-running vulnerability scans.

V. Overall Security Posture:

The cloud migration significantly improved Acme Manufacturing's overall security posture. The implementation of robust security controls in the AWS environment, coupled with the remediation of pre-migration vulnerabilities, resulted in a more secure and resilient infrastructure. Regular security assessments and penetration testing are recommended for continuous improvement.

VI. Appendix:

- Appendix A: Detailed pre-migration penetration testing report.

- Appendix B: Detailed post-migration penetration testing report.
- Appendix C: Detailed vulnerability scan reports (pre- and post-migration).
- Appendix D: Detailed remediation plans and verification results.

This report provides a summary of the security assessments. Detailed findings and remediation activities are available in the appendices. Regular security assessments are recommended for continuous improvement.