Incident Review: Unusual Network Activity at Maven Clinic

Tala Aoun, Cybersecurity Analyst

October 2024

Incident Overview

Key Points:

- **Date of Incident**: *September 20, 2023*
- **Affected Systems**: *DESKTOP-1234567, SERVER-12345, SQLSERVER-12345*
- **Type of Incident**: *Unauthorized remote logins, privilege escalation, lateral movement, potential data exfiltration*
- **Detection Method**: *Security logs and firewall alerts flagged unusual activity*
- **Severity**: *High - Sensitive medical data at risk*

Objective of the Investigation:

- Identify the nature of the unusual activity.
- Assess the impact on systems and data.
- Recommend mitigation and long-term security improvements.

Timeline of Incident

08:10:23 – *Remote login of user JOHNDOE on DESKTOP-1234567 (Source IP: 192.168.1.2)*

09:45:32 – *Policy change on DC-SERVER-01 to Administrator account*

10:33:45 – *SMB traffic from DESKTOP-1234567 to SERVER-12345 flagged by Windows Firewall*

13:23:15 – *SSH traffic from 192.168.1.25 flagged by firewall*

15:23:52 – *SQL Server corruption detected on SQLSERVER-12345*

17:34:56 – *Final containment actions: Blocked IP 117.80.77.27, disconnected compromised systems*

Response Containment & Eradication Plan

Immediate Steps:

- ***Account Security*****:** Implement multi-factor authentication (MFA) for all privileged accounts.
- ***Password Policy Update***: Enforce stronger password policies with complexity requirements and account lockout mechanisms.
- ***SQL Server Monitoring***: Enhance real-time monitoring of critical systems, particularly SQL databases, for faster anomaly detection.
- ***Patch and Update Systems***: Ensure all systems, including the firewall and server software, are patched to mitigate known vulnerabilities.

Long-Term Measures:

- ***Network Segmentation***: Separate critical systems like SQL servers and administrative servers from general network traffic to limit lateral movement.
- ***Regular Security Audits***: Conduct periodic security assessments and penetration tests to identify vulnerabilities before attackers do.
- ***Employee Training***: Provide cybersecurity awareness training, focusing on recognizing phishing attempts, weak credentials, and proper use of privileged accounts.
- ***Incident Response Drills***: Establish a formal incident response plan with regular drills to test the team’s readiness for handling future incidents.

Review of Incident Response

WHAT WENT WELL

Timely Detection: Unusual activity was quickly flagged by the firewall and security logs.

Immediate Containment Actions: Compromised systems were disconnected promptly, and malicious IPs were blocked.

Collaboration with CTO: Close coordination with Gemma Chan (CTO) helped streamline the investigation and decision-making process.

WHAT COULD BE IMPROVED

Better Password Policies: Weak credentials allowed privilege escalation; stronger password policies could have mitigated this risk.

Multi-Factor Authentication (MFA) Missing: Lack of MFA for privileged accounts made it easier for attackers to access administrative privileges.

Delayed Response on SQL Corruption: SQL server corruption detection took longer than expected, suggesting a need for more robust monitoring on critical servers.

Limited Network Segmentation: Lateral movement between systems using SMB and SSH indicates that better network segmentation could have limited the attack's spread.

Stakeholders & Business Impact

Relevant Stakeholders:

- ***CTO (Gemma Chan)***: Led the technical response and decision-making process.
- ***Legal Counsel***: Required to assess any potential legal implications, particularly regarding data breaches and compliance with healthcare regulations.
- ***Public Relations (PR)***: In case of external exposure, the PR team must prepare a communication strategy to handle public concerns.
- ***IT Security Team***: Directly responsible for incident containment and system recovery.
- ***Database Administrators***: Involved in addressing SQL corruption and data integrity issues.

Business Impact:

- ***Data Privacy Risks***: Potential exposure of sensitive medical data, which could lead to legal action and reputational damage.
- ***Operational Downtime***: Systems such as the SQL server may need to be temporarily taken offline for investigation and restoration.
- ***Regulatory Compliance***: Incident may trigger mandatory reporting under healthcare regulations (HIPAA).
- ***Reputation Damage***: Any publicized breach could harm Maven Clinic's trust with patients and clients.

Conclusion & Next Steps

Conclusion:

- The incident at Maven Clinic exposed critical security gaps that need immediate attention.
- The swift identification of malicious activity minimized potential damage.
- Effective collaboration between teams, including the CTO and security staff, was key to handling the incident efficiently.

Next Steps:

1. **Implement Immediate Security Fixes:**
   - Strengthen access control measures (MFA, password policies).
   - Update firewall rules and network segmentation.
   - Secure SQL databases and backup protocols.
2. **Conduct a Full Security Audit:**
   - Review all systems for vulnerabilities.
   - Ensure compliance with security standards and legal regulations.
3. **Improve Incident Response:**
   - Refine communication channels for faster response times.
   - Provide training on security best practices for all employees.
4. **Monitor for Future Threats:**
   - Set up continuous monitoring and alerts for any unusual activity.
   - Conduct periodic penetration testing and vulnerability scans.