Response, Containment, and Eradication Plan

Prepared By: Aishwarya Shankar (Lead Security Analyst)

Short-Term Plan

To respond to the incident and prevent further damage and spread of the malicious activity, we have determined that the following actions should be performed:

1. Isolate the suspected affected systems DESKTOP-1234567 and SERVER-12345 from the company network. Backup the systems to retain a snapshot of the environments.
2. Lock out user JohnDoe on DESKTOP-1234567.
3. Change admin credentials on DESKTOP-1234567.
4. Perform malware analysis on the suspicious unknown program, unknown.exe, running on SERVER-12345.
5. Examine the SQL database on SQLSERVER-12345 to return it to operational state.
6. Examine systems to determine the extent of the potential data exposure and what data (particularly PHI and other PII) had been exposed on DESKTOP-1234567, SERVER-12345, and SQLSERVER-12345.
7. Restore the affected systems using uncorrupted backups.

Long-Term Plan

To improve the company's security posture in the long-term, we propose the following actions:

1. Implement a strong password policy and MFA on company systems.
2. Update antivirus software on systems.
3. Close unused ports in order to minimize the company network's attack surface.
4. Enhance security monitoring. Implement an NIDS solution to enable continuous monitoring of network traffic, in addition to the existing host-based monitoring and logging.
5. Implement DLP software to prevent data exfiltration from the company network.
6. Ensure that systems are regularly backed up.
7. Invest in comprehensive, thorough security awareness training for employees.