INCIDENT ANALYSIS / RESPONSE

A. Vulnerabilities

Attack Success 1: A successful phishing attack took place. John was convinced to click on the malicious link in the email sent to him Friday afternoon and a payload was presumably delivered to John's machine.

Attack Vulnerability 1: Employees do not have sufficient training to be able to distinguish between a real email and a targeted phishing campaign or at least the training to not click through suspicious links. This allowed the attackers to successfully phish an employee.

Attack Success 2: Attackers successfully deleted and downloaded the volunteer database enabling them to attempt an escalated phishing campaign asking for funds using information obtained in the database.

Attack Vulnerability 2: Database was not backed up and encrypted to allow for confidentiality and integrity of the data. This allowed the attackers to use the information in the database for further attacks.

B. CIA Compromises

Confidentiality Compromise: A proper password policy was not put in place. This allows for the potential abuse, compromise, unauthorized sharing, and access to data that needs to remain confidential.

Integrity Compromise: Database not properly backed up compromised Azumer Waters ability to maintain the integrity of the data.

Availability Compromise: Database was deleted. This completely removes availability of the data to Azumer Water.

PII Compromise: Personal information was leaked from the stolen database.

Industry Standard 1: ISO IEC 27002 Section 10.5.1 Information Back-up

Application 1: Ensures availability of systems by requiring proper backup documentation to be in place. This prevents the database from being deleted entirely.

Application 2: Suggests encryption as a means of increased confidentiality of data. This allows the database to be stored without fear of unauthorized access.

Industry Standard 2: ISO IEC 27002 Section 14.1.3 Developing and implementing continuity plans including information security

Application 1: Ensures plans are in place to restore operations and ensure the availability of information for critical business operations. Having these policies in place increase the likelihood that proper responses are taken during an emergency and ensures that information going forward cannot be deleted in entirety. Furthermore, this will benefit Azumer Water by providing a framework for employees to refer to when emergencies like the loss of the database occur

Application 2: Developing a business continuity plan increases data integrity by identifying information that needs to be more protected in this instance the database was not properly protected to deletion or modification.

C. Federal Regulation Violations

Regulation: Federal Privacy Act 1974

Instance of violation: Public notice of the system of records (Azumer water's database) was not given in accordance with the federal regulation. Federal regulation requires that an agency publicizes the system in the federal register. Furthermore, this act requires that the information be accessible to the owner and a process to verify and change information needs to be in place.

D. Recommended Mitigations

Step 1: Communication with everyone affected by the data breach needs to be sent out immediately along with a screenshot or description of the emails in question warning of a phishing attempt and to not click on any suspicious links or donate any money.

Mitigations: Mitigates the impact by increasing awareness of attack to hopefully prevent any more employees or volunteers from clicking any more malicious links.

Step 2: Require a companywide password reset.

Mitigations: This will ensure that everyone has updated strong passwords that have not been shared or compromised. Ensures that further access to Azumer Water's systems is enabled only to authorized personnel.

E. Incident Response Plan

Benefit 1: Implementing a response plan helps employees identify when an incident has occurred.

Example: John Smith was not aware of a successful phishing attack therefore was unable to enact a response to the attack. Had he been aware of the incident IT staff could have been notified of the phishing attack and steps taken to mitigate the damage as soon as the incident occurred.

Benefit 2: Implementing an incident response plan increases the likelihood that the company recovers from an incident.

Example: The database at Azumer Water was gone had an incident response plan been in place a responder could have used a backup to restore the deleted database immediately.

RISK ASSESSMENT / MANAGEMENT

F. Processes

Process 1: Azumer water must notify the federal register of the database to remain in accordance with the federal privacy act.

Process 2: A system to enable the change of personal information within the database needs to be formally implemented and documented to allow for personal information stored in the update to be verified as correct by the owner of the information.

G. Technical Solutions

Solution 1: Implement WPA2-Enterprise.

Prevents: Network breach due to outdated implementation of wireless security. WEP is an outdated technology and should be replaced with a modern solution. WPA2-Enterprise requires using a RADIUS server to authenticate users adding a layer of access protection to the wireless network. This prevents unwanted network access and snooping.

Solution 2: Implement Mobile Device Management

Prevents: Unauthorized use of company resources and networks and lost or stolen data due to loss of device. Employees can use their own devices on the networks which is dangerous from a network security standpoint due to the risk of unauthorized activity, software, websites, etc. Implementing management software allows a company to keep tabs on the devices using their systems, the software also allows for remote wipe technology in case of lost or stolen devices with restricted information on them.

H. Organizational Structures

1. IT management will be performed by a System Administrator. They will be responsible for maintaining IT systems, configuring and updating hardware and software, provisioning user accounts, and backup and recovery processes. They will report to the Chief information Officer for security training, and guidance on how to properly implement security controls.

2. Security Management will be performed by the Chief Information Officer. They will be responsible for developing and maintaining security procedures and policies. They will also be heavily responsible for security training of individuals within the organization.

3. Mitigation and discovery of incidents will be performed by a security architect. They will be responsible for developing plans of action in case of incidents, assessing the controls and deficiencies in those controls.

4.Both the System administration and security architect will report to the chief information officer. The chief information officer will have the final say in what security policies will be implemented by the security architect. Any major changes to network and IT functions will be determined by the CIO as well.

I. Risk Management Approach

Risk 1: Cell towers and SMS coverage may not be functional during an emergency relief effort disallowing communications company wide due to reliance on the technology.

Likelihood: Moderate due to the chances of a natural disaster on that scale is rare

Severity: 2 because this is a major incident with a very significant impact on the business.

Impact: Leaves the company without communication in a situation where communication is critical. The company delivers water to affected disaster areas and if communication is out logistics will suffer.

Risk 2: Canceled deliveries of water due to Elecktores Malicious activities

Likelihood: High due to the ongoing cyber campaign from Elecktores

Severity: 2 this is a major incident with significant impact on the organization.

Impact: Interruption of daily operations and deliveries, inaccurate or missing deliveries, loss of reputation, unable to provide services

I recommend using the approach outlined in NIST SP 800-37.

Prepare: Establish the context and priorities for managing risk at Azumer Water.

Azumer water needs another emergency communication technology in case the areas they are serving do not have cell phone coverage.

Categorize: Systems, information processed, stored, or transmitted based on the impact of a loss.

Transmitted information: Communication between employees and volunteers regarding area of disaster, relief operations, and evacuation orders.

Select: Determine the initial set of controls for the system and form the controls to reduce risk to an acceptable level.

Develop a radio operations program / system.

Implement: Enact the controls and document how the controls are applied to the system and operation environment.

Implement radio communications and training.

Assess: Determine if controls are implemented correctly or producing the desired outcomes.

We can communicate with volunteers if cell towers and coverage are down.

Authorize: Enable common controls to be put in place once the risk to organizational operations has been reduced to an acceptable level.

Add radio communications as an official documented control in case of emergencies.

Monitor: Continue to monitor controls, document changes, and effectiveness of controls.

Evaluate if radio communications are effective during emergency operations.

REFERENCES

NIST SP 800-37

Federal Privacy Act 1974

ISO IEC 27002