By: Mahdi Ghaznawy

KOP1

First Part: Understanding the Incident and crafting a response

A. Reasons why the Attack that occurred was Successful

The attack on Azumer Water succeeded because, after reading the case study, I found out that its infrastructure and security practices had several significant vulnerabilities:

1. **Phishing Attack:** John Smith clicked on a link in an email that appeared to be a legitimate offer, but it was a link crafted by malicious attackers. This mistake was due to a lack of employee security awareness training, which could have prevented it with proper training on phishing identification. Employees were vulnerable to social engineering tactics because of their avoidance of simulated phishing exercises and frequent cybersecurity awareness sessions. The attack exploited human error, one of the most common and effective attack vectors.
2. **Weak Authentication and Password Policies:** At Azumer Water, employees could keep the same passwords indefinitely, and there was no password expiration or change policy, posing a risk of credential compromise. The absence of multi-factor authentication (MFA) further weakened security, allowing attackers to gain access with no secondary verification. This lack of credential management made credential stuffing or brute-force attacks possible and appealing to the attackers, which could have widened the breach if attackers had attempted to use compromised credentials on other services.
3. **Insecure Network:** The organization used the outdated Wired Equivalent Privacy (WEP) protocol for its wireless Network, which is susceptible to hacking. WEP encryption has a weak key scheduling algorithm and is vulnerable to attacks that can be carried out in minutes. This insecure network setup exposed critical infrastructure to eavesdropping and unauthorized access.
4. **Lack of Proactive Security Measures:** Despite recommendations from Pruhart Tech to conduct vulnerability assessments, the CEO, Maria Rodriguez, went with a reactive approach (waiting for something to happen and then reacting), so the company was unprepared for cyber threats. Without regular security assessments, penetration testing, or audits, vulnerabilities remain unpatched and sometimes unknown, creating multiple attack surfaces that could be exploited by attackers.

B. Compromise of Confidentiality, Integrity, and Availability

Using the NIST 800-53 framework, Azumer Water's security principles were compromised in multiple ways:

1. **Confidentiality:** The volunteer database contained Personal Identifiable Information (PII) such as contact details, background checks, and partial social security numbers. Unauthorized access to this data creates a risk of identity theft (NIST AC-3 Access Control). Such a breach could lead to social engineering attacks on volunteers by attackers posing as official personnel to prey on victims.

2. **Integrity:** Attackers spoofed John Smith's email to send out false donation requests, misleading volunteers and destroying Azumer Water's credibility. This violates the NIST System and Information Integrity, which requires message authenticity. The lack of domain security measures such as DMARC, SPF, and DKIM allowed attackers to impersonate the organization, thereby increasing the risk of fraud.

3. **Availability:** Deletion of the volunteer database interfered with operations. The absence of data backups violated NIST Contingency Planning and ISO/IEC 27002, Section 12.3 (Backup) requirements for Backup and recovery procedures. Without redundancy, the organization experienced significant downtime, which delayed relief efforts and undermined trust among volunteers and stakeholders.

C. Federal Regulation Violation

Azumer Water likely violated the Federal Information Security Modernization Act (FISMA) by failing to implement adequate security controls while working with FEMA:

1. **Failure to protect PII:** Inadequate access controls led to unauthorized exposure of sensitive information, violating federal data protection standards.

2. **Lack of data backup:** Failure to comply with federal data retention and disaster recovery regulations meant that vital volunteer information was not recovered.

3. **Potential GDPR Violation:** If international volunteers were affected, Azumer Water may also be violating the GDPR, which requires stringent Data Protection and breach notification requirements.

D. Immediate Steps for Azumer Water to Mitigate the Impact

To contain and minimize damage, Azumer Water should:

1. **Isolate Compromised Systems:** Disconnect affected machines to prevent further data breaches.
2. **Reset Employee Credentials:** Enforce immediate password changes and enable MFA.
3. **Investigate the Email Breach:** Analyze email logs to determine whether John's account was compromised.
4. **Notify Volunteers:** Inform volunteers about the phishing scam and advise them not to provide payment details.
5. **Recover Lost Data:** Attempt to restore the database from available USB backups and implement a formal backup strategy.

E. Benefits of an Incident Response Plan for Azumer Water

A structured Incident Response Plan (IRP) would benefit Azumer Water in terms of overall security posture and response capabilities. One benefit is increased awareness among employees since training programs such as phishing simulations could have prevented incidents like John's mistake. An IRP also establishes backup and recovery procedures to minimize the risk of data loss through regular backups. It also helps define roles and responsibilities to better respond to security incidents faster and more effectively. In addition, security monitoring through continuous logging, alerting, and anomaly detection would definitely help identify unauthorized access attempts before they cause serious damage to Azumer Water. In general, a well-implemented IRP would help Azumer Water prevent, detect, and mitigate security threats in an efficient and timely manner.

Second Part: Risk Assessment and Management

F. Processes to Increase Information Assurance and Compliance at Azumer Water

1. **Implement a Comprehensive Data Backup Plan:**
    - Perform daily encrypted backups to a secure cloud and offsite location.
    - Automate backups to ensure continuous data protection.
    - Regularly test data recovery procedures.

2. **Enhance Employee Security Training**
    - Conduct mandatory cybersecurity training on phishing and social engineering.
    - Implement quarterly security assessments.
    - Develop phishing attack exercises.

G. Recommended Technical Solutions for Azumer Water

A series of technical solutions must be implemented and used to improve Azumer Water's cybersecurity posture and prevent future attacks that are either similar to what happened or completely different. First, firewall enforcement should be prioritized to ensure proper configurations to prevent unauthorized access and minimize potential network threats. The firewall should only allow trusted traffic and packets. It is necessary to replace the outdated WEP protocol with WPA3 encryption to secure wireless communications and prevent network eavesdropping. Endpoint protection with anti-malware and intrusion detection software deployed on all systems will identify and mitigate threats before they escalate.

Multi-factor authentication (MFA) must additionally be mandated for employee logins to avoid credential-based attacks. Email protection measures, including DMARC, SPF, and DKIM, will reduce domain spoofing and phishing attacks and also minimize the chance that phishing emails are delivered on behalf of the organization. Lastly, a robust patch management policy should be introduced to update all software and systems to fix security holes. All these efforts will help Azumer Water defend itself against cyberattacks and protect its assets.

H. Recommended IT & Security Organizational Structure at Azumer Water

The recommended IT and Security organizational structure should consist of several key roles with different responsibilities for each. The IT Manager should oversee the overall IT infrastructure and compliance with applicable rules and policies. The Security Officer should lead security initiatives, conduct risk assessments, and direct incident response efforts. A system administrator who is qualified for the position must be selected. That person is responsible for user access, system performance, and security of IT Systems. Additionally, an Incident Response Team should detect, analyze, and respond to security threats to the organization's digital assets. Together. These roles provide a framework for a secure and efficient IT environment.

I. Risk Management Approach

Risk 1: Phishing attacks

- Likelihood: High (Employees lack security training)
- Severity: High (Compromised data, reputation, and finances)
- Impact: Unauthorized access to employee accounts, potential ransomware infection, loss of public trust
- Mitigation: Implement employee phishing awareness training. Deploy email filtering solutions such as DMARC, SPF, and DKIM. Enforce MFA for email access.

Risk 2: Data Loss

- Likelihood: Medium (No backup strategy)
- Severity: High (Critical data loss could halt operations)
- Impact: Inability to coordinate volunteers. Breach of federal compliance regulations.
- Mitigation: Implement automated daily backups. Store backups offsite and in the cloud. Regularly test recovery procedures.

J. Application of NIST 800-37 Risk Management Framework (RMF)

To strengthen security and compliance, Azumer Water should adopt the NIST 800-37 Risk Management Framework (RMF), which follows these seven steps.

1. **Prepare:** Identify and classify assets, create security policies, and perform risk assessments.
2. **Categorize:** Define the confidentiality, integrity, and availability impacts of security threats on information systems.
3. **Select:** Choose appropriate security controls to protect against identified risks.
4. **Implement:** Install selected security measures such as firewalls, endpoint protection, and MFA.
5. **Access:** Get management approval for system operations after ensuring that all security controls meet compliance standards.
6. **Authorize:** Get management approval for system operations after ensuring that all security controls meet compliance standards.

7. **Monitor:** Track, detect, and respond to new emerging threats.

Why Azumer Needs to Follow NIST 800-37:

Azumer Water should adopt the NIST 800-37 framework for its security and compliance efforts. For one, it helps with compliance; following this framework ensures compliance with federal regulations like FISMA and increases the protection of Personal Identifiable Information (PII). It also encourages proactive security, which is a risk-based approach versus a reactive one. A risk-based approach helps the organization prepare for threats before they arise. Implementing NIST 800-37 also improves operational resilience and business continuity and reduces the risk of future breaches. In addition, adherence to this framework establishes trust and credibility among volunteers, partners, and stakeholders by demonstrating good cybersecurity practices. Adopting NIST 800-37 will improve Azumer Water's security and keep it in compliance with federal regulations for years to come.

References

National Institute of Standards and Technology (NIST). (2020). *Risk Management Framework for Information Systems and Organizations (SP 800-37 Rev. 2)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-37r2

National Institute of Standards and Technology (NIST). (2020). *Security and Privacy Controls for Federal Information Systems and Organizations (SP 800-53 Rev. 5)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

International Organization for Standardization (ISO). (2022). *Information Security, Cybersecurity and Privacy Protection - Information Security Controls (ISO/IEC 27002)*. https://en.wikipedia.org/wiki/ISO/IEC_27002