The Smart Meter Co.

Incident Report

September 14, 2024
Prepared by Aurnob Jahin Islam

1. Executive Summary

Smart Meter Co, an IIoT-based company providing smart electricity meters, suffered a cybersecurity attack that led to a sensitive data breach. The attacker employed a phishing email to trick employees into revealing their credentials. Weak access controls and inadequate authorization measures allowed the attacker to infiltrate the critical file server and database, ultimately compromising highly sensitive information.

2. Incident Details

- **Short Description of Attack (include the attack vector and intrusion point)**: Smart Meter Co experienced a significant cybersecurity incident resulting in employee credentials and sensitive data leakage. A malicious attacker used phishing email to lure company employees to enter their credentials which led the attacker to move through the network easily due to poor network segmentation.
- **Date and Time**: December 14, 2023; 08:00:10
- **Incident Severity**: High

3. Root Cause Analysis

1. High Level Observations from Logs:

- **Observation 1 –** Email server log

The email server log indicates that a mail from the IP address 18.8.10.10 which belongs to the domain mail.mercifulredeemerchruch.com was accepted by the CEO of Smart Meter Co John's mailbox. The attacker used the following email address <micr0soft@microsft.support.accounts.mercifulredeemerchurch.com> to send the phishing email. Based on the sender's email address, it looks the attacker pretended to be a support account by Microsoft to provide maintenance support to user. Based on the log, the user John was notified by Microsoft Office 365's internal sensor that the email was sent from an external sender. The email was forwarded by John to multiple other users including Jack, Vinod, Mary and Chillantra in their company email. According to the email server log, the phishing email was designed to collect user input as data commands which would be transmitted back to the email sender, which in this case is the attacker owning the mercifulredeemchurch.com domain.

Based on the email server log, the attacker gained the credentials via phishing email as employees entered their credentials in this method. The email server log highlights how poor the security of the email server used by Smart Meter Co is, that it accepts external emails and sends them directly to the inbox of users. It also highlights that there is no security in place to detect sensitive data going out of the company network.

- **Observation 2 –** File server log

Based on the file server log, it is evident that there is segregation or access control implemented within the file server, allowing all users to traverse through the directories and perform actions such as read/copy/update. Regardless of roles within the company, files within the critical server are easily accessible by any user which imposes critical vulnerability to gain root level permissions. The attacker modified and collected important files such as IIOTProductSourceCode.txt and EmployeeXMasBonuses.docx. The attacker also tried to delete important directories from the critical server by posing as the user Jack who is the CEO of Smart Meter Co but failed to do so.

The file server log shows that the attacker is very patient and persistent with the performed actions as the attacker is taking enough duration between each action to hide malicious activity from being detected.

- **Observation 3 –** SQL server log

Analyzing the SQL server log, there is no segregation of roles in place. The following roles app_user, db_admin and admin are all able to perform all types of database management actions within the DB table. It is also evident that any Smart Meter Co company user who has access to the database can use the abovementioned roles to manipulate the database.

The SQL server log shows that the attacker first manipulated and populated the database, then used the user CEO Jack's privilege to download the stored data in CSV format, which gave the attacker access to all the sensitive information stored in the SQL DB.

2. High Level Interview Insights:

- **Insight 1 –** Interview with CEO Jack

The attacker impersonated a known vendor, requesting credentials for maintenance. After the CEO entered his credentials and saw no result, he forwarded the phishing email to his employees. The email server lacked any detection mechanisms to block or flag the malicious email. Additionally, the CEO showed no concern when noticing and excel file being downloaded form the database server, further compromising security.

- **Insight 2 –** Interview with IIoT Engineer John

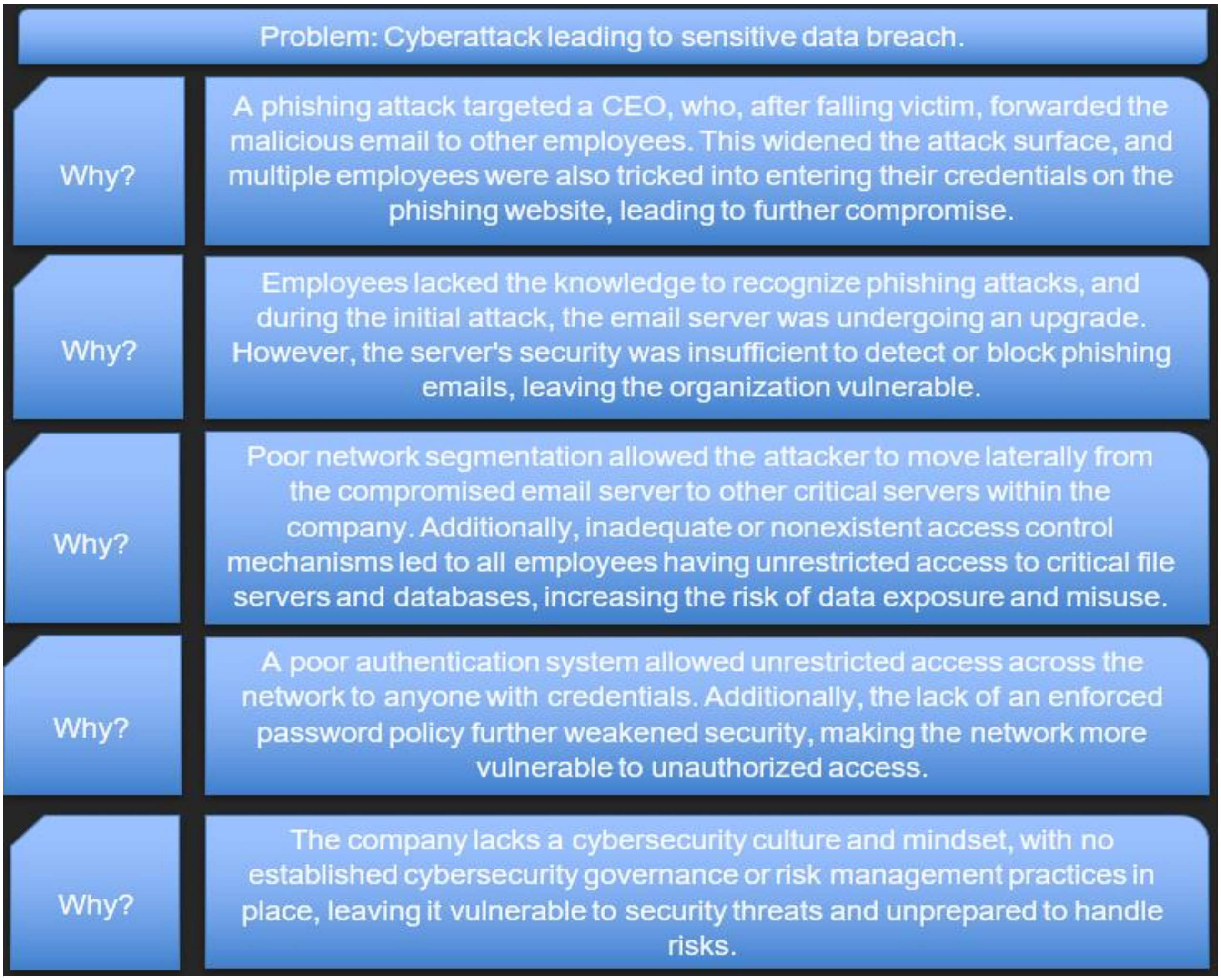
The urgency of the phishing email prompted the IIoT engineer, John, to immediately enter his credentials after clicking the malicious link. John also admitted to using the same password across all his accounts, making them highly vulnerable to breaches. A key takeaway from the interview was the CEO making code changes to enable remote access to the IIoT platform, suggesting the attacker may have gained unauthorized remote access to the company's critical systems.

- **Insight 2 –** Interview with HR Manager Chillantra

Although the HR manager recognized several red flags typically found in phishing emails, she ultimately followed the instructions due to her trust in the employee who forwarded the email to her, leading to a security lapse.

3. Root Cause Analysis Screenshots

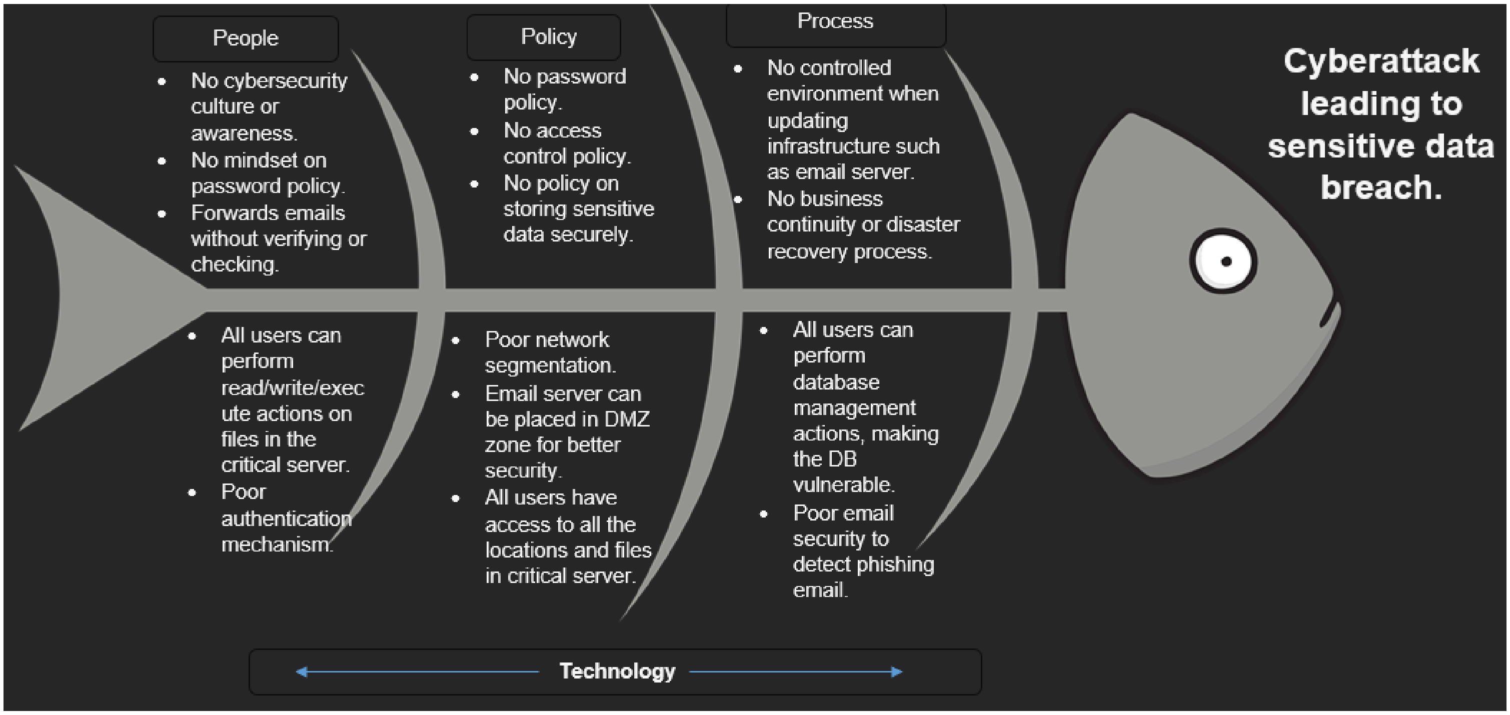
- **5 Whys Analysis (for problem statement) screenshot:**



Problem: Cyberattack leading to sensitive data breach.

Why?	A phishing attack targeted a CEO, who, after falling victim, forwarded the malicious email to other employees. This widened the attack surface, and multiple employees were also tricked into entering their credentials on the phishing website, leading to further compromise.
Why?	Employees lacked the knowledge to recognize phishing attacks, and during the initial attack, the email server was undergoing an upgrade. However, the server's security was insufficient to detect or block phishing emails, leaving the organization vulnerable.
Why?	Poor network segmentation allowed the attacker to move laterally from the compromised email server to other critical servers within the company. Additionally, inadequate or nonexistent access control mechanisms led to all employees having unrestricted access to critical file servers and databases, increasing the risk of data exposure and misuse.
Why?	A poor authentication system allowed unrestricted access across the network to anyone with credentials. Additionally, the lack of an enforced password policy further weakened security, making the network more vulnerable to unauthorized access.
Why?	The company lacks a cybersecurity culture and mindset, with no established cybersecurity governance or risk management practices in place, leaving it vulnerable to security threats and unprepared to handle risks.

- **Fishbone Analysis Screenshot:**



People

- No cybersecurity culture or awareness.
- No mindset on password policy.
- Forwards emails without verifying or checking.

Policy

- No password policy.
- No access control policy.
- No policy on storing sensitive data securely.

Process

- No controlled environment when updating infrastructure such as email server.
- No business continuity or disaster recovery process.

Cyberattack leading to sensitive data breach.

- All users can perform read/write/execute actions on files in the critical server.
- Poor authentication mechanism.

- Poor network segmentation.
- Email server can be placed in DMZ zone for better security.
- All users have access to all the locations and files in critical server.

- All users can perform database management actions, making the DB vulnerable.
- Poor email security to detect phishing email.

Technology

4. Attack Vector: Email, an attacker used a phishing email to bait company employees to provide their credentials which lets attacker access sensitive and critical locations within the company network.

5. State the intrusion point: The attacker was able to move through the network laterally due to poor network segmentation, lack of access control policy and password policy.

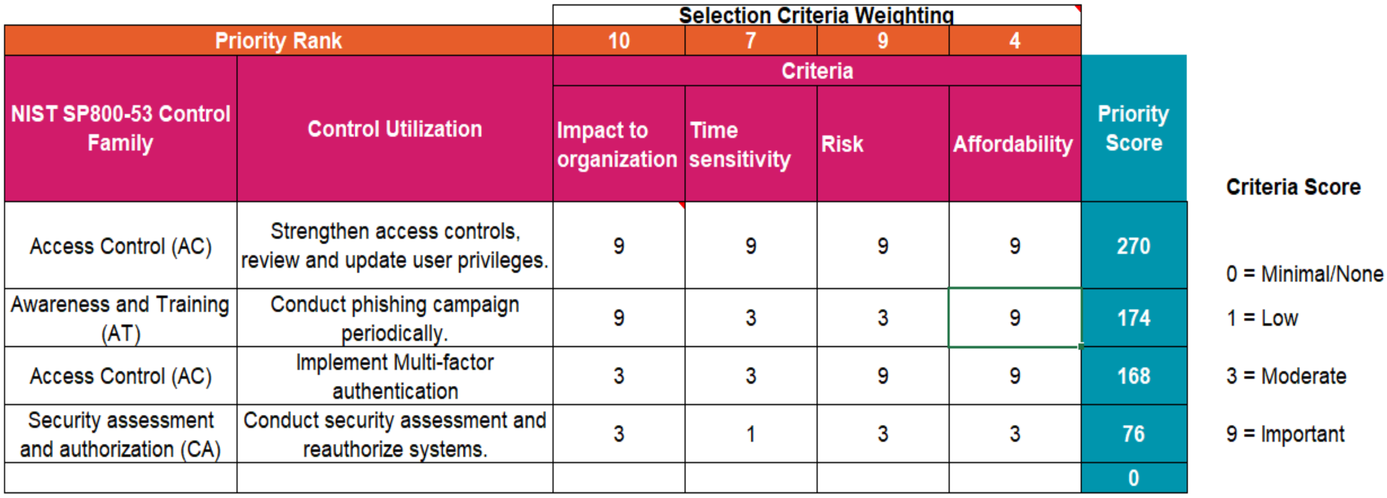
4. Failed Controls

- **Access Control (AC) Family:**
  - **Failed control 1 –** Access Control Policy and Procedures
  - Reason: Users across all departments and ranks have unrestricted access to network resources beyond their roles, creating a significant vulnerability to unauthorized access and potential security breaches.
- **Identity & Access Management (IAM) Family:**
  - **Failed control 2 –** Strong Password Policy and Procedures
  - Reason: Users rely on the same password for all their accounts, and the company lacks a policy to enforce periodic password changes, further increasing the risk of unauthorized access and security breaches.
- **Configuration Management (CM) Family:**
  - **Failed control 2 –** Access Restrictions for Change

    - Reason: The ability of a CEO to modify IIoT platform code and download database content, or an engineer to alter salary bonus files highlights a serious lack of access restrictions, exposing the company to potential security and operational risks.
- **Awareness and Training (AT) Family:**
    - **Failed control 2 –** Security Awareness Training
    - Reason: Inability to identify phishing emails, entering credentials on unverified websites, and forwarding malicious emails to colleagues indicate a significant lack of cybersecurity awareness. This failure undermines the effectiveness of security awareness training and exposes the organization to increased risk.

5. Prioritized Recommendations Based on Overall Risk

Prioritization template Screenshot:



		Selection Criteria Weighting				
Priority Rank		10	7	9	4	
NIST SP800-53 Control Family	Control Utilization	Criteria				Priority Score
		Impact to organization	Time sensitivity	Risk	Affordability	
Access Control (AC)	Strengthen access controls, review and update user privileges.	9	9	9	9	270
Awareness and Training (AT)	Conduct phishing campaign periodically.	9	3	3	9	174
Access Control (AC)	Implement Multi-factor authentication	3	3	9	9	168
Security assessment and authorization (CA)	Conduct security assessment and reauthorize systems.	3	1	3	3	76
						0

Criteria Score

0 = Minimal/None	
1 = Low	
3 = Moderate	
9 = Important	

6. Conclusion

It is highly recommended to implement robust access control mechanisms and update user roles and privileges immediately, as this poses a significant risk to the organization. Given the urgency, any delay in deploying access controls leaves the entire network infrastructure exposed and vulnerable to potential threats.