Incident Report for SmartMeter Co.

12/13/2024
Frederic Gariepy

Table of Contents

1. Executive Summary

A phishing attack resulted in the compromise of several user credentials, further compromise of sensitive and confidential data stored on SmartMeter Co’s servers.

On December 14th, an email phishing attack compromised user credentials, including the CEO and critical system employees. These credentials were used to further exploit SmartMeter's vulnerable systems and resulted in attackers compromising sensitive and confidential data.

Follow this document for details on this incident report, consult the prioritization table in section 5 and recommendations in the conclusion at the end of this document.

2. Incident Details

- Short Description of Attack:

  On December 14 at 08:00:00, the public facing SMTP Email Server received a phishing attack containing phishing emails to 5 organization members.

  The attack resulted in the confirmed credential leak of 3 members, including the CEO, critical service employees, and HR.

  Attackers used stolen credentials to access the internal network which is marked by several vulnerabilities, most notably:
  - Public facing EOL Email server in-line to internal unsegmented network.
  - Shared system resource with no robust access control implementation.

  The attackers were able to compromise confidential and sensitive information from the system.

- Date and Time: Dec 14th
- Incident Severity: High

3. Root Cause Analysis

1. High Level Observations from Logs:

- **Observation 1 - Email Server Logs:**

  Absence of firewall.
  The public-facing email server was not preceded by a firewall which could have prevented packets from spoofed /malicious/bad reputation IPs and added a layer of security.

  Absence of Email Filtering and/or Spam Protection.
  The EHLO Command specifying a domain, and the MAIL FROM command specifying a sender email address passed through without check, and shows the absence of Email Filtering and/or Spam Protection to check for sender addresses.

  Absence of email security protocols.
  The SMTP email server lacks SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting & Conformance). These email security protocols help verify that emails are actually coming from the domain they claim to be from.

- **Observation 2 - File Server Logs:**

  Lack of strong access control.
  Users of various accounts have unrestricted access to /CriticalFileServer/ unrelated to their organizational roles. This clearly indicates that no well established RBAC policy is set in place. A Delete failure on /CriticalFileServer/ subfolders indicates that there is some ABAC in place, however the ABAC is not robust enough to control over all system files based on user attributes.

  Lack of security logging and log monitoring system.
  User access and actions on sensitive folders and files is not appropriately logged as security events. Log monitoring systems such as a SIM, SEM, or SIEM should be further implemented for proper alerting or action on logged security events.

  System administration failure.
  A single file server contains a /CriticalFileServer/ which users use as a working directory, indicating lack of good system administration practice. Separate servers, or single servers with different shared folders supporting management through Active Directory should be employed to enforce permissions & group policies as a basic security practice. Organization may also consider the use of LDAP systems to keep track of

un/authorized access to, or exfiltration of sensitive folders and files.

- **Observation 3 - SQL Server Logs:**

  Lack of database alerting.
  The repeated SQL actions:

app_user SELECT SELECT * FROM SmartMeterCoDB.Readings WHERE MeterID = '12345';
admin UPDATE UPDATE SmartMeterCoDB.Readings SET Value = '100' WHERE MeterID = '54321';
db_admin DROP TABLE DROP TABLE SmartMeterCoDB.Readings;

  Did not create an alert or log errors, as the SQL table was dropped by db_admin and operations were attempted on a dropped table. Alerts as to system errors or important database actions should be logged.

  Seeming lack of database access control.
  Multiple users have access to the same SQL table, and *may* have overlapping permissions leading to potential security risks and data integrity issues. Fine-Grained permissions and/or RBAC should be employed to mitigate these risks.

2. High Level Interview Insights:

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

  Lack of awareness training at the executive level.
  When asked if he could recognize the phishing attempt, Jack replied:
  "I didn't have any information to help with detecting a fake page or phishing email."
  This points to an absence of awareness training in the organization.

  Lack of role responsibility definitions at the executive level.
  When asked about the aftermath of leaking his credentials to the phishing email, Jack replied: "...I forwarded the email to John and Vinod to look into". The user did not follow a well established escalation procedure and mishandled the issue due to a lack of role responsibility definition, resulting in further spread of the phishing attack.
  This points to a lack of role responsibility and lack of training on the cybersecurity engagement that organizational members ought to uphold and participate in.

  No incident response policies and incident response training.
  When asked if he reacted to indicators of compromise, Jack replied:
  "Jane...did you take any immediate actions to mitigate potential risks? Jack: No… "
  This points to an absence of incident policies, SOPs, Playbooks, awareness and training regarding incident response policies.

Uncontrolled BYOD.
Jack mentioned that other users use his personal word device "they use my blackberry often." This points to a lack of device separation of duty, lack of MDM, and generally an uncontrolled bring your own device (BYOD) environment which weakens endpoint security for the organization.

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

Lack of awareness training at the technical level.
When asked about the phishing email John replied that "It looked pretty standard to me;" indicating a lack of awareness training on recognizing phishing attacks.

No MFA.
When asked about why he leaked his credentials John replied: "I don't hesitate and I enter my credentials all the time for these emails." which indicates an immature security culture and a lack of MFA systems in place.

Lack of role responsibility definitions and engagement at the technical level.
When asked if he noticed any indicators of compromise, John replied:
"I did see some odd updates from Jack in the code, which is odd because he's the CEO", this points to a lack of responsibility definition and engagement, as such events should have been reported.

- **Insight 3 - Interview with HR Manager Chillantra**

Lack of awareness training at the HR level.
When asked about the phishing email, Chillantra explained that it "looked odd to me" but leaked her credentials because "It was from John, so I thought I could trust it.". This illustrates that the user recognized a phishing attempt but erroneously relied on delivery from senior members.

Lack of policy, policy awareness and training.
The organization member did not follow through with action such as reporting or escalating the issue. This is due to an absence of awareness training, absence of security policies themselves (SOP, Playbooks, Guidelines), and use of policies where applicable.

3. Root Cause Analysis

a) 5 Whys Analysis

Problem statement	Why did a phishing attack result in the compromise of several user credentials and further compromise of sensitive and confidential data stored on SmartMeter Co's servers?
1rst Why?	Members of the team received a phishing email.
2nd Why?	The phishing email was not blocked or dropped and reached the email server, and the organization members lack basic security training (anti-phishing).
3rd Why?	The email server is not behind a firewall, and all member's credentials were leaked through the attack.
4th Why?	Overall network topology is insecure (internal network accessible through unguarded email server, non-segmented network, EOF server software) and the credential compromise lead to a data breach.
5th Why?	The organization has a low cybersecurity maturity level, and has many gaps not limited to and including: awareness training, access controls, system and communications protection, media protection…etc.

b) Fishbone Analysis

Causes		Effect
People	**Policy**	
Lack of awareness training (Phishing, device management, work security procedures).	No policy enforcement of access control over user permissions (No RBAC or ABAC).	
Immature security culture. Lack of role responsibility definitions and engagement.	No centralized logging security solution (No SEM, SIM or SIEM).	
	Lack of MDM policy. Lack of BYOD policy.	
Seeming lack of awareness and practical use of incident response plans, security SOPs, Playbooks.	No authentication policy, (MFA, password strength), policy on use of password management solutions.	
	Seeming lack of incident response plans, security SOPs, Playbooks.	
		Successful phishing attack lead to a data breach.
Automated SQL processes do not have safety checks or failure notifications (Select, Update on a Dropped table).	Internal network exposure through an in-line unprotected email server. Weak network topology design.	
	No SIEM, SIM, SEM, EDR, or other endpoint security.	
No Automated alerts when sensitive documents are accessed. (No DLP, RBAC, ABAC, EDR system).	Lack of network segregation, logical segmentation, VLANs, firewall misplacement, layered security (Lacks DMZ with 2 firewalls)	
No MDM for BYOD.	Seeming lack of host AV (Browser phishing link detection, malware detection)	
Seeming lack of host AV (Browser phishing link detection, malware detection).	Use of EOL technology (Microsoft Exchange 2003, Blackberry 6230, Windows 10 (nearing EOL)).	
Process	**Technology**	

4. Attack Vector:

Email server, the phishing attack occurred on a public facing SMTP email server without firewall and seemingly without proper email authentication configurations (DMARC, SPF, DKIM).

5. Intrusion point:

Using leaked credentials from successful phishing attacks, attackers were able to access the internal network through several possible methods:

- Moving laterally from the public facing email server (EOL Email server) into the unprotected and unsegmented internal network.
- Remote access into the internal network using the leaked credentials.
- Remote access into the internal network through the CEO's EOL device.
- Leveraging credentials to exploit alternative entry into the internal network.

4. Failed Controls

Control Family	Failed Control	Reason
Access Control	AC-3(7): Role-based Access Control	The File Server Logs indicate that system users have no enforced access control over information and system resources. The organization does not enforce a role-based access control policy over subjects and objects of the system.
Identification and Authentication	A-2(1): Multi-factor Authentication to Privileged Accounts	Organization failed to implement MFA for privileged accounts. MFA could have mitigated against further system exploitation by having MFA implemented.
Awareness and Training	AT-1: Policy and Procedures	Organization does not have awareness, training or possess policy documentation that addresses the scope, roles, and responsibilities of members vis-a-vis the organization's cyber security environment.
Awareness and Training	AT-2: Literacy Training and Awareness	All levels of the organization (executive, technical, human resources) failed to recognize a phishing attack, escalate or act according to policies in place.
System and Services Acquisition	SA-22: Unsupported System Components	Organization uses EOL services, Microsoft Exchange 2003, Blackberry 6230 (and near-EOL, Windows 10 workstations). These system components result in an opportunity for adversaries to exploit weaknesses in unmaintained services.
System and Communications Protection	SC-4: Information in Shared System Resources	File Server Logs indicate that the organization works inside a shared system resource (critical server) that lacks segmentation and access control. Leading to unauthorized and/or unintended information transfer.
System and Communications Protection	SC-7: Boundary Protection	Network topology fails to protect the internal network via unprotected public facing service (Email server), lack of endpoint monitoring (foreign logon alerts), absence of logically subnetted internal network, absence of robust network access control, and poorly implemented network topology.
System and Communications Protection	SC-28: Protection of Information at Rest	The initial mention of "...compromise of sensitive and confidential data stored on SmartMeter Co's servers" entails that data at rest ***may*** *well have been* unencrypted and therefore the organization failed to protect the information at rest.

5. Prioritized Recommendations Based on Overall Risk

Prioritization Table

		Selection Criteria Weighting				
Priority Rank		5	4	4	3	
NIST SP800-53 Control Family	Control Utilization	Criteria				Priority Score
		Impact to organization	Time sensitivity	Risk	Affordability	
System and Communications Protection	**SC-7**: Boundary Protection	9	9	9	9	144
System and Communications Protection	**SC-28**: Protection of Information at Rest	9	9	9	9	144
System and Communications Protection	**SC-4**: Information in Shared System Resources	9	3	9	9	120
Access Control	**AC-3(7)**: Role-based Access Control	9	3	9	9	120
Identification and Authentication	**A-2(1)**: Multi-factor Authentication to Privileged Accounts	9	3	9	9	120
System and Services Acquisition	**SA-22**: Unsupported System Components	9	3	9	3	102
Awareness and Training	**AT-2**: Literacy Training and Awareness	9	3	9	3	102
Awareness and Training	**AT-1**: Policy and Procedures	3	1	3	3	40

*Possible criteria scores:
0 = Minimal - None
1 = LOW
3 = Moderate
9 = Important

6. Conclusion

It is recommended to immediately do the three following actions:

- **Establish boundary protection** by placing the firewall at the forefront of the network and not exposing services without firewall protection, this should come at no additional cost and require minimal configuration.

- **Change user credentials** using best practices (strong passwords, password management) to stop further intrusion into the compromised system, this comes at no cost and requires minimal configuration.

- **Implement encryption for sensitive and confidential files**, this comes at no cost and requires minimal configuration

Following these immediate actions is of the utmost importance to prevent further damage and system compromise.