Incident Response Plan

Introduction

Maven Clinic, recently flagged some unusual network activity that has raised alarms. The senior management is taking this incident very seriously, given the medical data contained on the network. Task is to identify the nature of this alert, its potential impact, suggest mitigation strategies, and compile a review.

This incident response report analyzes a series of security events that occurred on September 20, 2023, on the workstation DESKTOP-1234567. The events indicate a potential compromise of the system, including successful login attempts, policy changes, brute force attacks, resource exhaustion, application errors, and network traffic anomalies.

Goals for Cyber Security Incident Response

When a cyber security incident occurs, timely and thorough action to manage the impact of the incident is a critical to an effective response process. The response should limit the potential for damage by ensuring that actions are well known and coordinated. Specifically, the response goals are:

1. Preserve and protect the confidentiality of constituent and employee information and ensure the integrity and availability of MAVEN CLINIC systems, networks and related data.

2. Help MAVEN CLINIC personnel recover their business processes after a computer or network security incident or other type of data breach.

3. Provide a consistent response strategy to system and network threats that put MAVEN CLINIC data and systems at risk.

4. Develop and activate a communications plan including initial reporting of the incident as well as ongoing communications, as necessary.

5. Address cyber related legal issues.

6. Coordinate efforts with external Computer Incident Response Teams and law enforcement.

7. Minimize MAVEN CLINIC's reputational risk.

Incident Response Plan

Incident Response Life Cycle Process

Cyber incident response management is an on-going process with a cyclical pattern. The specific incident response process elements that comprise the Cyber Incident Response Plan include:

1. **Preparation:** The on-going process of maintaining and improving incident response capabilities and preventing incidents by ensuring that systems, networks, applications, and data handling processes are sufficiently secure, and employee awareness training is in place.

2. **Identification:** The process of confirming, characterizing, classifying, categorizing, scoping, and prioritizing suspected incidents.

3. **Notification:** Alerting Incident Response Team members to the occurrence of an incident and communicating throughout the incident.

4. **Containment:** Minimizing financial and/or reputational loss, theft of information, or service disruption. Initial communication with constituents and news media, as required.

5. **Eradication:** Eliminating the threat.

6. **Recovery:** Restoring computing services to a normal state of operation and the resumption of business activities quickly and securely. Provide reputational repair measures and news media updates, if needed. Provide credit monitoring services to effected constituents, or other remediation measures, as appropriate.

7. **Post-incident Activities:** Assessing the overall response effectiveness and identifying opportunities for improvement through, ‘lessons learned’ or mitigation of exploited weaknesses. Incorporation of incident’s learnings into the cyber fortification efforts and the response plan, as appropriate.

Incident Response Plan

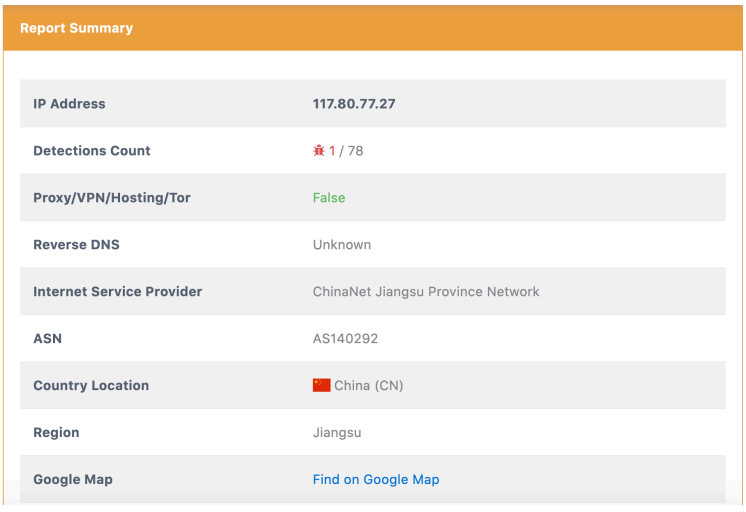
Incident Response Process Detail

1- Identification

Log analysis

40	9.130.84.96	Canada	Montreal	Quebec	IBM	IBM	45.5019	-73.5674
41	194.21.100.25	United States	Seattle	Washington	Amazon.com	Amazon.com, Inc.	47.4815	-122.246
42	134.237.134.32	Japan	Kitakyushu	Fukuoka	SoftBank Corp.	Yaskawa Electric Corporation	33.8656	130.771
43	117.80.77.27	China	Nanjing	Jiangsu	China Telecom	Chinanet JS	32.0607	118.763
44	165.202.226.130	Hong Kong	Cheung Sha Wan	Sham Shui Po	CLP Power Hong Kong Ltd	CLP Power Hong Kong Ltd	22.3331	114.16
45	99.217.248.98	Canada	Toronto	Ontario	Rogers Communications Canada Inc.	Rogers Cable Inc. PR	43.67	-79.3794
46	134.80.86.191	United States	Sierra Vista	Arizona	RCC-C	USAISC	31.5552	-110.35
47	24.104.97.67	United States	York	Pennsylvania	Comcast Cable Communications	Do It Outdoors	39.9517	-76.7161
48	116.22.77.219	China	Guangzhou	Guangdong	Chinanet	Chinanet GD	23.1181	113.2539
49	34.43.135.24	United States	Mountain View	California	Google LLC	Google LLC	37.422	-122.084
50	192.18.68.42	United States	Redwood City	California	Oracle Corporation	Oracle Corporation	37.5307	-122.262

Having a bulk of IPs, I looked them up through bulk IP lookup and information like the Country, region, ISP were shown. After that, I would checked the reputation of IPs through the IP reputation check. For example, the IP (117.80.77.27) was flagged malicious as shown on the figure down below. We should document this IP for future references.



Incident Response Plan

Analysis of the dataset of logs. Timeline of events:

Date	Time	Event	Computer
09/20/2023	08:10:23 PT	Successful Login.	DESKTOP: 1234567
09/20/2023	09:45:32 PT	System Audit Policy was changed	DC-SERVER-01
09/20/2023	10:32:17 PT	Failed to logon	DESKTOP: 1234567
09/20/2023	10:32:19 PT	Failed to logon	DESKTOP: 1234567
09/20/2023	10:32:21 PT	Successful Login.	DESKTOP: 1234567
09/20/2023	10:33:45 PT	Low Virtual Memory condition	DESKTOP: 1234567
09/20/2023	12:01:15 PT	Application Error. Explorer failing.	DESKTOP: 1234567
09/20/2023	13:23:15 PT	Rule has been added to the Windows Firewall exception list	DESKTOP: 1234567
09/20/2023	14:10:12 PT	Error Security Auditing	SERVER: 12345
09/20/2023	15:23:52 PT	MS SQL Error	SQLSERVER : 12345
09/20/2023	15:34:56 PT	Failed to logon	DESKTOP: 1234567
09/20/2023	15:34:56 PT	Failed to logon: Unknown username or bad password	SERVER: 12345
09/20/2023	16:45:32 PT	Security Auditing. Windows filtering platform has allowed a connection	SERVER: 12345

Incident Response Plan

Some abnormal behavior:

- Indication of Brute Force Attack determined by repeated login attempts targeting the administrator account.

  Impact assessment:

  - Privilege escalation: successful login attempt followed by a policy change granting administrative privileges. The attacker may have gained privileges access.

  Mitigations actions:

  - Lock accounts after 5 failed attempts.
  - Set up alerts for repeated failed login attempts within a short period.

  Investigations actions:

  - Analyze the events timeline checking for suspicious activities.
  - Correlate login attempts with known malicious IPs using threat intelligence feeds.
  - Review access logs to identify the attack's origin and block the source IP address.
  - Conduct a password policy review to ensure adherence to strong password requirements.

  Post-incident actions:

  - Reset the compromised administrator account password.
  - Implement multi-factor authentication for privileged accounts.
  - Implement alerts for failed login.

- Audit Policy change on DC-SERVER-01.

  Description: a change on the audit policy was detected on the system, which may affect the logging of security events.

  User/Account: Administrator.

  Authorized changed?: success.

  Impact assessment:

  - Potential Risk: Unauthorized changes could indicate an attempt to cover up malicious activities.
  - Systems affected.

Mitigations Actions:

- Enable real-time alerts for critical policy changes using SIEM tools.
- Implement strict change management protocols for audit policies.
- Increase monitoring for audit-related events.

Investigations actions:

- Analysis performed: Confirmed the account responsible for the audit policy change by analyzing the subject field of Event ID 4719.
- Analyze user permissions to determine if the account has legitimate access to modify audit policies.
- Review other security events around the same time to check for suspicious activity.

Post-incident Actions:

- Restore the audit policy to its original state.
- Conduct a comprehensive review of audit logs to identify hidden malicious activities.
- Restrict permissions for modifying audit policies to a specific group.

- Application error.

Description: The application crashed due to an access violation (Exception code: 0xc0000005), indicating it attempted to access restricted memory. This can be caused by corrupted files, resource limitations, or faulty hardware.

Mitigation Actions:

- Enable application-level logging to capture detailed crash information.
- Use automated monitoring tools to detect memory leaks or faults in real-time.

Investigations access:

- Found memory-related errors in logging happening at 10:33:45 PT.
- Check for signs of exploitation such as injected code or buffer overflows.
- Determine if the crash is tied to recent updates, deployments, or hardware changes.

Post-Incident Actions:

- Patch or reinstall the affected application.
- Review application resource requirements and allocate sufficient hardware.
- Conduct a penetration test to assess vulnerabilities exploited in the crash.

- Low virtual memory condition on a Windows system

Description: It indicates that the system is running out of memory resources. The system is running into low memory while handling SSH connections, which could result of high traffic or potential misuse, such as brute-force SSH attempts.

Mitigation Actions:

- Increase virtual memory or adjust the paging file size.
- Restart non-critical services consuming high memory.
- Add physical memory if persistent.
- Limit concurrent SSH sessions using configurations such as MaxSessions, MathAuthTries in sshd_config.
- Enforce key-based authentication and disable password logins.
- Use a tool (like Fail2Ban) to block IPs after multiple failed attempts.
- Monitor SSH and network traffic using tools like Wireshark, and block IPs initiating brute-force attacks using firewall rules.

Investigations Actions:

- Check SSH logs for signs of brute-force attempts or failed logins.
- Review system logs for memory usage alerts or related resource exhaustion issues.
- Inspect processes: identify processes consuming excessive memory using Task Manager, or monitoring tools.
- Traffic inspection: analyze traffic to detect abnormal patterns such as excessive SSH connections. Is there a high volume of login attempts over a short period of time?

Post-Incident Actions:

- Update SSH access policies
- Configure alerts for memory usage and failed login attempts.

- Record all findings, mitigations actions, and new configurations for future reference.
- Educate team members about resource management and securing SSH access.

- MS SQL Error 823 (Disk I/O Issues)

  Description: indicates a severe issue with reading or writing data (Error 823). It is categorized as a high-severity error (Severity 24), often related to hardware or storage corruption.

  Mitigation Actions:

  - Temporarily take the affected database offline to prevent further corruption.
  - Run disk diagnostics to identify and address hardware faults.
  - Replace any failing storage devices.
  - Restore the database form the most recent backup if integrity checks fail.

  Investigations actions:

  - Check system and SQL logs.
  - Check Windows Event Logs for disk-related warnings.
  - Check database for consistency issues.
  - Investigate hardware issues on the server or drive health.

  Post-Incident Actions:

  - Review and improve backup frequency and redundancy for critical databases.
  - Consider implementing cloud storage for higher reliability.
  - Document root causes, actions takes, and resolutions to improve response to similar issues.
  - Deploy tools for proactive disk monitoring to detect early signs of failure.

- Network compromise

  Description: The traffic blocked by the firewall and the suspicious network communications suggest the possibility of a network compromise.

Mitigation Actions:

- Immediately block IP addresses for suspicious activity using firewall rules.
- Isolate affected systems or subnetworks to prevent further spread.
- Update rules to detect and block similar traffic patterns.

Investigations actions:

- Analyze logs to identify traffic patterns, source IPs, and connection types.
- Use tools like Wireshark to analyze packet captures and look for signs of malicious activity.
- Inspect systems communicating with flagged IPs for signs of malware or unauthorized access.

Post-Incident Actions:

- Review firewall rules and IDS/IPS configurations for better threat detection and mitigation.
- Share and gather information on flagged IPs or malicious activity from threat intelligence sources.
- Train team members to recognize and respond to network compromises quickly.
- Create a detailed report, including all blocked traffic, actions taken, and systems affected.

2- Notification

Stakeholders and the team must be quickly notified about the incident.

- **IT Department:** All members of the IT team, including system administrator, network engineers must be notified and take necessary steps to closely monitor the network.
- **Executives:** C-level executives, board members, and other key decision-makers.
- **Affected Users:** Employees, customers, or partners who may be impacted by the incident.This case Host machine DESKTOP-1234567

and user John doe must be notified, the file or server owner must be informed about the incident.

- **External Parties:** Law enforcement, regulatory agencies, or other third parties as needed. In case of data breach of sensitive information that involves other parties must be communicated directly.

3- Response Containment and Eradication

Containment objective: to limit the damage from an incident and prevent further unauthorized access or damage.

Immediate actions:

- Isolate affected systems.
- Implement access controls.
- Identify affected assets.
- Analyze the attack, understand how the breach occurred to better manage containment.

Temporary fixes:

- Intrusion Prevention Systems: use network security devices to block malicious traffic and protect unaffected systems.
- Modify security policies, such as updating configurations to strengthen defenses against similar attacks.

Communication:

- Inform stakeholders: notify team members, management, and customers about the incident and containment actions taken.

<u>Eradication</u>

Objective: to remove the threat and vulnerabilities from the environment completely.

Having the threats identified, it is time to remove them.

- Restore systems: replace affected files, clean backups ensuring that all traces of the incident are removed.
- Patch vulnerabilities: keep software and system up-to-date.
- Review security configurations: adjust security settings based on findings from the incident.
- Perform scans to ensure that vulnerabilities have been addressed and no remnants from the threats remain.
- Penetration testing to confirm that the environment is secure against similar attacks in the future.
- Inform the team and stakeholders.

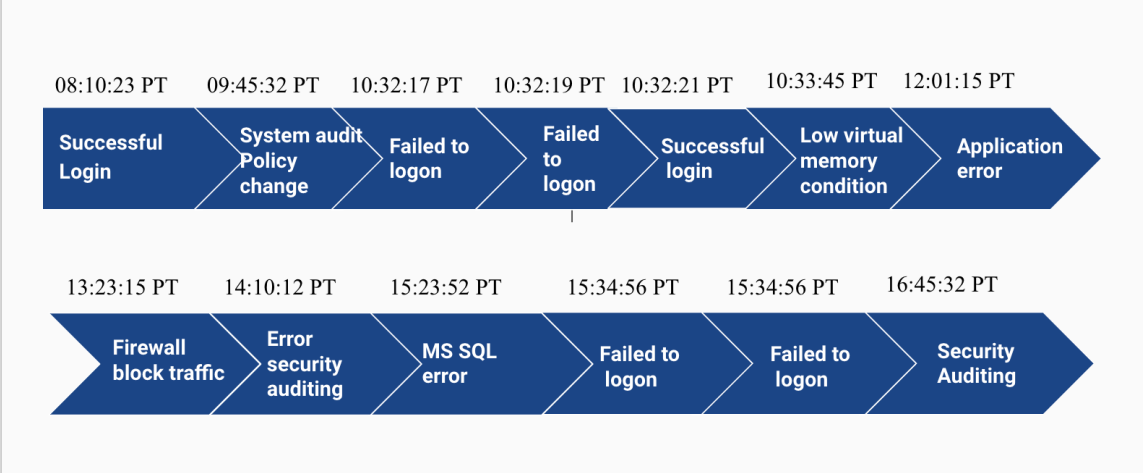
4- Post-incident Review

Incident Date: 09/20/2023

Prepared by: Ingrid Fuentes

Overview

- Incident Type: Unauthorized access attempt
- Incident Description: multiple SSH and RDP login attempts were detected, indicating possible brute-force attack.
- Incident Timeline:



Incident Response Plan

- The potential impact of this incident includes:

  - **Data Exfiltration:** Sensitive patient data stored on the workstation may have been compromised.

  - **Disruption of Services:** The compromised workstation may have affected the availability of critical services.

  - **Reputational Damage:** A data breach could damage Maven Clinic's reputation and public trust.

  - Regulation compliance such as HIPAA and GDPR must be focused and take steps if any customer data that may have been exposed or compromised.

  - Downtime: operational disruption or unavailability of data.

  - Customer Impact: Take necessary actions if any sensitive data or PII / health related data exposed.

  - Financial Loss: Estimate of financial costs due to the incident.

- What went wrong?

  - **Weak Password Hygiene:** The primary cause of the breach was the use of a weak password for the workstation's administrator account. This underscores the importance of enforcing strong password policies and using multi-factor authentication (MFA).

  - **Lack of Regular Security Assessments:** The absence of regular vulnerability assessments may have allowed the attacker to exploit known vulnerabilities in the system.

  - **Insufficient Monitoring:** The system may not have been adequately monitored for suspicious activity, allowing the attacker to gain a foothold and escalate privileges.

Incident Response Plan

- Lessons learned:

  - **Importance of Strong Passwords:** The breach highlights the critical importance of using strong, unique passwords for all accounts.
  - **Regular Security Assessments:** Regular vulnerability assessments are essential for identifying and addressing potential risks.
  - **Employee Education:** Security awareness training can help employees recognize and prevent phishing attacks.
  - **Incident Response Planning:** A well-defined incident response plan can help organizations respond effectively to security incidents.
  - **Conduct a Post-Incident Review:** Analyze the incident to identify lessons learned and areas for improvement.
  - **Implement Preventive Measures:** Strengthen security measures to prevent similar incidents in the future.

By addressing these Lesson learned and implementing the recommended measures, Maven Clinic can significantly enhance its security posture and reduce the risk of future breaches. But first of all, the Incident Response Team should:

- **Evaluate the goals**, such as improve the existing defense, then improve preventative actions, and evaluate the cost-effectiveness of the current defense given the its performance in this incident, assess the damage this incident caused and confirm no further damage will occur.
- **Assess roles** by identifying each individual affected by the incident whether they were involved or should have been involved. We should ask the questions: were they able to successfully defend? Were they impacted by the incident?
- Create a list of **questions** that concern at least one stakeholder, and focus on the ‘what’, ‘why’, and ‘how’.
- Complete a **timeline** to connect the dots of the incident.