Contents

SCENARIO

Rogue Wireless Access Point: Employees reported Wi-Fi issues from the cafeteria due to an unauthorized AP. Network security measure and any previous similar incidents are not detailed.

Incident Type

Rogue Wireless Access Point

1. Introduction

Scope:

This playbook outlines response steps to the incident of a rogue wireless access point within Viva la Vita Online' s network infrastructure. These steps are based on the NIST Computer Security Incident Handling Guide (Special Publication 800-61 Revision 2) that can be used to:

- Gather evidence
- Contain and then eradicate the incident
- recover from the incident
- Conduct post-incident activities, and feedback processes

Assumptions:

- The organization has an existing wireless network infrastructure and security controls in place.
- The rogue access point (AP) may have been intentionally or unintentionally introduced, posing potential security risks.
- The organization's Security Incident Response team is familiar with high level understanding of such incidents assuming the organization has a basic existing Incident Response playbook.
- An automated ticket/case get raised incase of an incident.
- The company has an escalation matrix hierarchy.

Audience:

This document has been created for computer security incident response teams (CSIRTs), system and network administrators, security staff, technical support staff, chief information security officers (CISOs), chief information officers (CIOs), computer security program managers, and others who are responsible for preparing for or responding to, security incidents like Legal Advisors, and Management.

2. Incident Response Team

Roles and Responsibilities:

- Incident Response Manager: The primary point of contact who will coordinate the overall incident response plan, manages the team, and ensures all SLAs are met in the assigned deadline.
- IT Security Analyst: Responsible for conducting in-depth analysis of the incident, including investigating the rogue access point in the network and identifying the scope of the breach by providing technical guidance.
- Network and Systems Engineer: Responsible for containing the incident, restoring systems, and implementing network security measures to prevent such incidents in the future.
- Application and E-commerce Specialist: Analyzes the security implications of the incident and recommends appropriate mitigation strategies for the online store and other connected systems.
- Legal and Compliance Advisor: Provides guidance related to the incident on legal and compliance requirements , and coordinates with regulatory authorities if necessary.
- Communications and Public Relations Coordinator: Responsible for handling external communications and manages the organization's public image to third party vendors, customers during and after the incident.
- Human Resources Representative: Assists with any actions related to personnels, or managing employee communications and informing other employees through proper communication channels.

3. Preparation

Tools and Resources:

- Network Controls
  - Perimeter Firewall on the network egress points (Fortinet FortiGate 7.4)
  - Intrusion Prevention Sensors on the internal network (Suricata 6.0.15)
  - Email Gateway with Anti-malware Anti-Spam Protection (Symantec Mail Security for Microsoft® Exchange 7.10)
  - Security Information and Event Management (IBM QRadar 7.5)
- Host Controls
  - Anti-malware Endpoint Protection on all devices (Symantec Endpoint Protection Client for Windows 14.3)
  - Full Disk Encryption on employee laptops (Bitlocker for Windows 10 and 11 versions)
- Other Controls
  - Vulnerability Patching Management (Tenable Nessus 10.6)
  - Backup and restoration tools

- Forensic analysis tools (e.g., EnCase, AccessData FTK, Autopsy)

The above tools and resources should be regularly reviewed and updated to address evolving threats and technologies.

Communication Channels:

- Establish secure and multiple communication channels for the Incident Response Team, such as encrypted email, secure messaging platforms, and dedicated conference lines to exchange reports.
- Open a conference bridge war room for the incident.
- Ensure that communication channels can be quickly adapted to the specific needs of the incident as adaptability will be needed in the situation.
- Use of Microsoft Teams, Skype, Outlook for communication between employees working on company premises and remotely.

4. Identification

Incident Detection Methods:

- Using the Fortinet FortiGate firewall, monitor wireless network activity for unauthorized devices and AP connections.
- Implement Wireless Intrusion Detection Systems (WIDS) and Wireless Intrusion Prevention Systems (WIPS) to get alerts on rogue APs.
- Check that there is no unauthorized device connected in the building, especially the perimeters surrounding the cafeteria.

Incident Reporting Mechanism:

- Confirm an automated ticket/case has been raised for the incident. If not, IT security analyst or staff should manually raise one.
- All network traffic from the rogue AP should be blocked.
- Gather and analyze information gained through internal communications like dedicated email groups, hotlines, or the incident reporting portal for such incidents.
- Establish clear procedures and report information about the incident by following the escalation matrix.
- Ensure that all employees are aware of the reporting mechanism and their responsibilities in the event of an incident, such as reporting Wi-Fi issues or unauthorized devices.

Initial Assessment Procedure:

- Gather and analyze available information about the incident, including the location of the rogue AP, potential impact on the network, the affected systems.
- Determine the scope of the incident and the potential risk to the company and notify relevant stakeholders.
- Assess the immediate actions required to contain the incident and prevent further damage.
- Find unusual network traffic and check logs wherever necessary.

5. Containment

Short-term Containment Strategies:

- Locate and Physically Disable AP: Use wireless network analysis tools and the Fortinet FortiGate firewall to locate the rogue AP and physically disable or remove it from the premises.
- Isolate Affected Network Segment: Isolate the network segment where the rogue AP was detected using the Fortinet FortiGate firewall and Suricata IPS to prevent potential lateral movement or further unauthorized access.
- Implement Temporary Security Measures: Implement temporary security controls, such as disabling wireless access in the affected area, increasing network monitoring using the IBM QRadar SIEM, and enhancing access controls.
- Monitor for Further Suspicious Activity: Closely monitor the company's wireless network and systems for any additional signs of compromise or suspicious activity using the existing security tools and controls.

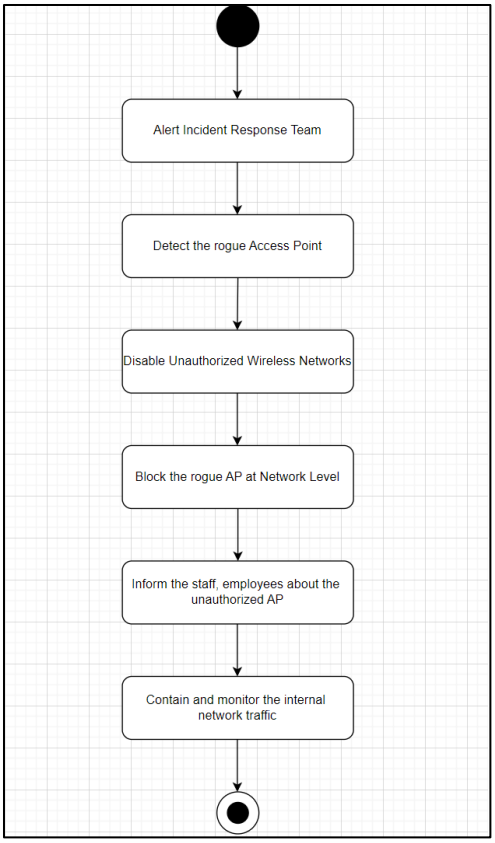

Figure : Short Term Containment Strategy

Long-term Containment Measures:

- Conduct a comprehensive risk assessment to identify and address any vulnerabilities that may have contributed to the incident, using the Tenable Nessus vulnerability management tool.
- Implement stronger Wi-Fi security measures, like certificate-based authentication.
- Review, audit, and monitor wireless networks for unauthorized devices.
- Regularly review and update the organization's incident response plan and playbooks to address evolving threats and lessons learned.

6. Eradication

Root Cause Analysis:

- Determine the extent of the compromise and the impact on customers and their orders with the help of Security Analyst by investigating the source and nature of the rogue AP.
- Analyze the other potential risk associated, such as network disruptions, data breaches, malware attacks.

- Analyze the security and weaknesses around the perimeter of the physical location of the routers, Wi-Fi modems.

Eradication Procedures:

- Determine the extent of the compromise and the impact on customers and their orders with the help of Security Analyst by investigating the source and nature of the rogue AP.
- Analyze the other potential risk associated, such as network disruptions, data breaches, malware attacks.
- Analyze the security and weaknesses around the perimeter of the physical location of the routers, Wi-Fi modems.

7. Recovery

System Restoration Process:

- Restore the affected network segment and wireless infrastructure to a secure and operational state, ensuring that all unauthorized devices and connections have been removed, using the Fortinet FortiGate firewall and Suricata IPS.
- Verify the integrity and security of the restored systems before allowing wireless access and connectivity.
- Implement additional network security controls, such as monitoring and network segmentation, to prevent future incidents.

Validation Checks:

- Verify that Wi-Fi networks are fully functional and secure.
- Conduct comprehensive testing and validation to ensure restored systems are fully functional and secure.

Ongoing Monitoring:

- Implement continuous monitoring and alerting mechanisms, using the Suricata IPS and IBM QRadar SIEM, to detect and respond to future activities.
- Review and update the company’s network security controls and incident response procedures on regular intervals to address evolving threats.

8. Post-Incident Activity

Lessons Learned Session:

- Review the incident response procedure in detail, taking into account the team's performance, the playbook's effectiveness, and any potential areas for development.

- Document the lessons learned and incorporate them into the company's incident response plan and playbooks.
- Establish a timeline, mention key findings and recommendations for future incident response efforts.

Incident Report Writing:

An incident report should be written and made available to all the audience as mentioned earlier. The following topics can be considered as part of the structure of the incident report:

- Initial cause of the incident
- Actions and timelines of important events
- Incident impact
- Root cause analysis
- Actions taken
- Indicators of Compromise (IOCs)
- Lessons learned

9. Appendices

Legal and Compliance Guidelines:

- Review any applicable laws, regulations, and industry standards that may govern the organization's response to this type of incident, such as removal of backup tapes notification requirements, in coordination with the Legal and Compliance Advisor.
- Consult with legal counsel to ensure that the incident response process and any actions taken are in compliance with current laws and regulations.

Contact Information:		
IT Director		
IT Staff		
Extended Team		
Helpdesk		
IT Manager		
Legal and Compliance Advisor		

Other Numbers/Contacts:

- Human Resources Representative
- Communications and Public Relations Coordinator
- IT Vendors