INCIDENT RESPONSE PLAYBOOK

Viva la Vita

Sowmyashree Bevur Mandya Venkatesh

NUID: 001099849

CY5010: Foundations of Information Assurance

Date: 13th April 2021

ABSTRACT

Incident response playbook (IRP) are highly detailed pre-planned procedures to be followed in the event of a security incident and is tailored to the enterprise's business goals and objectives. The purpose of IRPs is to handle the incident efficiently while minimizing the damage, cost, and time associated with it. It comprises of the following sections: Identification, Analysis, Containment/Eradication, and Recovery/Post Incident.

Computer Security Incidence Response Team (CSIRT) is responsible for handling such incidents when occurred in the organization. They are to prepare and maintain IRP for common incidents that can/has occurred in the enterprise.

In this paper we will be covering 3 incidents occurred at the Viva la Vita Online store: Unauthorized Access, SQLi vulnerability and connection from blacklisted IP. Our CSIRT team involve Incident Response Manager, team of Security Analysts, CISO, CIO/CTO, Technology and Operations Team Lead, Senior Management, Business Line Head of Departments, Human Resources, Legal/General Counsel and Relations Officer.

Incident 1: Unauthorized attempt to access payroll records

Introduction

In this incident, credentials of an employee John Saw are compromised due to a vishing attack and it is used to access the employee's payroll records. This can lead to exposure of sensitive information like financial details which can further lead to frauds.

1. Identification

- Installed SIEM software detected unusual access to employee's payroll records.
- Access to the system through abnormal ports/protocols and/or use of TOR/I2P connections.
- User unable to login to the account.
- Unusual remote logins outside business hours.
- Multiple attempts to access the record using same user credentials.

2. Notification

- Incident Response Manager and team of Security Analysts needs to be informed to analyze and rectify the issue.
- CISO and CTO needs to be notified of the attempt.
- Technology and Operations Team Lead need to be alerted to contain/rectify the issue
- All employees need to be notified of the vishing attack occurred.
- In case of any compromise of employee information the Human Resources needs to be notified to inform the employees.
- In case of compromise of sensitive information Legal counsel needs to be alerted.

3. Analysis

- The security team is to analyze logs of logins and access of payroll records recorded by SIEM.
- Evidence to be collected from the help desk like the authentication procedure carried out for password reset.
- Check logs of access to employee database prior to and after the password reset.

- Check for insider's involvement in compromise of employee's information and other possible breach to access the data.
- Check the resources and permissions that employee is assigned based on his designation and check for privilege escalation.
- Check the integrity of the payroll records to ensure it is not tampered.

4. Containment/Eradication

- The password of the employee needs to be reset immediately.
- Ensure principle of least privilege is maintained if found to be escalated.
- Rollback the payroll records to the original form if integrity is found to be compromised.

5. Recovery/Post Incident:

- Update and train the employees to protect against social engineering attacks.
- Update the authentication procedure involved in changing/providing access to sensitive information like password. For example, including Multi-Factor Authentication,
- Take required legal action against the attacker.

Incident 2: SQL injection vulnerability

Introduction

SQL injection is an attack where a malformed SQL query is inserted into an application (via client-side input) to allow for database manipulation. Here a vulnerability to this attack was found in one of the applications whose privileges can allow for write, modify, and delete the employee table. If exploited, it can compromise the confidentiality and integrity of the employee records of the enterprise.

1. Identification

- Reported anomalies experienced by site visitors.
- Manual analysis of the web, application, and database logs.
- Employees' data exposed on the internet.
- Suspicious modification of employee records.
- Alert from installed Intrusion Detection System (IDS).

2. Notification

- Incident Response Manager and team of Security Analysts needs to be informed to analyze the vulnerability and come up with controls to mitigate it.
- CISO and CTO needs to be notified.
- Technology and Operations Team Lead and Senior Management needs to be notified to take appropriate measures to patch the vulnerability.
- In case of an attack, the legal team needs to be notified.

3. Analysis

- The team should analyze the application code base for usage of vulnerable code elsewhere.
- The team should analyze the web logs for HTTP GET/POST request packets received to check if the vulnerability is exploited.
- Compare SQL logs generated by the application and the database and check for anomalous query statement execution.

- The team should ensure that the code used in the front-end servers sanitizes the input parameters.
- Verify that the employee table is not tampered with.
- If the attack was successfully exploited, determine the type of SQLi and come up with related patches for the same.

4. Containment/Eradication

- Fix the vulnerable pages by replacing string-based queries with strongly typed parametrized/bound queries with placeholder substitution markers and if required replace the vulnerable query with stored procedures.
- Test and replace dynamic query interface usage wherever necessary.
- In case of an attack and a table modification, restore backups/ perform data correction analysis.
- Ensure least privilege is maintained i.e drop write/modify/delete permissions and making it read-only with the access to views of the table.

5. Recovery/Post Incident

- Install and use readily available SQL injection tools to analyze newly designed interactive pages of the application.
- Install Web Application Firewall (WAF) at host and network levels to detect SQLi attacks.
- In case of SQLi worm attack, add the signature of the worm to the IDS and WAF.
- The sensitive data stored in the database should be strongly encrypted.
- Train developers to promote secure coding practices.

Incident 3: Blacklisted IP is seen in the VPN connections

Introduction

A blacklisted IP connected to company's resources using the identity of the employee John Saw. This connection was made using the company's VPN. The impact of allowing such connections widely depends upon the intentions held and actions performed.

1. Identification

- Alert from Intrusion Prevention System and HIPS.
- Event message found in syslog server.
- Log entry in web access logs.
- Notification from Internet Service Providers.

2. Notification

- Incident Response Manager and team of Security Analysts needs to be informed to analyze the connection and intention behind it.
- CISO and CTO needs to be made aware.
- Technology and Operations Team Lead and Senior Management needs to be notified to take appropriate measures to contain and reverse any actions performed.
- The legal counsel needs to be alerted if the connection led to a security breach and consequently even the PR Officer needs to be made aware.
- If this incident led to compromise of business objective/function, Business line HODs need to be notified too.
- The Human Resource needs to be notified if any foul play from an employee is detected.

3. Analysis

- The security team to capture packets inbound from the blacklisted IP for analyzing and trace back to the session information issued for the connection.
- Verify with the employee if this connection was made intentionally or not. And if found to be intentional, look for means of compromise of the user credential.
- Trace and capture the communication with the internal resources accessed by that IP Address.

- Check for privilege escalation and injection of malicious code into the enterprise resources.
- If malicious code is injected, then locate all the resources affected by this and isolate the malware/worm and analyze its working and business impact it holds and search possible patches that can be applied.

4. Containment/Eradication

- Update Firewall and IPS, HIPS IP blacklisting rule with this IP address to drop all packets in/out the enterprise network.
- Reset the credentials of the employee to prevent it from being reused.
- Revert the privileges to appropriate permissions if found to be escalated.
- Disinfect all systems resources if malware was found and ensure its integrity is not compromised.

5. Recovery/Post-Incident

- Restore the resources back to a trusted backup if found to be tampered.
- If this connection was made with a malicious intent by the employee intentionally, take appropriate legal actions against the employee.

REFERENCES:

Incident Response Consortium, https://www.incidentresponse.com/playbooks/unauthorized-access

Dell Secureworks, *SQL injection Attacks*, https://www.secureworks.com/blog/sql-injection-attacks

Justin Folkerts, *Incident Handlers Guide to SQL Injection Worms*, https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-guide-sql-injection-worms-33133

Ghafir, Ibrahim & Prenosil, Vaclav. (2015). Blacklist-based Malicious IP Traffic Detection. 10.1109/GCCT.2015.7342657.