Create an Incident Response Plan

Page 1 of 3

Detailed Incident Response Plan

1. Detection Methods

1. **Automated System Alerts**

   - **Intrusion Detection Systems (IDS)**: Set up IDS to monitor for suspicious login activity, especially after redirections from external sites. IDS can send real-time alerts for high volumes of failed login attempts.

   - **Phishing Detection and Web Filtering Tools**: Use these tools to flag suspicious links shared within the platform, blocking known phishing domains and alerting administrators to potential phishing campaigns.

   - **Behavioral Analytics**: Analyze account activity, such as large, unusual in-game purchases or changes in IP addresses, indicating a potential account compromise.

2. **User Reports**

   - **In-Game Reporting Mechanism**: Offer a streamlined process for users to report unusual activity directly from their accounts, such as unauthorized purchases or changes in profile settings.

   - **Customer Support Hotline**: Allow users to contact support to report unexpected behavior, such as lockouts, password changes, or strange in-game conversations.

3. **Audit Log Analysis**

   - **Session Logging**: Track user login history across SSO providers (Google, Facebook, Xbox Live, etc.) and review off-hours logins, changes in IP, or multiple failed login attempts.

   - **Change Management Logs**: Monitor unexpected changes in account settings, such as altered contact information or billing details, to detect compromised accounts.

4. **External Notifications**

    - **Threat Intelligence Feeds**: Subscribe to security bulletins and alerts from cybersecurity organizations. Notifications from partners or third-party researchers (e.g., Check Point) help identify industry-specific threats.
    - **Law Enforcement Alerts**: In cases of large-scale attacks, law enforcement can provide valuable alerts and updates on emerging threats.

Page 2 of 3

2. Incident Classification

Low (Level 1):

- Isolated phishing link clicked with no credential compromise.
- Minor unauthorized access attempts detected but blocked by 2FA.

Medium (Level 2):

- Multiple user accounts displaying signs of phishing-related credential theft.
- Successful unauthorized transactions across several accounts.

High (Level 3):

- Large-scale phishing attack with significant credential theft.
- Widespread impersonation or unauthorized access to user data, impacting multiple accounts.

3. NIST Incident Response Lifecycle Example

Scenario: Phishing Attack on Fortnite Accounts

Phase 1: Preparation

- **Existing Measures**:
    - **Two-Factor Authentication (2FA)**: Strongly encouraged for all accounts.
    - **User Training**: Conduct regular security awareness campaigns on phishing risks.
    - **Updated SSO Security**: Secure and tested SSO system that minimizes risk of redirect vulnerabilities.

Phase 2: Detection & Analysis

1. **Detection**:
    - IDS alert indicating high volumes of failed login attempts.
    - Reports from users regarding unauthorized purchases or inability to log in.
2. **Analysis**:
    - Assemble the incident response team (IRT) to investigate the origin of the phishing links.
    - Use forensic tools to trace the SSO redirect vulnerability and determine how many accounts were impacted.
    - Classify this as a Medium (Level 2) or High (Level 3) incident based on the scale of impact.

Page 3 of 3
Phase 3: Containment, Eradication & Recovery

1. **Containment**:
    - **Account Suspension**: Temporarily lock accounts showing signs of unauthorized access.
    - **Redirect Blacklisting**: Block malicious redirects at the network level to prevent users from being redirected to phishing sites.
2. **Eradication**:
    - **SSO Patch**: Update SSO protocols to validate redirect URLs, ensuring they point only to trusted sites.
    - **Phishing Blocklist Update**: Add known malicious domains to a blocklist to prevent further distribution of phishing links.
    - **Remove Phishing Links**: Delete or quarantine phishing links from all Epic Games communications.
3. **Recovery**:

- **Reset Compromised Accounts**: For affected users, require a mandatory password reset and strongly encourage 2FA.
- **Systems Test and Validation**: Run end-to-end tests on the SSO system to confirm the vulnerability is patched and redirect protections are in place.
- **Enhanced Account Monitoring**: Increase monitoring for affected accounts to detect any signs of reinfection or compromised security.

Phase 4: Post-Incident Activity

1. **Lessons Learned**:
   - Conduct a full review with the incident response team to analyze how the vulnerability was exploited and how future detection can be improved.
2. **Improvements**:
   - **Update Security Tools**: Enhance IDS and phishing detection tools to identify new variations of similar attacks.
   - **User Education**: Conduct ongoing cybersecurity training for users, emphasizing recognizing phishing links.
3. **Reporting**:
   - **Detailed Report**: Prepare a full incident report detailing the scope, response, and security improvements. Share with relevant stakeholders, such as executives or security partners.
   - **Notify Impacted Users**: Inform affected users of the incident, urging them to maintain strong passwords and use 2FA.
4. **Training**:
   - **Phishing Awareness Training**: Implement more focused user training, including simulated phishing exercises to help users recognize suspicious links.

Throughout the response process, keep clear and regular communication with users, especially when implementing mandatory password resets or security updates affecting their accounts.

This expanded plan provides more detailed detection methods, incident classifications, and response steps while adding specific tools and recommendations for a thorough approach.

Develop a Comprehensive Security Policy

1. Key Security Rules/Guidelines

1. **Access Control and Authentication**

   - **Rule**: Enforce strong, unique passwords and implement two-factor authentication (2FA) on all accounts.

   - **Purpose**: Protects against unauthorized access by adding an extra layer of security to user accounts.

   - **Guideline**: Passwords must be at least 12 characters long and contain a mix of uppercase, lowercase, numbers, and symbols. Users should not share passwords or reuse them across different platforms.

2. **Data Protection and Encryption**

   - **Rule**: Encrypt all sensitive data, both in transit and at rest, using industry-standard encryption protocols.

   - **Purpose**: Prevents unauthorized access to data, ensuring that information remains secure even if intercepted.

   - **Guideline**: All sensitive data, including personal information and financial details, must be encrypted. This applies to data stored in databases, backups, and data transmitted over networks.

3. **Regular Security Audits and Vulnerability Assessments**

   - **Rule**: Conduct security audits and vulnerability assessments on all systems and applications quarterly.

   - **Purpose**: Identifies and mitigates potential security risks proactively.

   - **Guideline**: Audits should include network security, access control, and application security. Vulnerability assessments should use automated tools and manual checks to identify and remediate weaknesses.

2. Incident Response Plan

In case of a security breach, the following incident response plan will be implemented to contain, eradicate, and recover from the incident:

1. Detection and Analysis

- **Step 1**: Monitor automated alerts and user reports for suspicious activity, such as unauthorized access attempts or abnormal network traffic.

- **Step 2**: Confirm the breach by analyzing logs and audit trails to determine the nature and scope of the incident.

- **Step 3**: Assemble the incident response team to assess the situation, classify the incident level (Low, Medium, or High), and proceed accordingly.

2. Containment

- **Step 4**: Contain the breach by isolating affected systems from the network to prevent further damage.

- **Step 5**: Block suspicious IP addresses and disable compromised accounts to halt unauthorized access.

3. Eradication

- **Step 6**: Remove the source of the breach by patching vulnerabilities, updating security protocols, and removing any malware or malicious code found during analysis.

- **Step 7**: Conduct a thorough scan to verify all traces of the breach have been removed.

4. Recovery

- **Step 8**: Restore systems from secure backups and verify the integrity of restored data.

- **Step 9**: Monitor systems closely after reactivation to detect any signs of residual or new malicious activity.

5. Post-Incident Review and Improvements

- **Step 10**: Conduct a post-incident review to identify weaknesses in the incident response process and implement improvements.

- **Step 11**: Update security protocols and educate users on new security measures to prevent similar incidents in the future.

3. Maintaining the CIA Triad (Confidentiality, Integrity, Availability)

These security policies and procedures reinforce the CIA Triad as follows:

1. **Confidentiality**:

   - **Access Control and Authentication** ensure that only authorized users can access sensitive information, preventing data leaks and unauthorized access.

   - **Data Protection and Encryption** protect confidential data, making it unreadable to anyone without proper authorization.

2. **Integrity**:

   - **Regular Security Audits and Vulnerability Assessments** help identify potential integrity risks, ensuring that systems and data remain reliable and unaltered by unauthorized actors.

   - **Incident Response Plan** includes steps to verify and restore data integrity after a security breach, safeguarding against data tampering.

3. **Availability**:

   - **Incident Response Plan** ensures systems are quickly contained and restored following a breach, minimizing downtime and preserving access to critical services.

   - **Data Protection and Encryption** and **Regular Security Audits** ensure that data is available and accessible to authorized users without unnecessary exposure to security threats.

Apply Encryption Techniques

1. **AES Encryption and Decryption**:

   - **Encrypted Text (AES)**: Ye+51Aq2w0J9GJfg+WmZ+Pdk2eq32UKq+3Q2WHyrmY7H+BT4o2OWzFyhLk7omMeL

   Secret code: 1234546789123456

   - **Decrypted Text**: "This is a sample text for encryption."

2. **SHA-256 Hashing**:

   - **Decrypted Text**: "This is a sample text for encryption."
   - **SHA-256 Hash**:

   1590c5873b3cef9f9662168f6cead24842a227751db842e542b2c1d44e8c5a86

Demonstrate Legal and Ethical Compliance

Legal and Ethical Compliance

In managing security incidents, compliance with legal regulations and adherence to ethical standards are critical to maintaining user trust and ensuring responsible handling of sensitive data. This section outlines key laws and ethical considerations that guide our incident response process.

1. Relevant Laws and Regulations

1. General Data Protection Regulation (GDPR)
- Overview: The GDPR, applicable to companies handling data of EU citizens, mandates strict requirements on data protection and privacy. It includes obligations for timely breach notifications, secure data handling, and user rights to data access and deletion.
- Compliance in the Incident Response Plan: The plan includes timely breach notifications, especially for incidents involving personal data. In alignment with GDPR's 72-hour breach notification requirement, our response team is prepared to assess incidents and notify affected users and authorities promptly if user data is compromised.

2. California Consumer Privacy Act (CCPA)
- Overview: The CCPA provides California residents with rights over their personal information, such as the right to know what data is collected, the right to delete it, and the right to opt out of data sales.
- Compliance in the Incident Response Plan: The plan includes secure handling of personal information and emphasizes timely response and transparency if user data is compromised. This includes notifying affected users of any data breach, as required by the CCPA, and providing options for data correction or deletion if necessary.

2. Ethical Consideration: User Privacy and Transparency

- Overview: Protecting user privacy is an ethical responsibility, especially in an environment where personal information can be vulnerable. Maintaining transparency with users about data usage, security practices, and breaches is essential to uphold trust and accountability.
- Application in the Incident Response Plan: This plan prioritizes transparency by notifying users if their data has been compromised and advising on protective actions. Additionally, the plan includes ongoing security training for staff to reinforce ethical data handling, especially regarding users' personal information.

3. How the Plan Upholds Legal and Ethical Standards

- Timely Notifications: By addressing breach notifications promptly, this plan complies with GDPR and CCPA requirements, ensuring affected users and relevant authorities are informed quickly in the event of data exposure.
- Data Integrity and Security: The plan emphasizes data encryption and access control to safeguard personal information, aligning with legal requirements and the ethical responsibility to protect user privacy.
- User Empowerment: Our plan supports users' rights to understand, access, and manage their data by including steps for secure data access and responding to user requests for data deletion or correction after an incident.

By adhering to these legal requirements and ethical principles, this incident response plan reinforces trust, maintains compliance, and demonstrates a commitment to responsible, transparent handling of user data.