Incident Response Plan for Sony PlayStation Network Breach

Organization Name: Sony PlayStation Network
Document Title: Incident Response Plan
Document Date: [Insert Date]

---

1. Introduction

In light of the 2011 PlayStation Network (PSN) breach, this Incident Response Plan establishes a systematic approach to detecting, containing, eradicating, and recovering from security incidents. This plan is tailored to address the unique challenges of large-scale network security for gaming and online service platforms, aiming to minimize damage, secure user data, and restore services promptly. It also includes an overview of cyberattack types to enhance Sony's understanding of potential threats.

---

2. Detection of Security Incidents

Detection Method: Intrusion Detection System (IDS) and Network Monitoring

- **Description**: Sony employs an Intrusion Detection System (IDS) along with robust network monitoring tools to detect abnormal behavior, unauthorized access attempts, and unusual traffic patterns within the PlayStation Network.
- **Advantages**:
    - Real-time monitoring helps detect and respond to threats immediately.
    - Enables proactive identification of suspicious activity, such as data transfers outside normal patterns or access from unrecognized IP addresses.

---

3. Containment Strategy

Containment Method: Immediate System Isolation and Role-Based Access Control

- **Description**: Upon detecting a security incident, affected servers and segments of the network will be isolated to prevent the spread of any malicious activity. Additionally, Role-Based Access Control (RBAC) is enforced to restrict access only to essential personnel.

- **Steps**:
    - Disconnect affected servers and services from the network until containment is confirmed.
    - Temporarily disable accounts that were compromised or show unusual access patterns.
    - Notify relevant teams to prepare for controlled access and limit network activity in the affected areas.

---

4. Eradication and Recovery

Eradication Steps

1. **Identify and Remove Malicious Files**: Run comprehensive malware and antivirus scans on all affected systems to locate and remove any malicious files or code.
2. **Patch Vulnerabilities**: Investigate vulnerabilities used in the attack and apply necessary patches, including software and system updates to reinforce defenses.
3. **Enhance Security Protocols**: Strengthen firewalls, improve encryption standards, and ensure secure configuration settings to prevent further exploitation.

Recovery Steps

1. **Data Restoration**: Recover affected data from backups that are verified as clean and malware-free.
2. **Testing and Monitoring**: Before bringing the PlayStation Network back online, conduct extensive testing to ensure systems are secure. Monitor all restored systems closely for any suspicious activity.
3. **Stakeholder Communication**: Inform users, partners, and regulatory bodies about the incident, actions taken, and any additional security measures implemented to ensure data integrity.

---

5. Cyberattack Type: Malware

- **Description**: **Malware** refers to malicious software designed to infiltrate and disrupt systems without user consent. In the context of Sony's PSN breach, malware could include trojans or backdoor software that allowed unauthorized access to sensitive customer information, including personal details and potentially credit card data.
- **Detection**: Malware detection relies on antivirus software, IDS, and behavior-based monitoring that identifies unusual data patterns or access requests.
- **Impact**: Malware incidents can compromise the confidentiality and integrity of user data, degrade system performance, and result in user downtime. In Sony's case, the breach

led to the exposure of millions of users' personal information, extensive downtime, and significant financial losses.

---

6. Summary

This Incident Response Plan is crafted to enhance Sony's readiness for potential security incidents on the PlayStation Network. By utilizing IDS and network monitoring for detection, network isolation for containment, and a structured eradication and recovery approach, Sony can better protect its users' data and its platform's integrity. Recognizing and preparing for cyberattack types like malware ensures Sony is equipped to respond effectively and secure its systems against similar incidents in the future.

Comprehensive Security Policy

Organization: Sony PlayStation Network (PSN)
Document Title: Comprehensive Security Policy
Document Date: [Insert Date]

---

1. Introduction

The Sony PlayStation Network (PSN) Comprehensive Security Policy establishes key security rules and guidelines designed to protect user data and network integrity. This policy outlines critical steps to prevent security breaches, respond to incidents effectively, and uphold the principles of the CIA Triad: Confidentiality, Integrity, and Availability.

---

2. Key Security Rules/Guidelines

Rule 1: Access Control and User Authentication

- **Policy**: All PSN employees must use strong, unique passwords and multifactor authentication (MFA) for accessing network resources. Role-Based Access Control (RBAC) is implemented to ensure employees only access data relevant to their roles.
- **Guidelines**:
    - Passwords must be at least 12 characters with a combination of letters, numbers, and symbols.
    - MFA (e.g., SMS or email-based verification) is mandatory for all network accounts.
    - Regularly review and update access rights based on role changes or employee terminations to limit unnecessary access.

Rule 2: Data Encryption

- **Policy**: All sensitive data, including user credentials and payment information, must be encrypted in transit and at rest to protect confidentiality.
- **Guidelines**:
    - Apply AES-256 encryption for stored data and SSL/TLS for transmitted data.
    - Ensure that sensitive data is never transmitted over insecure channels or stored in plaintext.
    - Encrypt all backups and secure them in trusted storage facilities.

Rule 3: Security Audits and Patch Management

- **Policy**: Conduct regular security audits to identify vulnerabilities and keep all systems updated with the latest security patches.
- **Guidelines**:
    - Perform quarterly security audits on critical systems and applications to detect and rectify vulnerabilities.
    - Apply critical patches within seven days and non-critical patches within 30 days.
    - Use automated patch management tools for efficient tracking and installation of updates.

---

3. Incident Response Plan

Objective

The Incident Response Plan is designed to contain, investigate, and recover from security breaches with minimal impact. Key steps are outlined below to manage incidents effectively.

Incident Response Steps

1. **Detection**:
    - Utilize the Intrusion Detection System (IDS) and Security Information and Event Management (SIEM) to monitor for unauthorized access, unusual traffic patterns, or malicious behavior on the network.
2. **Containment**:
    - Immediately isolate affected systems from the network to prevent the spread of malicious activity.
    - Revoke access to compromised user accounts and inform necessary stakeholders of containment actions taken.
3. **Eradication**:
    - Identify the root cause of the breach (e.g., malware, phishing) and remove all malicious components from affected systems.
    - Apply patches to eliminate exploited vulnerabilities and improve defenses against future attacks.
4. **Recovery**:
    - Restore systems from clean backups, ensuring that all systems are secure and functioning correctly.
    - Monitor restored systems for signs of remaining threats and assess them for vulnerabilities.
5. **Post-Incident Review**:
    - Conduct a thorough review of the incident to identify gaps in existing policies.
    - Implement corrective actions based on lessons learned and update the incident response plan if necessary.

---

4. Maintaining the CIA Triad

Confidentiality

- **Access Control** and **Data Encryption** safeguard sensitive user information by limiting access to authorized personnel and protecting data from unauthorized viewing.

Integrity

- **Patch Management** and **Regular Security Audits** prevent unauthorized modifications by ensuring vulnerabilities are promptly addressed, reducing the risk of data alteration.

Availability

- **Incident Response and Recovery** plans ensure that systems are quickly restored following a breach, minimizing downtime and ensuring users have consistent access to PSN services.

Through these policies and procedures, Sony PlayStation Network can uphold the principles of Confidentiality, Integrity, and Availability, ensuring that users' data is protected and that the network remains secure and operational.

3) Hashing, Encryption and Decryption

Hashing Method: MD5
Input: Abinav_101
Output: baaad7c9c8785f0020b7fd2fa3efb4f7

Encryption method: SHA-256
Input: password1
Output: 0b14d501a594442a01c6859541bcb3e8164d183d32937b851835442f69d5c94e

AES Encryption:
Input: Password1
Output: 53616c7465645f5f3cbb4a2907286997da2a613611f25e485d3999d51ba0270f
Passphrase: password

4)

Legal and Ethical Compliance

Objective:
This section outlines Sony PlayStation Network's (PSN) commitment to legal and ethical standards in its incident response practices. By adhering to relevant laws and regulations, PSN ensures compliance, accountability, and protection for user data, helping maintain user trust and uphold ethical responsibilities during and after security incidents.

---

1. Relevant Laws and Regulations

Law 1: General Data Protection Regulation (GDPR)

- **Description**: The GDPR is a European Union regulation that protects the personal data and privacy of EU citizens. It imposes strict requirements on organizations handling data of EU residents, including data security and the mandatory reporting of data breaches within 72 hours.
- **Compliance in Incident Response**:
    - The PSN incident response plan complies with GDPR by ensuring rapid **detection, containment, and reporting** of data breaches involving EU users' personal data. If a breach occurs, the plan includes notifying regulatory authorities and impacted users within the 72-hour window to maintain transparency and limit the risk of harm to users.
    - By implementing strong data encryption policies and limiting data access through Role-Based Access Control (RBAC), PSN safeguards data in line with GDPR's security and confidentiality requirements.

Law 2: California Consumer Privacy Act (CCPA)

- **Description**: The CCPA provides California residents with rights over their personal data, including the right to know, access, and delete information collected by organizations. The CCPA mandates that businesses handling Californians' personal information notify individuals and relevant authorities promptly if a data breach occurs.
- **Compliance in Incident Response**:
    - The incident response plan aligns with CCPA requirements by defining protocols for **prompt containment, user notification, and recovery** when breaches involve California residents' data. Transparency measures are in place to notify affected individuals of the nature of the incident and data impacted.
    - Policies for user access and deletion requests are included, supporting Californians' rights over their personal data, as well as encryption practices to protect data in storage and transit.

---

2. Ethical Considerations

- **Ethical Principle: Transparency and Accountability**
    - **Explanation**: PSN prioritizes transparency by openly communicating with users about data incidents that may compromise their information, acknowledging its responsibility to protect user data and remediate any impacts from a breach.
    - **Application in the Incident Response Plan**: The incident response plan reinforces transparency by mandating timely notifications to users if their data is compromised. Accountability is embedded through regular security audits, ongoing employee training, and a post-incident review process that ensures lessons learned are applied to strengthen data protection and response strategies.

---

3. Upholding Legal and Ethical Standards

- **Legal Compliance**:
    - The PSN incident response plan includes specific measures for rapid detection, containment, eradication, and recovery, ensuring alignment with GDPR and CCPA requirements for data protection and breach response.
    - Through data encryption, restricted access policies, and ongoing audits, PSN fulfills security standards mandated by GDPR and CCPA, demonstrating a proactive approach to data protection.
- **Ethical Compliance**:
    - The incident response plan's commitment to transparent communication exemplifies ethical responsibility by promptly notifying users and stakeholders if their information is compromised, fostering trust and accountability.
    - Ethical obligations are further upheld by enforcing incident response accountability and continuous improvement practices, promoting a culture of responsibility and vigilance in data protection.