Elements of a Proper Incident Report

Executive Summary

Let's consider the `Executive Summary` as the gateway to our report, designed to cater to a broad audience, including non-technical stakeholders. This section should furnish the reader with a succinct overview, key findings, immediate actions executed, and the impact on stakeholders. Since many stakeholders may only peruse the `Executive Summary`, it's imperative to nail this section. Here's a more granular breakdown of what should be encapsulated in the `Executive Summary`:

Section	Description
Incident ID	Unique identifier for the incident.
Incident Overview	Provide a concise summary of the incident's events (including initial detection) and explicitly state its type. Was it a ransomware attack, a large-scale data breach, or both? This should also encompass the estimated time and date of the incident, as well as its duration, the affected systems/data, and the status (ongoing, resolved, or escalated)
Key Findings	Enumerate any salient findings that emerged from the incident. What was the root cause? Was a specific CVE exploited? What data, if any, was compromised, exfiltrated, or jeopardized?
Immediate Actions Taken	Outline the immediate response measures taken. Were the affected systems promptly isolated? Was the root cause identified? Did we engage any third-party services, and if so, who were they?
Stakeholder Impact	Assess the potential impact on various stakeholders. For instance, did any customers experience downtime, and what are the financial ramifications? Was employee data compromised? Was proprietary information at risk, and what are the potential repercussions?

Technical Analysis

This section is where we dive deeply into the technical aspects, dissecting the events that transpired during the incident. It's likely to be the most voluminous part of the incident report. The following key points should be addressed:

Affected Systems & Data

Highlight all systems and data that were either potentially accessed or definitively compromised during the incident. If data was exfiltrated, specify the volume or quantity, if ascertainable.

Evidence Sources & Analysis

Emphasize the evidence scrutinized, the results, and the analytical methodology employed. For instance, if a compromise was confirmed through web access logs, include a screenshot for documentation. Maintaining evidence integrity is crucial, especially in criminal cases. A best practice is to hash files to ensure their integrity.

Indicators of Compromise (IoCs)

IoCs are instrumental for hunting potential compromises across our broader environment or even among partner organizations. It might also be feasible to attribute the attack to a specific threat group based on the IoCs identified. These can range from abnormal outbound traffic to unfamiliar processes and scheduled tasks initiated by the attacker.

Root Cause Analysis

Within this section, detail the root cause analysis conducted and elaborate on the underlying cause of the security incident (vulnerabilities exploited, failure points, etc.).

Technical Timeline

This is a pivotal component for comprehending the incident's sequence of events. The timeline should include:

- Reconnaissance
- Initial Compromise
- C2 Communications
- Enumeration
- Lateral Movement
- Data Access & Exfiltration
- Malware Deployment or Activity (including Process Injection and Persistence)
- Containment Times

Go to Questions

Table of Contents

Introduction to Security Incident Reporting
The Incident Reporting Process
Elements of a Proper Incident Report
Communications
Real-world Incident Report

- Eradication Times
- Recovery Times

Nature of the Attack

Deep-dive into the type of attack, as well as the tactics, techniques, and procedures (TTPs) employed by the attacker.

Impact Analysis

Provide an evaluation of the adverse effects that the incident had on the organization's data, operations, and reputation. This analysis aims to quantify and qualify the extent of the damage caused by the incident, identifying which systems, processes, or data sets have been compromised. It also assesses the potential business implications, such as financial loss, regulatory penalties, and reputational damage.

Response and Recovery Analysis

Outline the specific actions taken to contain the security incident, eradicate the threat, and restore normal operations. This section serves as a chronological account of the measures implemented to mitigate the impact and prevent future occurrences of similar incidents.

Here's a breakdown of what the "Response and Recovery" section typically includes:

Immediate Response Actions

Revocation of Access

- Identification of Compromised Accounts/Systems: A detailed account of how compromised accounts or systems were identified, including the tools and methodologies used.
- Timeframe: The exact time when unauthorized access was detected and subsequently revoked, down to the minute if possible.
- Method of Revocation: Explanation of the technical methods used to revoke access, such as disabling accounts, changing permissions, or altering firewall rules.
- Impact: Assessment of what revoking access immediately achieved, including the prevention of data exfiltration or further system compromise.

Containment Strategy

- Short-term Containment: Immediate actions taken to isolate affected systems from the network to prevent lateral movement of the threat actor.
- Long-term Containment: Strategic measures, such as network segmentation or zero-trust architecture implementation, aimed at long-term isolation of affected systems.
- Effectiveness: An evaluation of how effective the containment strategies were in limiting the impact of the incident.

Eradication Measures

Malware Removal

- Identification: Detailed procedures on how malware or malicious code was identified, including the use of Endpoint Detection and Response (EDR) tools or forensic analysis.
- Removal Techniques: Specific tools or manual methods used to remove the malware.
- Verification: Steps taken to ensure that the malware was completely eradicated, such as checksum verification or heuristic analysis.

System Patching

- Vulnerability Identification: How the vulnerabilities were discovered, including any CVE identifiers if applicable.
- Patch Management: Detailed account of the patching process, including testing, deployment, and verification stages.
- Fallback Procedures: Steps to revert the patches in case they cause system instability or other issues.

Recovery Steps

Data Restoration

- Backup Validation: Procedures to validate the integrity of backups before restoration.
- Restoration Process: Step-by-step account of how data was restored, including any

decryption methods used if the data was encrypted.
- Data Integrity Checks: Methods used to verify the integrity of the restored data.

System Validation

- Security Measures: Actions taken to ensure that systems are secure before bringing them back online, such as reconfiguring firewalls or updating Intrusion Detection Systems (IDS).
- Operational Checks: Tests conducted to confirm that systems are fully operational and perform as expected in a production environment.

Post-Incident Actions

Monitoring

- Enhanced Monitoring Plans: Detailed plans for ongoing monitoring to detect similar vulnerabilities or attack patterns in the future.
- Tools and Technologies: Specific monitoring tools that will be employed, and how they integrate with existing systems for a holistic view.

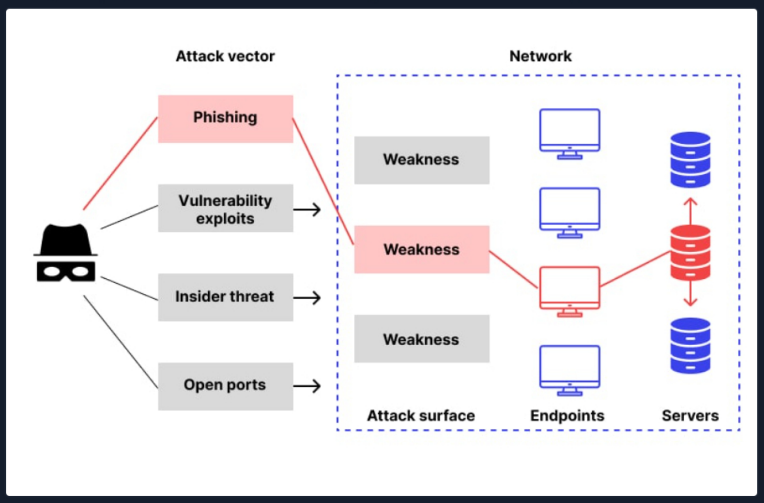
Lessons Learned

- Gap Analysis: A thorough evaluation of what security measures failed and why.
- Recommendations for Improvement: Concrete, actionable recommendations based on the lessons learned, categorized by priority and timeline for implementation.
- Future Strategy: Long-term changes in policy, architecture, or personnel training to prevent similar incidents.

Diagrams

Given that the narrative can become exceedingly complex, visual aids can be invaluable for simplifying the incident's intricacies:

- Incident Flowchart
  - Illustrate the attack's progression, from the initial entry point to its propagation throughout the network.
- Affected Systems Map
  - Depict the network topology, accentuating the compromised nodes. Use color-coding or annotations to indicate the severity of each compromise.
- Attack Vector Diagram
  - Utilize arrows, nodes, and annotations to trace the attacker's navigation and (post-)exploitation activities through our defenses visually.



Appendices

This section serves as a repository for supplementary material that provides additional context, evidence, or technical details that are crucial for a comprehensive understanding of the incident, its impact, and the response actions taken. This section is often considered the backbone of the report, offering raw data and artifacts that can be independently verified, thus adding credibility and depth to the narrative presented in the main body of the report.

The Appendices section may include:

- Log Files
- Network Diagrams (pre-incident and post-incident)
- Forensic Evidence (disk images, memory dumps, etc.)
- Code snippets
- Incident Response Checklist
- Communication Records
- Legal and Regulatory Documents (compliance forms, NDAs signed by external consultants, etc.)
- Glossary and Acronyms

Best Practices

- Root Cause Analysis: Always aim to find the root cause of the incident to prevent future occurrences.
- Community Sharing: Share non-sensitive details with a community of defenders to improve collective cybersecurity.
- Regular Updates: Keep all stakeholders updated regularly throughout the incident response process.
- External Review: Consider third-party cybersecurity specialists to validate findings.

Conclusion

A meticulously crafted incident report is non-negotiable following a security breach or attack. These reports offer an exhaustive analysis of what went awry, what measures were effective, the reasons behind them, and future preventive strategies.

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

+4 Name the type of a diagram that provides an overview of the attack path and the methods used by an attacker. (3 words)

Attack Vector Diagram

Submit