Security Incident Management Policy

Purpose

The purpose of this policy is to establish requirements and plans for reporting and responding to security incidents impacting <Company Name>'s corporate or customer systems.

Scope

This policy applies to all <Company Name> corporate and customer systems, and all employees and contractors.

All workforce members and contractors are required to report any suspicious events, policy violations, or security weakness to the Security Incident Policy owner, [POLICY OWNER]

.

Ownership

[POLICY OWNER]

is responsible for implementing and maintaining this policy.

Policy Statement

Security Incident Management Plan

The Security Incident Management Plan outlines the process for declaring and responding to security incidents, including the roles and responsibilities, and the internal and external communication necessary to take the issue to resolution.

Team Members

As the policy owner, [POLICY OWNER]

shall identify members of the security response teams and direct their roles and responsibilities during an active incident.

Response Steps

The security team triages employee-reported and alert-generated security events, and assigns them either medium, high, or critical severity. For security events of critical severity, the security response team must declare an incident and assemble in a secure, pre-prepared, virtual "war room" to coordinate and execute <Company Name>'s response to the incident.

Phase 1: Declaration and Notification

The declaration phase is focused on investigating whether the reported issue represents an actual or imminent security event or privacy breach. During this phase, the team gains a clear understanding of the nature of the compromise, and determines whether to declare an incident or dismiss the event as a false positive.

Unlike availability and uptime incidents, security incidents are not immediately announced to the whole company. Instead, communication is on a need-to-know basis, and only relevant business stakeholders and individuals whose expertise can aid the investigation are informed of the incident's details, as determined by the incident manager.

At this stage, all other employees may only be told that a security incident is ongoing.

[POLICY OWNER]

is responsible for leading the disaster recovery efforts, involving all necessary SMEs, and communicating to relevant stakeholders.

Phase 2: Containment

The incident response team investigates, patches, and scrubs data and playbooks in order to limit and mitigate the effects of the compromise. Actions may also include scrubbing system backups, disabling or reconfiguring networks, completely disabling an affected computing resource, as well as disabling or rotating credentials.

Phase 3: Retrospective and prevention

The Retrospective phase establishes a blame-free environment that allows all parties to gain a clear understanding of the incident and its resolution. A retrospective meeting should occur within 1 week of a disaster recovery event.

Retrospective meetings must definitively outline the root case and response timeline, along with any lessons, as well as action items for improving tooling, process, and software. Following the meeting, a retrospective report outlining key items should be created and shared with all participants and relevant stakeholders. Depending on customer impact, a customer-facing version of the report may be created and shared with customers as required by legal obligations and customer agreements.

The incident must be reported to the relevant law enforcement agency and/or customer if required by contractual or regulatory obligations. The team must receive legal counsel prior to reporting.

Documentation and Metrics

[POLICY OWNER]

ensures that all relevant information is verified and logged in <Company Name>'s project management tool. <Company Name> tracks the numbers, types, response times, resolution times, and cost of information security incidents over time in order to surface any trends across the business.

Security Incident - Testing

The Security Incident process is tested at least once a year if an actual incident has not occurred.

NIST recommends that the testing process include both technical tests as well as tabletop testing exercises, in which team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular situation, and a facilitator guides participants through a discussion of one or more scenarios. Incident testing should be followed by a retrospective meeting that produces both lessons and action items similar to those produced by a real event.