Security Information Breach Notification Policy

Nave

21 Apr 2019

Overview of Workflow

When a security incident is detected or reported, key first steps are to (1) contain the incident, (2) initiate an investigation of its scope and origins, and (3) decide if it qualifies as a Breach.

Identification

The identification phase of incident response has as its goal the discovery of potential security incidents and the assembly of an incident response team that can effectively contain and mitigate the incident.

Any employee of Nave may identify a potential security incident by observing suspicious system behavior or though external complaint/notification, or other knowledge of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of data.

Employees that suspect that the system data has been subject to accidental or unlawful destruction, loss, or alteration, or unauthorized disclosure or access, must immediately report the situation to sonya@getnave.com. Once the incident handler is aware of a potential incident, he will alert local system administrators. The incident handler will quarantine compromised hosts at the time of notification.

Verification

The incident handler verifies that the triggering alert is not a false positive. The incident handler will double-check the triggering alert, and correlate it against other alerting systems when possible.

The system administrator should provide a detailed description of the data at risk, including approximate numbers of unique data elements at risk, and the number, location, and type of files it is stored in. The system should be effectively remediated before the quarantine is lifted.

Containment

If the host cannot immediately be removed from the network, the incident handler will initiate a full-content network dump to monitor the attacker's activities and to determine whether interesting data is leaking during the investigation.

Whenever possible, the incident handler should eliminate attacker access via performing network quarantine at the time of detection. The incident handler will collect data from system administrators in order to quickly assess the scope of the incident, including:

- Preliminary list of compromised components
- Preliminary list of storage media that may contain evidence
- Preliminary attack timeline based on initially available evidence

The incident handler will perform an analysis of all data that is suspected of containing evidence. He will create an analysis plan to guide the next phase of the investigation. This is the most time-sensitive and also the most contextually-dependent phase of the investigation. The actions that need to be taken will depend on the nature and quantity of data at risk, and the suspected profile of the attacker. The most important goals of this phase are to eliminate attacker access to the systems as quickly as possible and to preserve evidence for later analysis.

Additionally, this is the phase where the incident handler works most closely with system administrators and system owners. During this phase, they are expected to take instruction from the incident handler and perform on-site activities such as attacker containment.

Analysis

The analysis phase is where an in-depth investigation of the available network-based and host-based evidence occurs. The primary goal of the analysis is to establish whether there is a reasonable belief that the attacker successfully accessed data on the compromised system.

Secondary goals are to generate an attack timeline and ascertain the attackers' actions. All analysis steps are primarily driven by the incident handler, who coordinates communications between other stakeholders, including system owners, system administrators, and relevant compliance officers. Questions that are relevant to making a determination about whether data was accessed without authorization include:

- Suspicious Network Traffic: Is there any suspicious or unaccounted for network traffic that may indicate data exfiltration occurred?
- Attacker Access to Data: Did attackers have privileges to access the data or was the data encrypted in a way that would have prevented reading?
- Evidence that Data Was Accessed: Are file access audit logs available that show whether the files have been accessed post-compromise?
- Length of Compromise: How long was the host compromised and online?
- Method of Attack: Was a human involved in executing the attack or was an automated "drive-by" attack suite employed? Did the tools found have capabilities useful in finding or exfiltrating data?
- Attacker Profile: Is there any indication that the attackers were data-thieves or motivated by different goals?

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the incident handler may consider the following factors, among others:

- Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information;
- Indications that the information has been downloaded or copied;
- Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported;

At the conclusion of the analysis, but before the final report is written, a peer review should be requested of the other technical staff. Then, the write-up of the notes should be completed, including conclusions, and processed source materials should be archived.

Recovery

The primary goal of the recovery phase is to restore the compromised host to its normal business function in a safe manner.

The system administrators will remediate the immediate compromise and restore the host to normal function. They will make a short-term system and business process changes to prevent further compromise and reduce operating risk.

Internal Reporting

The final report serves two main purposes. First, a recommendation is made to the relevant compliance officers as to whether the incident handler and the responsible officials feel there is a reasonable belief that application data was subject to accidental or unlawful destruction, loss, or alteration, or unauthorized disclosure or access. The report must be made in the most expedient time possible and without unreasonable delay. Second, a series of mid-term and long-term recommendations are made to the owners of the compromised data, including responsible management, suggesting improvements in technology or business process that could reduce operating risk in the future.

The incident handler will draft the final report after the investigation is complete. Preliminary reports should be avoided whenever possible since working conclusions can change substantially through the course of an investigation.

Data Retention

The incident handler will archive the final report in case it is needed for reference in the future; reports must be retained for 6 years.

Incident notes should be retained for 6 months from the date that the report is issued. This includes all processed investigation materials.

Raw incident data should be retained for 30 days from the date that the report is issued.