Recognize roles and responsibilities during escalation

You previously learned about various incident classification types and how those incidents can impact an organization.

This reading will discuss the roles of the various team members who are a part of the incident escalation process. Keep in mind that not all organizations are alike, and some roles and responsibilities may be identified using different terminology and definitions.

Data owners

A data owner is the person that decides who can access, edit, use, or destroy their information. Data owners have administrative control over specific information hardware or software and are accountable for the classification, protection, access, and use of company data. For example, consider a situation where an employee gains unauthorized access to software they do not need to use for work. This kind of security event would be escalated to the data owner of that software.

Data controllers

Data controllers determine the procedure and purpose for processing data. This role largely focuses on collecting the personal information of customers. The data controller determines how that data is used. The data controller also ensures that data is used, stored, and processed in accordance with relevant security and privacy regulations. If sensitive customer information was at risk, that event would be escalated to data controllers.

Data processors

Data processors report directly to the data controller and are responsible for processing the data on behalf of the data controller. The data processor is typically a vendor and is often tasked with installing security measures to help protect the data. Data processing issues are typically escalated to the individual who oversees the third-party organization responsible for data processing.

Data custodians

Data custodians assign and remove access to software or hardware. Custodians are responsible for implementing security controls for the data they are responsible for, granting and revoking access to that data, creating policies regarding how that data is stored and transmitted, advising on potential threats to that data, and monitoring the data. Data custodians are notified when data security controls need to be strengthened or have been compromised.

Data protection officers (DPOs)

Data protection officers are responsible for monitoring the internal compliance of an organization’s data protection procedures. These individuals advise the security team on the obligations required by the organization's data protection standards and procedures. They also conduct assessments to determine whether or not the security measures in place are properly protecting the data as necessary. DPOs are notified when set standards or protocols have been violated.

Key takeaways

Incident escalation requires various members of a security team to act as one. Entry-level analysts should be familiar with the roles and responsibilities of different team members on the security team. As an entry-level analyst, you will typically escalate incidents to your direct supervisor. However, it’s still important to have an understanding of the different team members as you move forward in your security career because it will help you recognize which incidents should be reported to whom.

Revision #1
Created 9 January 2024 15:06:05 by naruzkurai
Updated 9 January 2024 15:06:13 by naruzkurai