Discussion-6 Incident Response

Discussion Topic:

Establishing a plan for responding to a data breach, complete with clearly defined roles and responsibilities, will promote better response coordination and help educational organizations shorten their incident response time. Conduct research on efficient incident handling techniques and share your findings with your class. In your response, also include any personal experience you have with incident response during a potential data breach. If you do not have personal experience with incident responses, share an example of a recent data breach (within the last three years).

My Post:

Hello Class,

To create a responding to a data breach to help educational organizations shorten their incident response time, I looked at NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide (NIST, 2021) for security incident response plan standards, and at Carnegie Mellon University's (CMU) computer security Incident response plan (CMU Information Security Office, 2023) as a real example of an educational institution security incident response plan.

Based on the information gathered in the two documents, the best approach to help educational organizations shorten their incident response time is to separate the core security response strategy into three phases that follow a recursive process similar to a software development lifecycle.

1. The preparation phase involves creating or reevaluating policies, procedures, and communication plans. It is important that these policies, procedures, and communication plans are in place before an incident occurs, and that the right tools and staff are available and know how to respond quickly and efficiently to it.
2. The detection and analysis phase involves identifying occurring or occurred incidents. This can be done by using security tool alerts, and by real-time security report gathering in the form of data, alerts, and warnings from staff or from external parties. Note that once an incident is detected, it needs to be analyzed to understand the scope of the incident and potential remaining or ongoing risks.
3. The containment, eradication, and recovery phase involves limiting and containing the damage done by the incident by isolating affected systems. Once the damage is contained, the incident (threat) needs to be eradicated (fully removed) by patching the issues. Finally, after the threat is fully removed, the damaged system needs to be restored to normal operation, and the incident occurrences, damage done, eradication method used, and recovery method implemented need to be documented as “lessons learned.”

A plan is only as good as the people who execute it! Thus, it is crucial to establish an incident response team and define the role of its team members. The Computer Emergency Response Team (CERT) model is the best fit for educational organizations’ incident response plans. CERTs respond to security incidents in real-time and “tend to have a broader charter, responding whether systems are put out of action by

acts of nature, accidents, or hostile attackers. CERTs, too, tend to be more involved with broader disaster recovery efforts than a team focused primarily on security-related incidents" (uCertify, n.d., section 110). The CMU Information Security Office (2023) plan defines the role of its incident response team member as follows:

- The incident response coordinator acts as the contact liaison, ensuring everyone is on the same page.
- The incident response handlers are IT staff who are in charge of investigating the incident, preserving and documenting the evidence (incident information and data), and performing the hands-on work of damage containment, threat eradication, system recovery, and incident documentation. Note that some of the team members are also in charge of detecting and identifying incidents as they occur.
- Decision-makers from various departments, usually the head of departments, who have the authority to make critical choices during a crisis, such as shutting down critical systems.

The CMU plan response team role definition is excellent and provides a template that can be used by any educational organization.

A good example of a real incident involving a data breach happened on May 31, 2023, when MOVEit, a popular file transfer software, suffered data breaches via zero-day flaws (ORX News, 2024). MOVEit first identifies the vulnerability (May 31) in its transfer that could lead to escalated privileges and potential unauthorized access to the environment. The issue was a SQL Injection (CVE-2023-34362). Then Progress, the parent company of MOVEit, "promptly launched an investigation, alerted MOVEit customers of the issue and provided immediate mitigation steps, followed by the development and release of a security patch, all within 48 hours" (Progress, n.d., -May 31, 2023-). Additional related SQL Injection vulnerabilities (CVE-2023-34362) were identified on June 9, 2023. In light of the newly discovered vulnerabilities, Progress partnered with third-party cybersecurity experts to investigate, as a result, additional vulnerabilities were identified (distinct from the May 31, 2023, vulnerability). After releasing several patches, additional vulnerabilities were identified on June 15-16, 2023, prompting Progress to shut down HTTP and HTTPS traffic for MOVEit Cloud…
By June 18, 2023, Progress claims that all the vulnerabilities have been patched, and the HTTP and HTTPS traffic for MOVEit Cloud was restored

Sorry for the long post, a lot of information to unpack.

-Alex

References:

CMU Information Security Office (2023). Computer Security Incident Response Plan. Carnegie Mellon University.

NIST (2021). *NIST SP 800-61*. National Institute of Standards and Technology (NIST) – US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

ORX News (2024). *MOVEit transfer data breaches Deep Dive.* O.R.X. https://orx.org/resource/moveit-transfer-data-breaches

Progress (n,d). *MOVEit Transfer and MOVEit Cloud Vulnerability.* Progress. https://www.progress.com/trust-center/moveit-transfer-and-moveit-cloud-vulnerability

uCertify (n.d). Lesson 10: Incident Response and Recovery. *(ISC)² SSCP Certification Training Guide*. uCertify. ISBN: 976164493776.