Incident Response Plan a Critical Component of Cyber Security

By Almi Dumi, CISO, eMazzanti Technologies

A security breach can have devastating effects on your organization. In fact, a recent report from IBM lists the average cost of a data breach in the United States at $8.64 million. However, organizations that define and follow an incident response plan for all security incidents can mitigate exposure and risk.

Consequently, organizations should have a plan ready before an incident occurs. An incident response plan that begins with 24/7/365 monitoring will shorten the response time and increase the chances of a successful recovery. This post outlines the six phases of a typical incident response plan.

Breach vs. Incident

News reports refer to both "security incidents" and "security breaches." However, the two terms have different meanings. Understanding the difference between them will help organizations craft an appropriate response.

By definition, a security incident refers to a violation of an organization's security policies, an attempt to compromise data confidentiality, integrity and/or availability. A security breach, on the other hand, involves unauthorized access to data or systems. Thus, while all data breaches begin as security incidents, not all incidents necessarily lead to data compromise.

For example, the presence of malware in the system constitutes a security incident. But the presence of malware alone does not constitute a security breach. If the response team acts quickly to contain the malware, they can keep outside actors from gaining unauthorized access to data.

1. Preparation

Phase one of the incident response plan involves identifying the incident response team members, defining their roles, and equipping them for the task. When organizations identify response team members and responsibilities ahead of time, they can jump into action quickly.

As soon as an incident occurs, confirm contact information for each incident response team member. Assign specific tasks to each person and determine the role of executive management. Determine if legal counsel and insurance representatives need to be notified and with what frequency. Then make sure team members have the services, tools, and resources they need.

2. Identification

With the team assembled, assess the incident to determine its scope. Identify the systems involved and determine the extent of the damage. Be certain to preserve evidence to allow for forensic analysis. In addition, identify any regulatory requirements that may involve legal action. For instance, some regulations include notification clauses.

3. Containment

Once you have identified the nature of the incident, move quickly to minimize exposure and contain the spread of infection. Isolate the incident by disconnecting infected assets. Then implement security measures to strengthen your security posture. These could include an organization-wide mandatory password change, MFA and revised security policies.

4. Eradication

With the infection contained, begin the eradication process. Start with a root cause analysis to identify and eliminate the root cause of the incident. Remove all malicious code and harden the systems. This includes applying any applicable updates and security patches.

5. Recovery

In the recovery phase, you will soon determine the effectiveness of your business continuity and disaster recovery planning. Recover data from backups and restore compromised systems. Then evaluate your backups and take new images.

6. Lessons Learned

Before too much time elapses, gather the team to discuss the lessons learned and how to guard against similar situations in the future. Review the timeline of the incident and the response, identifying the efforts taken to recover. Ask what worked well and what improvements can be made. In the process, communicate honestly and refrain from pointing fingers.

Develop a Proactive Incident Response Plan

Hopefully, you follow many of these guidelines already. Before another security incident occurs, review your incident response plan. The cyber security experts at eMazzanti can help you identify gaps in your response strategy and then guide you through the process of developing and testing a plan that fits your organization.