Lodestone

MAY 2022

STATE OF CYBER

monthly newsletter

YOU PLAY LIKE YOU PRACTICE

If someone asked your IT teams how they would respond to an incident and walk step-by-step through the process, how well do you think they would respond? Would their answers align with the procedures documented in your runbooks or playbooks? If your IT teams were tested via a random, live exercise, how would they perform? Just as physical exercise provides the body with the conditioning to handle additional stress, cybersecurity exercises help your company build and strengthen critical reflexes that could minimize or even prevent cyberattacks.

Cybersecurity exercises generally fall under one of three categories: tabletop, live, and hybrid. In tabletop exercises, participants discuss how they would react to a theoretical attack or situation. Organizations might use tabletop exercises to establish relationships between different teams, identify weaknesses or gaps in recovery processes, or simply test the readiness of their teams in an informal environment. Live (i.e., functional) exercises are used to identify how well-equipped IT teams are to perform security duties. They provide more realistic training and may involve adversarial scenarios such as a red team carrying out a specific attack. Lastly, there are hybrid exercises. These are tabletop exercises that are combined with live, simulated events to maximize realism.

How does leadership know if the exercises being conducted are working? A good measure of a cybersecurity team's proficiency is its state of readiness. The ideal state of readiness is one in which the response to an incident is reflexive – everyone involved acts quickly and decisively because they understand their roles and responsibilities. Another good measure is a team's ability to take on increasingly challenging scenarios, and how they respond when circumstances place them outside of their comfort zones. Leadership should understand that a cybersecurity team's performance during an exercise (especially a live exercise) is usually the best indicator of how they would perform during an actual incident. A common adage among coaches is that "you play like you practice." When an incident is threatening your organization, how will your team play?

MITRE ATT&CK UPDATES – APRIL 2022

MITRE ATT&CK, a knowledge base of threat actor tactics and techniques based on observations around the globe, has released its latest updates. Improvements to this community-based cybersecurity resource now include explicit links to the data sources that should be collected each time suspicious artifacts are detected within an environment.

JIRA SECURITY ADVISORY 2022-04-20

A critical vulnerability in Jira's web authentication framework, Jira Seraph, could allow a remote, unauthenticated user to bypass authentication. Organizations using Jira Server and Data Center should verify which version they have and install patches immediately.

CLOUDFLARE THWARTS RECORD DDOS ATTACK PEAKING AT 15 MILLION REQUESTS PER SECOND

Cloudflare identified one of the largest HTTPS distributed denial-of-service (DDoS) attacks on record, in which 15.3 million requests per second were sent in an attempt to severely disrupt communications to an unnamed Cloudflar customer. While Cloudflare was able to defend against this attack, the primary use of data centers to perform this attack represented unorthodox threat actor behavior.

APT CYBER TOOLS TARGETING ICS/SCADA DEVICES

An alert has been released by the Cybersecurity and Infrastructure Security Agency (CISA) that provides detection and mitigation recommendations to harden systems against the latest threats to ICS and SCADA devices. An APT group has developed custom tools to target Schneider, OMRON, and Open Platform Communications Unified Architecture ICS/SCADA devices.

2021 TOP ROUTINELY EXPLOITED VULNERABILITIES

The CISA has rounded up the most commonly exploited vulnerabilities observed during the past year. Three of these top exploited vulnerabilities were also in the same list for 2020, indicating that organizations are being breached with preventable vulnerabilities in unpatched software.