CYBERSECURITY & TECH LEADERSHIP FOR START-UP, EMERGING & BEYOND
vCISO vCTO vCIO Consultants Experts

Riskigy vCISO Team Resources: Cybersecurity Tabletop Exercise Series

Our Scenarios to Help Prepare Your Incident Response Team

Exercise Title:

Network Compromise

TTE Scenario:

How would you react to reports from concerned citizens who have been sending you emails stating that one of your websites has been periodically inaccessible? Additionally, you have received information that a well-known hacktivist has tweeted your website's address with the hashtag #Down and has promised to carry out more attacks in the coming days.

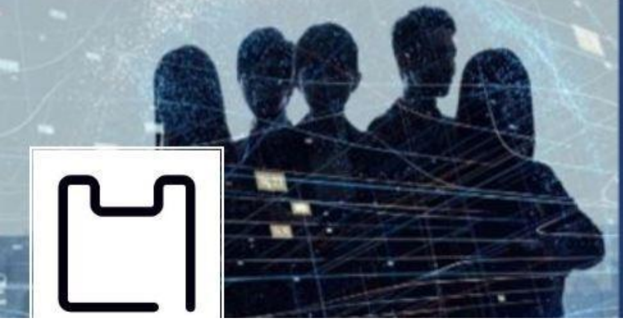
Cyber Attack:

The situation described in this scenario is indicative of a Distributed Denial of Service (DDoS) attack. In a DDoS attack, the attacker targets a network by flooding it with a large volume of traffic or requests from multiple sources, overwhelming the network's resources and making it unavailable to legitimate users. While a DDoS attack may not necessarily result in the attacker gaining access to the network or stealing data, it can cause significant disruption and damage to the network and the organization's operations. The hacktivist's tweet with the hashtag #Down suggests that they may have initiated the DDoS attack and may continue to target the website with further attacks in the future.

Incident Impact:

- Reputation damage: Network compromise attacks can damage an organization's reputation and erode customer trust, which can impact its long-term organization prospects.
- Increased cybersecurity risk: A network compromise attack can expose weaknesses in an organization's cybersecurity posture, increasing the risk of future attacks and making it more challenging to protect against them.
- Additional costs: An organization may incur additional costs associated with mitigating a DDoS attack, such as hiring cybersecurity experts, investing in additional infrastructure, or paying for cloud-based mitigation services.
- Service disruption or downtime: A DDoS attack can overwhelm a website or online service with traffic, causing it to become unavailable to legitimate users. This can result in lost revenue, reduced productivity, and damage to the organization's reputation.

Riskigy



Lesson to Learn:

- How can you find out the type of DDoS?
- What measures can you immediately put in place to reduce the impact?
- Who do you notify internally? Who do you notify externally?
- What functions could be impacted by this attack?
- What preventative measures can be taken to prevent this in the future?