CYBERSECURITY & TECH LEADERSHIP FOR START-UP, EMERGING & BEYOND

vCISO vCTO vCIO Consultants Experts

Exercise Title:

Service Compromise

TTE Scenario:

An attacker gains unauthorized access to your organization's database containing sensitive customer information, such as names, email addresses, and credit card numbers. The attacker uses this information to launch a phishing attack, sending fake emails to customers that appear to be from the organization and requesting that they update their account information. Customers who fall for the scam unwittingly provide the attacker with their login credentials, which the attacker then uses to access their accounts and steal additional information or make unauthorized purchases.

Cyber Attack:

This compromise of the organization's service can result in financial losses for both the organization and its customers, damage to the organization's reputation, and increased cybersecurity risk for all parties involved. This scenario is an example of a phishing attack. Phishing attacks typically target an organization's customers or employees and use social engineering tactics to gain unauthorized access to their accounts or sensitive information. If successful, a phishing attack can compromise an organization's services by allowing attackers to access sensitive data or systems, steal intellectual property, or install malware on the victim's device.

Incident Impact:

➢ Legal and regulatory consequences: A service compromise attack can result in legal and regulatory consequences if the organization is found to have inadequate security measures in place or if the attack results in harm to customers.

➢ Regulatory noncompliance:A phishing attack can result in noncompliance with regulatory requirements, such as data privacy or breach notification laws.

➢ Breach: The impact of a breach can vary depending on the data and personnel affected. Employees in departments such as financial accounting and human resources typically have access to highly sensitive and confidential data.

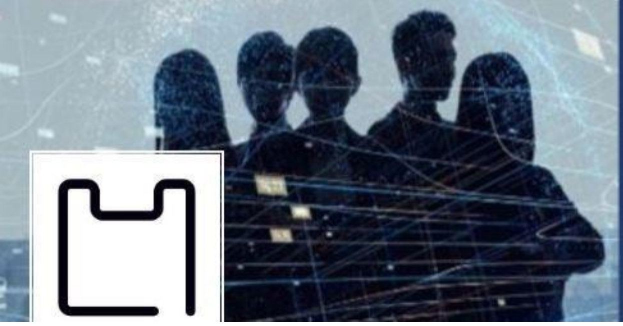
➢ Untrained staff: It is crucial for organizations to provide employee education and training on cybersecurity best practices, including how to identify and avoid phishing emails, to reduce the risk of these types of attacks.

Lesson to Learn:

➢ What does your policy say about reporting suspicious emails?

➢ What do you do if individuals within your organization click on malicious links found in emails?

Riskigy



- How do you educate users on identifying phishing emails and social engineering attempts?
- Do your end users know what to do with a suspicious email?
- How do you notify IT staff?