??????????????????

??????????????????

???Narayan Guntha

A data breach/attack is a cybersecurity incident that requires an incident handling/response team to investigate an alert. The organization needs a cybersecurity team for continuous monitoring of threats and implementing of security policies related to endpoint/perimeter devices, applications, and third-party security.

Data breaches occur in an increasingly number of ways. It can be challenging and downright intimidating for any business to stay on top of all of them. Here are three types that have been in the news lately, prompting a number of queries from businesses for our own cybersecurity client team:

- Play ransomware actors are using a new exploit method to bypass Microsoft's ProxyNotShell mitigations and gain initial access to Exchange servers.
- WordPress sites are under attack from a new Linux malware that is exploiting more than 30 content management system flaws.
- A BitRAT malware campaign is now using stolen sensitive bank data for phishing.

But this does not mean an organization needs a unique approach to fight and mitigate against every single kind of breach. To demonstrate this point, I am going to include here investigation and mitigation steps for the scenarios I’ve listed above. The below steps listed can be integrated into tools like security operations (SecOps) and security orchestration, automation and response (SOAR) to automate the incident response steps. This helps ensure that no aspect of an incident is overlooked and that help teams respond to incidents effectively. These steps are frequently updated based on the lessons learned from new data breaches.

Investigation Steps/Incident Response

For critical/high-severity issues, the Incident response/security operations center (SOC) team must identify the cause of breach/incident and involve the information security (InfoSec) and network teams and concerned stake holders to resolve the incident.

Based on the severity of incident, the incident response team sends out a breach notification to higher management. A war room is set up to investigate the most severe breaches. The InfoSec team maintains appropriate incident response playbook/procedures.

The National Institute of Standards and Technology (NIST)/SysAdmin, Audit, Network, and Security (SANS) framework can be used as a reference to investigate different types of attacks/breaches. The NIST incident response lifecycle breaks incident response down into these main phases:

- Preparation.
- Detection and analysis.
- Containment, eradication, and recovery.
- Post-event activity.

The above phases are useful for security teams implementing incident handling playbooks for various types of attacks.

The NIST/SANS framework also identifies investigation steps for the three types of breaches we have identified above. These steps can be further modified based on the lessons learned.

- Check if there are any high volumes of admin logins.
- Identify if there is any communication to URLs and domains/intrusion prevention systems (IPS) from a particular machine/application.
- Verify any spam/malicious campaign at the organization level and see if any emails are successfully delivered and accessed by users.
- Check and identify the services/process running on the infected machines in order to identify the traffic generated by the services/process
- Look for any intrusion detection system (IDS)/intrusion prevention system (IPS)/web application firewall (WAF) signature alerts on the application/internet protocol (IP) address.
- Scan the application/systems to check for recent activity of file download/execution.
- Check the application logs to understand if any suspicious requests are passed at application level.

- Check the traffic logs to verify any malicious/command and control traffic from the machines/servers.

- Verify any bypass of credentials/security tools on the machine/servers.

Mitigations Steps

Of course, it’s essential that any security team understand how to reduce or eliminate the potential impacts or consequences of an identified threat, including the ones we have cited above. This is where mitigation steps come into play.

Below are the some of the mitigation steps for the types of breaches identified at the beginning of this post:

- Remote PowerShell/other Shell prompts should be disabled.

- Encryption feature should be enabled on the systems (end user machine/servers)

- All the machines/servers need to be installed with EDR/anti-virus (AV) tools

- If possible, disable direct remote access to development/product environment.

- All the machines/servers/network devices should be scanned with a virtual machine (VM) tool.

- Vulnerabilities need to be patched on time, where the exploitation can be reduced for applications and operating systems. Note that vulnerability to exploitation can be reduced when all applications are up to date.

- Application development should follow secure coding practices.

- Application must go through a penetration test before being deployed into production.

- Third-party software should be upgraded regularly to avoid zero-day attacks.

- Make sure all required security controls are implemented at both endpoint and network level.

- For better security, applications should be configured behind a WAF so that controls can be implemented at each module of the application.

- Application hardening controls should be implemented (WordPress).

- In order to analyze application attacks, log capture needs to be enabled on applications.

- Network hardening rules should be implemented for both development and production systems.

- Users should be educated in identifying the spam/phishing emails.

Security teams can align with the MITRE ATT&CK framework, which focuses on different threat actors that can lead to the exploit of any network. Doing so will help in early detection and mitigation of breaches/attacks. The MITRE ATT&CK framework has different tactics and techniques that can be used for threat intelligence and hunting in the organization and can identify the loopholes in the infrastructure.

There are security information and event management (SIEM) technologies that can be integrated with MITRE ATT&CK framework or EDR detections. This will allow an organization to quickly detect and respond to the threats.

How Centific Can Help

Cybersecurity incidents and breaches can undermine any business, which may lead to data or monetary loss and damage to an organization’s reputation. Organizations need to align with standard security policies and procedures and timely security audits across the organization to minimize the risk. Centific can help.

At Centific, we define a comprehensive cyber strategy to reduce risk and help establish a secure enterprise. Our digital safety framework mitigates against various security threats and prepares enterprises to become more vigilant against vulnerabilities. Our InfoSec team can conduct regular tabletop exercises to help organizations consider different risk scenarios and prepare for potential cyber threats. We constantly mitigate against cybersecurity risks by implementing industry standard best practices such as vulnerability assessments, phishing simulations and anti-virus/malware controls. Contact us to learn more.

-

-
-
-
-
-