

Common Information Security Incidents and How to Respond

01

UNAUTHORIZED ACCESS

How to Respond:

- Immediately isolate the affected systems and disable compromised accounts.
- Review access logs to determine the scope and method of access.
- Strengthen authentication protocols, including multi-factor authentication (MFA).
- Conduct a thorough investigation to identify any data breaches or exfiltration.

02

PRIVILEGE ESCALATION ATTACK

How to Respond:

- Audit user permissions to ensure users have appropriate access levels.
- Disable compromised accounts and reset all associated credentials.
- Implement least privilege access control and regularly review privileges.
- Analyze logs to identify the attack vector and prevent future escalation.

03

INSIDER THREAT

How to Respond:

- Immediately restrict access to sensitive data for the suspected insider.
- Monitor for unusual activities or unauthorized access by employees.
- Perform a comprehensive audit of user actions and access logs.
- Implement data loss prevention (DLP) tools and encourage whistleblowing for unethical behavior.

04

PHISHING ATTACK

How to Respond:

- Educate employees on phishing tactics and train them to recognize phishing emails.
- Isolate affected systems and remove any malicious email attachments or links.
- Reset passwords for affected accounts and monitor for suspicious activity.
- Report the phishing attack to relevant authorities, such as your email service provider or law enforcement.

05

MALWARE / RANSOMWARE ATTACK

How to Respond:

- Isolate infected systems to prevent the malware from spreading.
- Identify the type of malware and run antivirus/anti-malware scans to remove it.
- Restore data from backups (if available) to minimize data loss.
- Communicate with the incident response team and law enforcement if a ransomware demand is involved.

06

DOS / DDOS ATTACK

How to Respond:

- Monitor network traffic to detect unusual spikes or patterns that may indicate an attack.
- Work with your ISP to block malicious IP addresses or use DDoS mitigation services.
- Configure web access firewalls (WAF) and rate-limiting techniques to prevent future attacks.
- Activate redundant systems to minimize downtime and maintain service availability.

07

MAN-IN-THE-MIDDLE ATTACK

How to Respond:

- Disconnect affected systems from the network and reset all encryption keys.
- Reinforce the use of HTTPS and enforce secure communication protocols across systems.
- Verify the integrity of data that was transmitted during the attack.
- Investigate how the attacker gained access to the communication channel and strengthen network security.

08

PASSWORD ATTACK

How to Respond:

- Force password resets for all affected accounts, especially those with weak or compromised passwords.
- Enable multi-factor authentication (MFA) to add an additional layer of protection.
- Monitor for brute-force attempts and block IPs that show suspicious behavior.
- Educate users on creating strong, unique passwords and regularly changing them.

09

WEB APPLICATION ATTACK

How to Respond:

- Perform a vulnerability scan to identify exploited weaknesses and patch them immediately.
- Apply web application firewall (WAF) rules to block malicious requests.
- Review application logs to understand how the attack occurred and trace any damage.
- Implement secure coding practices and conduct regular code audits to prevent future vulnerabilities.

10

ADVANCED PERSISTENT THREAT (APT)

How to Respond:

- Identify and isolate the threat to prevent further access or data exfiltration.
- Conduct a deep forensic investigation to understand the attack lifecycle and the extent of the breach.
- Implement stronger perimeter defenses and network segmentation to limit attacker movement.
- Monitor for unusual network traffic and set up honeypots to detect and mislead the attacker.