Applying the NIST CSF Framework

Summary

The company experienced a security event when all network services suddenly stopped responding. The cybersecurity team found the disruption was caused by a distributed denial of services (DDoS) attack through a flood of incoming ICMP packets. The team responded by blocking the attack and stopping all non-critical network services, so that critical network services could be restored

Identify

A malicious actor or actors targeted the company with an ICMP flood attack. The entire internal network was affected. All critical network resources needed to be secured and restored to a functioning state.

Protect

The cybersecurity team implemented a new firewall rule to limit the rate of incoming ICMP packets and an IDS/IPS system to filter out some ICMP trac based on suspicious characteristics.

Detect

The cybersecurity team configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets and implemented network monitoring software to detect abnormal trace patterns.

Respond

For future security events, the cybersecurity team will isolate a critical systems and services that were disrupted by the event. Then, the team will analyze network logs to check for suspicious and abnormal activity. The team will also report all incidents to upper management and appropriate legal authorities, if applicable.

Recover

To recover from a DDoS attack by ICMP Flooding, access to network services need to be restored to a normal functioning state. In the future, external ICMP flood attacks can be blocked at the firewall. Then, all non-critical network services should be stopped to reduce internal network trac. Next, critical network services should be restored first. Finally, once the flood of ICMP packets have timed out, all non-critical network systems and services can be brought back online

Summary

This morning, an intern reported to the IT department that she was unable to log in to her internal network account. Access logs indicate that her account has been actively accessing records in the customer database, even though she is locked out of that account. The intern indicated that she received an email this morning asking her to go to an external website to log in with her internal network credentials to retrieve a message. We believe this is the method used by a malicious actor to gain access to our network and customer database. A couple of other employees have noticed that several customer records are either missing or contain incorrect data. It appears that not only was customer data exposed to a malicious actor, but that some data was deleted or manipulated as well.

Identify

The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that an intern's login and password were obtained by a malicious attacker and used to access data from our customer database. Upon initial review, it appears that some customer data was deleted from the database.

Protect

The team has implemented new authentication policies to prevent future attacks: multi-factor authentication (MFA), login attempts limited to three tries, and training for all employees on how to protect login credentials. Additionally, we will implement a new protective firewall configuration and invest in an intrusion prevention system (IPS).

Detect

To detect new unauthorized access attacks in the future, the team will use a firewall logging tool and an intrusion detection system (IDS) to monitor a incoming traffic

Respond

The team disabled the intern's network account. We provided training to interns and employees on how to protect login credentials in the future. We informed upper management of this event and they will contact our customers by mail to inform them about the data breach. Management will also need to inform law enforcement and other organizations as required by local laws.

Recover

The team will recover the deleted data by restoring the database from last night's full backup. We have informed staff that any customer information entered or changed this morning would not be recorded on the backup. So, \re-enter that information once it has been restored from last night's backup.