**Applying the NIST CSF**

There are five core functions of the NIST CSF framework: identify, protect, detect, respond, and recover.



This morning, staff reported to the IT department that she was unable to log in to his portal. 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 staff indicated that she received an email this morning asking him to go to an external website to log in with his internal network credentials to retrieve a message. A couple of other employees have noticed that several customer records are either missing or contain incorrect data. Afterwards, the malicious actor used the compromised credentials to access data on user accounts. We believe that no sensitive information was stolen, but the breach may have disclosed and modified customers’ names and email addresses.

|  |  |
| --- | --- |
| Identify | The incident management team will access the devices on the network and access policies involved in the attack to ensure the attack surface is at the least minimal. The team found that a login and password were obtained by a malicious attacker and used to access data from our customer database. We also noticed logins outside working hours, indicating a possibility of a malicious actor. |
| Protect | We have decided to add new authentication policies to prevent future attacks: multi-factor authentication (MFA), login attempts limited to three tries, changing the password every three months and training for all employees on how to protect login credentials. |
| 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 all incoming traffic from the internet. The team will also be alert to detect indicators of compromise including logins outside working hours, brute force attempts and others |
| Respond | We disabled the staff portal whilst we tried to catch up with the intruder. We informed management about 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 | We 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, they will need to re-enter that information into the database once it has been restored from last night’s backup. |

These functions are essential for ensuring that our organization has effective security strategies in place. This organization has this in place so as to quickly recover from any damage caused by an incident to minimize its level of risk.