Incident Report Analysis – Applying the NIST Cybersecurity Framework

Summary

A phishing email impersonating a Microsoft Teams notification was sent to an employee in the marketing department. After clicking the link and entering credentials, an attacker used the compromised account to access internal HR files stored in the cloud. Sensitive documents were downloaded, and phishing emails were then sent from the compromised account to other employees.

Identify

The incident response team reviewed access logs and traced the activity to a single user account. It was confirmed that the attacker bypassed normal login behavior by accessing the account from an unusual geographic location. The team identified the affected cloud storage platform, several HR documents, and the source phishing URL.

Protect

Multi-factor authentication (MFA) had not yet been enforced for cloud storage access. The team is rolling out MFA for all remote access points. Training will also be updated and delivered to reinforce how to identify phishing emails. Firewall rules were also updated to block the malicious domain used in the phishing attack.

Detect

The security team will configure a cloud access monitoring tool and integrate alerts into the SIEM platform. Geo-restriction alerts and suspicious login behavior will be flagged going forward. Additional email filtering rules will be updated to detect and quarantine phishing attempts before they reach end users.

Respond

The compromised account was disabled immediately. Affected files were quarantined, and internal alerts were triggered to prevent further phishing propagation. Leadership, HR, and IT teams were informed. A notification is being drafted for affected individuals. The phishing domain was reported to the provider and law enforcement has been notified for record-keeping and investigation.

Recover

Account access was restored using a new password and MFA. The HR files were reviewed for integrity and reuploaded with permissions reset. End-user communication has been sent with reminders about phishing awareness. The IT department will perform a full cloud security audit to prevent future recurrence.

Reflections/Notes

This incident highlights how a lack of MFA and end-user awareness training can lead to credential compromise. Recovery was quick, but detection and prevention controls must be improved across all departments. Security awareness training needs to be reinforced regularly.