**Incident report analysis**

| **Summary** | Multiple users reported trouble accessing the company site; monitoring flagged unusual login behavior and data-access anomalies. Investigation found at least one employee credential was captured via a phishing page and then used to access customer data. Some records show signs of unauthorized viewing and modification (missing/altered fields). Immediate action is needed to contain access, notify stakeholders, and restore data integrity. | | |
| --- | --- | --- | --- |
| Identify | **Scope & assets:** Affected systems include the customer database, IAM/SSO, email, and the public web app. Inventory those hosts, service accounts, and related data flows.  **Users & access:** Compromised user account with excessive permissions accessed customer records. Review group membership, entitlements, and recent login sources.  **Gaps noted:** Phishing awareness gaps; lack of MFA on all accounts; incomplete least-privilege enforcement for the impacted role. (Use this to define risk and business impact.) | | |
| Protect | **Immediate safeguards:**   * **Enforce MFA for all accounts (especially privileged) and reduce entitlements to least privilege.** * **Update email filtering and URL rewriting policies; block the phishing domain(s).** * **Strengthen password policy (length, uniqueness) and require manager-approved resets for affected users.** * **Harden WAF/firewall rules in front of the app; enable anti-automation/bot controls on login endpoints.** * **Deliver targeted security awareness training on phishing and safe credential handling.** | | |
| Detect | **Monitoring & alerts:**   * SIEM correlation on **impossible travel**, atypical user agents, off-hours data pulls, and repeated failed logins. * Enable database activity monitoring for bulk reads/updates and sensitive table access. * Collect DNS/proxy logs to catch callbacks to newly registered or blocklisted domains. * Keep IDS/IPS sensors and signatures current for credential-harvesting and exfil indicators. | | |
| Respond | **Containment:** Disable the compromised account; revoke active sessions and refresh tokens; rotate affected app/API secrets.  **Analysis:** Preserve logs/forensics (email headers, web access logs, SIEM timelines); determine data accessed/changed.  **Eradication:** Takedown request for phishing site; update mail and web filters; remove malicious messages from mailboxes. **Communications & legal:** Notify management and (as required) customers/regulators; document response actions and lessons learned. | | |
| Recover | **Restoration:** Restore altered/deleted records from the most recent clean backup; reconcile changes between backup time and incident window.  **Validation:** Verify application functionality, access controls, and data integrity post-restore. **Improvements:** Incorporate findings into runbooks; schedule periodic phishing tests; expand MFA and least-privilege audits; update disaster-recovery checkpoints. | | |

| Reflections/Notes: This report applies the CSF’s “Identify → Protect → Detect → Respond → Recover” loop to a phishing-led credential compromise. Emphasis is on identity hardening (MFA/least privilege), endpoint & email controls, and closing monitoring gaps so future anomalies are caught early and recovery is predictable. |
| --- |