**Incident report analysis**

**Instructions**

NIST CSF incident analysis feedback

|  |  |
| --- | --- |
| **Summary** |  |
| Identify | The organisation's network stopped working due to an incoming flood of ICMP packets. Normal internal network traffic could not access the network resources. The team found that the intern who had reported the incidents’ username and password where obtained by a malicious hacker who had sent an email instructing her to click on an unauthorised link. |
| Protect | * Regular firewall maintenance with updates * Configure the firewall with a predetermined set of rules * Port filtering; which allows and blocks certain port numbers to limit unwanted communication * Install an IDS/IPS system to filter out some ICMP traffic based on suspicious characteristics * MFA login attempts limited to three tries. |
| Detect | * We used a network log analyser software to examine the network logs to identify threats * Install a SIEM tool with dashboard for consistent monitoring of network activity logs * upgrade /update the firewall and install an IDS/IPS which can send alerts for any unusual traffic and unauthorised access request to the network |
| Respond | In the event of another attack the following communication pathways should be followed   * Alert by SecOps team sent to management for awareness * SecOps team to isolate the attack IP device for inspection * Restore the business to normal operations to decrease down time * Security event procedures should be communicated to the IT team montly and saved on a central sharepoint * Any changes on the procedures should be clearly outlines ( who made the changes and what was changed on which date) - in order for tracking * Training to be conducted bi annually with end users on security procedures and process * Analysis report to be circulated to senior management following an attack within 7 business days post incident date * offline/isolate all affected devices for thorough analysis by IT Team |
| Recover | * Resources will the analyzed for any potential threats following attacks by IT team and signed off as secure/clean by IT/Security manager * These improvements to the SOP ( standard operating procedure) need to be done immediately ( with 2 days) and circulated for awareness. These are to be added to the Organisation’s Playbook * Team will recover the deleted data by restoring the database from last nights full backup. |

|  |
| --- |
| Reflections/Notes: |