|  |  |
| --- | --- |
| **SUMMARY** | Security event experienced by the company when suddenly all the network services responding stopped. The disruption caused by a distributed denial of services (DDoS) which the cybersecurity team found. The DDoS attack happen through the flood of incoming ICMP packets. The cybersecurity team stopped all non-critical network services by blocking the attacks, so that critical network services could be restored. |
| **IDENTITY** | To keep daily business activities from interruption, the company has assets to protect, asset such has firewall, public facing web server(s), web pages, internal servers, as well as social media platforms, safety in the internet space.  Some possible threat to these assets has been identified which are denial of service. (Dos)/DDoS, account hijacking (social media), web page login brute force among various other threat. |
| **PROTECT** | To limit incoming network traffic and an IDS/IPS system to filter out packets based on suspicious characteristics/signature, the cybersecurity team implemented firewall.  To prevent brute forcing of user account and any other possible attack, rate limiting has also been configured.  in other to get the company staff to be abreast of possible security threat and social engineering vises. Threat awareness training was organized for them. |
| **DETECT** | An investigation was conducted by the company cybersecurity team in the security and found that a malicious actor had sent a flood of ICMP pings into company’s network through an unconfigured firewall.  A malicious actor or actors targeted the company with an ICMP flood attack.  The daily workflow has been interrupted because the web server is longer than accessible, and client are stranded.  The entire internal network was also affected. |
| **RESPOND** | The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services.  A new firewall rule to limit the rate of incoming ICMP packets. |