Incident report analysis

Summary	This Morning the all internal network services suddenly stopped responding, after multiple reports, the cyber security team had investigated the incident and had found a malicious actor had sent a flood of ICMP pings into the companies network. This had stopped all legitimate internal network traffic for two hours, leaving employees unable to access any network resource.
Identify	The incident management team had responded by running a packet sniffer on the network and discovered multiple source addresses sending a large number of oversized ICMP pings. We started by blocking incoming ICMP packets, stopping all non crucial network services offline, and restoring critical network services whilst they investigated the issue further. Due to these pings coming from multiple source addresses , this indicated a DDOS attack had compromised the network through an unconfigured firewall. This vulnerability allowed malicious actors to overwhelm the company's network through a distributed denial of service (DDOS) attack.
Protect	The team has implemented a new firewall rule to limit the rate of ICMP packets, stopping an abnormal number of ICMP packets getting through into the network, as well as configured source IP address verification on the firewall to check for spoofed IP addresses on incoming ICMP packets, this ensures only legitimate traffic gets into the network, We have also implemented network monitoring software to detect abnormal traffic, alerting the cyber security team of any anomalies on the network, Lastly we have implemented IDS/IPS systems to filter out some ICMP traffic based on suspicious characteristics.

Detect	To Detect abnormal ICMP packets and illegitimate IP packets getting into the network the team have implemented an IDS/IPS system as well as configured the firewall to have source IP verification.
Respond	The team has sent a company wide email, informing users their had been a network outage due to a breach and what the teams steps are to prevent this happening in the future, The team has notified the upper management of the issue, how it happened and what the steps were to resolve this from happening again, The management will have to inform the relevant law enforcement and other organizations as required by local laws.
Recover	The team will enable all network services once the firewall rule has been enforced to bring the business back to an operational state and restore any affected or corrupted systems from last night's full backup.
