Incident report analysis

Summary	All network services unexpectedly stopped functioning. It was discovered by the team that the cause was a DDoS attack flooding the network with incoming ICMP packets. The response involved blocking non-critical network services and then restoring critical services.
Identify	The company was attacked with an ICMP flood. It was urgently necessary to secure resources and restore the entire affected system.
Protect	A firewall was implemented to limit the frequency of ICMP packets, along with possibly an IDS to filter ICMP traffic based on dangerous characteristics.
Detect	A source IP verification feature was configured on the firewall to check for spoofed IP addresses in incoming ICMP packets.
Respond	Affected systems were isolated to prevent further network disruption and to prepare for future incidents. These systems were then restored. Network logs will also be analyzed to check for any ongoing suspicious activity, and all incidents will be reported to all relevant stakeholders to determine how to proceed.
Recover	It is necessary to restore access to network services to a properly functioning state in order to recover. In the future, such attacks can be blocked at the firewall, or all non-critical network services should be stopped and critical services restored first.

Reflections/Notes: