Incident report analysis

Summary	In the company I work for, there was a DDoS attack on the company's internal network. An overload of ICMP packets caused a two-hour service delay on the network. The attack had some effects. The unavailability of network services affected internal and external customer-oriented operations. There was a risk of loss of productivity and damage to customer trust.
Identify	The attack type was determined to be a DDoS attack. Network infrastructures such as firewall, network administrator and access control systems were affected. All services running on the network are affected. Related security applications and monitoring software were not functional due to ICMP traffic.Internal systems became inaccessible because the company's network resources and servers were affected.
Protect	Hardenings should be placed on incoming traffic of ICMP packets. Stronger IP address verification procedures should be introduced. All network traffic should be constantly monitored and instant reports should be created for possible threats.
Detect	Advanced monitoring tools should be used to monitor traffic flow on network devices (router, switch, firewall) in real time. To detect deviations from normal network traffic, systems should be established to detect anomalies. Application security software that monitors user activities and access attempts should be used. Logs from all network devices and software should be analyzed.
Respond	When suspicious traffic is detected, network traffic should be limited immediately and necessary restrictions should be made through the firewall to

	prevent the spread of the attack. Once the incident is detected, relevant security measures should be strengthened. Firewall rules should be reviewed and intrusion detection and prevention systems (IDS/IPS) should be activated. After identifying the source of the incident, the software or configurations causing the vulnerability should be quickly updated or fixed.
Recover	The latest secure backup data must be available to quickly restore affected devices and systems. The backup plan should ensure that data can be restored quickly after the event. Affected devices should be safely rebooted and tested to prevent damage to the system after the attack. All security patches and updates should also be applied. Once the rescue is complete, the entire incident should be evaluated. A report should be created on how the attack occurred, which systems were affected and what vulnerabilities emerged.

Reflections/Notes: