Incident report analysis

Instructions

Summary	A multimedia company providing web design, graphic design, and social media marketing services faced a DDoS attack, causing a disruption in network services for two hours. The attack involved an influx of ICMP packets, rendering internal network resources inaccessible. The incident management team responded by blocking incoming ICMP packets and taking non-critical network services offline, restoring critical services. Upon investigation, the cybersecurity team discovered that an unconfigured firewall enabled a malicious actor to launch a DDoS attack, overwhelming the company's network.
Identify	The company's cybersecurity team found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall. This vulnerability allowed the malicious attacker to overwhelm the company's network through a distributed denial of service (DDoS) attack.
Protect	• **Firewall Configuration Policy**: Enforce a firewall configuration policy that mandates regular reviews and updates of firewall rules. All firewalls must be properly configured with default-deny policies and allow only essential traffic for business operations. • **DDoS Mitigation Policy**: Implement a DDoS mitigation policy that outlines the procedures and responsibilities for detecting and responding to DDoS attacks. This policy should include guidelines on how to activate DDoS protection services, when to escalate incidents, and how to coordinate with external DDoS protection providers if necessary.

	• **Access Control Policy**: Implement an access control policy that restricts access to critical network services based on the principle of least privilege. Only authorized personnel should have access to sensitive systems, and multi-factor authentication (MFA) should be enforced for privileged accounts.
Detect	• Deploy intrusion detection and prevention systems (IDS/IPS) to promptly detect and respond to suspicious or malicious activities on the network. • Set up network monitoring and logging to capture and analyze network traffic, helping to identify potential threats or indicators of compromise.
Respond	• Develop an incident response plan that outlines clear and swift actions to be taken in the event of future cybersecurity incidents, including DDoS attacks. • Train employees on incident response procedures to ensure a coordinated and effective response during an attack.
Recover	• Implement a robust backup and disaster recovery plan to ensure that critical data and services can be restored quickly after an incident. • Conduct post-incident analysis to understand the extent of the damage and take corrective actions to strengthen the network's resilience.

Reflections/Notes: