Incident handler's journal

Date: 18-01-2023	**Entry: 001** ICMP-based Distributed Denial of Service (DDoS) attack.
Description	At 14:03, internal systems detected an unusual spike in inbound ICMP traffic. By 14:07, all users reported service loss. The incident response team confirmed a full-scale DDoS attack using ICMP floods targeting network infrastructure.
Tool(s) used	**Tool(s) used** | SIEM (Security Information and Event Management), IDS/IPS system, firewall, NetFlow traffic analyzer
The 5 W's	**Who** caused the incident? Unknown external threat actor(s) using spoofed IPs to launch an ICMP flood attack. **What** happened? The company experienced an ICMP-based DDoS attack, rendering all services inaccessible. **When** did the incident occur? Wednesday, 14:03 – ICMP traffic spike detected; 14:15 – DDoS attack confirmed. **Where** did the incident happen? Entire internal and client-facing infrastructure of NextWave Solutions GmbH, including cloud services, email, DNS, and VPN access. **Why** did the incident happen? The attack exploited the network's openness to ICMP traffic to overload systems, likely as a disruption tactic or test of resilience.
Additional notes	The incident was contained by disabling non-critical services and applying ICMP drop rules. Future measures include improved firewall rules, source IP verification, regular staff training, DDoS simulations, and reevaluation of ISP agreements.