Incident report analysis

Guidelines

This data breach's incident report will be implemented with the National Institute for Standard and Technology (NIST) Cybersecurity Framework (CSF) guideline. The five (5) steps involved in this guideline are: Identify, Protect, Detect, Respond, and Recover.

Summary	The company experienced a data breach event where the official website is no longer accessible to the clients and staff members alike. This event was reported to the IT team by an intern in the company. The attack surface exploited by the threat actor(s) is the network. The incoming ICMP protocol packet was flooded with unprecedented number of request – which is a distributed denial of service (DDoS) attack. The security team has shut down the affected network, which was previously segmented – so as to keep other systems free from being infected.
Identify	The security team has identified that the threat actor(s) deployed an ICMP flood attack on the company’s networks. More thorough checks are still ongoing to ensure no backdoor was created by the criminals.
Protect	The affected networks has been isolated from other networks and infrastructure used in the company. This is to ensure that further attacks is not made possible.
Detect	In an effort to uncover the root cause and source of the attack, the IT team ran a tcpdump command in the command line; to learn more about the message displayed in the company’s website.

Respond	In response, more security best practices measures were ensured. These includes multi-factor authentication (MFA), defense-in-depth, reconfiguration of the firewalls, addition of intrusion detection and intrusion prevention systems. Also, a secure password principle was applied in the company’s systems, and the employees are also trained and mentored on the need for shared security responsibility.
Recover	The ICMP prototcol was replaced with a more secure port and infrastructure altogether. And the firewalls is also configured to block any IP address that sends certain amount of ICMP protocol request. This is also applicable to passwords use. Certain number of wrong password inputs with be dismissed as well.

Reflections/Notes: