Policies & Procedures

DDOS PROTOCOLS

By Derek Mayen

Captured User Data Policy

Unauthorized access to personal user information is captured or identified

Protocol

Escalate to upper management on next steps which may invoke the company playbook to mitigate the threat. This escalation may involve further escalation on the origins of the data breach.

Information may have been obtained via reconnaissance or unauthorized network monitoring.

Unauthorized PII Access Policy

PII (Personally Identifiable Information) breach. Internal or external information is compromised.

Protocol

Escalate to appropriate superiors as well as proper law enforcement for any case of PII (Personally Identifiable Information) breach. Frequent Data audits should be performed regularly to meet compliance with SOP.

Traffic Light Protocol (TLP) Policy (RED)

Identify appropriate departments, individuals, and organizations who have authorization to potentially sensitive information.

Protocol

Identify TLP colour code to determine the level of discretion. Once TLP code is identified, proceed with a direct need to know basis when handling information. Some information may be confidential or restricted.

Data Retention & Destruction Policy

Identifying systems that may have been compromised and systems that have not been affected amongst corrupted or lost data.

Protocol

Isolating infected systems from healthy systems and securing network traffic to unaffected systems. Identifying the contents within the affected system, and developing an action plan to recover breached data.

Log Retention Policy

Documenting internal and external authorized access to systems, this information may include time, personal identifiers (ie login information), devices used, operating systems, IP addresses, and location

Protocol

Retaining these logs will help identify IoC’s such as unauthorized users by cross referencing legitimate logs, with suspected fraudulent logs.