**Cybersecurity Incident Report: Network Attack**

**Incident Summary:**

This afternoon an automated alert associated with the web server that hosts the company’s sales web page indicated there was a problem with the web server. Upon attempting to access the sales page a timeout error was received in the browser. Logs indicate that the web server was receiving an abnormally large number of SYN packets from an unknown IP address. Thus the conclusion is that the web server was subject to a SYN Flood Attack from a malicious actor.

To establish a connection with the web server the TCP protocol is utilized. The client device sends a SYN packet to the web server, the server responds by sending a SYN/ACK packet back to the client device which then sends an ACK packet back to the server to establish the connection between the two devices.

The excessive amount of SYN packets being sent to the server were impeding its ability to establish a connection with any device attempting to communicate with it and overwhelming its processing capabilities. The malicious actor was attempting to either crash the server or bog it down to the point employees of the company couldn’t use it to perform their work.