MAZEBOLT

Ultimate DDoS Coverage for Insurance Companies

The DDoS Problem

The DDoS mayhem is only getting bigger and worse. In 2020, over 100 exchanges, insurers, and other financial firms globally were targets of the same type of DDoS attacks. Additionally, the Neustar International Security Council (NISC) analysis has disclosed that nearly 70% of organizations were targeted with ransomware DDoS attacks, and 36% agreed to pay the ransom.

As a proactive plan, insurance companies must assess ongoing DDoS vulnerabilities and patch them to avoid downtime.

However, current vulnerability identification tools require maintenance windows, and the security personnel cannot use such disruptive tools continuously. So, then how can insurance companies build the most efficient DDoS protection strategy to block all damaging DDoS attacks?

In 2021, Avaddon, the ransomware group, threatened the insurance giant AXA with a barrage of DDoS attacks to cause further damage if the insurance company refused to engage with their demands. Launching DDoS attacks followed by ransomware attacks has now become a popular attack tactic.

The DDoS Pain

Insurance companies have to continuously upgrade service policies and technology to meet the dynamic industry requirements. As a result of such digital transformation, several vulnerability points are created in the network; those can become susceptible to DDoS downtime if not detected and fixed timely. Security personnel can patch ongoing DDoS vulnerabilities only if they get real-time insights. However, traditional testing tools cannot be used to identify ongoing DDoS vulnerabilities because such tools perform only when the website is in maintenance mode. As a result, the dire need for insurance companies to stay online minimizes the application of traditional testing tools for vulnerability identification. It means the security team does not get real-time information, and the test results become obsolete whenever there are any changes in the network.

Why DDoS Mitigation Solutions are Not Enough

Damaging attacks are penetrating the best mitigation solutions

DDoS mitigation solutions need manual configuration after every minor upgrade in the system. So unless the security team ensures its reconfiguration, there is no guarantee the solution can protect the network from a sophisticated DDoS attack.

In addition, the solutions are reactive in nature, meaning they are designed to act only after a DDoS attack has already been launched at the network. Therefore, waiting for a mitigation solution to identify an ongoing DDoS attack is risky because the network will suffer downtime in case of delays or failure to detect the attack.

Benefits of Simulating DDoS Attacks with New Technology - RADAR™

Companies can validate the deployed mitigation policy and confirm if it is truly protecting networks by continuously simulating DDoS attacks using the latest sophisticated DDoS vectors. As a result, companies can identify DDoS vulnerabilities in real-time and perform quick remediation.

MazeBolt's new technology, RADAR™, is the only 24/7 automatic DDoS attack simulator. Working with any mitigation solution installed, RADAR™ offers superior DDoS coverage and automated DDoS protection. RADAR™ simulates over 100 attack vectors with all public-facing IPs 24/7, giving real-time visibility to all DDoS vulnerabilities with zero downtime.

Learn more about RADAR™

About MazeBolt

MazeBolt introduces a new standard in DDoS coverage, automatically detecting, analyzing, and prioritizing remediation across the network, doubling coverage, and virtually eliminating DDoS exposure without shutting down organizational operations. MazeBolt's continuous defense supercharges the performance of CISOs as well as the mitigation service provider.

www.mazebolt.com | info@mazebolt.com