MAZEBOLT

CASE STUDY
Business Continuity and Information Integrity of Parliamentary Elections 2019

0%
Downtime

520,000
Visitors Experience Seamless Performance

100%
Site Security and Information Integrity

"The continuous deep insight combined with the level of information and user-friendly reporting provided by the DDoS RADAR™ allowed us to dramatically reduce our DDoS risk and ensure the Parliamentary elections' integrity." **Chief Information Officer, Government Agency**

This Government Agency's infrastructure included a central point of government information and services for all offices and enterprise companies.

During the 2019 parliamentary elections, the infrastructure which included IoT / mobility devices, and third-party vendor applications worked at optimal speed, with zero downtime and uncompromised security.

The Challenge

The customer wanted to ensure that its existing infrastructure would not be compromised during the 2019 parliamentary elections due to DDoS attacks. It was critical that the infrastructure displayed seamless performance, reliability, and security at all times but even more so during peak traffic periods.

To meet the above goals, the customer needed to be able to detect & block malicious traffic 24/7 while proactively eliminating DDoS mitigation vulnerabilities that could be exploited to impact the network availability.
The customer also wanted to know whether the existing DDoS Mitigation was effective & could reconfigure defense policies, as required, in line with any network changes. Leaving nothing to chance, it was important to ensure that the DDoS Mitigation was detecting and mitigating Layers 3, 4, 7 as well as new sneakier DDoS attacks 24/7, and in real time.

Customer snapshot

Description

The customer provides public with centralized simple and fast access to government information from all the government branches, on one innovative and mobile compatible website.

Industry

Government

Business stats

This government agency's site hosts information from the Prime Minister's Office, the Ministry of Justice, the Population and Immigration Authority, the ministries of Tourism, Culture and Sport, Public Security, Transport and Road Safety, Energy, Construction and Housing and the Law Enforcement and Collection System Authority and so forth.

The Solution

To ensure business continuity, peak performance and 24/7 availability, MazeBolt evaluated the existing DDoS mitigation postures and suggested the implementation of the **DDoS RADAR™, a patented technology** that enables Continuous Feedback on top of any DDoS Mitigation system. DDoS vulnerabilities were eliminated and drastically reduced within 2 weeks.

Operating with existing DDoS Mitigation on the live production network, the DDoS RADAR™ found and eliminated many DDoS vulnerabilities. The customer was reassured of IT system continuity, despite peak demand across all services.

Real-time Reports clearly indicated where the vulnerabilities were, allowing quick action to fix, re-assess and ensure that the vulnerabilities identified were indeed correctly closed by the DDoS Mitigation vendor. The Executive Report offered extensive reporting to analyze milestones achieved towards eliminating DDoS vulnerabilities.

The Benefit

On the day of the elections, the network received unprecedented volumes of traffic:

> 1,340,000 hits*

> 6,535,000 page views*

> 520,000 users* At peak times

> 74,000 hits*

> 16,000 users simultaneously*

[*publicly available data]

- DDoS vulnerabilities were eliminated and drastically reduced DDoS risk within 2 weeks.
- The Infrastructure performed at its maximum capacity and ensured that there was no downtime.
- The customer has now extended the contract to make DDoS RADAR™ an integral part of DDoS Protection Strategy across additional sections of infrastructure.

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.

For more information,

please visit: www.mazebolt.com

or e-mail: info@mazebolt.com