Strengthening the DDoS Protection Infrastructure of a Large Israeli Bank

RED BUTTON
DDoS Experts

BACKGROUND

The bank is one of Israel's leading financial groups, operating over 150 retail branches and engagements in investment banking, trust services, and portfolio management.

Israeli banks regularly suffer from cyberattacks. Known for its advanced cybersecurity methods, the bank has a large security team including security architects and research personnel, in addition to the more traditional SOC/NOC and network teams.

THE CHALLENGE

The bank was looking to strengthen its DDoS protection posture and proactively searched for external experts to lead the process. Upon receiving recommendations from another financial institute, the bank selected Red Button.

Prior to our consulting, the bank had already implemented several DDoS mitigation mechanisms. While the existing architecture provided sufficient protection in previous years, the bank's security team wanted to ensure it was protected against larger volumetric attacks going into the future.

THE SOLUTION

Audit and Architecture Optimization

After carefully auditing the existing protection architecture, our team recommended re-vamping the bank's DDoS defense, offering two architecture options, and moving key protection components to the cloud. Following extensive discussion, the bank selected one of the recommended options. Because of its nature and how it redistributes traffic, CDN provided a perfect protection solution, helping the bank ensure that an attack would not reach the origin server and render the bank's site unavailable.

Knowledge Transfer

Although training and skill improvement were not among the formal deliverables, our consulting included ongoing knowledge transfer, which increased the DDoS expertise of the bank's security team and made the bank much more knowledgeable and effective in its engagement with solution vendors.

Vendor Selection

We provided the bank with a vendor shortlist that best suited the selected DDoS protection topology. At this point, our team joined the bank again to assist with an extensive, formal POC process. Our team helped evaluate the vendors based on a detailed template with over 80 evaluation criteria, as well as conducted testing, evaluating the results using a controlled DDoS attack.

Configuration Optimization

Following the selection of a vendor, our team provided a detailed recommendation for the security configuration of the selected DDoS protection software.

As a result of the DDoS hardening project, the bank's ability to withstand sophisticated DDoS attacks (as evident from its **DDoS Resiliency Score**) increased dramatically.