NimbusDDOS

ARTICLE :

Often-Overlooked Cyber Security Guidelines for Regional Banks

For regional banks, the threat of a DDoS attack is very real.

Malicious actors prey on vulnerabilities in online infrastructure, identifying architectural weaknesses and targeting unprotected resources. The attack overwhelms systems with massive volumes of traffic, crashing servers, and leaving behind a wake of destruction.

Though cybersecurity technology and awareness are at an all-time high, banks are still top targets. Since smaller banks may not have the resources and capabilities of their larger counterparts, the threat is even greater. Business continuity and damage to reputation aside, the cost of recovery is significant, often costing into the hundreds of thousands to resolve.

What is a DDoS Attack?
A Distributed Denial of Service (DDoS) attack is when multiple systems overwhelm a bank's online resources. Online banking systems, marketing websites, and customer service portals are among the targets most frequently impacted by attackers. If the attack is sustained, it can be crippling.

Motivations can include extortion, disgruntled employees or customers, and hacktivism attempts. In any case, the endgame is to cause as much chaos and disruption as possible.

DDoS attacks have been responsible for some of the costliest attacks in history. Recent attacks include GitHub and the Czech Statistical Office, the latter of these delayed vote counting in their last election, while the former is currently the largest and most sustained DDoS attack on record at 1.3 Tbps.

Regulations And Guidelines You May Not Be Aware Of
The Federal Financial Institutions Examination Council (FFIEC) sets out guidelines and practices for banks aimed at standardizing attack preparedness as well as the reporting and compliance process.

Since banks are under scrutiny from a range of regulatory bodies, a standardized and consolidated effort supports proactive measures, such as increased risk awareness and a better understanding of the expectations.

NimbusDDOS

Without a DDoS strategy, you risk:

- Obstruction of Customer Service, leading to direct revenue loss from online banking systems being down.
- Reputation Damage. DDoS is bad PR. Current and potential customers alike will worry their money and personal data isn't safe.
- Loss of Productivity. DDoS can potentially tie up your IT team for weeks at a time. Incident response efforts divert IT resources, and delays planned projects.
- Regulatory Scrutiny. A DDoS attack results in significant regulatory scrutiny, resulting in undue attention and a great deal of time lost answering to regulatory committees and auditors.

If you are prepared, you can prevent all four of these adverse outcomes. Learn more about DDoS Risk Assessments and schedule yours today.