NimbusDDOS

ARTICLE :

What Financial Institutions Are Overlooking

As a financial institution, cybersecurity is important to you, and you've taken thorough measures to ensure your systems are safe. However, there may be a type of attack that your current protocols leave you defenseless against: DDoS Attacks.

A DDoS attack is a network attack in which a cybercriminal intends to make your organization's online resources unreachable to customers and legitimate users. Often, these attacks are associated with extortion attempts or intended to conceal data theft.

DDoS attacks are becoming more prevalent; in fact, they increased by 30 percent in Q3 of 2019. If you are attacked, the fallout can be catastrophic for your company.

Reasons You Are Overlooking DDoS Threats

You may be unaware of DDoS threats, or you might be ignoring them for the following reasons:

- Overwhelming Process. Protecting one's company against DDoS attacks involves detailed assessment of your company's unique environment, creating a protection protocol, and training IT personnel.

- Trusting DDoS Mitigation Vendors. Many organizations blindly trust their DDoS mitigation vendors to protect them against DDoS attacks. This often leaves you exposed and surprised when a DDoS attack circumvents their protection. True protection requires experienced vendors that are regularly tested for effectiveness in your environment.

- Thinking Your Company Is "Too Small to Be at Risk." You might think that your institution is too small for cybercriminals to target.

- Solutions Are Too Expensive. Additional cybersecurity defensive measures might not be a priority for your budget.

- You're Afraid to See Testing Results. You're afraid a poor testing result would reflect badly on your company or internal teams.

NimbusDDOS

Reasons to Pursue Protection Against DDoS Attacks

Refusing to address the concerns discussed above are not legitimate reasons to avoid creating a DDoS protocol. Here are some reasons you should prioritize DDoS preparedness:

- Existing and Upcoming Regulations
  New regulations and guidance are being developed to help financial institutions improve their cybersecurity defenses. You will **or might already** need to be compliant with these regulations regardless the size of your institution.

- Your Profitability
  Every day that your system is down because of a DDoS attack, you lose money. Further, the costs associated with remediation can prove costly.

- Your Reputation
  A DDoS attack will damage your institution's reputation. Your clients will feel their finances are not safe with you. As a result, they will be wary of trusting you in the future.

- System Downtime
  A DDoS attack can wreak havoc on your IT department for weeks at a time. Your IT department could be completely consumed with a DDoS attack and be unable to address important day-to-day tasks.

- Avoid Extortion
  Some attackers will threaten your institution with an attack if you do not pay them to not attack you. If you are uncertain of your cybersecurity capabilities, you will be more susceptible to such threats.

Getting Started

If you think creating a DDoS attack protection protocol is right for your institution, NimbusDDOS can help. While other vendors focus mainly on technology, we go beyond and focus on the processes and personnel necessary to have a successful response to an attack.

Are you interested in learning about how NimbusDDOS can help protect you from an attack? Contact us today.