NimbusDDOS

ARTICLE :

Is Your Institution in Compliance with the FFIEC in Preventing DDoS Attacks?

Each day, Financial Services organizations face a multitude of cybersecurity challenges. This evolving landscape can seem to expand at a relentless pace, with a constant threat of data theft, malware, and break-in attempts. Often lost in the mix are DDoS attacks, which through their broad reach often cause widespread outages and system unavailability. Aside from direct financial impact of downtime, DDoS attacks cause significant reputation damage, and an increased burden on already overworked IT organizations. Whether you know it or not, your organization has a target on its back and following the FFIEC guidance can significantly improve your odds of surviving a DDoS attack.

What Is A DDoS Attack?

In brief, a distributed denial of service (DDoS) attack is an attempt by a bad actor to disrupt your IT resources by overwhelming them with connections and data packets. This is usually performed by compromising systems outside of your network and then utilizing them simultaneously to create a digital traffic jam in vulnerable areas of your IT infrastructure. This disruption may be the only aim of the attack but, often, targeted companies are contacted with extortion offers to cease the DDoS attack.

Know the FFIEC Guidelines

DDoS attacks have become such a problem in recent years that the Federal Financial Institutions Examination Council (FFIEC) published guidelines in 2014 outlining steps that financial institutions should take in order to be adequately prepared for the risk of DDoS attacks. These include (Reference 1):

- Maintain an ongoing program to assess information security risk that identifies, prioritizes, and assesses the risk to critical systems, including threats to external websites and online accounts;
- Monitor Internet traffic to the institution's website to detect attacks;
- Activate incident response plans and notify service providers, including Internet service providers (ISPs), as appropriate, if the institution suspects that a DDoS attack is occurring. Response plans should include appropriate communication strategies with customers concerning the safety of their accounts;
- Ensure sufficient staffing for the duration of the DDoS attack and consider hiring pre-contracted third-party servicers, as appropriate, that can assist in managing the Internet-based traffic flow. Identify how the institution's ISP can assist in responding to and mitigating an attack;
- Consider sharing information with organizations, such as the Financial Services Information Sharing and Analysis Center and law enforcement because attacks can change rapidly and sharing the information can help institutions to identify and mitigate new threats and tactics; and
- Evaluate any gaps in the institution's response following attacks and in its ongoing risk assessments, and adjust risk management controls accordingly.

Additionally, the FFIEC has published their Cybersecurity Assessment Tool (CAT), which has specific maturity models focused on DDoS attack controls. These controls include criteria for appropriate mitigation systems, as well as formal testing of controls with DDoS attack tests (Reference 2, page 53).

NimbusDDOS

Which Organizations Must Comply?

All FFIEC member organizations must comply with the guidance. This includes:

- All institutions regulated by the Federal Deposit Insurance Corporation (FDIC)
- All institutions regulated by the National Credit Union Administration (NCUA)
- All institutions regulated by the Federal Reserve Board of Governors (FRB)
- All institutions regulated by the Office of the Comptroller of the Currency (OCC)
- All institutions regulated by the Consumer Financial Protection Bureau (CFPB)

Summary

Despite the brisk business of the cybersecurity industry, this year saw the largest DDoS attack in history. Don't risk your financial institution being the next headline. Take the time to familiarize yourself with both the risk factors and the published guidance because the consequences of being unprepared can be severe. It is an expectation of both regulators and your customers that you will comply with these guidelines and protect the interests of all parties from the kinds of disruptions a DDoS attack can bring.

References:

1. FFIEC Joint Statement (https://www.ffiec.gov/press/PDF/FFIEC%20DDoS%20Joint%20Statement.pdf)
2. FFIEC Cybersecurity Assessment Tool (https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf)