EVALUATING VENDOR CONTROLS & THE SSAE No. 16 REPORT

IN THIS ISSUE

DDOS ATTACKS
pg. 7

SO, GIMMIE ALL GRANNY’S MONEY
pg. 15

THE STANDARDS:
AUDIT PLANNING
pg. 18
DDoS ATTACKS

By: Above Security, Canadian-based global IT security service provider
Just one minute of downtime after a DDoS attack could cost $22,000... and that’s only the financial loss. Are you prepared?

In February 2013, the National Credit Union Association (NCUA) issued an alert on the risks associated with distributed denial of service (DDoS) attacks. This warning was published only a few weeks after two US credit unions, Texas-based University Federal Credit Union ($1.5 billion in assets) and California-based Patelco Credit Union ($3.8 billion), had fallen prey to large-scale DDoS attacks – a term that gained momentum overnight (Radware, 2013). It is evident that the trend that caused much stir amongst cybersecurity experts has now taken its toll on credit unions. In the increasingly complex and evolving global cybersecurity landscape, DDoS attacks are but one of the countless malicious activities that can impair organizations. SPAM, phishing emails, viruses, social engineering and data leakage have all made international headlines and now represent real threats to individuals and businesses alike.

Due to their destructive nature and ability to affect networks with relative ease, DDoS attacks have become especially worrisome. And even though they have been around for more than a decade, the scale and frequency of these attacks are increasing faster than the capacity of most organizations to absorb them (Verisign, 2013). With over 89 million members nationwide, equalling about 44 percent of the economically active population, US credit unions would be well-advised to worry. Larry Ponemon, chairman and founder of the Ponemon Institute, acknowledges these dangers by stating that “there is a frightening gap [...] between the increasing severity of cyberattacks and the level of preparedness that exists in the industry” (MarketWatch Inc, 2012).

What does this mean for credit unions?
The 2012 Cyber Security Study, conducted by the Ponemon Institute and Radware Inc., revealed that one minute of downtime can cost organizations $22,000 on average, or up to $100,000 in very severe cases. Annually, the average cost of DDoS attacks can reach an alarming $3 million. Let’s apply this finding to the two aforementioned DDoS victims: for the University Federal Credit Union, 1.5 hours of downtime translates to a total cost of $1.98 million. With 5 hours of downtime, Patelco’s costs can easily climb to the dizzying height of $6.6 million. Both calculations are based on a very conservative figure of $22,000 per minute of downtime and emphasize the urgency of implementing procedures and systems that protect an institution’s most critical and sensitive IT assets.

What are DDoS attacks anyway?
Denial of service (DoS) and DDoS attacks are attempts to bring down sites, networks and applications. By intentionally misusing a victim’s bandwidth resources, attackers aim to temporarily or indefinitely interrupt the Internet services that an organization provides to its clients. The real question is why and how attackers are carrying out...
these attacks. While the detrimental impacts of DDoS attacks are clear, the motives behind them are not. A variety of reasons can begin to shed light on the core motivation behind these types of threats including competition (6%), extortion (5%), angry users (9%) and politics/hacktivism (21%). However, most unsettlingly of all, 58% of all attacks present unknown motives. In 2013, organized gangs will perpetrate at least half of the cybercrimes against financial services, gaming and other e-commerce companies, as offshore gangs thrive and foreign governments look the other way. (Gartner, 2013) Furthermore, attack types have remained highly diversified over the years, which has greatly increased the risks of becoming a victim. Attackers use a number of different attack vectors, such as Web, DNS, TCP-SYN Flood, VoIP, among others.

The primary impacts of DDoS attacks.

These attacks can be launched at any time and many make use of automated programs that allow thousands of users to attack a network or an application. By overtaxing the capacity of the network, DDoS flood attacks will deny service to legitimate users, ultimately triggering substantial business impacts such as: loss of revenues, diminished brand reputation, potentially long-term service interruptions and distraction for other attacks and internal inefficiency. Prime targets for such attacks are financial institutions, governments, ecommerce, Internet service providers (ISPs) and many more.

In order to demonstrate the severity of these attacks, we should approach them from a numerical standpoint. 65% of organizations have experienced an average of three DDoS attacks in the last 12 months. The durations of these interruptions vary widely, but the average downtime for a single DDoS attack has lasted 54 minutes. Attacks now last longer than ever before, primarily due to their higher level of complexity. In fact, 23% of attacks in 2012 persisted for over an entire week and have become increasingly sophisticated through the use of wide-ranging and complex attack vectors. With the average size DDoS attack now at 1.77GB/sec, and many larger attacks going on (2.5% of attacks were over 10GB/sec in Q1 2013), Internet connectivity can easily be saturated for a lot of organizations (Arbor Networks, 2013).

How can credit unions take action?

It is no secret that organizations should take immediate action to prevent threats before they inflict significant damage, but this may be easier said than done. There is one effective strategy to mitigate risk: Partnering with those who are most familiar with risk mitigation and incident management strategies and who can provide a holistic approach to network security. Credit unions can protect revenue-generating online activities, avoid liability issues while ensuring that they remain compliant to various regulations, and ultimately protect the integrity of their network by seeking out a third-party security provider that can offer 24/7 managed security services, all while including DDoS mitigation support. In fact, security providers that offer a unified approach to security will allow organizations to become proactive about securing their networks, instead of being reactive to unexpected attacks.

When a DDoS attack is identified, a security service provider or other capable teams of experts would follow a process similar to below:

- An incident is created to report the issue.
- A team of expert security analysts work together to manage the incident until it is resolved.
- If the attack is confirmed to be malicious, the IP addresses linked to the source are blocked.
- A comprehensive investigation takes place to determine the impact of the attack and a damage report is produced.

Remember, this is not an IT issue. The truth is that even the most experienced security experts cannot possibly predict when and where the next DDoS attack will happen, whose networks will be targeted and what the extent of the damages will be. What can be predicted, however, is whether and how well organizations are prepared to face them. Credit unions must begin to prioritize, strengthen and assess the security of their critical information assets on a regular basis by making information security an integral part of their corporate culture. After all, securing networks and information within an organization is a business process, not an IT process.

The risks associated with DDoS attacks are very real for all businesses that process or store large amounts of confidential data and these types of attacks are here to stay. Unfortunately, there are still too many organizations that don’t take this risk seriously enough. With definitive proof that credit unions are far from being immune, it is simply dangerous to be lulled into a false sense of security. Organizations must understand and, most importantly, prepare for potential DDoS attacks. Only if credit unions decide to take a strong position on security, will they be able to wage a persistent and formidable battle against one of today’s biggest cyberthreats.

About Above Security

Above Security is a global IT security service provider (www.abovesecurity.com/pdf/ Company_Overview.pdf), with expertise firmly planted in risk management and an unwavering focus on providing exceptional incident response management to clients in industries with highly sensitive information.

Since 1999, Above Security has been providing peace of mind to hundreds of clients through its market-leading solutions in managed security services (www.abovesecurity.com/ pdf/Managed_Security_Services_Brochure_ En_February_2013.pdf). Strategic consulting capabilities combined with expert 24/7 managed security services allow its clients to concentrate on their core business, safe in the knowledge that they can count on Above Security for their IT security needs.

Please read more about our managed defense against DDoS attacks here (www.abovesecurity.com/pdf/Managed_DDoS_Defense__En.pdf).

www.abovesecurity.com