BE FREE

CASE STUDY

BE FREE OF RISK

The Road to Enhanced Security Confidence

A federal credit union was concerned about its vulnerability level toward sophisticated hacking attempts.

Briefing
A federal credit union was concerned about a its risk level from a memo that it received about a rise in the amount of denial of service attacks (DDoS) happening to financial instsutitions. BestIT was called in to help them identify all of the gaps in their security and provide a plan to seal them.

TALK WITH OUR EXPERTS 1.877.222.8615

The Road to Enhanced Security Confidence

Client
Federal Credit Union

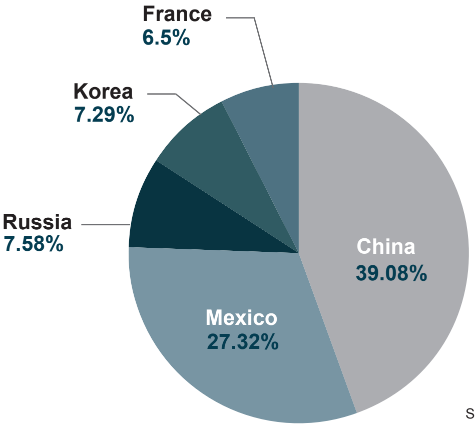
Industry
Banking

Challenge
This banking institution received a memo about an increase in distributed denial-of-service (DDoS) attacks towards banking institutions. The credit union called BestIT to help them determine their level of risk to this type of attack and identify any other gaps in their IT security infrastructure.

Services Provided
- Internal and External Attack and Penetration
- Vulnerability Assessment
- Wireless Attack and Penetration
- Social Engineering
- Network Configurations
- Security Engineering
- Physical Security

Introduction
Security breaches are a constant threat to businesses around the globe. Frequent security health checks are important to combating the strategic and invasive maneuvers of cyber criminals—internally and externally. The client, a U.S. based federal credit union, received a memo about an elevated DDoS attack that was hitting banking institutions. Hackers were working hard to steal money from banks and commit fraud. The company wanted to know if its IT security infrastructure could prevent hackers using advanced methods from gaining access to confidential data.

The Problem
While the credit union was confident that it would be able to prevent hackers from breaking into the institution through ways that they were already aware of, they wanted an outside entity to determine if their system could be breached with more sophisticated attack methods. They wanted to know if their IT security would successfully detect a breach with more advanced hacking methods and tools and determine the amount of bandwith they would need to fend off a targeted DDoS attack if one were to hit the credit union.



The Top 5 Countries Where DDoS Attacks Originate

In Q2 of 2013, there was a 33% increase in the overall amount of DDoS attacks. China is the leader with the largest amount of DDoS attacks that can be traced back to the country. Mexico comes in second, booting the U.S. out of the second spot from Q1. According to Prolexic, the average attack rate bandwidth rose 925% from the previous quarter.

Source: Prolexic, Quarterly Global DDoS Attack Report Q2 2013

The Solution
The BestIT security team went on-site to the organization to perform a security assessment. One of the more non-technical aspects of the assessment is a physical security check of the building. Although the company was equipped with biometric scanners and a guest policy, the security team was able to access a

data center room and breach all security barriers that protected the company's IT infrastructure. The BestIT security team gathered a full floor plan of the building after getting into the server room within the first 10 minutes of the engagement. After returning to the designated room to complete the security assessment, the security team was able to gain complete control of the organization from a minimum privilege system through four different parallels. First, through a cracked account at a desktop that had a default password on a web server, second, from a weak password on a database, third, from an employee who left a computer unlocked and the final was through genuine hacking.

Phase Two: A Breach In Real-Time

The other concern of the organization was the strength of its anti-virus software. The IT leader at the credit union was convinced that his anti-virus control would be able to alert them the moment an intrusion was taking place. Demonstrating a live intrusion is not something that most security vendors do. The IT department at the credit union watched as BestIT security experts cracked company passwords and achieved domain access for the organization as it happend—the anti-virus software did not detect the intrusion while the employees saw the breach occur live. Instead of disabling the anti-virus on the power shell, the BestIT security experts completely evaded detection.

The Results

After five days at the federal credit union's headquarters, BestIT put together a comprehensive report and presentation outlining all of the details of the security assessment. Overall, the credit union had good security parameters in place to prevent against most attacks on the organization. They had a total of 10 vulnerabilities on their organization—most of which could be patched by hardware upgrades from vendors. The DDoS threat could easily be evaded if the attack was on a more basic scale but an advanced, elaborate attack would not be easily prevented with the current securtiy landscape. BestIT recommended a few software upgrades to the system and went over the security policies for the company. The federal credit union had the confidence in their organization to effectively block any attacks against the organization and now were aware of the vulnerabilities within their system that were weak against more advanced hacking methods.

Conclusion

By participating in the risk assessment, the federal credit union was now equipped with the necessary tools and information they needed to prevent attacks on their systems. While performing a security assessment and live hacking at your business may seem a little invasive at first, being aware of the vulnerabilities that exist within your system by an IT security provider is better than remaining reactive and putting your business at risk of a security breach. Contact BestIT today to see how we can help strengthen the IT security infrastructure of your business.

> "Thank you for you and your team's professionalism — our IT team speaks highly of your team, and we look forward to our continued partnership."
>
> — Director of Risk Management
>
> **Credit Union**

Benefits

- Show due diligence in looking at advanced security questions
- Get expert advice that applies to physical and electronic security
- Cost vs. Benefit trade-off analysis
- Augment security engineering support for senior IT staff

Contact us for more information.
BestIT HQ
3724 N. 3rd Street
Phoenix, Arizona 85012

+1.877.222.8615 | info@bestit.com
www.BestIT.com