March 2013
Vol. 30 | Issue 3

InformationToday

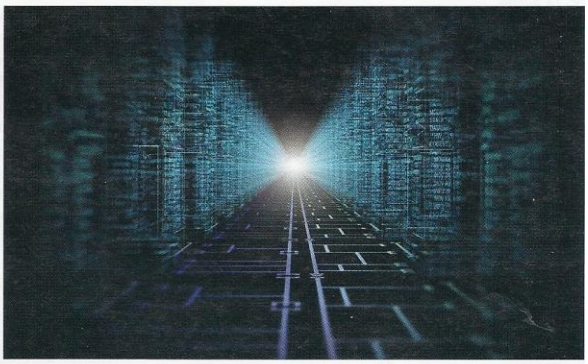
The Newspaper for Users and Producers of Digital Information Services | www.infotoday.com

BY KEVIN GAO | PRESIDENT AND CEO, COMM100

INSIDER'S PERSPECTIVE

What If Your Business Is Hacked

Insider's Perspective gives guest columnists a chance to write about challenges and solutions in their corner of the information technology industry.



Hacking efforts through Distributed Denial of Service (DDoS) attacks or other means are persistent threats for companies. A large-scale attack can interrupt connections to the company's servers, causing a complete shutdown of its operations. Once hackers realize they can disrupt service, they often attack the same company again, often with a demand of blackmail payment before they will stop.

But companies are taking steps to turn themselves into less-appealing targets and are mitigating the damage of any hacking intrusion that does occur.

*It's **a dynamic game,** with hackers trying new angles every day. ...*

Before an attack occurs though, enterprise-level firms are increasingly relying on proactive monitoring of server status. This allows companies to spot any unusual activity, as well as to send alerts to system administrators and other technicians who can immediately check the server to spot any issues.

Immediate Action After an Attack

One example of a DDoS attack occurred several months ago at Comm100. Although the hacker tried to blackmail us, these efforts were unsuccessful, and we worked quickly to remedy the situation. After the attack began, we took several immediate measures, such as updating the system patches and closing unused ports, to minimize attack points and reduce the chances of future attacks. We also increased the bandwidth of our servers to a large degree and deployed DDoS mitigation software to filter TCP (transmission control protocol) requests and the actual attack traffic. The software and a third-party defense service were technologies that we built to work together to filter out the abnormal traffic before it reaches the server.

We have more than 200,000 customers who run core parts of their businesses on our hosted service, so we understand the importance of maintaining reliability and stability. After battling this persistent hacker, we went to work looking at ways to further strengthen our defenses. For example, we set up a special team that watches the server 24/7 in conjunction with our real-time monitoring system. It's a dynamic game, with hackers trying new angles every day, so all companies need to proactively put the right safeguards in place that make them an unattractive hacking target going forward.

We also have several set procedures in place to manage attacks. After determining the technical characteristics of the type and scope of the attack, our company contacts the data center that hosts the company's servers to see if there are network errors, if they detected the attack, what kind of threat is occurring, and what they are doing to protect the server. Once the attack is confirmed and existing defense measures could not protect the server, more advanced defense systems that suit the company's needs needed to be reviewed. As the attack is corrected, our IT staff continues to monitor the server and make further improvements as necessary.

While automated monitoring, firewalls, and other systems simply need to operate, there is a human element to managing hacking. Staff training is vital to successfully repel an attack, with staff ideally receiving training on the attack types and methods used by sophisticated hackers as well as the typical effects of the most common threats. When an odd event occurs, the team can use simple, quick methods to check the status and resource use of the server. Technicians use such a test to identify the type of attack and its methods and then take appropriate measures.

*The **management of customer data** is an especially important concern for companies. ...*

Coordination among multiple departments is critical to quickly manage hacking threats. The system administrator team is the first to take the appropriate measures to

strengthen the security system. The team should also be attuned to industry trends and should receive updates on the latest hacking methods and the best defense techniques. Next, the developers should adjust program settings, if necessary, followed by testing by the staff members, who need to ensure that all systems are functioning properly. Each department needs to know its role and should be able to work autonomously to ensure threats are stopped as quickly and efficiently as possible.

Managing Data Security Concerns

The management of customer data is an especially important concern for companies that offer a hosted product that provides a cloud-based service to manage personal customer interactions. Many firms employ several best practices that can reduce the risks of data falling into the wrong hands, even in the case of cloud environments.

Complicated password verifications are critical for proper server login credentials management and should be managed to ensure hackers are not given an easy method of accessing information. An intrusion prevention system is another recommended practice that can be used proactively to spot port or bug scans.

Customer data encryption is another popular move, with encryption key access only granted to a few staff members. Diligent review of system visit logs also allows administrators to spot suspicious behaviors that should be investigated.

The risks of threats are very real and can potentially damage a company's relationships. Threats need to be managed in a logical process to not only keep the business going but also for legal reasons, where the business needs to show that it responded to the threat in a reasonable manner. While not all threats can be prevented, companies that implement a collaborative plan to spot and resolve threats can make themselves a less-appealing target.

Kevin Gao, president and CEO of Comm100, is a software developer and a small-business expert. He founded Comm100 in 2009 to revolutionize online customer service and communication. Since its launch, the company has served more than 200,000 clients worldwide with its integrated cloud-based solutions, including Live Chat Software, Email Marketing, Support Ticket, Help Desk, Forum, and Knowledge Base. Send your comments about this article to itletters@infotoday.com.