Strategies for Cyber-Attack Protection:

Managed Web Security Services

Akamai
FASTER FORWARD

TABLE OF CONTENTS

INTRODUCTION 3

WHY MANAGING ONLINE SECURITY IS A NECESSITY TODAY 3

THE IN-HOUSE CHALLENGE 3

COMMON CYBER THREATS 4

- Data breaches 4
- Distributed Denial of Service (DDoS) 4
- Hacktivism 4
- Website defacement 5

TAKE A PROACTIVE DEFENSE WITH A MANAGED WEB SECURITY SERVICE 5

- Interactive monitoring, detection, and threat mitigation 5
- Active maintenance and web app configuration assistance 5
- Strategic review of web security configuration 6

BENEFITS OF A MANAGED WEB SECURITY SERVICE 6

HOW AKAMAI CAN HELP 7

CONCLUSION 7

Introduction

Reminiscent of the bustling downtown department stores of the past and the mega malls of not so long ago, today's Internet-based businesses are teeming with consumer sales, B2B transactions and users of Software-as-a-Service (SaaS) applications and online games. But while owners of brick-and-mortar businesses could secure their shops with lock and key and sophisticated alarm systems at the end of the day, online business owners must adopt web security solutions to keep unwanted visitors out – today's sinister hackers and cyber criminals – while keeping their web-based shops open 24/7.

It only takes a look at recent headlines or an online search for *2014 cyber attacks,* and you'll find many well-known companies mentioned. If cyber criminals can take down these large, respected global brands, then any Internet-based organization of any size is at risk. The scary truth is that it is not *if* but *when* an online business will come under some level of cyber-attack – and with the expansion of applications and data stores to the cloud and other complexities of today's Internet, online businesses are more vulnerable than ever before to cyber-attack threats.

This white paper explores strategies for staying a step ahead of cyber-attackers by building a strong defense with managed web security services. It will also provide an overview of the most common types of cyber-attacks and concludes with a discussion of the benefits of a managed web security services solution that can provide 24/7 protection against network and application-layer attacks.

Why managing online security is a necessity today

Clearly, there is a lot at stake when it comes to protecting an e-commerce website against cyber-attacks. The following statistics reported by Singapore-based ReferralCandy, a company that automates programs for online retailers, were compiled from sources such as the U.S. Census Bureau and the Internet Retailer's Top 500 Guide for 2013. They illustrate just how much revenue online retailers in the U.S. alone risk losing if their websites were to be rendered inaccessible by a cyber-attack:

- 61,728 online retailers generate at least $25k in revenue (up 12.8 percent from the previous year)
- 38,157 e-commerce merchants generate at least $50k in revenue (up 12.3 percent from the previous year)
- 23,587 online merchants generate at least $100k in revenue (up 13.6 percent from the previous year)

Revenue loss is not the only fallout from a cyber-attack. Whether a website is down for a few minutes or several days, brand reputation and customer loyalty can plummet as disgruntled customers repeatedly try and fail to complete transactions or access SaaS applications. The same is true for investor confidence, especially if the cyber-attack or data breach becomes the lead story on the nightly news. Some victims of DDoS attacks and data breaches have seen stock prices fall after the attack became public knowledge.

Not only online retailers, but governments and other organizations with an online presence, continue to be at high risk of losing availability of Internet-based services and user confidence. As reported in *Akamai's Q2 2014 Global DDoS Attack Report*, powerful reflection-based attacks pose a significant danger to businesses, governments and other organizations that risk having an entire data center made unavailable for the duration of a DDoS cyber-attack.

The in-house challenge

Many enterprises have made significant investments in an IT infrastructure, which is often managed with internal resources. In most cases, cybersecurity also becomes the responsibility of this internal IT group. This approach, however, presents a number of significant challenges.

First, security professionals are hard to hire, train and retain. In addition, while changes in technology can be planned for months in advance, cyber threats change daily and require immediate action. Unfortunately, cyber-attackers have far more resources at their disposal (botnets and crowd sourcing, for example), and can launch attack campaigns that last weeks or months. Not surprisingly, marshalling the required level of resources to maintain an effective cyber defense against an on-going and frequently changing threat is simply beyond all but the world's largest organizations. As a result, many organizations opt for a managed services model when it comes to cybersecurity.

Common cyber threats

Regardless of how cybersecurity is handled, industry or business-sector knowledge is powerful when building a defense against today's most common types of cyber threats, which include:

Data breaches

Data breaches are one of the most complex security issues to mitigate. The complexities of application attacks, combined with changing or poorly defined requirements and unknown risks, have resulted in thousands of vulnerabilities[1] being disclosed each year. Recently, attackers breached a critical system in a well-known organization and stole nearly $10 million using relatively unsophisticated methods and tactics. During the investigation it was determined that the attackers could have come in from several different technology paths, including an insecure web gateway system, a poorly updated web management system, or the public-facing site of the company.

To provide a base level of security, data may be stored in an encrypted format, but the application itself, and sometimes end users, still need to be able to interact with unencrypted information. Attackers will try to trick the system into disclosing this data in the clear by way of whatever compromise they can find. Cyber adversaries will target every input on the site, every parameter, every cookie, and every request header in order to inject malicious payloads in search of a viable compromise.

Attackers try to obtain as much personally identifiable information as possible. This knowledge can empower cyber criminals to create an endless stream of new credit accounts, purchases made on those accounts, and even an entirely new identity.

Distributed Denial of Service (DDoS)

A DDoS attack is an attempt to make a computer resource (i.e. website, e-mail, voice or a whole network) unavailable to its intended users. By overwhelming it with data and/or requests, the target system either responds so slowly as to be unusable or crashes completely. The data volumes required to do this are typically achieved by a network of remotely controlled zombie or botnet [robot network] computers. These have fallen under the control of an attacker, generally through the use of Trojan Horse programs.

Unfortunately, all online organizations and businesses are at risk of becoming the targets of DDoS attackers. According to Akamai's Q2 2014 Global DDoS Attack Report, from April to June 2014 the average bandwidth of DDoS attacks was up 72 percent, and peak bandwidth increased 241 percent, while attack duration was only half as long compared to Q2 in the previous year. Most telling is the trend of attacks being largely fueled by reflection-based vectors, which misuse common Internet protocols on open and vulnerable servers, and server-side botnets that take advantage of web vulnerabilities in web applications, such as WordPress, Joomla and their plugins. With server-based attacks, cyber attackers can cause more damage with fewer of their own resources.

Hacktivism

Hacktivism is a cyber-attack movement in which computer network hacking is motivated by social activism or political protest. Cyber hacktivists, such as the well-publicized group Anonymous, launch distributed denial of service (DDoS), website defacement, data exfiltration, and other cyber-attacks on the websites of global brands and organizations to protest political issues and promote their own ideology. Lulz Security (LulzSec), Operation Payback, and Antisec are other active hacktivist groups.

Hacktivists typically use homegrown hacker toolkits that are readily available to anyone through the Internet, either free or at a low cost, and they are designed to be easy for anyone to use. These toolkits are particularly sinister because they can contain many different types of DDoS attack vectors, and consequently allow hacktivists and other cyber-attackers to exploit multiple vulnerabilities of an Internet-facing system. Hacking tooklits such as DirtJumper, booter shell scripts, High Orbit Ion Cannon and Low Orbit Ion Cannon.

Website defacement

Defacement is a cyber-attack that gives hackers administrative access to a website for the purpose of changing its visual appearance, such as replacing existing content with content authored by the hacker with malicious intent. One method of defacement involves breaking into a web server and replacing the hosted site with the hacker's website. Other methods involve deleting core files from the server and uploading malware. Site visitors run the risk of unknowingly launching malware or even a cyber-attack if they click on a website link or image that has been infected. In some cases, the malware may infect the computers of site visitors, which obviously leads to a very poor customer or user experience and the resulting loss of confidence in the business or organization whose site has been defaced.

Take a proactive defense with a managed web security service

In the fight against cybercrime, sometimes even the most robust security technology is not enough. Akamai recommends a proactive, multi-layer defense against cyber threats – a combination of cutting-edge attack detection and mitigation technology enhanced by managed web security services. In simple terms, managed web security consists of outsourced services specifically designed to give online businesses a proactive defense against data breaches, DDoS attacks, and the complete evolving landscape of emerging cyber threats. Seasoned web security experts on the provider's security team not only detect and mitigate attacks, but also act as web security consultants who ensure that web applications and network systems are always up-to-date and protected against emerging threats. Managed web security services ideally focus on delivering multi-layers of threat protection and ongoing consultation and support, including the following expertise:

Interactive monitoring, detection, and threat mitigation

Early detection and immediate mitigation of cyber-attacks are the hallmarks of a best-in-class managed web security services offering and a proactive defense against Internet-based threats. Dedicated technicians in the provider's Security Operations Center (SOC) monitor the customer's network 24/7 for any signs of malicious traffic. This level of monitoring and detection is a specialized IT skill that most in-house IT resources do not have, but it is vital to ensuring early detection of a cyber threat.

Why is early detection so important? Time is literally money when mitigating a DDoS attack, data breach or other type of cyber-attack. According to *Develop a Two-Phased DDoS Mitigation Strategy,* a May 2013 report by Forrester analyst John Kindervag, financial services companies experienced an estimated $17 million loss per DDoS incident in 2012. The estimated financial impact [of DDoS attack] is $2.1 million dollars lost for every 4 hours of downtime and $27 million for a 24-hour outage. These figures can be extrapolated beyond the financial services industry to apply to any industry, government or organization that does business or provides applications via the web. Faster attack mitigation saves money and reduces the impact of damaged brand reputation, lost customers and declining stock prices.

Active maintenance and web app configuration assistance

Web applications are easy prey for cyber attackers and often open the door for data breaches and theft of personally identifiable information (PII). Attackers look for the weakest links and try to trick the web application into disclosing data in any way they can. Web applications that have stale rules and are out-of-date are usually most vulnerable and pose the greatest risk of allowing access to attackers. Within a managed web security solution, customers can augment the best practice of a secure software maintenance lifecycle with a scalable Web Application Firewall (WAF) solution from the services provider and expert guidance from the SOC experts.

Why active maintenance of web applications is so critical: Akamai customers reported 768 application-layer attacks in 2012 and 1153 in 2013, a 50 percent increase year over year. Veracode predicts that three out of four companies will be targeted at some point by web application exploits and that web applications represent 54 percent of all hacking-based data breaches.

Strategic review of web security configurations

Most organizations do not have IT resources with the expertise to maintain and optimize web security configurations. A typical company would require at least three full-time IT employees to provide 24/7 coverage, plus overtime on weekends, for round-the-clock, in-house web security operations. Cost considerations notwithstanding, it is very difficult to find and retain IT talent with this level of specialized web security expertise and experience in configuring such systems.

Managed web security services providers meet the challenge by helping organizations stay fully prepared for future cyber-attacks. Regular strategic reviews of the web security configuration by SOC experts ensure that the solution is always fine-tuned, up-to-date, and ready to defend against the latest attack vectors and toolkits. In regularly scheduled threat abatement reviews, for example, the technicians can perform analyses of false positives and malicious traffic and change rules accordingly, if needed, without compromising the security of the web applications being protected. A managed web security services provider can also provide other expert recommendations on custom adjustments and updates to rule sets that will ensure the best protection for the business.

Benefits of a managed security service

Managed web security services provide value both during attack incidents and at other times by ensuring that an online organization is optimally protected at all times against data breaches, DDoS, hacktivism, and all present and future cyber threats. Some of the key business benefits include:

- Always-on monitoring that ensures an immediate response to any cyber-attack without the expense of building an in-house 24/7 security operations center and hiring web security experts
- Access to industry-leading security expertise from SOC technicians on the front lines of the threat landscape as part of an affordable managed web security services package
- Ongoing assessment and maintenance of the web security solution to adapt quickly to rapidly changing cyber threats, business requirements and industry trends
- Dedicated expertise in cyber threat identification, monitoring and mitigation, so companies can focus IT resources on core business initiatives and better control IT costs

Key operational benefits of using managed services for web security also add up to cost reductions and time and efficiency gains:

- Real-time analysis of alerts to detect threats faster
- Protect legitimate traffic by reducing occurrences of false positives
- Build a secure infrastructure while keeping site functionality and performance intact
- Offload application maintenance time and effort

Perhaps most importantly, providers of managed web security services have a bird's eye view of the threat landscape and have up-to-the-minute knowledge of the latest attack vectors and toolkits. Their SOC experts have experience in serving customers across many different industries and geographic areas, both domestic and abroad. Most of all, they are at the forefront of creating and using the latest counterattack measures – often developed on the fly during attacks – to take cyber threat protection beyond just software to a robust, reliable business partnership in the fight against cybercrime.

Although acceptable risk varies from company to company, most companies map risk into buckets, each with a tangible financial risk. Because of the risk to the enterprise IT infrastructure, data breaches are almost always in the high-risk bucket and have a high-priority spot in the annual budget.

How Akamai can help

Akamai Managed Kona Site Defender Service is an on-going professional service that provides proactive monitoring, configuration assistance, and expert security support and guidance designed to help companies keep modern website application attacks andDDoS attacks at bay.

Akamai's service gives you access to Akamai security experts and provides security event monitoring through which our teams proactively alert you on observed threats to your web properties. Features included in the service are: Threat Update Reviews, Security Configuration Assistance, Security Event Monitoring, Emergency Configuration Assistance and Security Incident Management. With the Internet threat landscape evolving continuously, Managed Kona Site Defender Service gives you the ability to review, optimize and monitor your website defense and react quickly to potential threats through proactive security event monitoring and security incident response.

Conclusion

Network security technology alone, while vital, cannot adequately stop attacks from ever-changing toolkits and innovative attack vectors of sophisticated cyber criminals. A managed web security service is an essential piece of a proactive online security defense that pits highly experienced SOC technicians and state-of-the-art equipment against cyber attackers – giving the good guys a much needed edge in this scenario.

In the end, most companies do not have the resources,expertise or budget to successfully implement and manage a complete 24x7 web security monitoring initiative in-house. It makes perfect sense to outsource web security to experts, just as outsourcing non-core processes such as accounting and legal services has become a strategic approach to managing operational costs and efficiencies.

Akamai maintains that managed web security services coupled with leading attack monitoring and mitigation technology in a multi-layered approach is the best, most effective and most proactive way to fight back and win against cyber threats now and in the future. To learn more visit www.akamai.com.

Sources:

[1] *National Institute of Standards. "NVD - Statistics Search." NVD - Statistics Search. National Institute of Standards, 21 July 2014. Web. 21 July 2014. <http://web.nvd.nist.gov/view/vuln/statistics>.*

Akamai FASTER FORWARD