2014

Crucial Cloud Hosting

Crucial Research

[WEB HOSTING SECURITY 2014]

Security is a growing threat for hyper-connected and Internet-dependent businesses whose activities increasingly rely on web hosting servers. This paper examines the extent to which businesses are vulnerable to security breaches and gives an overview of best strategies for protection.

Table of Contents

Web Hosting Security 2014

Introduction

> *Cyber-attacks grow in strength year by year and this menace has always been a much-discussed topic in the online world. As companies continue moving business activities to online media and cloud servers, cyber security remains a particularly sensitive issue for both web service providers and client companies.*

The rise of cloud computing and on-demand web-based technology has additionally perpetuated security concerns, making them a constant preoccupation for modern CIOs/CTOs. While the number of cloud tenants grows, cyber-attacks seem to become more importunate and more aggressive, which is why security systems implementation has become a precondition for successful online operations.

For web hosts, which are partly responsible for ensuring their client's data, security is certainly a feature they need to invest most thought into. In a turbulent online market, where reliable web host is necessary to any business, security has become one of the major success factors and a precondition for achieving competitive advantage in the industry. No web host can achieve a reputable status until they are ready to promise and deliver maximum server stability, data security and general reliability. Therefore, security is by no means an exhausted topic in the tech world. In fact, it is a topic everybody from individual users to large organizations should discuss in order to identify most frequent problems and design more efficient solutions.

To help in raising awareness of web hosting security threats, this paper outlines the biggest breaches of the first half of the year 2014, examines most frequent forms of cyber-attacks, and gives an overview of protection systems.

A Year in Review: State of Web Hosting Security 2014

Constant access to information, easy communication and availability of web services are some of the most important advantages the Internet has offered to the modern world. All these benefits, however, have their dark side - security and privacy issues whose importance grows parallel to the development of new technologies. The number and strength of cyber-attacks substantially increased over the last few years, which is why they remained a huge concern for modern web hosts.

In 2014, certain large-scale security breaches appalled the tech world and affected millions of web users. Their effect was twofold: while on one hand increasing the fear of doing business online, they contributed to increasing the awareness of the importance of security systems on the other.

Top Security Breaches of 2014

Heartbleed Bug

Probably the most widespread impact of a single security breach was that of an OpenSSL bug named Heartbleed, which was discovered in April, 2014.

The vulnerability that allows attackers to read data from web servers has existed in the most widely used encryption protocol for over two years and it affected more than half million web servers.

Some of the most popular websites affected by Heartbleed vulnerability are Amazon, Pinterest, Reddit and WordPress.

eBay Data Breach

Another major data breach occurred in May, 2014 when dozens of the company employees' accounts were hacked after months of malevolent activities in the company's network.

145 million of eBay's customers were required to change their passwords in order to prevent hackers from obtaining sensitive data.

AOL Mail Spoofing

Back in April, AOL reported a major security breach that affected 2% of their tens of millions of users. The company started investigating potential breach after they noticed increased amount of "spoofed emails" from AOL mail addresses.

The hackers were able to access users' email addresses, postal addresses, encrypted passwords and encrypted answers to security questions, as well as certain employee information.

Since not all the companies go public about security breaches, it is very difficult to determine their exact number and scope. One thing is for sure - their number is astonishingly high and is very likely to further grow in the following years unless a greater number of companies starts implementing efficient security systems.

60% increase in the number of attacks

87% companies experienced DDoS attacks multiple times

39% increase in average bandwidth

Biggest Web Threats

DDoS Attacks

DDoS Attacks are a nightmare for web hosts. While the hosting technology improves and the number of websites increases, DDoS attacks get ever more sophisticated.

In the Neustar *Annual DDoS Attacks and Impacts Report*, 47% of respondents saw DDoS attacks more serious than last year. The percentage of companies attacked increased by 60%, while 87% of companies experienced DDoS attacks more than once.

15% increase in malware

196 million unique malware examples identified in 2013

In the first quarter of 2014, Prolexic saw a 39% of increase in average bandwidth and the largest-ever DDoS attack in the Prolexic DDoS mitigation network.

Ransomware

Ransomware is an increasing threat to website owners. McAfee Labs Threats Report identified a 15% increase in malware with 196 million unique malware examples being found in 2013. Ransonmare is a type of attack targeted at a particular company aimed at freezing their website until a requested sum of money is paid to the attackers.

40% increase in number of suspect URLs in 2013

In 2014, we saw many major companies attacked by ransomware, with most of them deciding not to pay to hackers.

Suspect URLs

Suspect URLs and IP addresses are those hosting low reputation websites that might be trying to spread malware across web host's servers. There are many ways a website can get bad reputation and both individual companies and web hosts need to monitor their web logs in order to identify unusual activities connected to particular URLs on time. Hosting suspect URLs many eventually lead to hacking, and this is why the huge increase in their number is an alarming fact for web hosts.

Phishing attacks

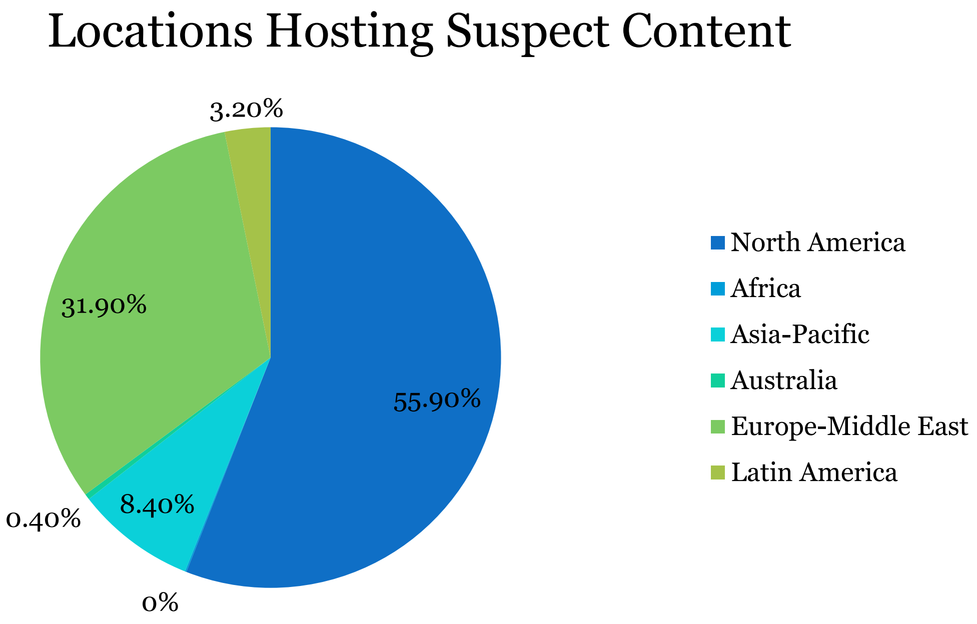
This is one of the most dominant forms of website attacks and it is carried out by sending malicious emails in bulk to the chosen websites. Quite unsurprisingly, phishing activities are mostly aimed at financial institutions or ecommerce websites in order to obtain financial data from the website users.

Symantec's *Internet Security Threat Report* from April 2014, revealed the percentage of phishing attacks by sectors and they came to the following statistics:

Sectors	Phishing Percentage
Financial	71.7%
Information Services	21.0%
Others	7.0%
Government	0.2%

Locations

Malicious content can come from various sources. However, North American web servers seem to be the major resource of suspect content judging from the McAfee Labs Threats report that gives the following chart:



Protection Strategies

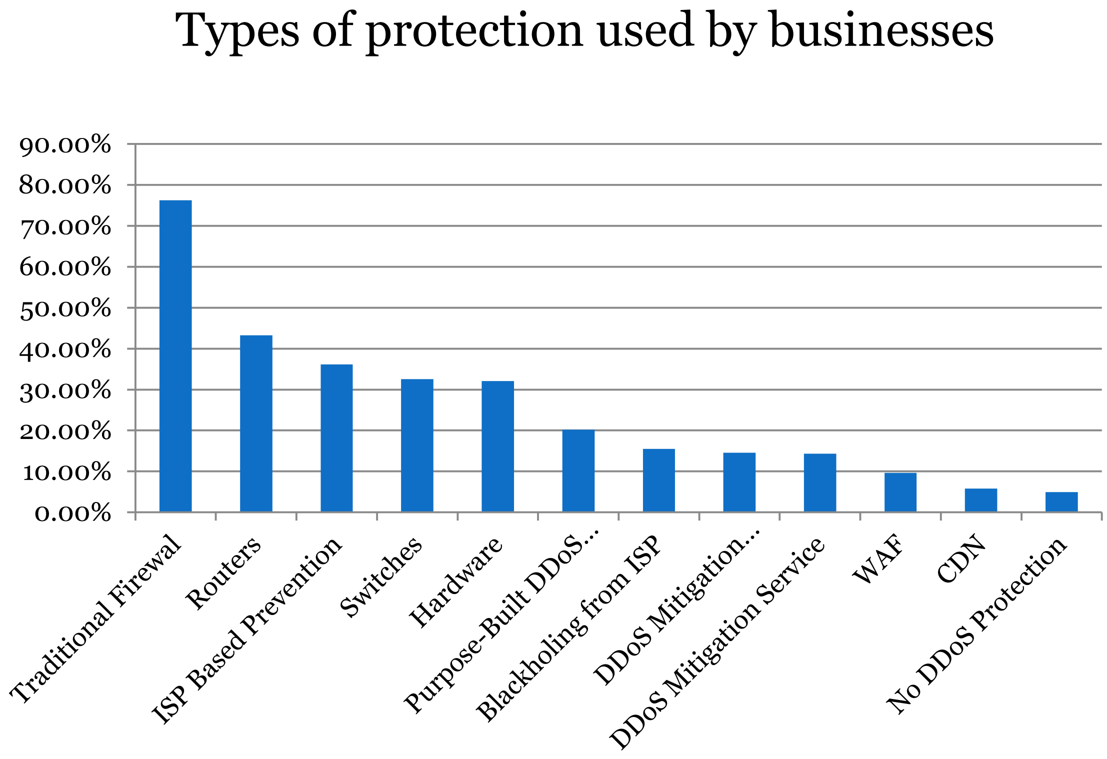
Securing the web is a task for both end users and web hosting service providers. If proper data protection strategies are deployed on both sides, the risk is lower despite the fact that hacking technologies constantly advance.

DDoS Protection Systems

Considering their strength and corresponding damage potential, DDoS attacks require advanced protection systems whose implementation is crucial for securing both servers and data transfers.

Neustar *Annual DDoS Attacks and Impacts Report* looked into the current DDoS protection systems, noting that financial institutions are far more likely to have DDoS-specific protection than companies from other industries. Apparently, this industry has the adoption highest rate of anti-DDoS attack systems.

The list of the most frequently used DDoS protection systems and the summary of survey responses is given in the table below.



Encryption strategies

35% reported greater awareness of security practices

The year 2014 was named the year of encryption as a result of increased focus on using encryption as the main means of data protection across industries. In the aftermath of Edward Snowden's cyber-surveilance and security breach revelations, different industries have become more serious about encryption. The *Global Encryption Trends* survey reveals that 35% of respondents reported greater awareness of security practices of their cloud providers, as opposed to 29% of companies in previous years.

This certainly has a lot to do with the general decrease of trust to web hosting service providers. In relation to this, Carole Murphy, Director is Product Marketing at Voltage Security points out:

> *"The recent spotlight on government surveillance has thrust the need for new, easy to use and pervasive encryption technologies into popular media and into consumers' minds like never before, creating awareness and concern."*

Vulnerability Assessment

Monitoring website logs and identifying unusual activities as they start happening is one of the crucial activities when it comes to protecting a website from malevolent attacks. Security professionals in charge of company's servers are expected to cope with intruders any time, but they also need to be able to find potential network holes before hackers do.

With available vulnerability assessment tools that automate exploration processes, these activities should be relatively easy to carry out. VA tools can be host-based, which are the ones used to scan system wide vulnerabilities such as configuration errors and registry permissions, or network-based, i.e. those used to scan network for open ports or vulnerabilities of services running on these ports.

Some of the most widely used network-based security scanners are SAINT, ISS Internet Scanner and Nessus Security Scanner. As for the host-based ones, there are ISS System Scanner, Symantec's Enterprise Security Manager and Pedestal Software Inc.'s SecurityExpressions.

Penetration Testing

Security penetration testing is another important step in securing data transfer, especially in companies that run online business from their own servers. To ensure both internal and external networks are fully protected, there are two corresponding types of penetration tests that translate into simulating real-world attacks.

Penetration testing has become particularly important for web service providers, since the offering and demand of such services has substantially increased over the last couple of years, due to the rise of mobile device usage.

Strong Password Policy

Adequate password policies are of paramount importance for overall security on the web. Developing strong password policy includes each and every employee that has access not only to company's servers, but also other accounts associated with business activities. It is also essential that employees use strong passwords for their personal accounts and this may require internal regulations, as well as raising awareness of the importance of using strong passwords.

Access Control

Depending on the company's organization and the type of business run, webservers may be managed internally or externally. Regardless of the management team in charge of web server configuration and maintenance, it is crucial that server administrators are highly skilled and reliable. This includes organizing trainings for staff accountable for security systems, as well as introducing regulations with respect to persons authorized to access different corporate accounts.

Conclusion

The web is growing at an astonishing pace, and it now hosts all sorts of corporate or otherwise sensitive information that needs to be guarded by all available means. With the rise of e-commerce, e-banking and other activities involving financial transfers, the web is certainly an appealing target for hackers, who keep developing new methods for breaking into corporate systems. Even though most tech experts are aware of the potential risks that lie in wait from insufficiently protected servers, many companies that use web hosting services do not have adequate security strategies. Clearly, web protection is a task for both hosting providers and clients, meaning that security systems need to be implemented on multiple levels.

As the number of cyber-criminal victims rises, it is getting more and more important to potential web threats and discuss possible security practices. Nowadays, most web hosts keep improving their security systems and regulation, but a part of responsibility is still on client companies that need to ensure they are well informed about and ready to adopt advanced security systems.

Resources

Cisco. Cisco 2014 Annual Security Report. http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

Symantec Corporation. Internet Security Threat Report. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_appendices_v19_221284438.en-us.pdf

McAfee Labs Threat Report. http://www.mcafee.com/sg/resources/reports/rp-quarterly-threat-q4-2013.pdf

Prolexic. DDoS Attack Report, Q1 2014. http://www.prolexic.com/knowledge-center-ddos-attack-report-2014-q1.html

Neustar Annual DDoS Attacks and Impacts Report, 2014. *The Danger Deepens*. http://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf

IDG Connect. *The State of Encryption*. http://www.idgconnect.com/blog-abstract/6180/the-state-encryption-part-how-changing

SANS Institute. Network- and Host-Based Vulnerability Assessments: An Introduction to a Cost Effective and Easy to Use Strategy. http://www.sans.org/reading-room/whitepapers/auditing/network-host-based-vulnerability-assessments-introduction-cost-effective-easy-1200

Crucial Blog. *Securing the Australian Cloud: Privacy and Security Requirements for 2014*. http://www.crucial.com.au/blog/2014/03/07/securing-the-australian-cloud-privacy-and-security-requirements-for-2014/